LAB REPORT

Digital Forensics

2012 DC National Art Gallery Attack

Richard Flores

Northern Virginia Community College

ITN 262 01YA

Prof. “Michael” Hon

December 4, 2023

I. Summary

This report covers a period of time between approximately July 6, 2012, to July 15, 2012, involving two separate crime plots intermingled together due to the connection of one person, Tracy (a.k.a. Coral), in both conspiracies. Tracy is a divorced mother of one who is having financial struggles and is likely unable to continue affording the private school her daughter, Terry, attends. She has asked her ex-husband, Joe, for assistance, but he has made no commitments to help.

Some memorandums involving shipping details and insurance for a stamp display coming to the DC Art Gallery have come across Tracy's desk, and she becomes aware of their value. She enlists the assistance of her brother, Pat (a.k.a. Perry), and a police detective, who is willing to assist his sister in the planning of the theft of the stamps. Pat recently caught a parolee, king, in violation of his parole. King now owes Pat a favor, so he is blackmailed into helping as the robber for the plot.

The second plot involves a group of Krasnovians and Krasnovian sympathizers who plan on defacing a Majavian art display at the art gallery. Carry (a.k.a. Cat) is contacted by her "uncle" (family friend), Alex, and both start planning for the attack on the art display. Alex is sending several Krasnovian militants to the US to assist Carry in the plot. Carry sends some files to assist in the forgery of ePassports to get them into the country. She is coordinating with a flash mob coordinator, Drex Mustafar (a.k.a. Mike), who is likely one of the Krasnovian militants. It is unclear if they are going to use a flash mob as a distraction, or if this is merely a codeword for the attack. Carry enlists Tracy's help in smuggling her tablet into the art gallery which is used to transport details of the security, events, locations, and images from the art gallery.

Both plots came to attention of authorities after Joe informed the police of his suspicions. Joe had installed a keylogger on Tracy's computer to track the activities of his daughter Terry prior to their divorce, and he was still receiving emails to his inbox from her computer. Once he became suspicious of Tracy's activities, he informed the police and devices were seized from Tracy and Carry. Images were made of the devices and are to be analyzed.

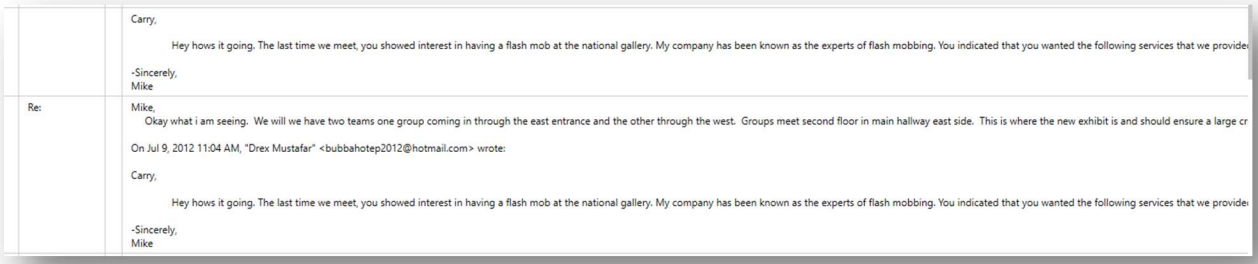
The investigation will proceed by analyzing each device on their own and digging as far as possible into each device to answer the questions of the case. Devices will likely be revisited later as the details of both plots become more apparent. Screenshots of key evidence will be taken and attached to the answers they correspond to.

II. Questions

1. Flash Mob

A. Who planned the flash mob and was there an accomplice?

a. Carry planned the flash mob with Mike, the flashmob coordinator.



Carry,

Hey hows it going. The last time we meet, you showed interest in having a flash mob at the national gallery. My company has been known as the experts of flash mobbing. You indicated that you wanted the following services that we provide

-Sincerely,
Mike

Re:

Mike,
Okay what i am seeing. We will we have two teams one group coming in through the east entrance and the other through the west. Groups meet second floor in main hallway east side. This is where the new exhibit is and should ensure a large cr

On Jul 9, 2012 11:04 AM, "Drex Mustafar" <bubbahotep2012@hotmail.com> wrote:

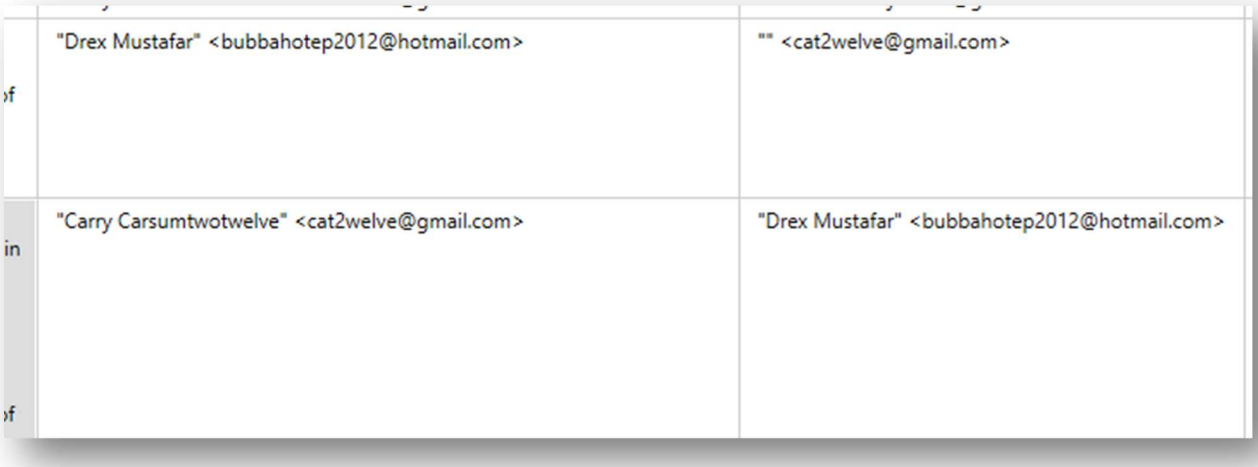
Carry,

Hey hows it going. The last time we meet, you showed interest in having a flash mob at the national gallery. My company has been known as the experts of flash mobbing. You indicated that you wanted the following services that we provide

-Sincerely,
Mike

Carry Tablet

b. Suspiciously, “Mike” contact is saved as someone named Drex Mustafar. Is the flash mob really a distraction, or are they talking in code for the two teams to enter from different entrances and the items to steal are the location?



of	"Drex Mustafar" <bubbahotep2012@hotmail.com>	"" <cat2welve@gmail.com>
in	"Carry Carsumtwotwelve" <cat2welve@gmail.com>	"Drex Mustafar" <bubbahotep2012@hotmail.com>
of		

Carry Tablet

c. There may be another participant or accomplice that Carry was meeting with. They seem to be using codewords such as “Cosby”. Talked about meeting at the same trail. Search history and photos show she visited a trail at Roaches Run Waterfowl Sanctuary.

subj...	s..	body	fromAddress	toAddresses
Re: Cosy?	On 7/	On 7/12/2012 11:07 AM, Carry Carsumtwotwelve wrote: Cosy? How about in the morning?	"supershien@live.com" <supershien@live.com>	"Carry Carsumtwotwelve" <cat2welve@gmail.com>
Re: Cosy?	OK. Sa	On 7/12/2012 9:41 PM, supershien@live.com wrote: On 7/12/2012 11:07 AM, Carry Carsumtwotwelve wrote: Cosy? How about in the morning? OK. Same trail that you were talking about before?	"Cat" <cat2welve@gmail.com>	"supershien@live.com" <supershien@live.com>

Carry Tablet

Records: 4

_id	data1	singleResult	displayQuery	latitude	longitude
1	art museumes			200000000	200000000
2	cosi			200000000	200000000
3	roaches			200000000	200000000
4	roaches run waterfowl sanctuary, arlington, va		Roaches Run Waterfowl Sanctuary, Arlington, VA	200000000	200000000

Carry Tablet

timestamp	destination_latitude	destination_longitude	destination_title	destination_address	source_latitude	source_longitude
2012-07-12 11:24:19	38.864506	-77.039995		Roaches Run Waterfowl Sanctuary Arlington, VA 22202	38.883797	-77.103551

Carry Tablet

d. Tracy was aware of the flashmob, but did not directly participate in its planning.

