Contents Page

Introduction

The Report

This report is an expert witness digital forensics report investigating an internal company matter in which an employee conspired to steal valuable stamps at the National Art Gallery Museum. The main purpose of this report is to identify how the conspiracy was plotted. A disk image of the external hard drive in question has been created and Autopsy will be used to examine the image forensically.

Background Information

The National Art Gallery is a Museum in Washington, DC. It has many staff members, but this investigation mainly focuses on Tracy, who works as a supervisor. This museum experienced an incident that involved an employee, Tracy, conspiring with other external accomplices to steal valuable stamps at the National Gallery. After the divorce, Joe, her husband, installed a keylogger tracker on Tracy's computer, which exposed their conspiracy plot.
Tracy’s laptop was found, and it contained the names, emails, and conversations of the accomplices.
A disk image of Tracy’s external hard drive has been created and handed over to the investigator. The purpose of this report is to answer the questions in Figure 1 below.

	Questions
1.	Who was involved in this conspiracy?
2.	How did Tracy and her accomplices plan to execute the conspiracy?
3.	What were the different forensic artifacts used

Figure 1 - Questions to be answered by forensic investigation

Report Structure and Contents

The main body of this report will detail the findings from the forensic process. Analysis of these findings will be completed, and screenshots will be provided from Autopsy of the findings from the disk image.

The report will also contain a conclusion to summarize the findings from the expert witness report.

A personal reflection will outline the investigator's experience after completing this investigation.

ACPO Principles

The Association of Chief Police Officers has created a set of principles that outline how digital data should be handled and forensically analyzed. When dealing with digital forensic investigations, these principles should be followed and, if followed correctly, would give a higher chance of evidence being suitable for use in a court. (Forensic Control, 2022)

The four ACPO principles have been followed when carrying out this investigation. These are explained below:

ACPO Principle 1 - *"No action should be taken by an analyst that should change data held on a computer or other media which may subsequently be relied upon in Court."* (Williams, 2022)

It is presumed that the disk image was created using write blockers to ensure that the original disk drive was not modified. Working on an image rather than the live disk ensures that no modifications are made to the original disk and ensures the integrity of the data. The MD5 hash of the image can be checked before and after the investigation to ensure that no changes have been made during the investigation.

ACPO Principle 2 - *"In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and implications of their actions."* (Williams, 2022)

In this case, data is not accessed from the original drive so there are no concerns about ACPO principle 2.

ACPO Principle 3 - *"An audit trail or other record of all processes applied to computer-based evidence should be created and preserved. An independent third party should be able to examine these processes and achieve the same result."* (Williams, 2022)

Throughout the forensic process using Autopsy an audit trail will be recorded of all processes carried out. This will ensure a third party can verify the processes taken and reach the same conclusion.

ACPO Principle 4 - *"The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to."* (Williams, 2022)

The case officer of this investigation will ensure that all relevant laws and ACPO guidelines are followed. The forensic investigator's name has been recorded within this report and any queries about the investigation can be discussed further.

Software Used

Type	**Software**
Operating System	1. Microsoft Windows 10 Enterprise Build - 17763 2. Kali Linux
Tools: 1. Forensic Analysis 2. John The Ripper	1. Autopsy 4.19.3 2. John The Ripper

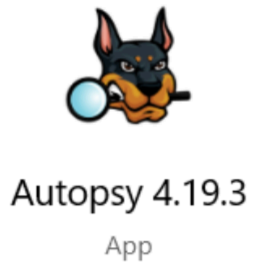
	 Autopsy 4.19.3 App

Figure 1 - Software used during forensic investigation

Investigation

Items Analysed

An image of Tracy's external hard drive has been taken. The image file was provided to the investigator in one section:

- tracy-external-2012-07-16-final. E01

The investigator is reliant upon this image received and does not take responsibility for the imaging process.

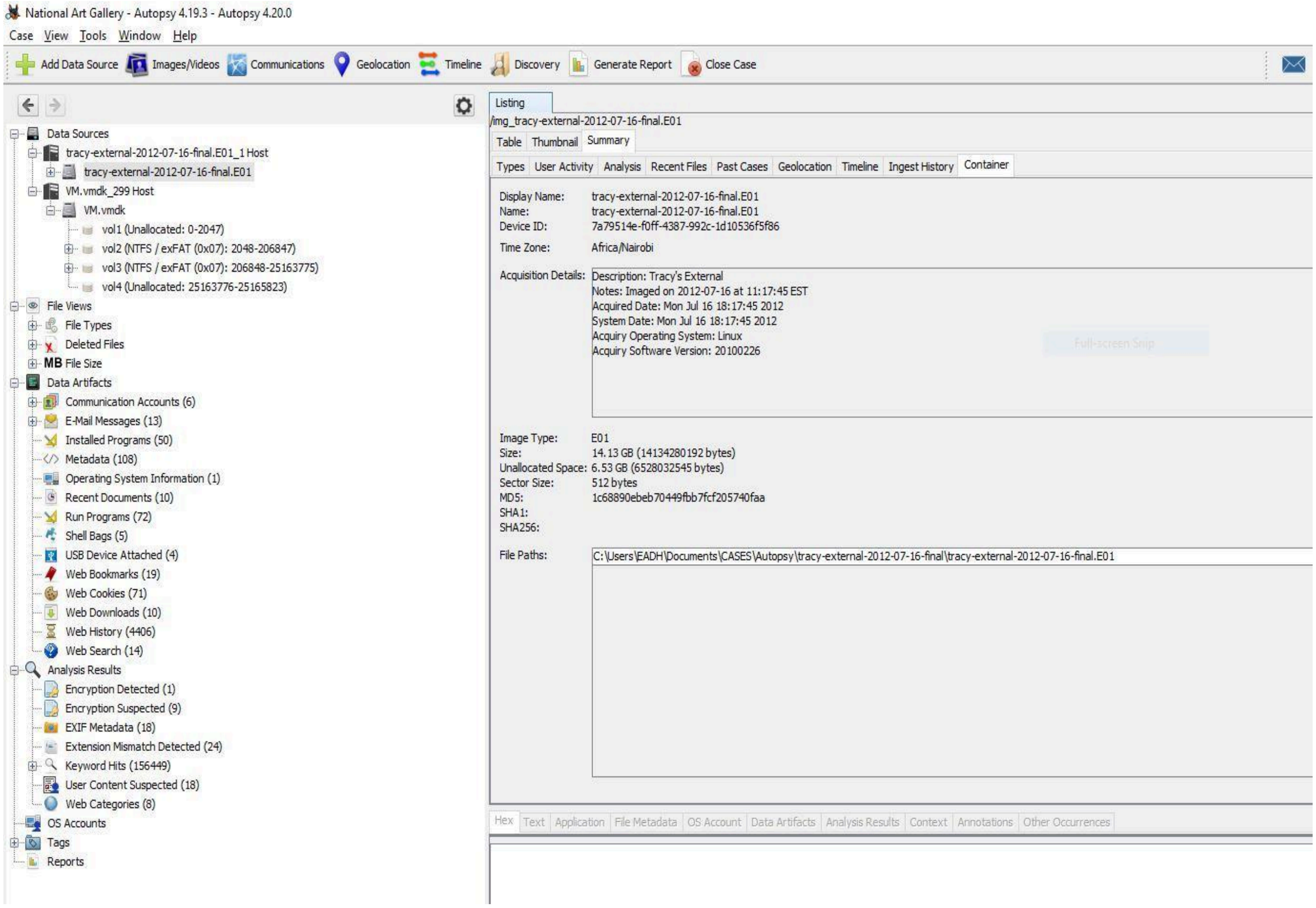
Author Authority

The authority to investigate Tracy's external hard drive is provided by the National Art Gallery.

Preservation of evidence

The image file "tracy-external-2012-07-16-final.E01" was given to the forensic investigator. To ensure the integrity of the evidence, the hash value will be recorded at the start and checked against it once the forensic investigation has finished.

The image details and MD5 hash value of "tracy-external-2012-07-16-final.E01" can be in figure 3 below:



Display Name: tracy-external-2012-07-16-final.E01
Name: tracy-external-2012-07-16-final.E01
Device ID: 7a79514e-f0ff-4387-992c-1d10536f5f86

Time Zone: Africa/Nairobi

Acquisition Details:
Description: Tracy's External
Notes: Imaged on 2012-07-16 at 11:17:45 EST
Acquired Date: Mon Jul 16 18:17:45 2012
System Date: Mon Jul 16 18:17:45 2012
Acquiry Operating System: Linux
Acquiry Software Version: 20100226

Image Type: E01
Size: 14.13 GB (14134280192 bytes)
Unallocated Space: 6.53 GB (6528032545 bytes)
Sector Size: 512 bytes
MD5: 1c68890ebeb70449fbb7fcf205740faa
SHA1:
SHA256:

File Paths: C:\Users\EADH\Documents\CASES\Autopsy\tracy-external-2012-07-16-final\tracy-external-2012-07-16-final.E01

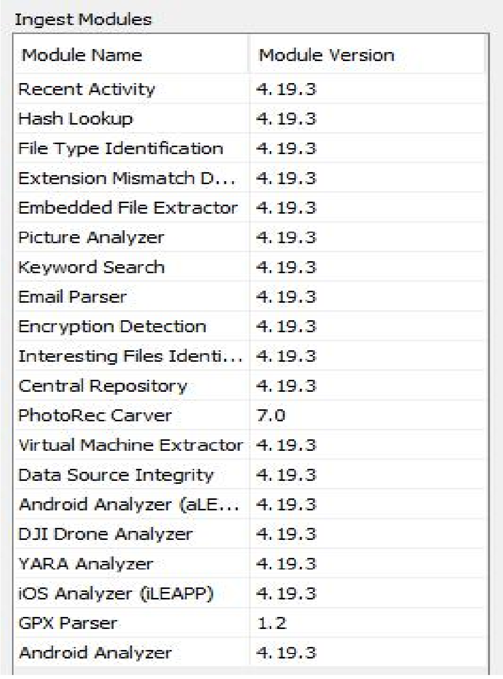
Figure 3 – Data source summary

Examination process

To forensically examine the disk image the software package Autopsy will be used (Autopsy, 2022). After reviewing all the information provided about the case the following information will be searched for:

- Email communications among Tracy, Pat, and King
- Shared timestamps documents.
- Encrypted files and encryption algorithms.
- Relevant deleted files, browser histories.
- Timeline of events

Autopsy has been chosen as the software is free of cost and the investigator has experience using the software from their university module. Within Autopsy, the ingest modules in figure 4 have been used.



Ingest Modules

Module Name	Module Version
Recent Activity	4.19.3
Hash Lookup	4.19.3
File Type Identification	4.19.3
Extension Mismatch D...	4.19.3
Embedded File Extractor	4.19.3
Picture Analyzer	4.19.3
Keyword Search	4.19.3
Email Parser	4.19.3
Encryption Detection	4.19.3
Interesting Files Identi...	4.19.3
Central Repository	4.19.3
PhotoRec Carver	7.0
Virtual Machine Extractor	4.19.3
Data Source Integrity	4.19.3
Android Analyzer (aLE...	4.19.3
DJI Drone Analyzer	4.19.3
YARA Analyzer	4.19.3
iOS Analyzer (iLEAPP)	4.19.3
GPX Parser	1.2
Android Analyzer	4.19.3

Figure 4 – Autopsy ingest modules used

The image file "tracy-external-2012-07-16-final.E01" was imported and all recommended modules were selected. This was to ensure no data was missed.

Findings

Users

"tracy-external-2012-07-16-final.E01/img_VM.vmdk/vol_vol3/Users" contains the following users:

- All Users
- Coral
- Default
- Default User
- Public

Installed Programs

See Appendix A for a list of installed programs.

Notable installed programs:

- MPlayer2
- AddressBook
- Connection Manager

- Mozilla Thunderbird
- DirectDrawEX

Email Usage

- Tracy’s email account was setup on 28th June 2

- Email communication between 6th July 2008 and 21 July 2008

Peripheral Devices

The following peripheral devices were connected to Tracy's external hard drive:

- USB Scanner
- USB Driver
- ROOT_HUB20
- CBM2080 / CBM2090 Flash drive controller
- Virtual USB Hub
- Virtual USB Hub
- Virtual Mouse
- Flash Disk 256 MB

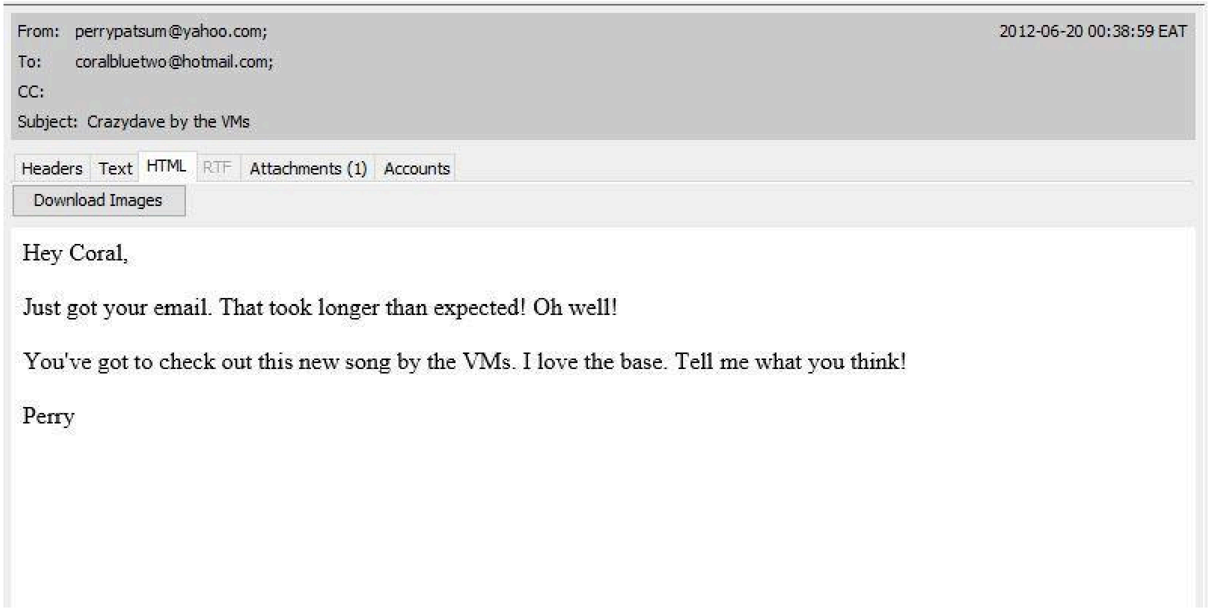
Evidence Findings

Emailed Audio evidence

Email communication was searched first as email is a well-known source for phishing attacks.

To search Tracy’s sent and received emails, global-messages-db.sqlite files were searched for on the disk image.

This screenshot below (figure 8) shows that Tracy received an email from Pat which had an MP3 audio file attachment (Crazydave1.mp3) that contained more details on how to set up a VirtualBox VM on a host computer, which was to be used in this conspiracy. It was sent at 2012-06-20 00:38:59 EAT.



From: perrypatsum@yahoo.com; 2012-06-20 00:38:59 EAT
To: coralbluetwo@hotmail.com;
CC:
Subject: Crazydave by the VMs

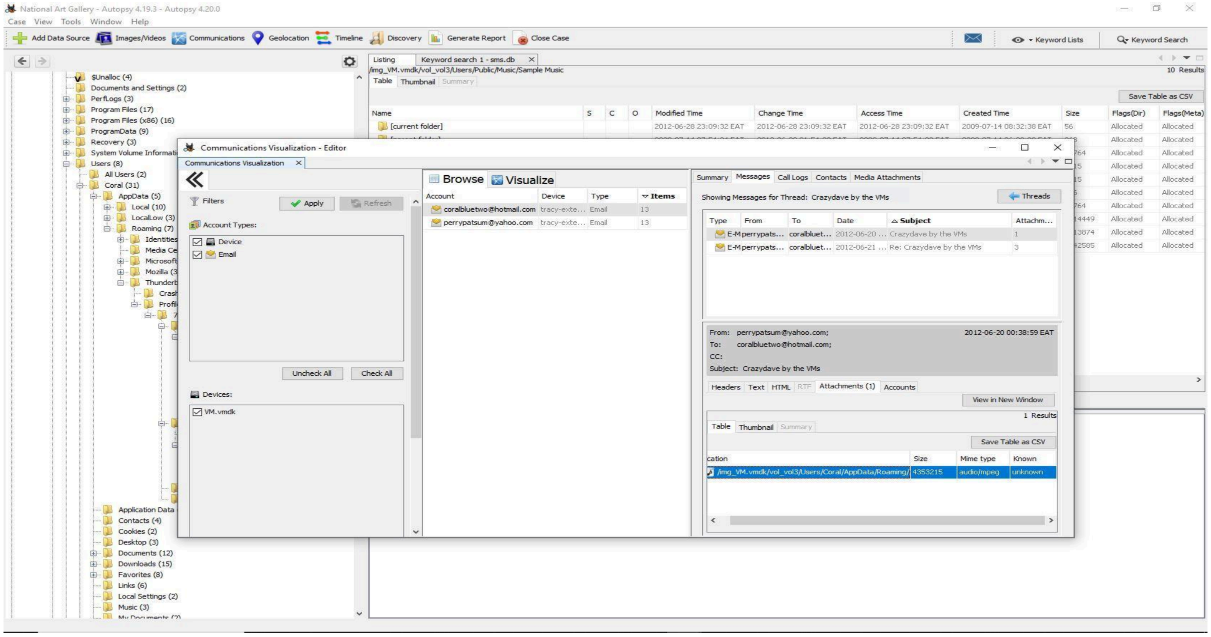
Hey Coral,

Just got your email. That took longer than expected! Oh well!

You've got to check out this new song by the VMs. I love the base. Tell me what you think!

Perry

Figure 5 – Screenshot of email



/img_VM.vmdk/vol_vol3/Users/Public/Music/Sample Music

Account	Device	Type	Items
coralbluetwo@hotmail.com	tracy-exte…	Email	13
perrypatsum@yahoo.com	tracy-exte…	Email	13

Showing Messages for Thread: Crazydave by the VMs

Type	From	To	Date	Subject	Attachm…
E-M	perrypats…	coralbluet…	2012-06-20 …	Crazydave by the VMs	1
E-M	perrypats…	coralbluet…	2012-06-21 …	Re: Crazydave by the VMs	3

From: perrypatsum@yahoo.com; 2012-06-20 00:38:59 EAT
To: coralbluetwo@hotmail.com;
CC:
Subject: Crazydave by the VMs

1 Results

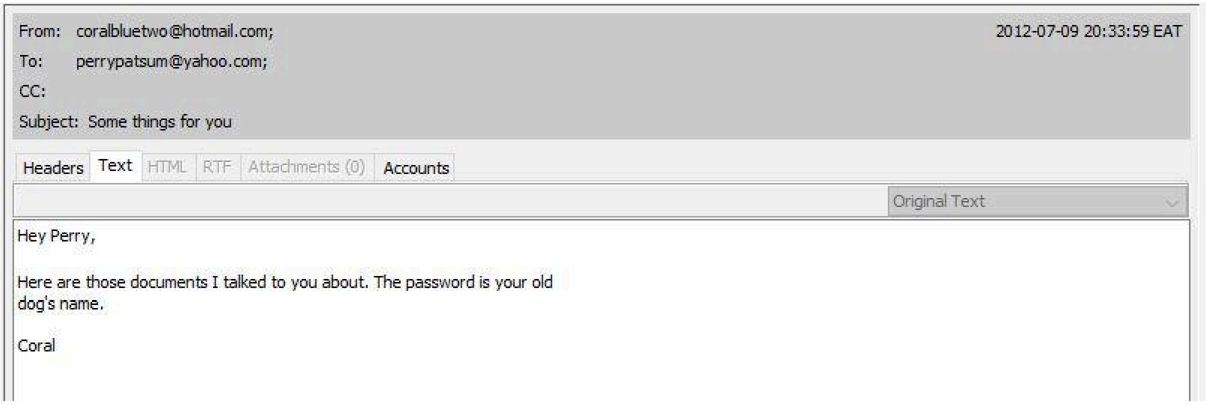
cation	Size	Mime type	Known
/img_VM.vmdk/vol_vol3/Users/Coral/AppData/Roaming/	4353215	audio/mpeg	unknown

Figure 6 – Screenshot of crazydave mp3 audio file

Emailed Encrypted stamp evidence

In this instance, Tracy (Coral) emailed Pat (Perry) the stamp documents, but the documents were in an encrypted folder called **documents.zip.** This folder was encrypted on 2012-07-09 20:17:11 EAT as observed on Tracy's external Hard drive. They are located on img_VM.vmdk/vol_vol3/Users/Coral/Documents/documents.zip. To be able to access the folder one has to have the password.

Tracy went further to tell Pat that the password is his old dog's name.



From: coralbluetwo@hotmail.com;
To: perrypatsum@yahoo.com;
CC:
Subject: Some things for you

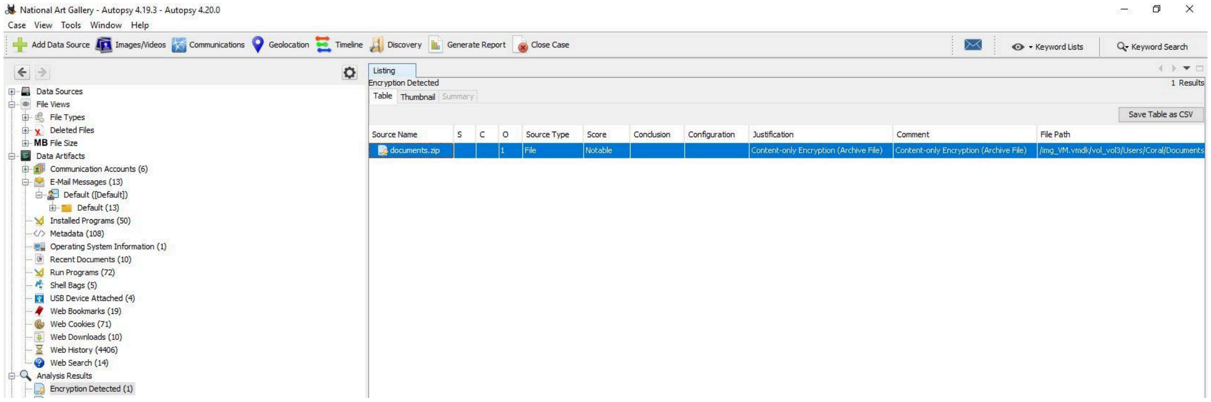
2012-07-09 20:33:59 EAT

Hey Perry,

Here are those documents I talked to you about. The password is your old dog's name.