31	Carry	12027252124	1342010948	7/11/12 12:49 PM	Just meet me out front, I'll ta
32	Carry	12027252124	1342112805	7/12/12 5:06 PM	How's the flashmob going
33	Terry	17038296071	1342141330	7/13/12 1:02 AM	I really want to go to Dad's th

Tracy Phone

B. What locations are the flash mob?

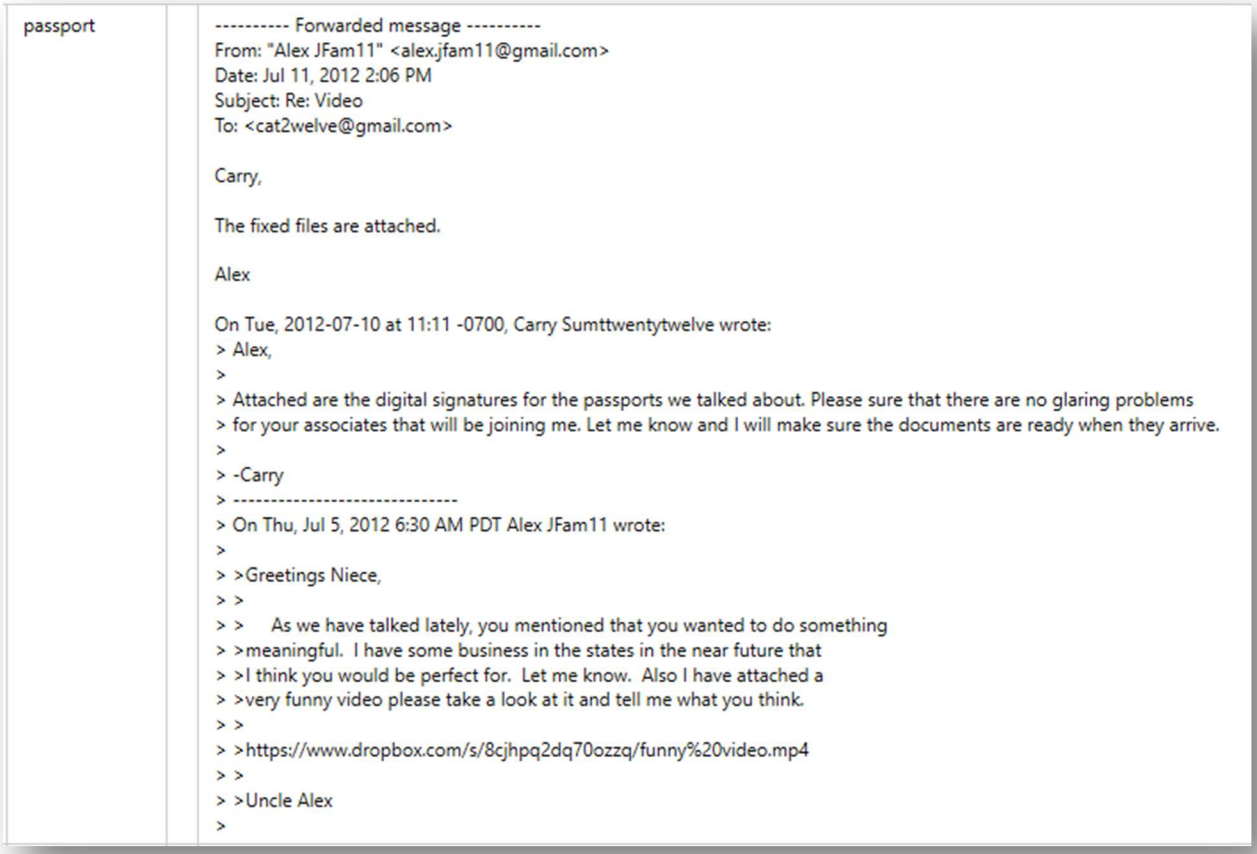
a. Participants enter from both east and west entrances. Meet on second floor main hallway east side where the new exhibit is. Looks like Carry wants to gather a large crowd, likely as a distraction for the defacement crime plans.

Okay what i am seeing. We will we have two teams one group coming in through the east entrance and the other through the west. Groups meet second floor in main hallway east side. This is where the new exhibit is and should ensure a large crowd. I want the event to kickoff at 12:00 PM sharp. The other details i leave up to you.

Carry Tablet

2. Forgery

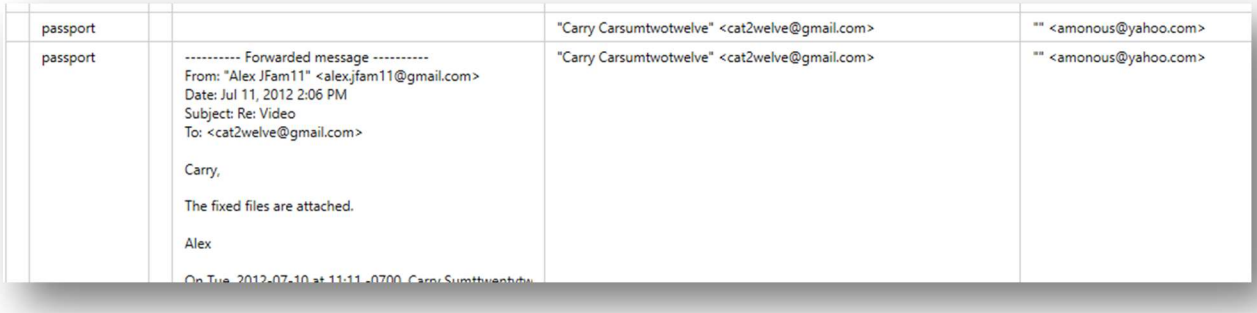
A. From Cary's Tablet, Uncle Alex is forging passports?



passport		---------- Forwarded message ---------- From: "Alex JFam11" <alex.jfam11@gmail.com> Date: Jul 11, 2012 2:06 PM Subject: Re: Video To: <cat2welve@gmail.com> Carry, The fixed files are attached. Alex On Tue, 2012-07-10 at 11:11 -0700, Carry Sumttwentytwelve wrote: > Alex, > > Attached are the digital signatures for the passports we talked about. Please sure that there are no glaring problems > for your associates that will be joining me. Let me know and I will make sure the documents are ready when they arrive. > > -Carry > ------------------------------ > On Thu, Jul 5, 2012 6:30 AM PDT Alex JFam11 wrote: > > >Greetings Niece, > > > > As we have talked lately, you mentioned that you wanted to do something > >meaningful. I have some business in the states in the near future that > >I think you would be perfect for. Let me know. Also I have attached a > >very funny video please take a look at it and tell me what you think. > > > >https://www.dropbox.com/s/8cjhpq2dq70ozzq/funny%20video.mp4 > > > >Uncle Alex >

Carry Tablet

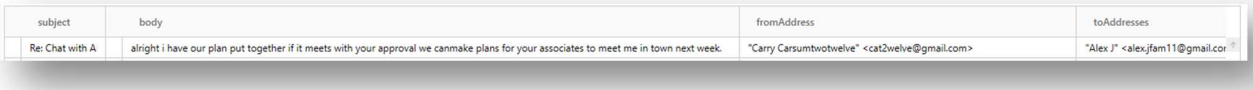
B. Carry forwards some of the correspondence to an unknown person.



passport		"Carry Carsumtwotwelve" <cat2welve@gmail.com>	"" <amonous@yahoo.com>
passport	---------- Forwarded message ---------- From: "Alex JFam11" <alex.jfam11@gmail.com> Date: Jul 11, 2012 2:06 PM Subject: Re: Video To: <cat2welve@gmail.com> Carry, The fixed files are attached. Alex On Tue, 2012-07-10 at 11:11 -0700, Carry Sumttwentytw	"Carry Carsumtwotwelve" <cat2welve@gmail.com>	"" <amonous@yahoo.com>

Carry Tablet

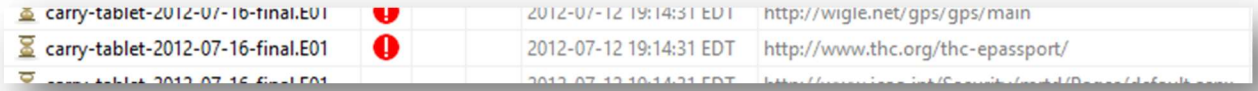
C. Alex is planning on meeting with Carry's associates when he comes to town.



subject	body	fromAddress	toAddresses
Re: Chat with A	alright i have our plan put together if it meets with your approval we canmake plans for your associates to meet me in town next week.	"Carry Carsumtwotwelve" <cat2welve@gmail.com>	"Alex J" <alexjfam11@gmail.cor

Carry Tablet

D. Visited thc.org site for ePassport forgeries.



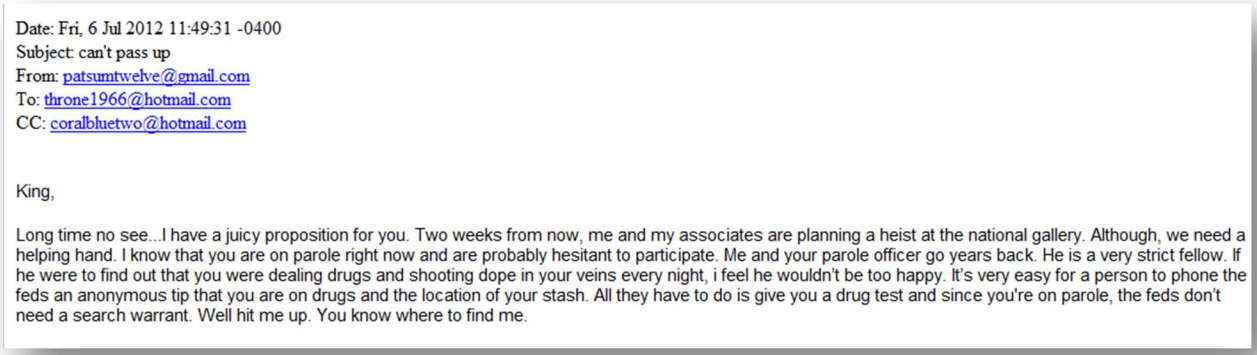
carry-tablet-2012-07-16-final.E01		2012-07-12 19:14:31 EDT	http://wigle.net/gps/gps/main
carry-tablet-2012-07-16-final.E01		2012-07-12 19:14:31 EDT	http://www.thc.org/thc-epassport/

Carry Tablet

Carry Tablet

3. Majavian Artwork (Alex/Cary)

A. Perry Patsum asks King for help with the heist and threatens/blackmails King to get his parole officer to drug test if he doesn't help.



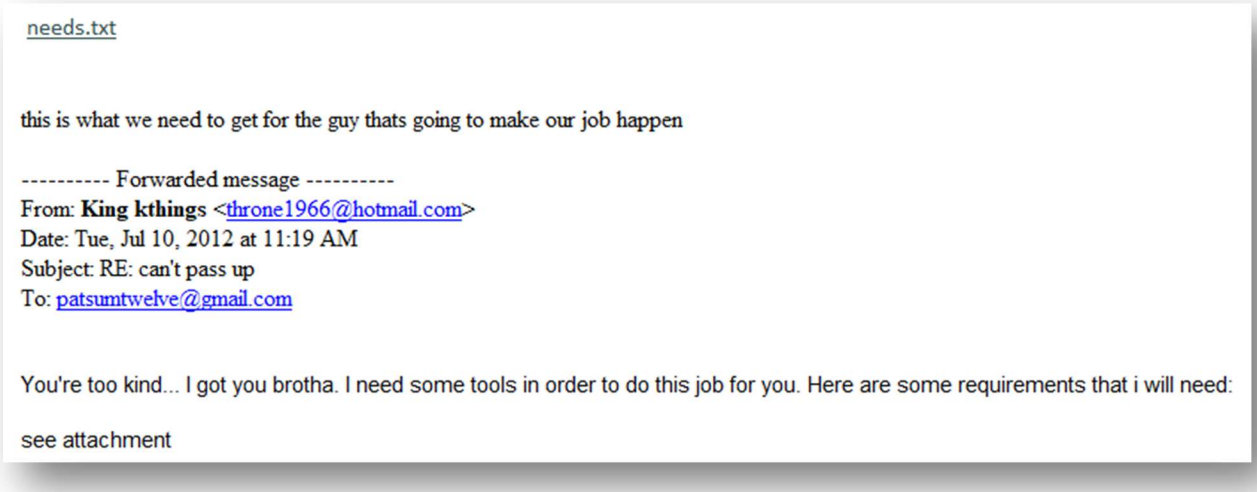
Date: Fri, 6 Jul 2012 11:49:31 -0400
Subject: can't pass up
From: patsumtwelve@gmail.com
To: throne1966@hotmail.com
CC: coralbluetwo@hotmail.com

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 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.

Tracy Phone

B. King agrees to help and needs some supplies.



needs.txt

this is what we need to get for the guy thats going to make our job happen

---------- Forwarded message ----------
From: **King kthings** <throne1966@hotmail.com>
Date: Tue, Jul 10, 2012 at 11:19 AM
Subject: RE: can't pass up
To: patsumtwelve@gmail.com

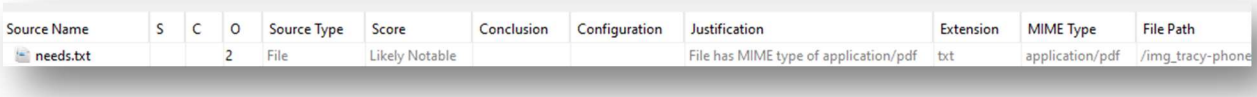
You're too kind... I got you brotha. I need some tools in order to do this job for you. Here are some requirements that i will need:

see attachment

Tracy Phone

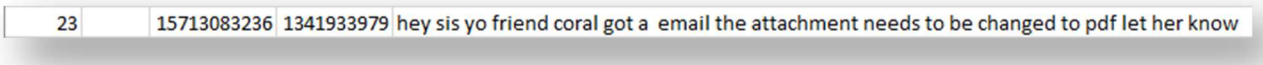
C. The needs.txt file appears to be encrypted or corrupted in some way if you open it as a .txt file, but it can be opened as a PDF.

Tracy Phone



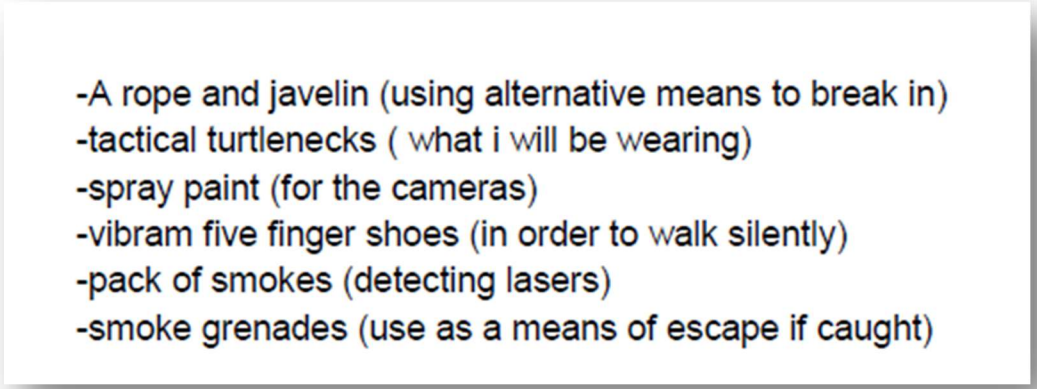
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Extension	MIME Type	File Path
needs.txt			2	File	Likely Notable			File has MIME type of application/pdf	txt	application/pdf	/img_tracy-phone

Tracy Phone



23		15713083236	1341933979	hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know

Tracy Phone



Tracy Phone

4. For the tablet, can you:

   A. Suspicious applications:

      a. Forevergone – data overwriting application

2012-07-06 13:24:03.339000	com.kovit.p.forevergone	com.kovit.p.forevergone.Activity_ForeverGone

Carry Tablet

com.kovit.p.forevergone	https://play.google.com/store/apps/details?id=com.kovit.p.forevergone

Carry Tablet

ft	Name	Install Time	Update Time	Install Originator	Installer	Code Path	Public Flags	Private Flags
2012-07-06 14:57:40	com.kovit.p.forevergone	2012-07-06 14:57:40.091000	2012-07-06 14:57:40.091000		com.android.vending	/data/app/com.kovit.p.forevergone-1.apk	0x0	0x0

Carry Tablet

FOREVER GONE (SD CARD CLEANER) APP

######### Note ########## Please read carefully what this app does, this app will fulfill your SD Card with many blank files(*.blank) then delete all of its, to make your deleted files on SD Card cannot recover by any File Recovery Apps. Please don't rate 1 star just because it fill junk files to your SD Card and you didn't read anything. If you think this app is virus or malware, I'll glad that you report to Google.

From Google Search

b. Sly stego – steganography application?

Timestamp	Display	query
2012-07-11 20:31:56	dropbox	dropbox
2012-07-11 22:33:15	skype	skype
2012-07-12 12:49:53	sly stego	sly stego

Carry Tablet

org.alexmbrown.sly	https://play.google.com/store/apps/details?id=org.alexmbrown.sly

Carry Tablet

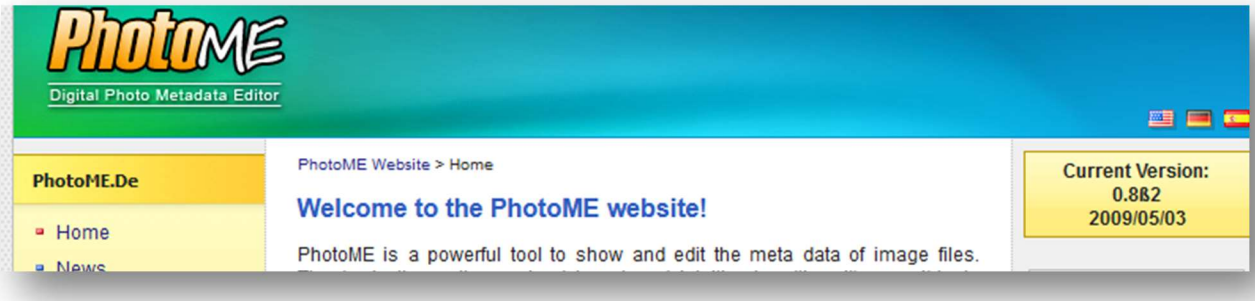
ft	Name	Install Time	Update Time	Install Originator	Installer	Code Path	Public Flags	Private Flags
2012-07-12 12:50:57	org.alexmbrown.sly	2012-07-12 12:50:58.191000	2012-07-12 12:50:58.191000		com.android.vending	/data/app/org.alexmbrown.sly-1.apk	0x0	0x0

Carry Tablet

c. Visited download page for PhotoMe – photo metadata editor

carry-tablet-2012-07-16-final.E01	2012-07-12 19:14:31 EDT	http://www.photome.de/download_en.html	Chrome History	carry-tablet-2012-07-16-final.E01

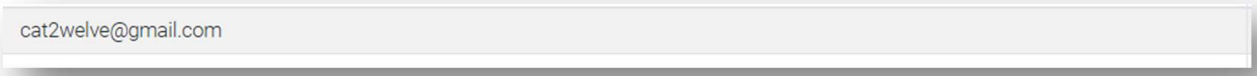
Carry Tablet



From Google Search

B. Account associated with apps:

a. Only active google account on device is cat2welve@gmail.com



Carry Tablet

C. List of stored passwords with user names

Records: 4

_id	name	type	password
1	cat2welve@gmail.com	com.google	1/Mxq54RXI-i7ILkYiZ988ffUQmBFhA7khF54ZE8kh9V4 RMopeTeTndnEbRO2xw-YhbQA
2	cat2welve@gmail.com	com.dropbox.android.account	
3	carrysum2012@yahoo.com	com.android.email	ftptb!
4	carry.sums	com.skype.contacts.sync	284151