Coral

Figure 7 Screenshot of shared documents email



National Art Gallery - Autopsy 4.19.3 - Autopsy 4.20.0

Encryption Detected

1 Results

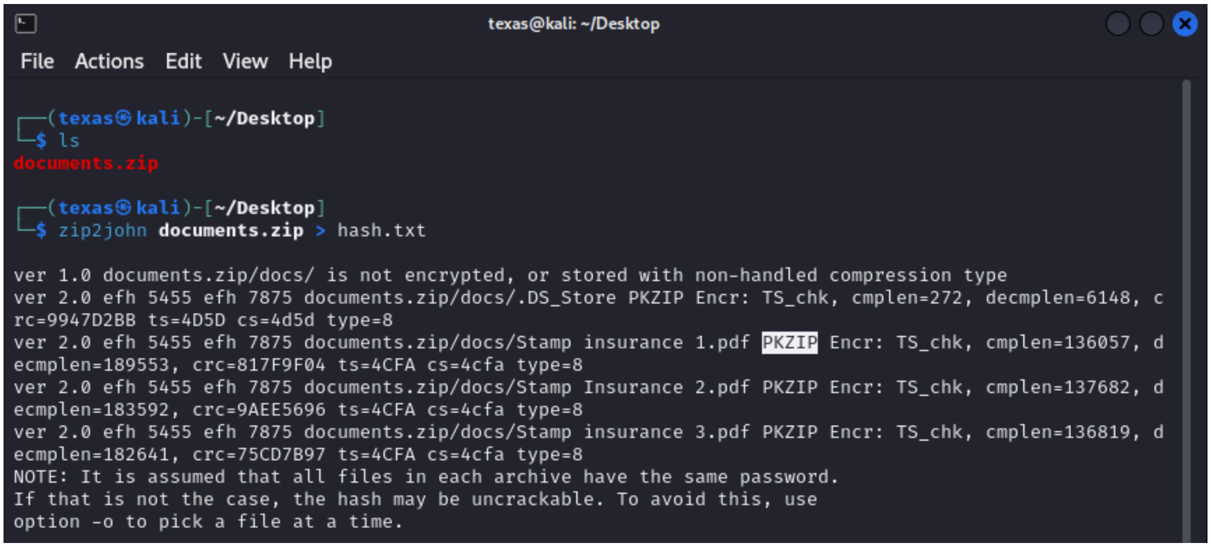
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Comment	File Path
documents.zip			1	File	Notable			Content-only Encryption (Archive File)	Content-only Encryption (Archive File)	/img_VM.vmdk/vol_vol3/Users/Coral/Documents

Figure 8.1.0– Screenshot of zipped & encrypted folder with the stamps

There was no other communication that suggested the dog's name, so the only solution was to crack the password.

I used John The Ripper tool to crack the password using the following steps:

1. Identify Hash Mode: Since the password-protected file is encrypted using PKZIP encryption, you'll need to use the zip hash mode in John the ripper. **zip2john** successfully extracted the hash of the password-protected file within the ZIP archive (documents.zip). The hash was saved to a file named hash.txt.



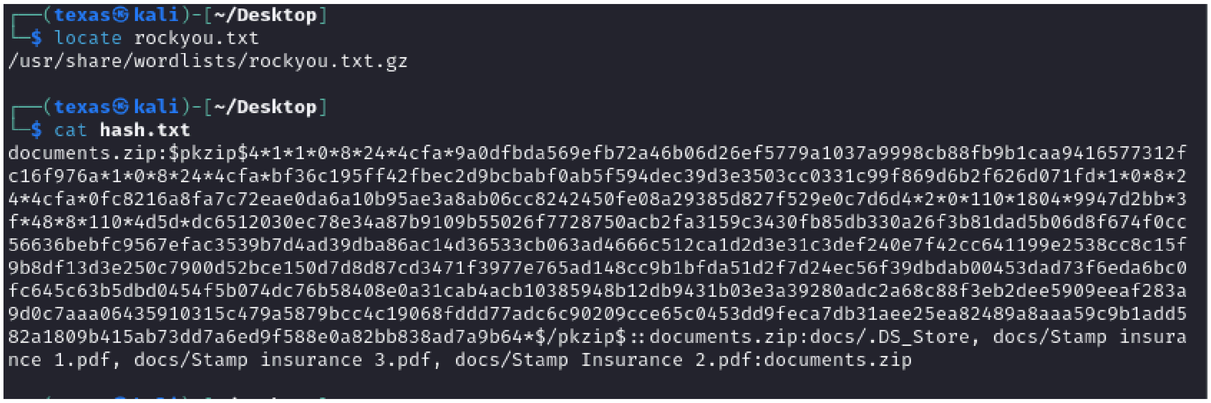
```
┌──(texas㉿kali)-[~/Desktop]
└─$ ls
documents.zip

┌──(texas㉿kali)-[~/Desktop]
└─$ zip2john documents.zip > hash.txt

ver 1.0 documents.zip/docs/ is not encrypted, or stored with non-handled compression type
ver 2.0 efh 5455 efh 7875 documents.zip/docs/.DS_Store PKZIP Encr: TS_chk, cmplen=272, decmplen=6148, c
rc=9947D2BB ts=4D5D cs=4d5d type=8
ver 2.0 efh 5455 efh 7875 documents.zip/docs/Stamp insurance 1.pdf PKZIP Encr: TS_chk, cmplen=136057, d
ecmplen=189553, crc=817F9F04 ts=4CFA cs=4cfa type=8
ver 2.0 efh 5455 efh 7875 documents.zip/docs/Stamp Insurance 2.pdf PKZIP Encr: TS_chk, cmplen=137682, d
ecmplen=183592, crc=9AEE5696 ts=4CFA cs=4cfa type=8
ver 2.0 efh 5455 efh 7875 documents.zip/docs/Stamp insurance 3.pdf PKZIP Encr: TS_chk, cmplen=136819, d
ecmplen=182641, crc=75CD7B97 ts=4CFA cs=4cfa type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

Figure 8.1.1– Screenshot of identifying the hash mode

2. Choose Wordlist: Select a wordlist or dictionary file to use for the password cracking attempt. You can use common wordlists like rockyou.txt, which is a local wordlist in kali linux
3. Extract Hash: Use zip2john to extract the hash of the password-protected ZIP file. This is the hash created.

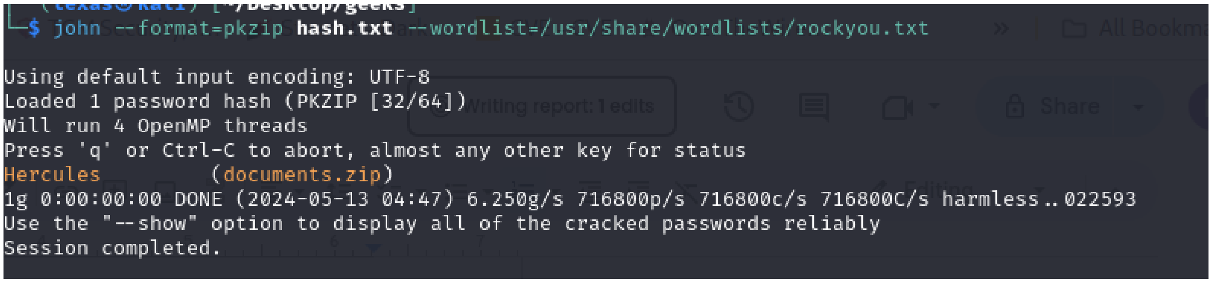


```
┌──(texas㉿kali)-[~/Desktop]
└─$ locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz

┌──(texas㉿kali)-[~/Desktop]
└─$ cat hash.txt
documents.zip:$pkzip$4*1*1*0*8*24*4cfa*9a0dfbda569efb72a46b06d26ef5779a1037a9998cb88fb9b1caa9416577312f
c16f976a*1*0*8*24*4cfa*bf36c195ff42fbec2d9bcbabf0ab5f594dec39d3e3503cc0331c99f869d6b2f626d071fd*1*0*8*2
4*4cfa*0fc8216a8fa7c72eae0da6a10b95ae3a8ab06cc8242450fe08a29385d827f529e0c7d6d4*2*0*110*1804*9947d2bb*3
f*48*8*110*4d5d*dc6512030ec78e34a87b9109b55026f7728750acb2fa3159c3430fb85db330a26f3b81dad5b06d8f674f0cc
56636bebfc9567efac3539b7d4ad39dba86ac14d36533cb063ad4666c512ca1d2d3e31c3def240e7f42cc641199e2538cc8c15f
9b8df13d3e250c7900d52bce150d7d8d87cd3471f3977e765ad148cc9b1bfda51d2f7d24ec56f39dbdab00453dad73f6eda6bc0
fc645c63b5dbd0454f5b074dc76b58408e0a31cab4acb10385948b12db9431b03e3a39280adc2a68c88f3eb2dee5909eeaf283a
9d0c7aaa06435910315c479a5879bcc4c19068fddd77adc6c90209cce65c0453dd9feca7db31aee25ea82489a8aaa59c9b1add5
82a1809b415ab73dd7a6ed9f588e0a82bb838ad7a9b64*$/pkzip$::documents.zip:docs/.DS_Store, docs/Stamp insura
nce 1.pdf, docs/Stamp insurance 3.pdf, docs/Stamp Insurance 2.pdf:documents.zip
```

Figure 8.1.2– Screenshot of choosing wordlist & extracting the hash of the encrypted file

4. Crack Password: Use John the Ripper to crack the password using the extracted hash. The syntax is as follows:
   john --format=pkzip hash.txt --wordlist=/usr/share/wordlists/rockyou.txt. The password was **Hercules**

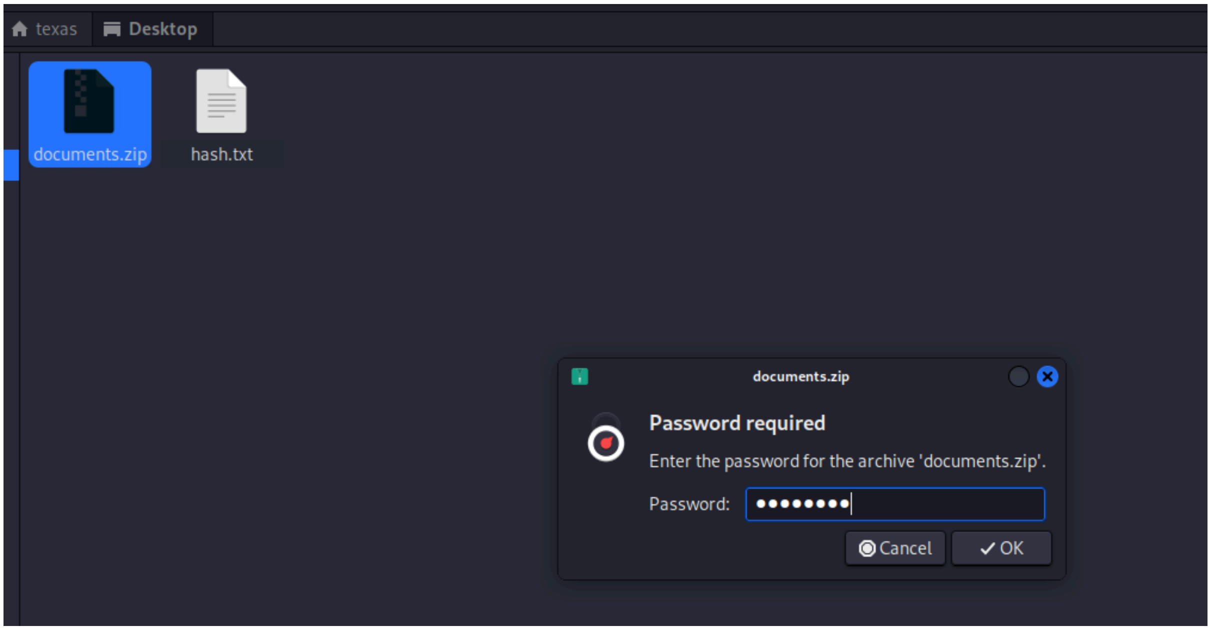


```
┌──(texas㉿kali)-[~/Desktop/geeks]
└─$ john --format=pkzip hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Hercules         (documents.zip)
1g 0:00:00:00 DONE (2024-05-13 04:47) 6.250g/s 716800p/s 716800c/s 716800C/s harmless..022593
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Figure 8.1.3– Screenshot of cracking the password using John The Ripper

5. Use the password to decrypt the folder as follows:



Password required

Enter the password for the archive 'documents.zip'.