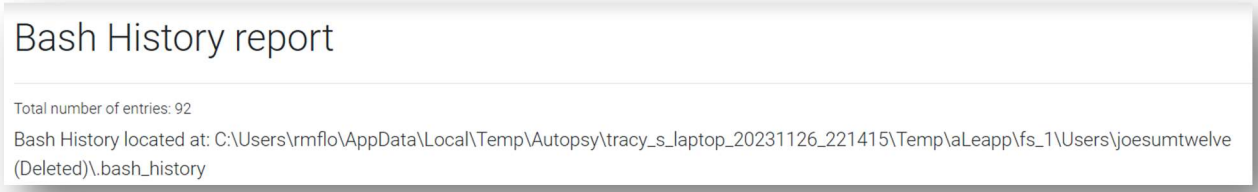
Carry Tablet

5. Focusing on the mac book, what evidence can you find that:

    A. Provides a way keystrokes could have been recorded unknowingly

        a. Joe setup a keylogger to email him the logs.

        b. Can be seen in the Bash history of commands entered



Tracy Laptop

13	cd com.fsb.logKext
14	more com.fsb.logKext
15	ls
16	rm com.fsb.logKext
17	sudo rm com.fsb.logKext
18	ls
19	ls
20	more com.fsb.logKext

Tracy Laptop

41	sudo logKextClient
42	sudo logKextClient
43	sudo logKextClient
44	sudo logKextClient
45	ls
46	vim com.fsb.logKext
47	sudo vim com.fsb.logKext
48	ls
49	rm com.fsb.logKext
50	sudo rm com.fsb.logKext

Tracy Laptop

79	sudo mail joe.sum.twelve@gmail.com
80	logKextClient
81	sudo logKextClient
82	sudo logKextClient
83	sudo logKextClient

Tracy Laptop

B. Evidence related to financial gain related to the theft of the stamps

   a. Keylogger emails sent to Joe show Tracy was looking out for items to come through her work.

SA

System Administrator
root@Tracys-MacBook-Air.local
6/29/2012 6:00:00 AM

Logfile
To: joe.sum.twelve@gmail.com

```
![LogKext Daemon created new logfile : Thu Jun 28 16:09:50 2012]
d
thun<del>Coral<tab>coralbluetwo@hotmail.com<tab>legalBeePerr<del><del><del><del>pe<del><del><del><del><del>Perry, <del>

I know what you meanj<del>. If anything comes up around the office that we can maybe... get in on... <del>,
<del><del><del><del><del>, please lets try to do so. Kiddo is getting really bent out of shape abou <del>t possibly having to switch
schools. I have been paying some more attention to the mmo<del><del><del>memos and papers that come across my desk. We get a bunch
of insurance type documents that plac val<del><del><del><del>e values on a certain objects. If anything stands out, I
![LogKext Daemon starting up : Fri Jun 29 09:04:12 2012]

![User 'tracysumtwelve' has logged in : Fri Jun 29 09:14:10 2012]

![LogKext Daemon starting up : Fri Jun 29 10:33:05 2012]

![User 'tracysumtwelve' has logged in : Fri Jun 29 10:33:25 2012]
9<del>legalBee
<del><del><del><del>

Be careful! We have enough problems as it is, we can't get <del><del><del><del>be getting in trouble or losing our jobs. Nothing
special has turned up here, but I am still keeping an eye out. We usually sot<del><del><del>start to host some interesting events
this time of the year, I'm sure som
```

Spyware Emails

```
![User 'tracysumtwelve' has logged in : Mon Jul  2 11:51:37 2012]
ega<del><del><del>legalBee
PerrySome good newsI<del>I use l<del><del><del><del><del><del><del><del><del><del><del>I<del>i<del><del>Perry,

I think I may have ac<del><del>come across someth
```

```
![LogKext Daemon created new logfile : Mon Jul  2 12:00:04 2012]
ing interesting. everyb<del><del><del><del><del><del>Erv<del><del>verybody around the office seems to be buzzed about a foreign
exhibit thats supposed to<del><del><del><del><del><del><del><del><del><del><del><del><del> is supposed to be coming over. There
hasn't been any official release in writing but we have been going through a q<del><del><del>quite an ordeal with all this
paperwork. From what I can tell, this exhibit<del><del><del>bit has to be a big deal. I'll let you know if I found out anything
else.
```

```
Okay, so there has e<del>been a lot of money bi<del>eing thrown around to get this exhibit over to us. I've been swimming through
paperwork and memos all day, but none if t<del>it seems to have any o<del>solid information that could help us.

I had to scan and very<del>ify some shipping informaio<del><del>tion, and compared to what it su<del><del>usually costs to ship
exhibits... this ones seems relatively cheap. I'm not sure if this is good or bad for us (or even an error on our
sid<del><del><del><del><del><del><del><del><del><del><del>), but hopefully I will be able to find ou
![User 'loginwindow' has logged in : Mon Jul  2 15:17:28 2012]

![User 'terrysumtwelve' has logged in : Mon Jul  2 15:17:29 2012]
t more later in the week.privateschool
```

```
![User 'tracysumtwelve' has logged in : Tue Jul  3 09:18:40 2012]
legalBee
So i was told t<del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del>I was ju<del><del>told that we are
supposed to be recie<del><del><del>e<del><del><del>receiving a rare collection of stamps. That would explain my
whi<del><del><del>shp<del>ipping <del><del><del><del><del><del><del><del><del><del><del><del><del><del> why the shipping information
looked a bit out of the ordinary to me. I'm not certain of the specifics for the stamps, but they seem to be very hih<del>ghly
valued by somebody. Mayve t<del><del><del><del>be this is our ticket.
```

b. An encrypted zip folder was sent containing memos showing the covered value of the stamps.

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

Tracy Laptop

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

Tracy Laptop

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.

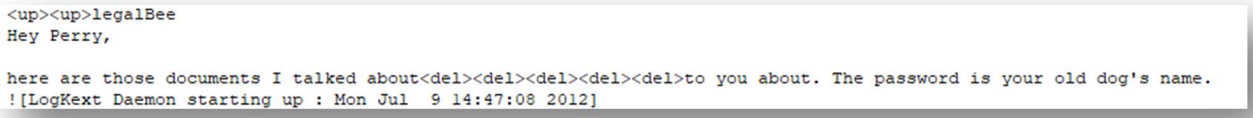
D'Mann

President National Gallery DC

Tracy Laptop

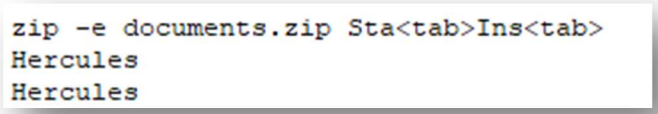
Tracy Laptop

c. There was a message talking about the password being the name of the former dog. Tracy sent these to someone named Perry.



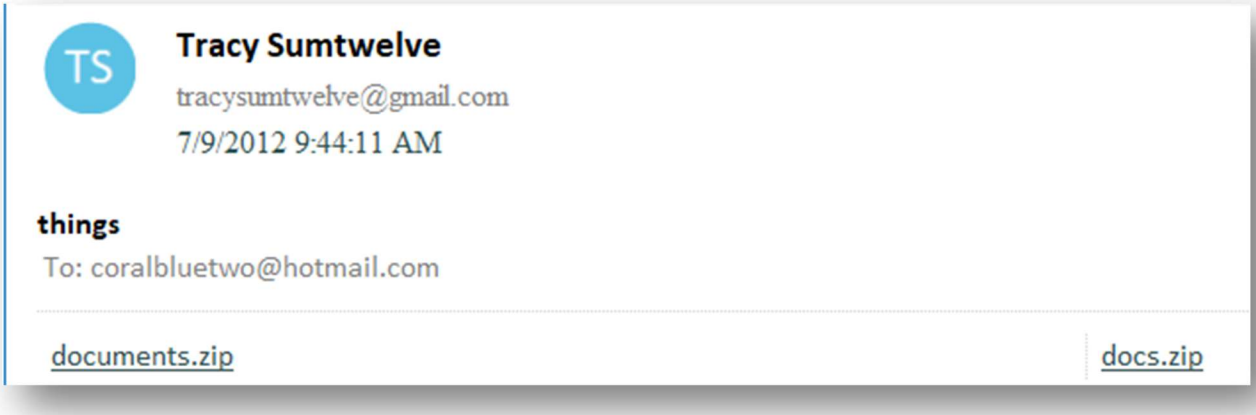
Spyware Emails

d. They keylogger emails showed terminal commands zipping the files using the password “Hercules”.



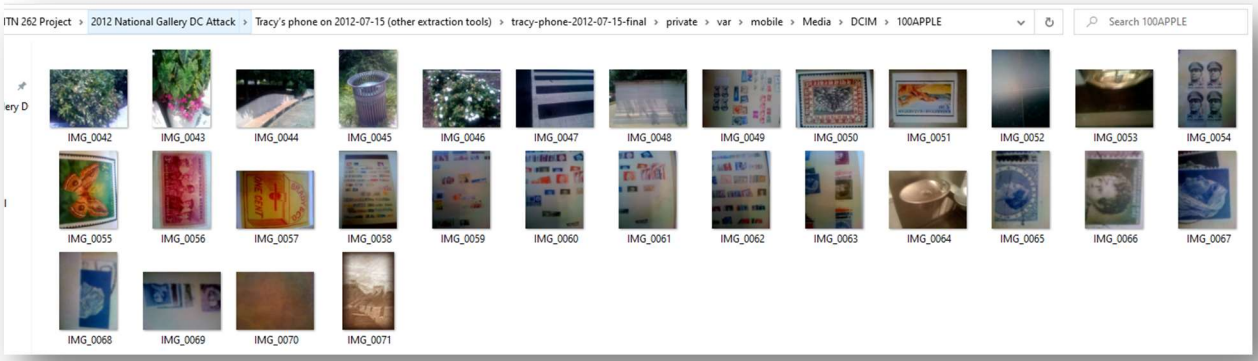
Spyware Emails

e. Tracy also emailed the documents to Carry.



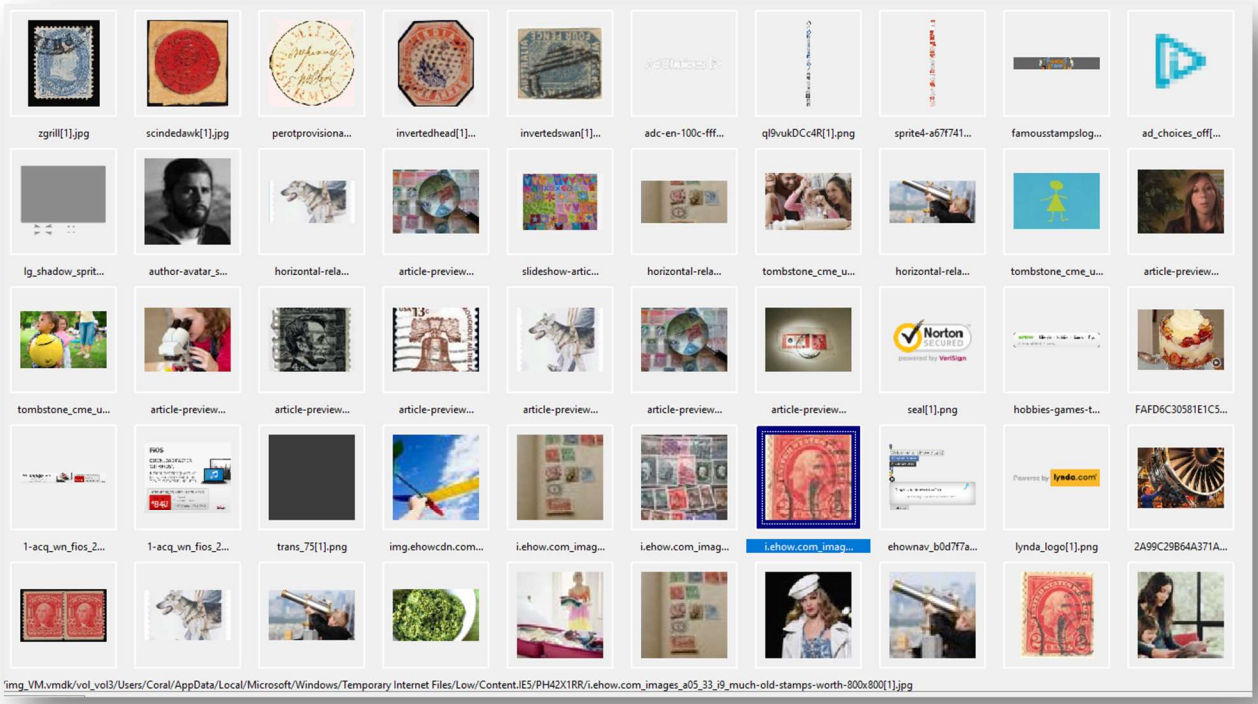
Tracy Phone

f. Tracey was taking photos of the stamps that were her theft target.



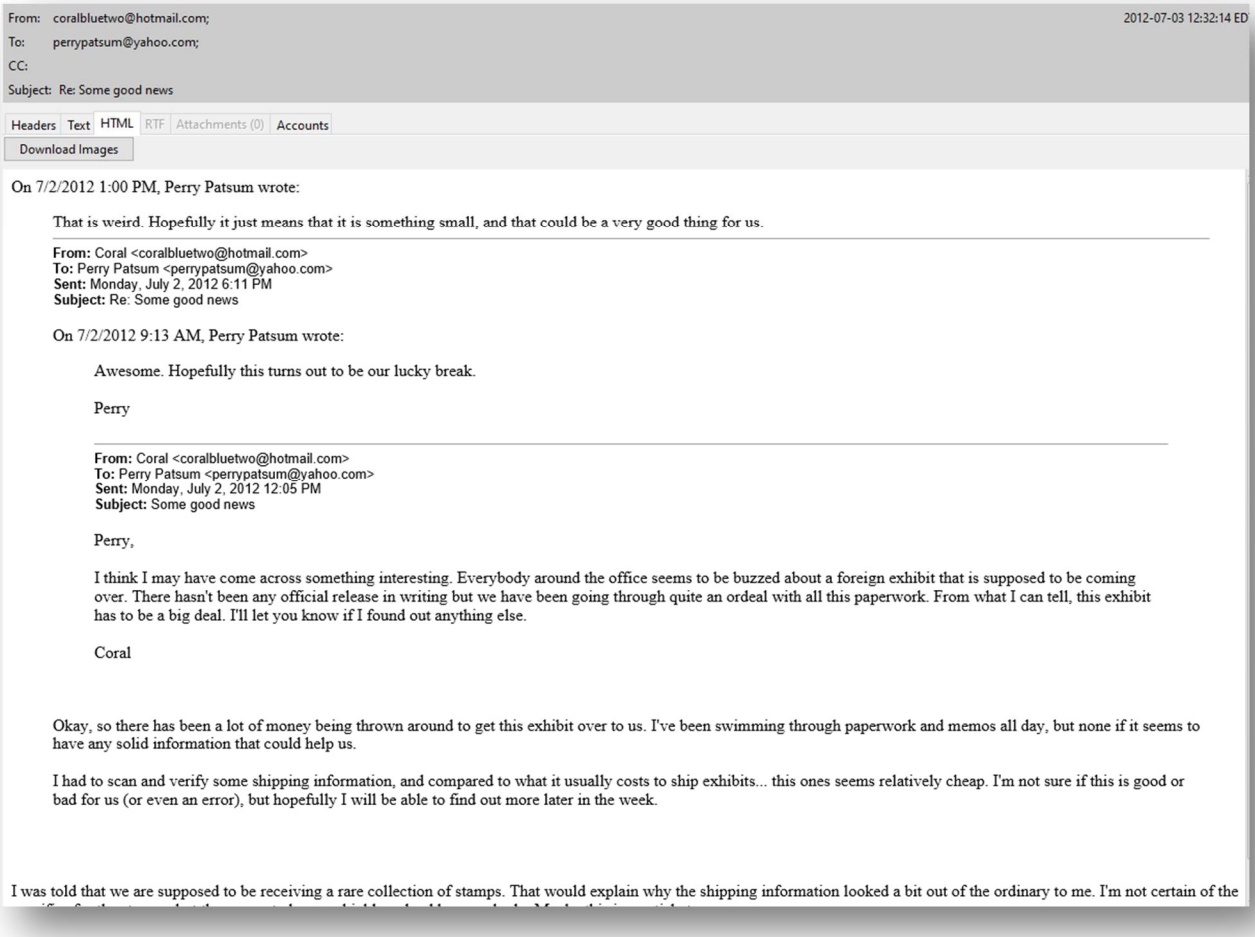
Tracy Phone

g. Tracy was performing research on value of old stamps.



Tracy External

h. Perry (Pat) and Coral (Tracy) e-mail traffic pertaining to stamps.



From: coralbluetwo@hotmail.com; 2012-07-03 12:32:14 ED
To: perrypatsum@yahoo.com;
CC:
Subject: Re: Some good news

Headers | Text | HTML | RTF | Attachments (0) | Accounts

Download Images

On 7/2/2012 1:00 PM, Perry Patsum wrote:

That is weird. Hopefully it just means that it is something small, and that could be a very good thing for us.

From: Coral <coralbluetwo@hotmail.com>
To: Perry Patsum <perrypatsum@yahoo.com>
Sent: Monday, July 2, 2012 6:11 PM
Subject: Re: Some good news

On 7/2/2012 9:13 AM, Perry Patsum wrote:

Awesome. Hopefully this turns out to be our lucky break.

Perry

From: Coral <coralbluetwo@hotmail.com>
To: Perry Patsum <perrypatsum@yahoo.com>
Sent: Monday, July 2, 2012 12:05 PM
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.

Coral

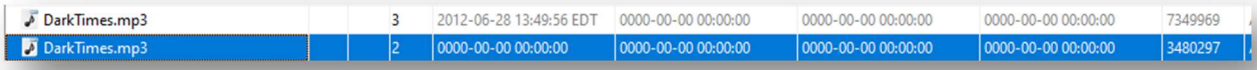
Okay, so there has been a lot of money being thrown around to get this exhibit over to us. I've been swimming through paperwork and memos all day, but none if it seems to have any solid information that could help us.

I had to scan and verify some shipping information, and compared to what it usually costs to ship exhibits... this ones seems relatively cheap. I'm not sure if this is good or bad for us (or even an error), but hopefully I will be able to find out more later in the week.