Password: ••••••••

Figure 8.1.4– Screenshot of using the cracked password to decrypt

6. Accessing the folder and eventually the stamp documents:

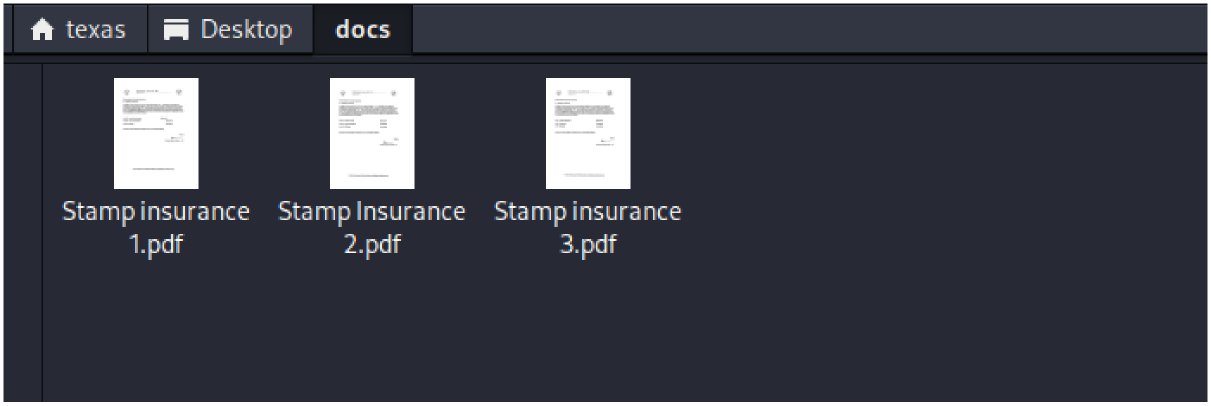
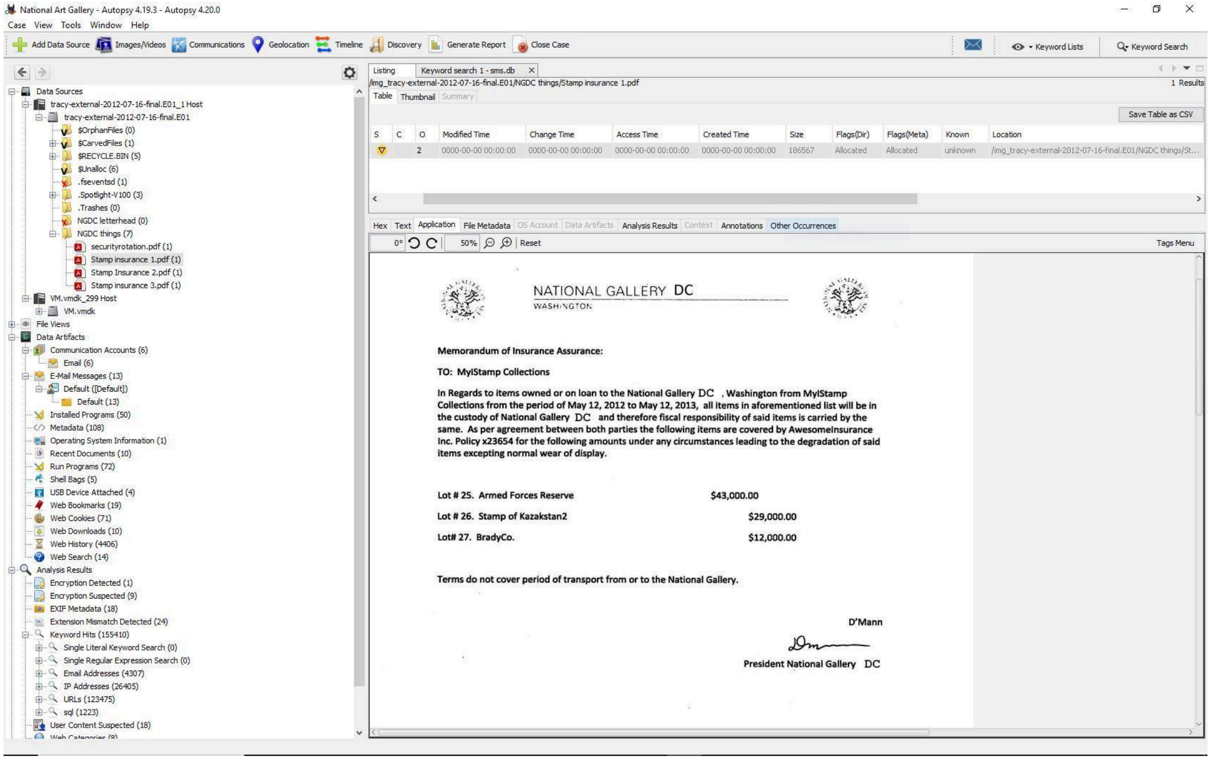


Figure 8.1.5– Screenshot of a successful access to the shared stamp files



/img_tracy-external-2012-07-16-final.E01/NGDC things/Stamp insurance 1.pdf

1 Results

S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
▽		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	186567	Allocated	Allocated	unknown	/img_tracy-external-2012-07-16-final.E01/NGDC things/St...

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**

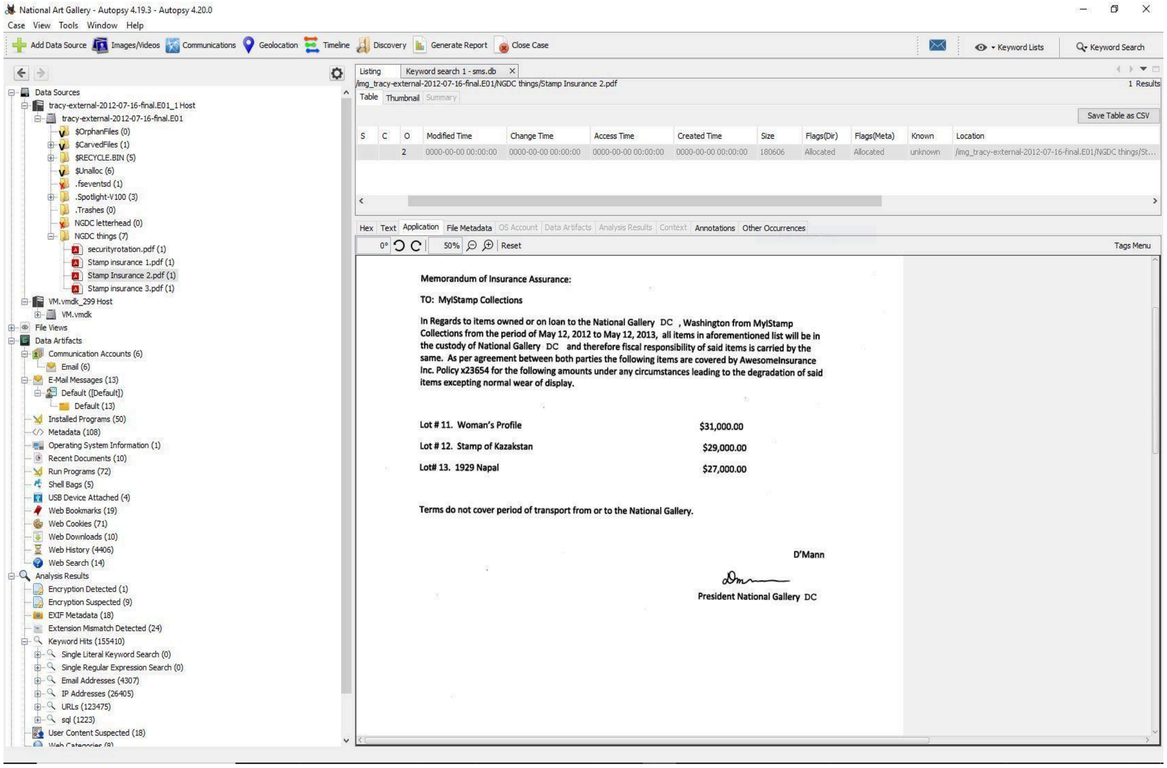
Terms do not cover period of transport from or to the National Gallery.

D'Mann

Dm

President National Gallery DC

Figure 8.2 – Screenshot of stamp 1



/img_tracy-external-2012-07-16-final.E01/NGDC things/Stamp Insurance 2.pdf

1 Results

S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
		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	180606	Allocated	Allocated	unknown	/img_tracy-external-2012-07-16-final.E01/NGDC things/St...

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.