I was told that we are supposed to be receiving a rare collection of stamps. That would explain why the shipping information looked a bit out of the ordinary to me. I'm not certain of the

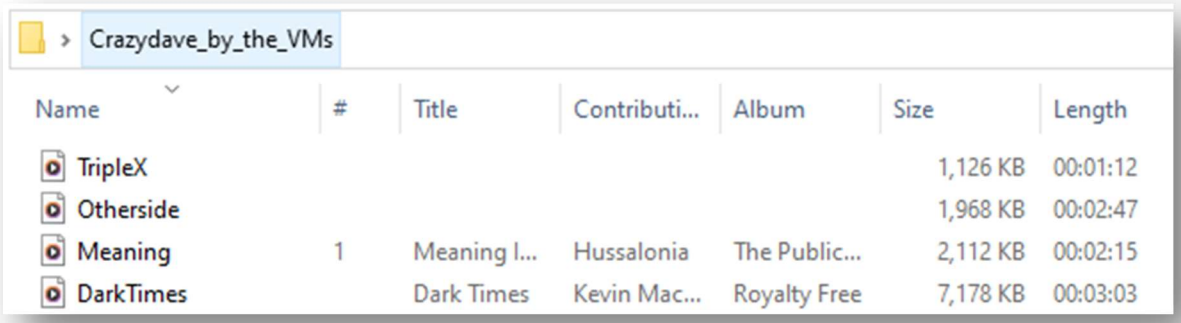
Tracy External

i. Coral (Tracy) and Perry (Pat) are using VM's to communicate and hide their activities. I think they sent them with the Crazydave_by_the_VMs.zip folder. Dark Times is an abnormally large file size and was originally only 3 GB; now 7 GB. The name of the file also seems suspicious.



DarkTimes.mp3		3	2012-06-28 13:49:56 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	7349969
DarkTimes.mp3		2	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	3480297

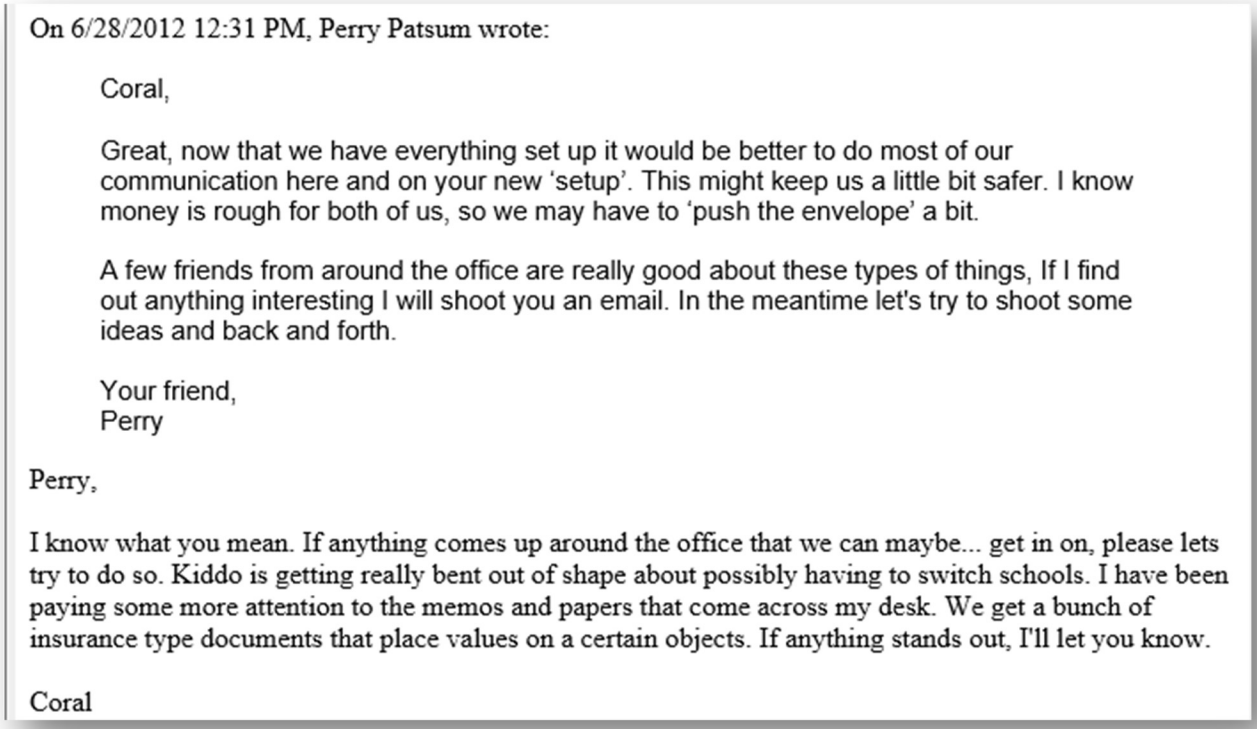
Tracy External



Crazydave_by_the_VMs

Name	#	Title	Contributi...	Album	Size	Length
TripleX					1,126 KB	00:01:12
Otherside					1,968 KB	00:02:47
Meaning	1	Meaning I...	Hussalonia	The Public...	2,112 KB	00:02:15
DarkTimes		Dark Times	Kevin Mac...	Royalty Free	7,178 KB	00:03:03

Tracy External



On 6/28/2012 12:31 PM, Perry Patsum wrote:

> Coral,
>
> Great, now that we have everything set up it would be better to do most of our communication here and on your new 'setup'. This might keep us a little bit safer. I know money is rough for both of us, so we may have to 'push the envelope' a bit.
>
> A few friends from around the office are really good about these types of things, If I find out anything interesting I will shoot you an email. In the meantime let's try to shoot some ideas and back and forth.
>
> Your friend,
> Perry

Perry,

I know what you mean. If anything comes up around the office that we can maybe... get in on, please lets try to do so. Kiddo is getting really bent out of shape about possibly having to switch schools. I have been paying some more attention to the memos and papers that come across my desk. We get a bunch of insurance type documents that place values on a certain objects. If anything stands out, I'll let you know.

Coral

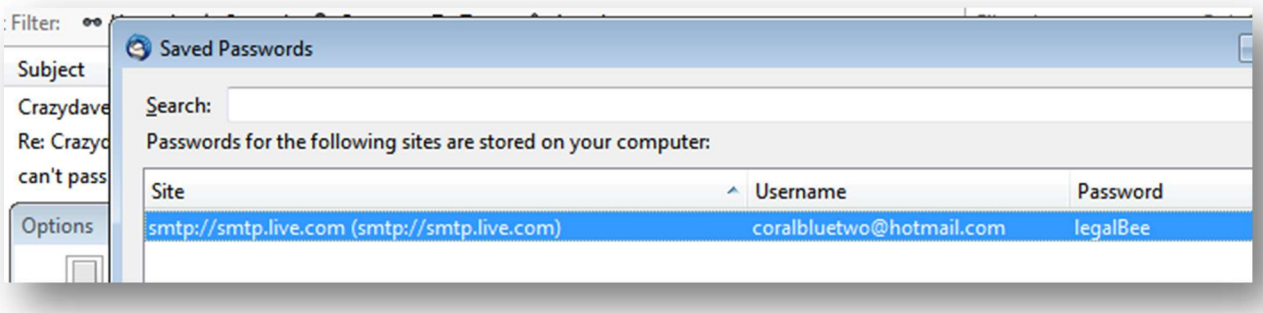
Tracy External

j. The audio file Crazydave1.mp3 had additional audio spliced into it that was likely not part of the original track, as it was instructions for Coral (Tracy) to install a VM. It is also revealed that they are calling the theft plan “Project Big Lift.” (DOUBLE CLICK TO PLAY)


Crazydave1.mp3

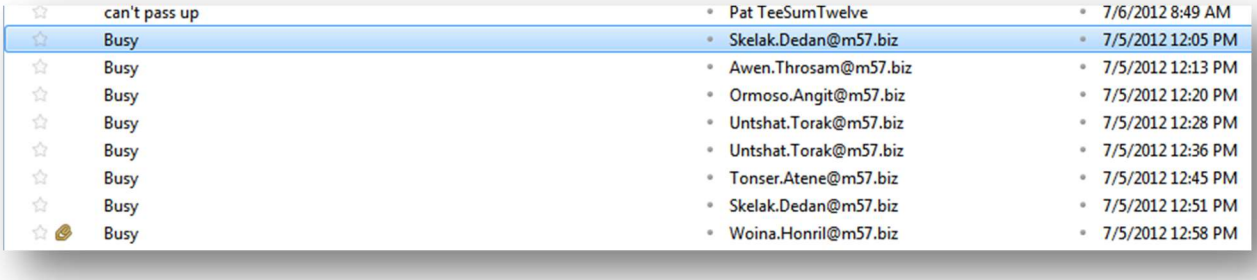

MessageFromCrazydave1.mp3.mp3

k. Started up the VM in VirtualBox to see if there was anything that could tell me what program was used to hide the VM, but I didn’t see anything installed other than Thunderbird. I was able to pull Coral’s password though. I had also seen this password typed several times in the keylogger emails to Joe.