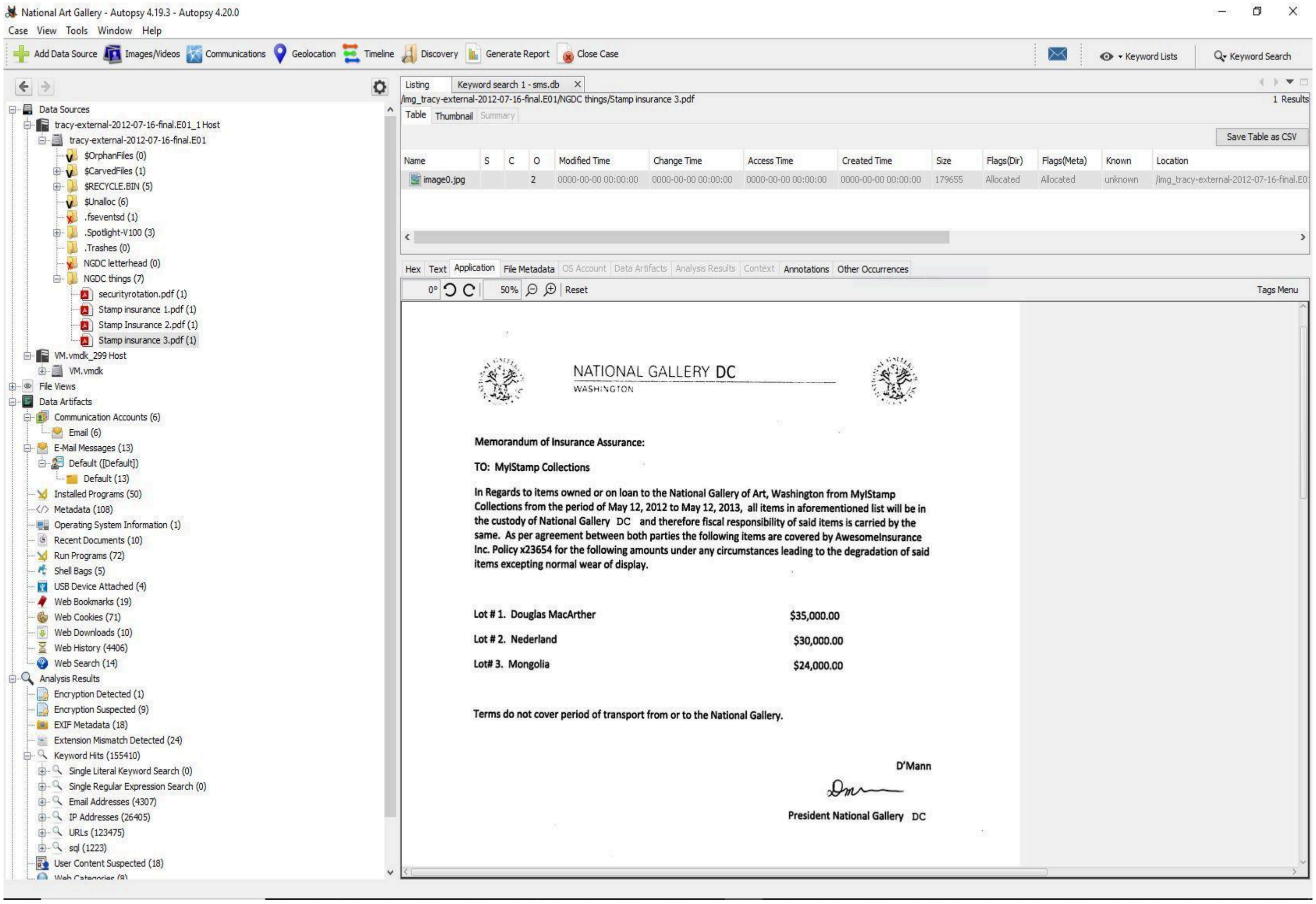
Lot # 11. Woman's Profile	**$31,000.00**
Lot # 12. Stamp of Kazakstan	**$29,000.00**
Lot# 13. 1929 Napal	**$27,000.00**

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

D'Mann

President National Gallery DC

Figure 8.3 – Screenshot of stamp 2



/img_tracy-external-2012-07-16-final.E01/NGDC things/Stamp insurance 3.pdf

1 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
image0.jpg			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	179655	Allocated	Allocated	unknown	/img_tracy-external-2012-07-16-final.E0

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.

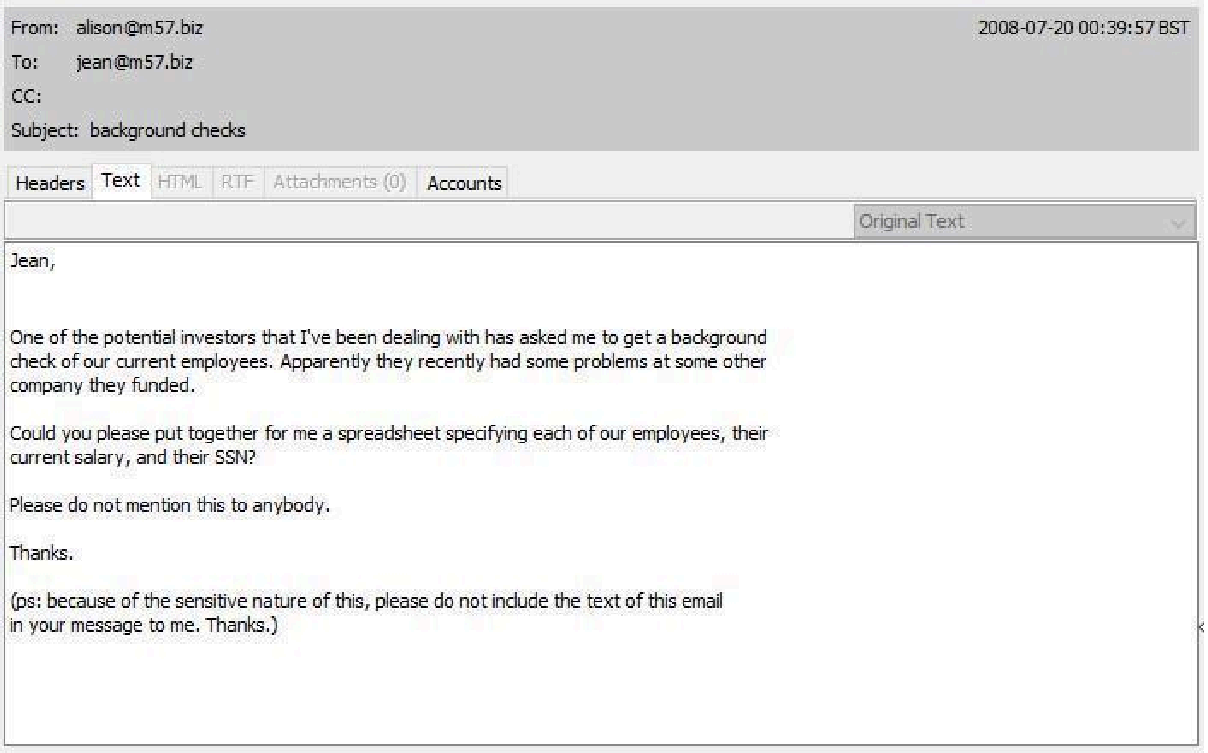
D'Mann

President National Gallery DC

Figure 8.4 – Screenshot of stamp 3

Other relevant emails

Email 1



From: alison@m57.biz 2008-07-20 00:39:57 BST

To: jean@m57.biz

CC:

Subject: background checks

Jean,

One of the potential investors that I've been dealing with has asked me to get a background check of our current employees. Apparently they recently had some problems at some other company they funded.

Could you please put together for me a spreadsheet specifying each of our employees, their current salary, and their SSN?

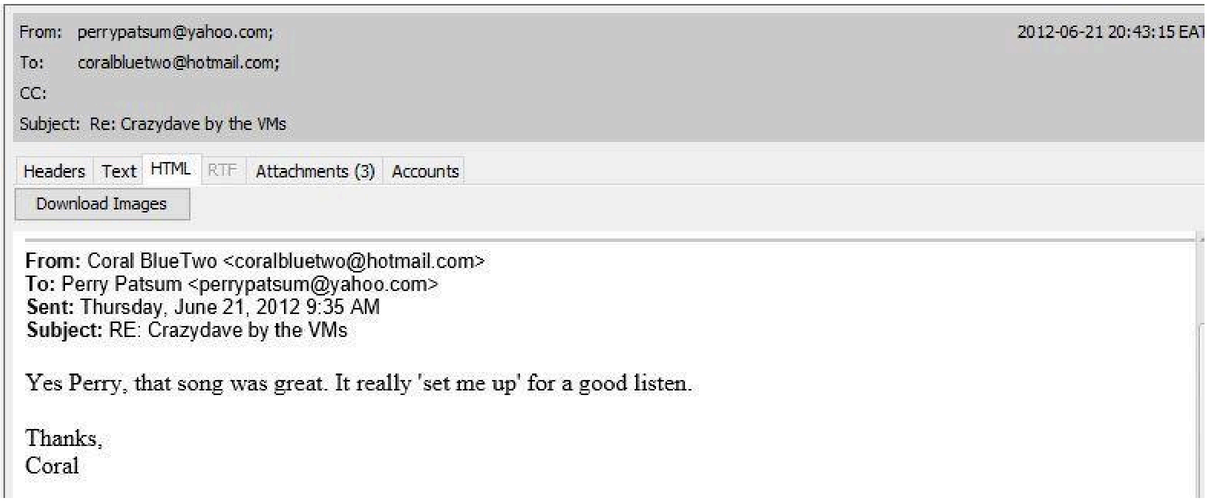
Please do not mention this to anybody.

Thanks.

(ps: because of the sensitive nature of this, please do not include the text of this email in your message to me. Thanks.)

Figure 9 – Email 1

Email shows Tracy (Coral) emailing Pat (Perry) confirming that the instructions sent earlier in the audio file helped her.



From: perrypatsum@yahoo.com; 2012-06-21 20:43:15 EAT
To: coralbluetwo@hotmail.com;
CC:
Subject: Re: Crazydave by the VMs

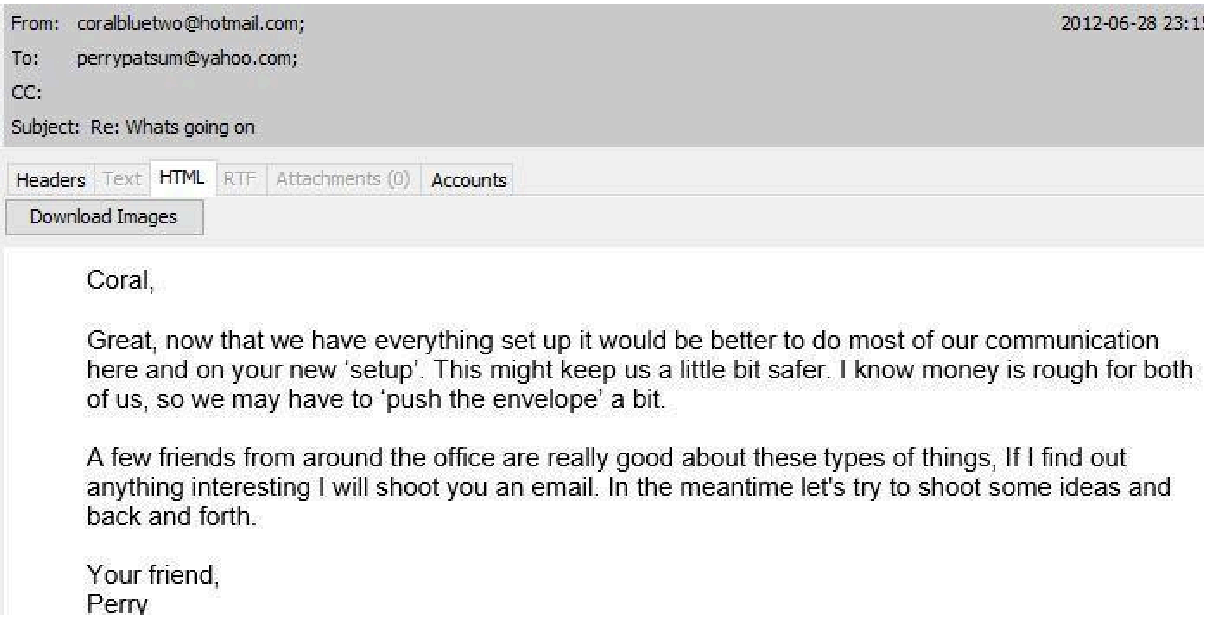
From: Coral BlueTwo <coralbluetwo@hotmail.com>
To: Perry Patsum <perrypatsum@yahoo.com>
Sent: Thursday, June 21, 2012 9:35 AM
Subject: RE: Crazydave by the VMs

Yes Perry, that song was great. It really 'set me up' for a good listen.

Thanks,
Coral

Figure 10 – Email 1

Email 2



From: coralbluetwo@hotmail.com; 2012-06-28 23:1
To: perrypatsum@yahoo.com;
CC:
Subject: Re: Whats going on

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.

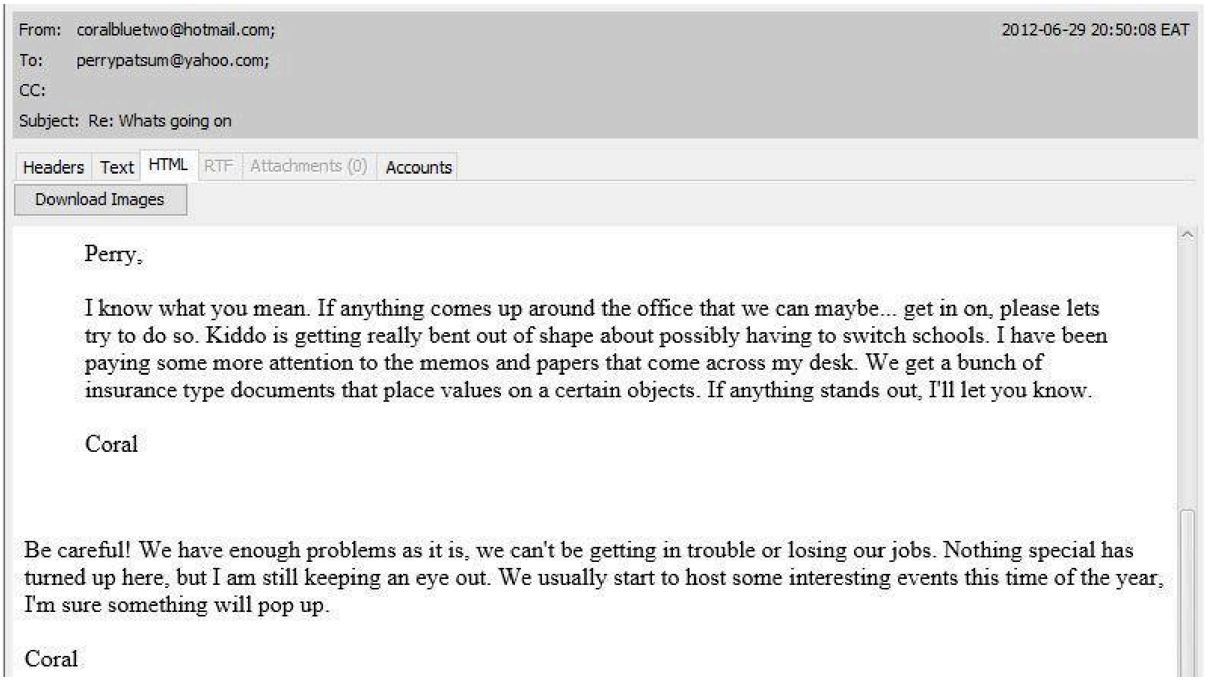
A few friends from around the office are really good about these types of things, If I find out anything interesting I will shoot you an email. In the meantime let's try to shoot some ideas and back and forth.

Your friend,
Perry

Figure 11 – Email 2

Pat (Perry) emails Tracy (Coral) asking her to henceforth communicate using the aliases and the virtual machine setup to keep them safer. He also indicates that they might have to get into riskier/illegal business since both of them were facing financial hardships. He tells her that few of his workplace friends were good at these businesses and that he will inform her should something pop up; in the meantime, they should keep discussing some ideas for the same.

Email 3



From: coralbluetwo@hotmail.com;

2012-06-29 20:50:08 EAT

To: perrypatsum@yahoo.com;

CC:

Subject: Re: Whats going on

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.

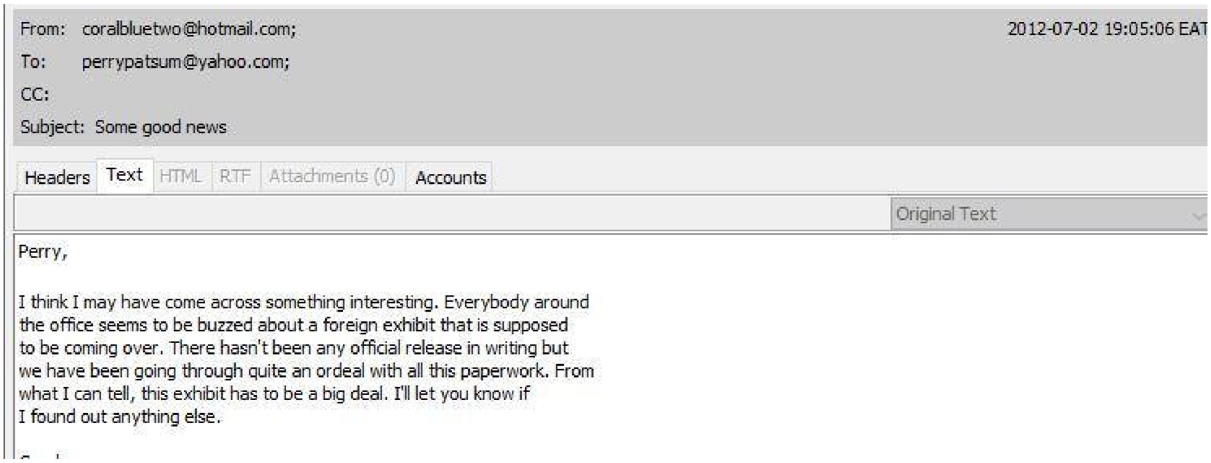
Coral

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

Coral

Figure 12 – Email 3

This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money. To Pat’s suggestion that they use the virtual machines and aliases to communicate and keep looking for ways to make money. Tracy indicates that she is paying attention to documents, especially insurance papers so that she could identify something of potential.



From: coralbluetwo@hotmail.com; 2012-07-02 19:05:06 EAT
To: perrypatsum@yahoo.com;
CC:
Subject: Some good news

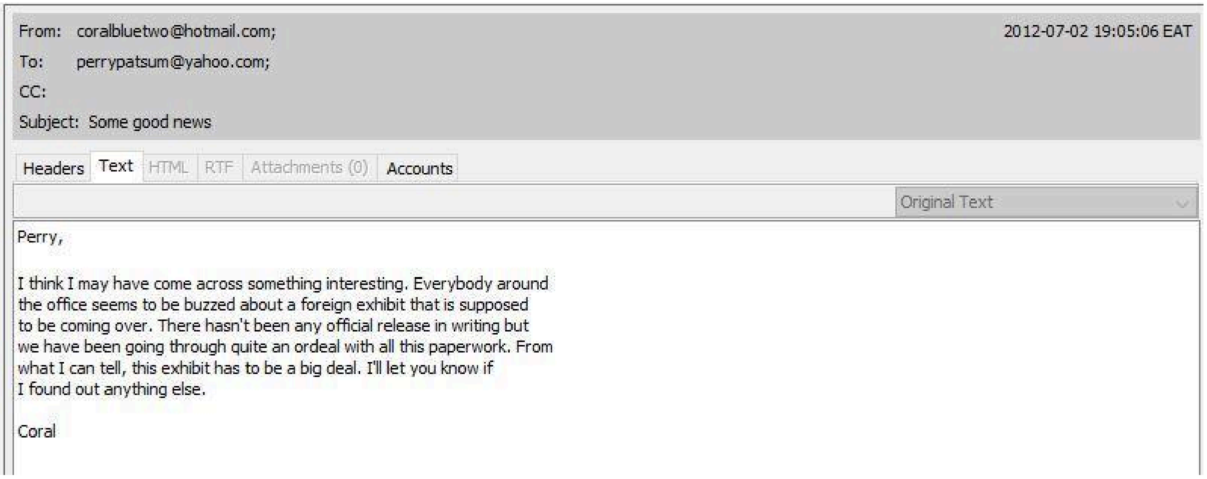
Perry,

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.

Figure 12 – Email 3 headers

Tracy (coral) emails Pat (Perry) mentioning that some interesting foreign exhibit is going to happen and that from assessing the paperwork she feels that it would be a big deal.

Email 4



From: coralbluetwo@hotmail.com;

To: perrypatsum@yahoo.com;

CC:

Subject: Some good news

2012-07-02 19:05:06 EAT

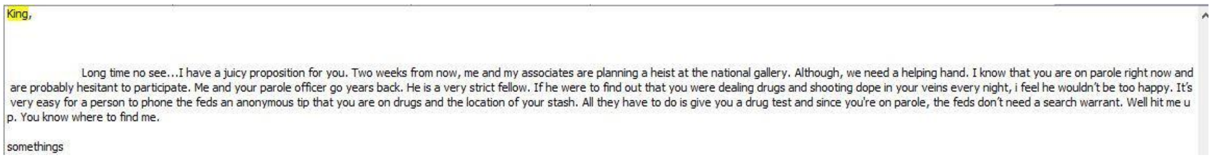
Perry,

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

Figure 13 – Email 4

Following up on the earlier email about the exhibit, Tracy (Coral) mentions going through documents related to the exhibit from which she found that the exhibit is worth a lot of money but the shipping cost is very low comparatively.



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 u
p. You know where to find me.

somethings

Figure 14 – Email 4 attachment

Pat emails King with Tracy (Coral) in cc, saying that he has a lucrative proposition.

Conclusion

In conclusion, from the evidence, it can be deduced that there was a plan for the occurrence, showcased when Tracy had expressed interest in stealing stamps out of the gallery.

This report aimed to answer the questions:

1.	Who was involved in this conspiracy?
2.	How did Tracy and her accomplices plan to execute the conspiracy?
3.	What were the different forensic artifacts used

Figure 20 - Questions to be answered by forensic investigation

Question 1

The investigator believes that Tracy and Pat had planned to steal the valuable stamps at the National Gallery with the help of Carry, and King.