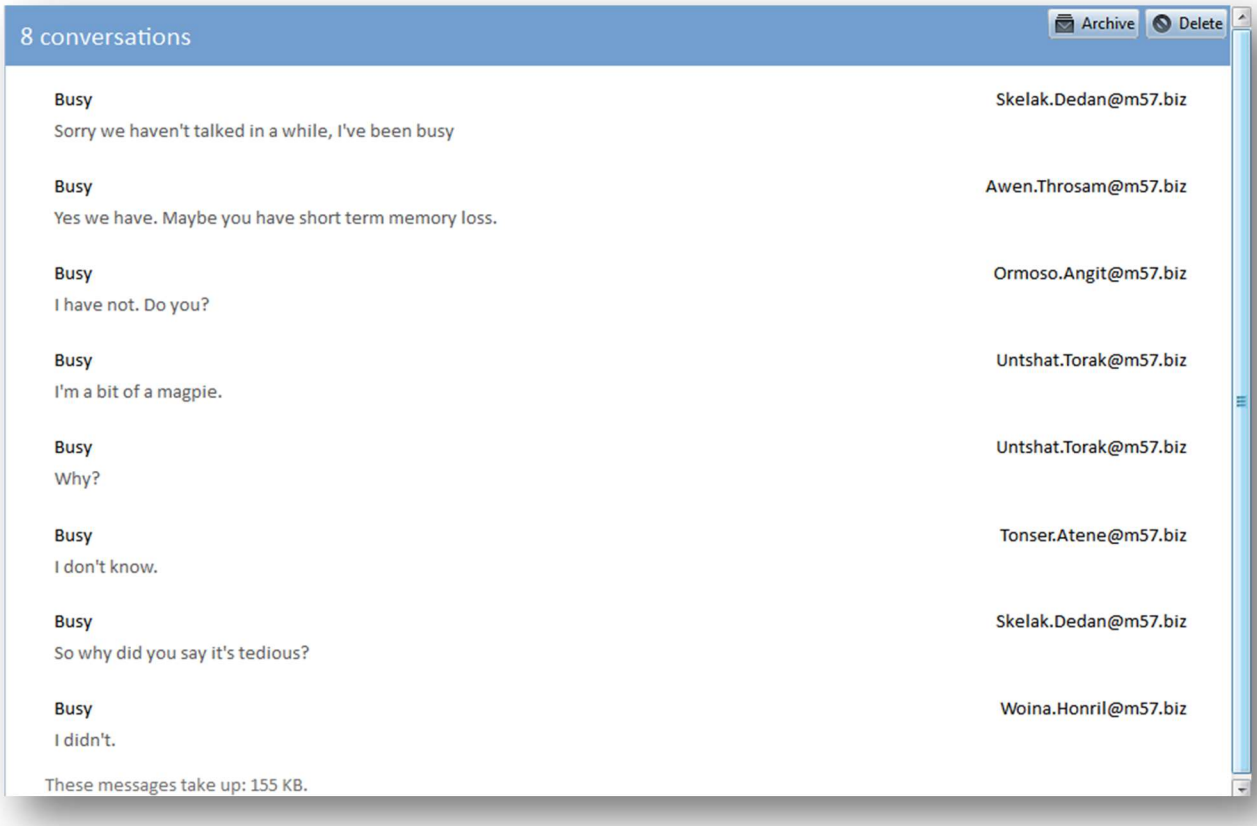
Tracy External (VM)

I. Who are these people that Tracy seams to be having a suspicious (possibly coded; coming from different emails but continuing conversation and same subject) conversation with?



can't pass up	Pat TeeSumTwelve	7/6/2012 8:49 AM
Busy	Skelak.Dedan@m57.biz	7/5/2012 12:05 PM
Busy	Awen.Throsam@m57.biz	7/5/2012 12:13 PM
Busy	Ormoso.Angit@m57.biz	7/5/2012 12:20 PM
Busy	Untshat.Torak@m57.biz	7/5/2012 12:28 PM
Busy	Untshat.Torak@m57.biz	7/5/2012 12:36 PM
Busy	Tonser.Atene@m57.biz	7/5/2012 12:45 PM
Busy	Skelak.Dedan@m57.biz	7/5/2012 12:51 PM
Busy	Woina.Honril@m57.biz	7/5/2012 12:58 PM

Tracy External (VM)



8 conversations — Archive — Delete

Busy — Skelak.Dedan@m57.biz
Sorry we haven't talked in a while, I've been busy

Busy — Awen.Throsam@m57.biz
Yes we have. Maybe you have short term memory loss.

Busy — Ormoso.Angit@m57.biz
I have not. Do you?

Busy — Untshat.Torak@m57.biz
I'm a bit of a magpie.

Busy — Untshat.Torak@m57.biz
Why?

Busy — Tonser.Atene@m57.biz
I don't know.

Busy — Skelak.Dedan@m57.biz
So why did you say it's tedious?

Busy — Woina.Honril@m57.biz
I didn't.

These messages take up: 155 KB.

Tracy External (VM)

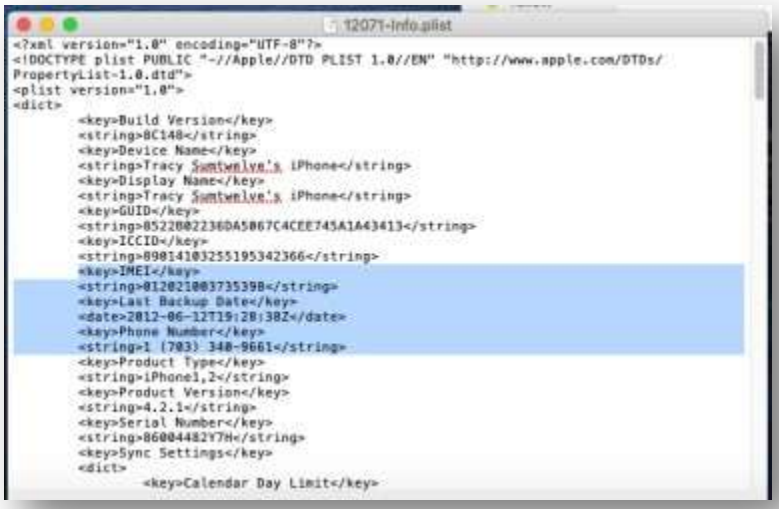
m. One of these messages had two attachments. Two random government documents. Do these contain the forged ePassports?

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Fla
000007.doc	▽		3	2012-07-12 11:01:43 EDT	2012-07-12 11:01:43 EDT	2012-07-12 11:01:43 EDT	2012-07-12 11:01:43 EDT	179200	Allc
000114.doc			3	2012-07-12 11:01:45 EDT	2012-07-12 11:01:45 EDT	2012-07-12 11:01:45 EDT	2012-07-12 11:01:45 EDT	19968	Allc

Carry Tablet

C. Phone number of an iphone 3G serial number 012021003735398

a. Searched for the IMEI as a keyword. Several files came up. Saw several were PLIST files, which google said could be opened on a mac. Was able to open the .PLIST files in a mac VM.

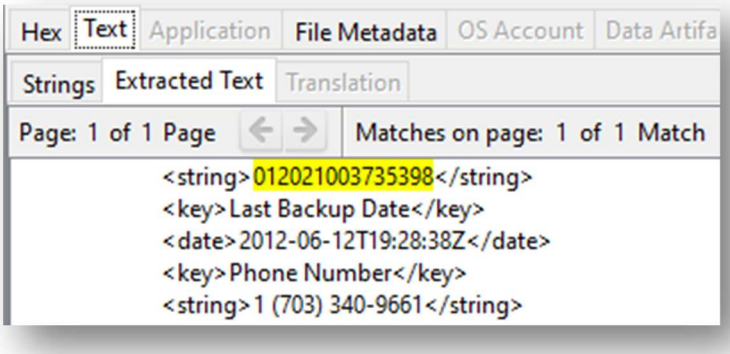


Tracy's Laptop

b. Phone number: 703-340-9661.

c. This is Tracy’s phone number.

d. I later realized how to view text within Autopsy.



Tracy's Laptop

6. Using the tablet image, provide a timeline that establishes the seven events in chronological order around: how the table was smuggled in, where the table was taken, what information was sent regarding security, and what images/files were sent to help with the crime

   A. Tracy offered to smuggle the tablet in for Carry.

```
Hey,

Yea sure, that shouldn't be muc <del>h of a
problem.<del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del
><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del><del>I can definitely help get
your tablet in. Our security guards can be pretty ridiculous sometimes! When would you want to get in and
look<del><del><del><del>take a look around?

Tracy
```

Spyware Emails

   B. Tracy pulled the security guard rotations.

Security Personnel Duty Schedule:

Shift A1 and A2 Personnel: In designated positions as of 6:00 AM till 3:00 PM F-T except for designated relief time or specific authorization via issued communication channels.

Shift B1 and B2 Personnel: In designated positions as of 6:00 AM till 3:00 PM W-SU except for designated relief times or specific authorization via issued communication channels.

Shift C Personnel: In designated positions as of 3:00 PM till 9:00 PM M-F except for designated relief time or specific authorization via issued communication channels.

Shift D Personnel: In designated positions as of 63:00 PM till 9:00 PM W-SU except for designated relief times or specific authorization via issued communication channels.

Support shift 1 Personnel: Relieve Shift A1 from 12:00 PM to 1:00 PM, Relieve Shift A2 from 1:15 pm to 2:15 PM

Support shift 2 Personnel: Relieve Shift B1 from 12:00 PM to 1:00 PM, Relieve Shift B2 from 1:15 pm to 2:15 PM

Office of Personnel Management

Tracy External

C. Tracy met Carry outside her work at the Art Gallery and smuggled the tablet inside on July 11, 2012 at ~1:00 PM.

	A	B	C	D	E	
1	ROWID	NAME	ADDRESS	DATE	CONVERTED DATE	TEXT
24	30	Carry	12027252124	1342010505	7/11/12 12:41 PM	I'm almost there where should I meet you?
25	31	Carry	12027252124	1342010948	7/11/12 12:49 PM	Just meet me out front, I'll take the tablet in.
26	32	Carry	12027252124	1342112805	7/12/12 5:06 PM	How's the flashmob going

SMS messages exported to Excel

D. Tablet Photos Timeline (locations determined using names/addresses within photos themselves, Google Lens image search, and Google Street View tracking between identified locations on either side of photo).

a. Carry meets someone for dinner at Firehook Bakery on July 8th. This does not match up with the time Tracy met her brother for lunch on July 6th. Could be a meeting for the defacement plot.

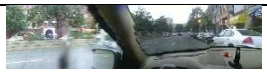
b. There are photos of security cameras the morning of Carry transferring the tablet to Tracy. Perhaps scoping out the outside security? There was no identifiable information or GPS data to pin down the location.

c. There are photos from Roaches run contained on the tablet the day after it was smuggled into the Gallery. Either the Shien person is another accomplice, or an alias of Carry and Tracy was returning the tablet to her there.

Photo	Location	Timestamp	
	Crate & Barrel 2800 Clarendon Blvd Arlington, VA 22201	July 7, 2012	5:49 PM
	Firehook Bakery 1909 Q. St. NW Washington, DC 20009	July 8, 2012	5:31 PM

	Firehook Bakery 1909 Q. St. NW Washington, DC 20009	July 8, 2012	5:31 PM
			5:31 PM
			5:31 PM
			5:31 PM
			5:31 PM
			5:31 PM
			5:31 PM

	Firehook Bakery 1909 Q. St. NW Washington, DC 20009	July 8, 2012	5:31 PM
			
			
	Circa at Dupont (CLOSED) 1601 Connecticut Ave NW Washington, DC 20009		5:33 PM
			5:33 PM
	Connecticut Ave NW 38.913309, -77.045632 Washington, DC 20009		5:38 PM
	Bethesda Bagels (CLOSED) 1718 Connecticut Ave. NW Washington, DC 20009		5:39 PM

	Bethesda Bagels (CLOSED) 1718 Connecticut Ave. NW Washington, DC 20009	July 8, 2012	5:40 PM
			5:40 PM
	Capitol Video Sales (CLOSED) 1729 Connecticut Ave. NW Washington, DC 20009		5: 40 PM
	Embassy of Côte d'Ivoire 2424 Massachusetts Ave. NW Washington, DC 20008		5:46 PM
	Christian Hague House 2349 Massachusetts Ave. NW Washington, DC 20008		5:46 PM
			5:51 PM
			5:51 PM

		July 8, 2012	5:51 PM
	Watergate Complex 2601 Virginia Ave NW Washington, DC 20037		5:52 PM
			5:52 PM
			5:53 PM
	Interstate 66 at Kennedy Center for the Performing Arts 38.89680, -77.05357 Washington, DC 20566		5:53 PM
			5:53 PM
	1024 N Utah St. 38.88299, -77.11386 Arlington VA, 22201	July 9, 2012	7:50 AM

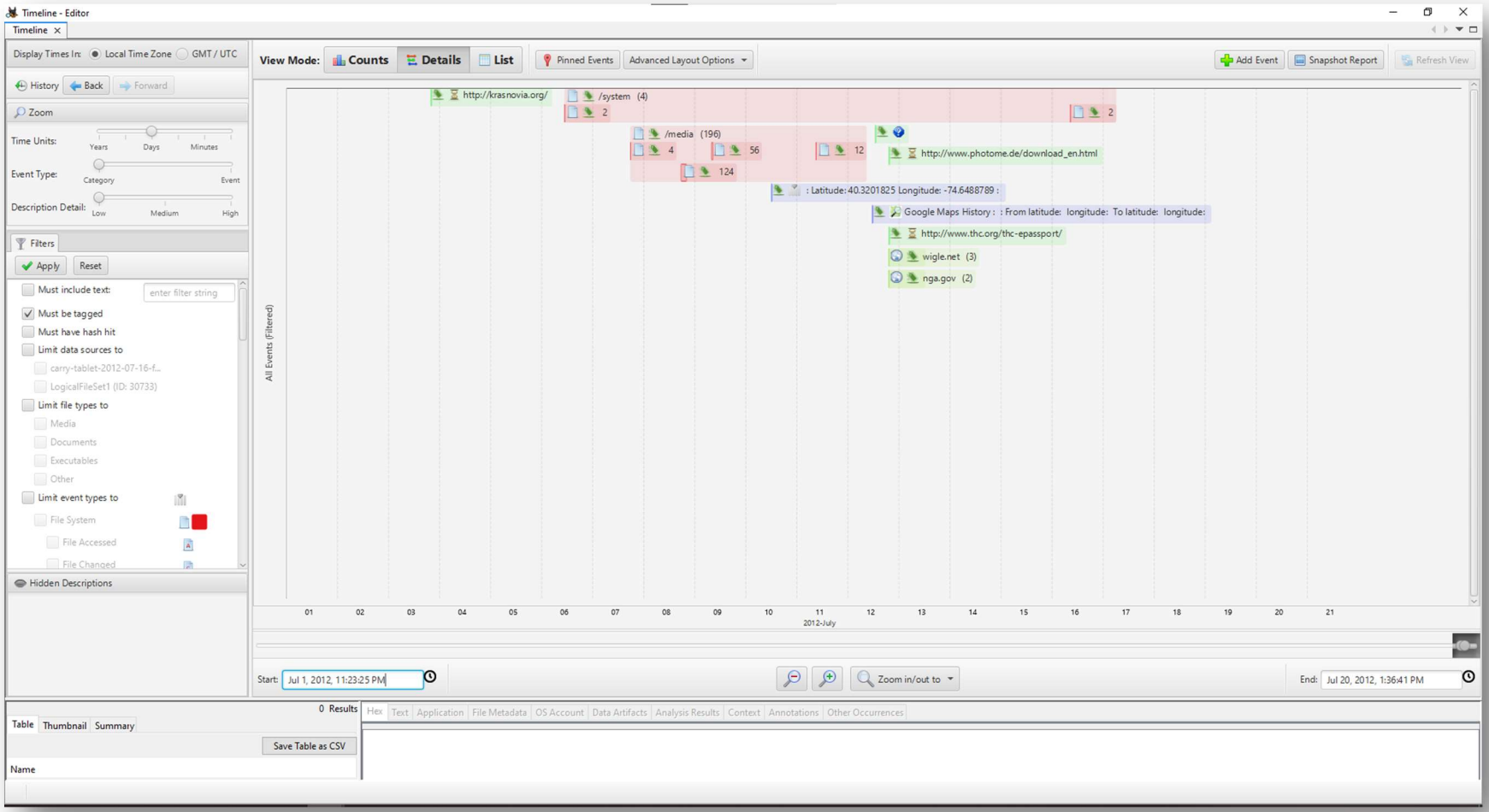
	1024 N Utah St. 38.88299, -77.11386 Arlington VA, 22201	July 9, 2012	5:50 AM
			7:51 AM
			7:51 AM
	Fairfax Dr. and N. Taylor St. 38.88213, -77.11269 Arlington, VA 22203		7:52 AM
			7:52 AM
	Ballston-MU Station (pre-MU) 4230 Fairfax Dr Arlington, VA 22201		7:52 AM
	Cosi (CLOSED) 4250 Fairfax Dr Arlington, VA 22203		7:53 AM

	Ballston Exchange Parking 4121 Wilson Blvd Arlington, VA 22203	July 9, 2012	8:34 AM
	National Science Foundation (CLOSED) 4201 Wilson Blvd. Arlington, VA 22203		8:34 AM
			8:34 AM
			8:49 AM
	The Westin Arlington 801 N. Glebe Rd. Arlington, VA 22203		8:50 AM
	N. Gleve Rd. and 9th st. 38.88119, -77.11539 Arlington, VA 22203		8:51 AM
	Security Cameras	July 11, 2012	9:01 AM

	Security Cameras	July 11, 2012	9:01 AM
			9:01 AM
	Roaches Run / Gravelly Point 38.86491, -77.03799 Arlington, VA 22202	July 12, 2012	11:53 AM
			11:54 AM

E. Map showing plots of photo locations and other GPS data from navigation and browsing history. (DOUBLE CLICK TO OPEN AND SEE PLOTS)

F. Timeline from Autopsy of flagged material/items/events.



III. People

1. A spreadsheet compiled of data of all the people involved.

Name	Description	Motivation	Association	Phone Number	Email
Alex J.	Wealthy Krasnovian businessman	Anti-American Sentiments	Carry's "Uncle"; Defacement Planner/Coordinator		alex.jfam11@gmail.com
Carry Sums a.k.a. "Cat"	Krasnovian supporter in the US.	Anti-American Sentiments	Suspect for Defacement Conspiracy Plot	2027252124	cat2welve@gmail.com
					carrysum2012@yahoo.com
Drex Mustafar a.k.a. "Mike"	Suspected Krasnovian militant		Flashmob Coordinator; Defacer?		bubbahotep2012@hotmail.com
unknown person	Possible Krasnovian militant?				amonous@yahoo.com
Perhem Shien ?	Possible Krasnovian militant?				perhem.shien@gmail.com
					supershien@live.com
King	Criminal; busted by Perry	Threatened/blackmailed	Robber for Theft		throne1966@hotmail.com
Perry Patsum a.k.a. "Pat"	Tracy's brother, Police Officer	Dirty cop; helping sister Tracy	Accomplice for Theft	5713083236	perrypatsum@yahoo.com
					patsumtwelve@gmail.com
Tracy Sumtwelve a.k.a."Coral"	Supervisor at National Art Gallery	Financial gain/hardships	Primary Suspect for Theft; Accomplice for Defacement	7033409661	tracysumtwelve@gmail.com
					tracy.sumtwelve@nationalgallerydc.com
					coralbluetwo@hotmail.com
Terry Sumtwelve	Tracy/Joe's Daughter			7038296071	just.terry.22@gmail.com
Joe Wumtwelve	Tracy's ex-husband				joe.sum.twelve@gmail.com
Jamie?	Who is Jaime?	??			

Flores_Richard_Project People.xlsx