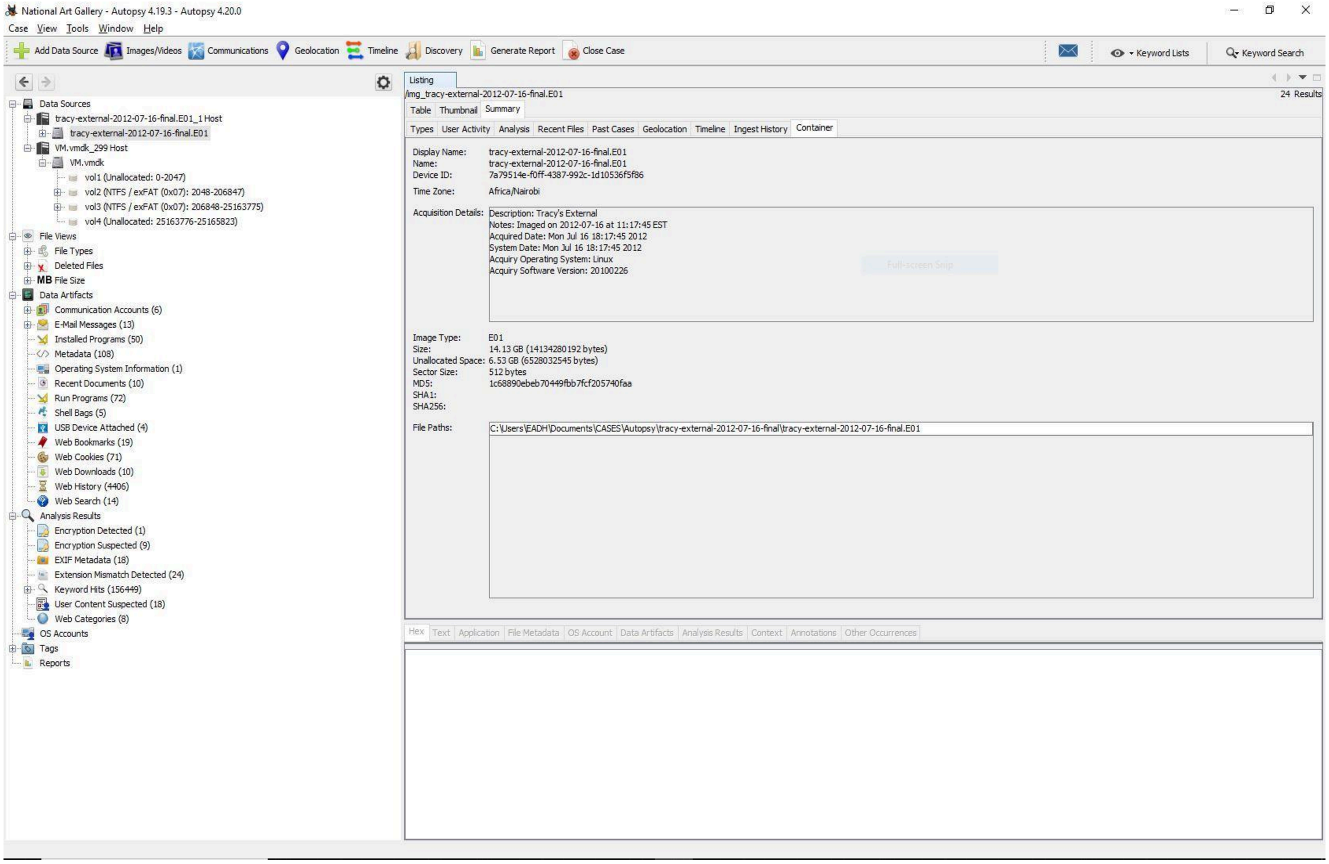
Question 2

Tracy had expressed her interest in stealing stamps out of the gallery to Pat. Further critical evidence surfaced in the form of email attachments, including insurance memoranda for the stolen stamps, Tracy and Pat, discussing the theft plans and coordination with an accomplice named King, Employment of encrypted folders and email aliases for concealing sensitive communications, and Tracy and Pat's financial desperation. Additionally, an MP3 audio file was utilized to relay instructions for setting up a Virtual Machine. Tracy's primary motive appeared to be financial gain, evident through her active participation despite facing financial hardships.

Question 3

The investigator believes that Tracy, Pat, Carry, and King were involved but the conspiracy had not yet been executed.

The MD5 hash was checked at the end of the investigation to ensure the disk image had not been modified. This can be seen in figure 21 below:



/img_tracy-external-2012-07-16-final.E01

24 Results

Display Name: tracy-external-2012-07-16-final.E01
Name: tracy-external-2012-07-16-final.E01
Device ID: 7a79514e-f0ff-4387-992c-1d10536f5f86

Time Zone: Africa/Nairobi

Acquisition Details: Description: Tracy's External
Notes: Imaged on 2012-07-16 at 11:17:45 EST
Acquired Date: Mon Jul 16 18:17:45 2012
System Date: Mon Jul 16 18:17:45 2012
Acquiry Operating System: Linux
Acquiry Software Version: 20100226

Image Type: E01
Size: 14.13 GB (14134280192 bytes)
Unallocated Space: 6.53 GB (6528032545 bytes)
Sector Size: 512 bytes
MD5: 1c68890ebeb70449fbb7fcf205740faa
SHA1:
SHA256:

File Paths: C:\Users\EADH\Documents\CASES\Autopsy\tracy-external-2012-07-16-final\tracy-external-2012-07-16-final.E01

Figure 21 – Data source summary

Recommendations

Based on the forensic investigation it would be recommended that The National Art Gallery consider the following measures to prevent future data theft occurrences:

- Install keyloggers on employee's work machines.
- Carry out regular cyber security awareness training sessions ensuring all employees are aware of the benefits of ethical adherence in and out of the workplace.
- Encrypt sensitive documents and prevent access from unauthorized personnel.

References

Williams, J., 2022. [online] Npcc.police.uk. Available at: <https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf> [Accessed 5 April 2022].

Autopsy. (2022, 03 21). Autopsy Digital Forensics. Retrieved from Auopsy:

https://www.autopsy.com/

Forensic Control. (2022). Retrieved April 02, 2022, from https://forensiccontrol.com/acpo-

guidelines-and-principles-explained/: https://forensiccontrol.com/acpo-guidelines-and-principles-explained/

Infosec Institute. (2018). Computer Forensics: digital evidence: what ethical issues need to be

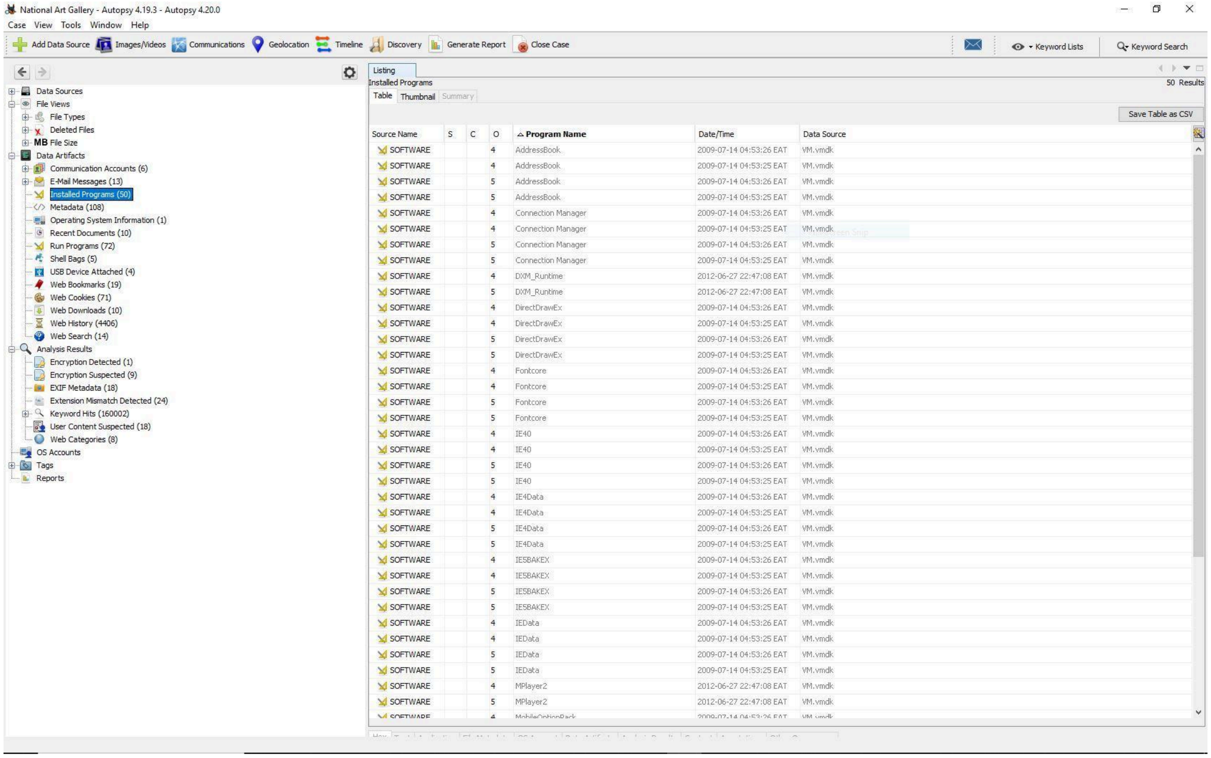
considered when evaluating digital evidence. Retrieved from https://www.computer.org/csdl/proceedings/hicss/2011/9618/00/05719007.pdf

Stood, A., & Enbody, R. (2014). Targeted Cyber Attacks. Elsevier Science.

Wang, W. (2012). Cyber security in the smart grid: survey and challenges. Netw: Comput.

Appendix 1

Softwares Installed

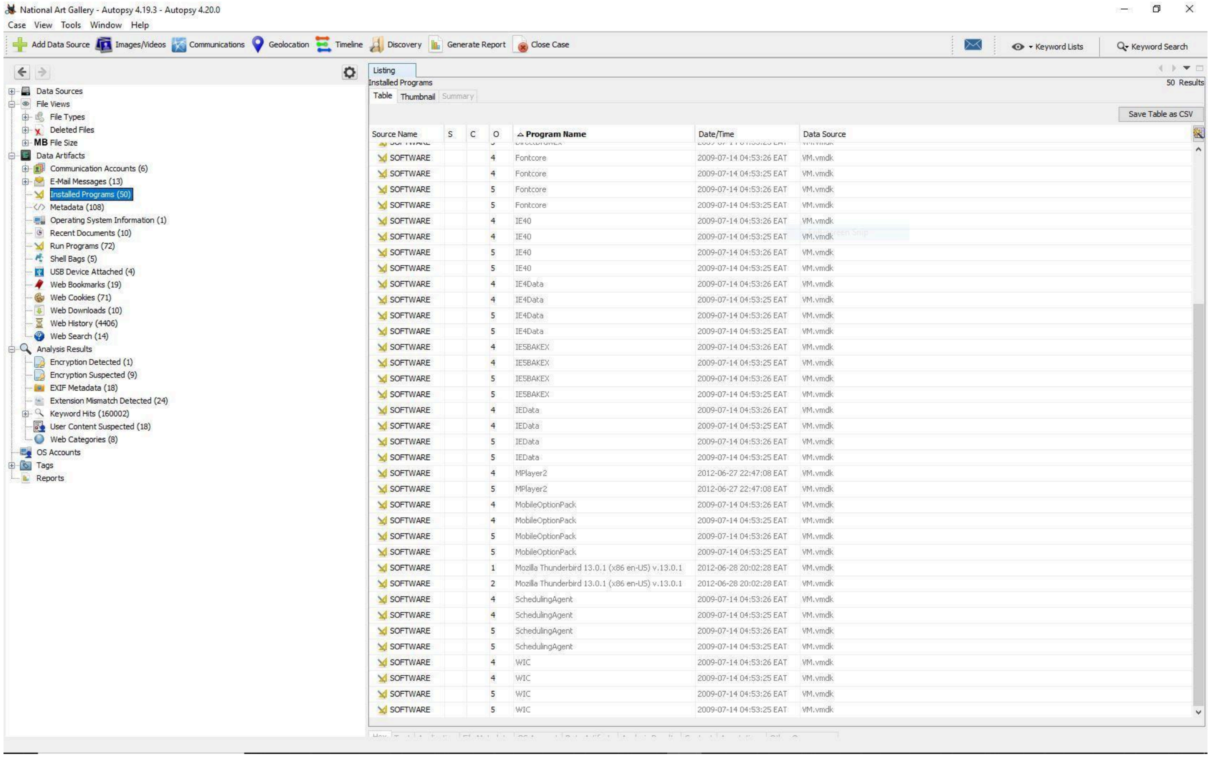


- Data Sources
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Communication Accounts (6)
  - E-Mail Messages (13)
  - Installed Programs (50)
  - Metadata (108)
  - Operating System Information (1)
  - Recent Documents (10)
  - Run Programs (72)
  - Shell Bags (5)
  - USB Device Attached (4)
  - Web Bookmarks (19)
  - Web Cookies (71)
  - Web Downloads (10)
  - Web History (4406)
  - Web Search (14)
- Analysis Results
  - Encryption Detected (1)
  - Encryption Suspected (9)
  - EXIF Metadata (18)
  - Extension Mismatch Detected (24)
  - Keyword Hits (160002)
  - User Content Suspected (18)
  - Web Categories (8)
- OS Accounts
- Tags
- Reports

Installed Programs

50 Results

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			4	AddressBook	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	AddressBook	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	AddressBook	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	AddressBook	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	Connection Manager	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	Connection Manager	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	Connection Manager	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	Connection Manager	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	DXM_Runtime	2012-06-27 22:47:08 EAT	VM.vmdk
SOFTWARE			5	DXM_Runtime	2012-06-27 22:47:08 EAT	VM.vmdk
SOFTWARE			4	DirectDrawEx	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	DirectDrawEx	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	DirectDrawEx	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	DirectDrawEx	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	Fontcore	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	Fontcore	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	Fontcore	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	Fontcore	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	IE40	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	IE40	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	IE40	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	IE40	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	IE4Data	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	IE4Data	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	IE4Data	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	IE4Data	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	IE5BAKEX	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	IE5BAKEX	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	IE5BAKEX	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	IE5BAKEX	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	IEData	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	IEData	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	IEData	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	IEData	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	MPlayer2	2012-06-27 22:47:08 EAT	VM.vmdk
SOFTWARE			5	MPlayer2	2012-06-27 22:47:08 EAT	VM.vmdk
SOFTWARE			4	MobileOptionPack	2009-07-14 04:53:26 EAT	VM.vmdk



- Data Sources
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Communication Accounts (6)
  - E-Mail Messages (13)
  - Installed Programs (50)
  - Metadata (108)
  - Operating System Information (1)
  - Recent Documents (10)
  - Run Programs (72)
  - Shell Bags (5)
  - USB Device Attached (4)
  - Web Bookmarks (19)
  - Web Cookies (71)
  - Web Downloads (10)
  - Web History (4406)
  - Web Search (14)
- Analysis Results
  - Encryption Detected (1)
  - Encryption Suspected (9)
  - EXIF Metadata (18)
  - Extension Mismatch Detected (24)
  - Keyword Hits (160002)
  - User Content Suspected (18)
  - Web Categories (8)
- OS Accounts
- Tags
- Reports

Installed Programs

50 Results

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			4	Fontcore	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	Fontcore	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	Fontcore	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	Fontcore	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	IE40	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	IE40	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	IE40	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	IE40	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	IE4Data	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	IE4Data	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	IE4Data	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	IE4Data	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	IE5BAKEX	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	IE5BAKEX	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	IE5BAKEX	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	IE5BAKEX	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	IEData	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	IEData	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	IEData	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	IEData	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	MPlayer2	2012-06-27 22:47:08 EAT	VM.vmdk
SOFTWARE			5	MPlayer2	2012-06-27 22:47:08 EAT	VM.vmdk
SOFTWARE			4	MobileOptionPack	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	MobileOptionPack	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	MobileOptionPack	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	MobileOptionPack	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			1	Mozilla Thunderbird 13.0.1 (x86 en-US) v.13.0.1	2012-06-28 20:02:28 EAT	VM.vmdk
SOFTWARE			2	Mozilla Thunderbird 13.0.1 (x86 en-US) v.13.0.1	2012-06-28 20:02:28 EAT	VM.vmdk
SOFTWARE			4	SchedulingAgent	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	SchedulingAgent	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	SchedulingAgent	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	SchedulingAgent	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			4	WIC	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			4	WIC	2009-07-14 04:53:25 EAT	VM.vmdk
SOFTWARE			5	WIC	2009-07-14 04:53:26 EAT	VM.vmdk
SOFTWARE			5	WIC	2009-07-14 04:53:25 EAT	VM.vmdk

The above images show softwares installed by Tracy (Coral)

Appendix 2

Timeline of events

The timestamps for this timeline are taken directly from Autopsy with the time zone set as

GMT.

Timestamp	Header Information	Key Information	Evidence Location/path	Attachment
	From: perrypatsum@yahoo.com To: tracysumtwelve@gmail.com Subject: Look me up sometime	Pat (Perry) emails Tracy to ask her to communicate using her alias.	Email	
Tue, 19 June 2012 14:38:59 -0700 EAT	From: perrypatsum@yahoo.com To:coralbluetwo@hotmail.com Subject: Crazydave by the VMs	Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine hidden in an audio file.	Email	Crazydave1.mp3
Thursday, June 21, 2012	From: perrypatsum@yaho	Pat(Perry) replies to Tracy (Coral) confirming that he was	Email	

9:35 AM EAT	o.com To: coralbluetwo@hotmail.com Subject: Re: ???	getting her emails.		
Thursday, June 21, 2012 9:35 AM EAT	From: coralbluetwo@hotmail.com To: perrypatsum@yahoo.com Subject:Re: Crazydave1.mp3	Pat (Perry) replies to Tracy (Coral) on an email thread about virtual machine installation saying that she should listen to some other songs as well. In the email thread Tracy (Coral) confirms that the instructions sent earlier in the audio file helped her.	Email	
6/28/2012 12:31 PM EAT	From: coralbluetwo@hotmail.com To: perrypatsum@yahoo.com Subject: What's going on?	Pat (Perry) emails Tracy (Coral) asking her to henceforth communicate using the aliases and the virtual machine setup to keep them safer. He also indicates that they might have to get into riskier/illegal business since both of them were facing financial hardships. He tells her that few of his workplace friends were good at these businesses and that he will inform her should something pop-up; in the meantime they should keep discussing some ideas for the same.	Email	
	From: Coral BlueTwo <coralbluetwo@hot	This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money. To Pat's suggestion that they use the	Email	

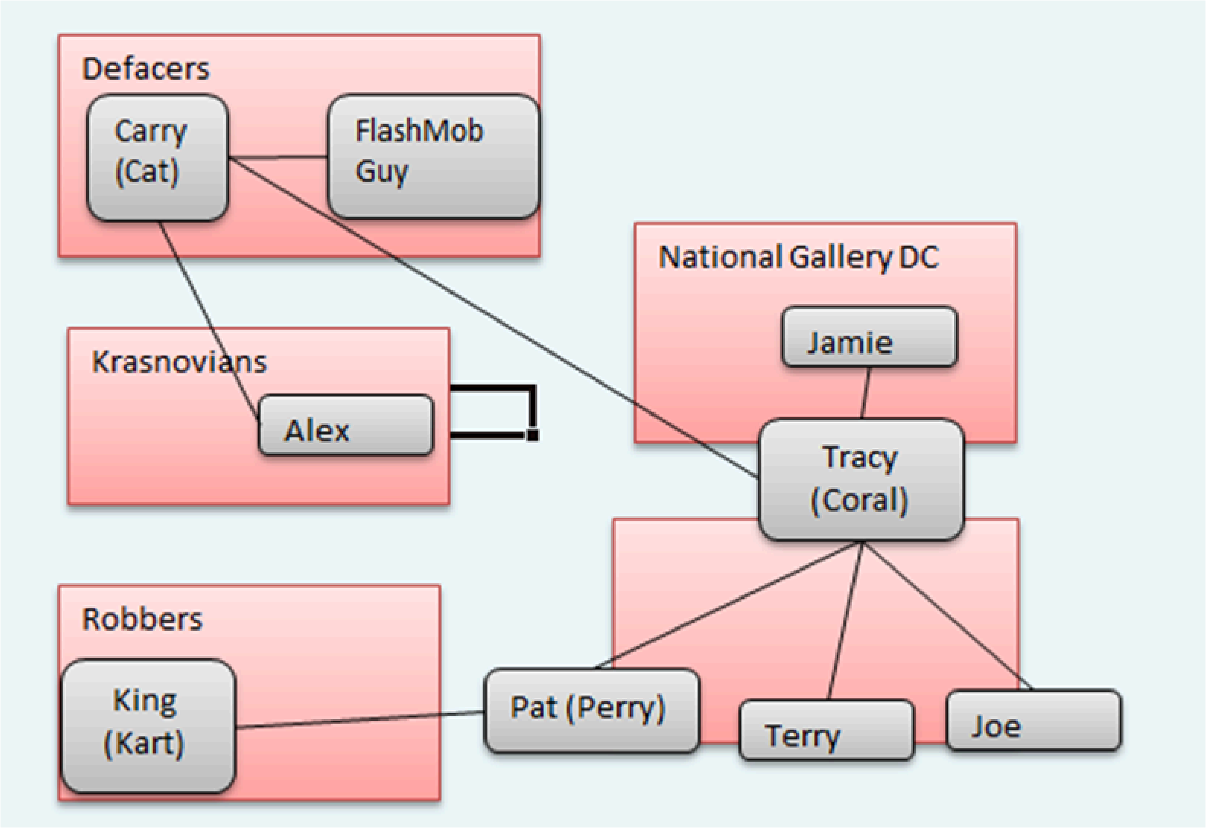
	mail.com> To: Perry Patsum <perrypatsum@yahoo.com> Subject: What’s going on?	virtual machines and aliases to communicate and keep looking for ways to make money, Tracy replies that she will keep her eyes open for opportunities and insists that Pat try to get in on some business soon, since her kind didn’t want to change schools. She also indicates that she is paying attention to documents, especially insurance papers so that she could identify something of potential. Pat assures that he will make something of potential. Pat assures that he will make something happen although he is nervous because IA has been sniffing around.		
6/29/2012 7:21 AM EAT	From: coralbluetwo@hotmail.com To: perrypatsum@yahoo.com Subject: What’s going on?	Pat (Perry0 replies to the email thread allyng Tracy’s (Coral) concern about sniffing IA sniffing around him. Tracy in her earlier email in the thread says that although nothing interesting has turned up yet she expects something soon. Pat in his email mentions that they can certainly get the job done if something like what they had earlier discussed pops up.	Email	
02/07/2012 19:03 EAT	From: coralbluetwo@hotmail.com To: perrypatsum@yahoo.com	Tracy (coral) emails Pat (Perry) mentioning that some interesting foreign exhibit is going to happen and that from assessing the paperwork she feels that it would be a big deal. Pat (Perry) replies back feeling hopeful about this being the opportunity they were looking for.	Email	

	Subject: some good news			
Monday, July 2, 2012 12:05 PM EAT	From: coralbluetwo@hotmail.com To: perrypatsum@yahoo.com Subject:Some good news	Following up on the earlier email about the exhibit, Tracy (Coral) mentions going through documents related to the exhibit from which she found that the exhibit is worth a lot of money but the shipping cost is very low comparatively. Pat (Perry) emails back saying that such a thing may mean that the exhibit is something small which would be a very good thing for them.	Email	
7/6/2012 15:49:31 EAT	From: patsumtwelve@gmail.com To: throne1966@hotmail.com Cc:coralbluetwo@hotmail.com Subject: can't pass up	Pat emails King with Tracy (Coral) in cc, saying that he has a lucrative proposition, a heist at the national gallery. He also threatens King to comply or else he would put King’s parole in jeopardy.	Email	

Figure 19 – Timeline of events

Appendix 3

Persons Investigated


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