

ITIS 5250
Akshay Desai
Graduate Lab Forensics Report (“The Case of Robbin’ Robert”)
04/25/2020

Overview:

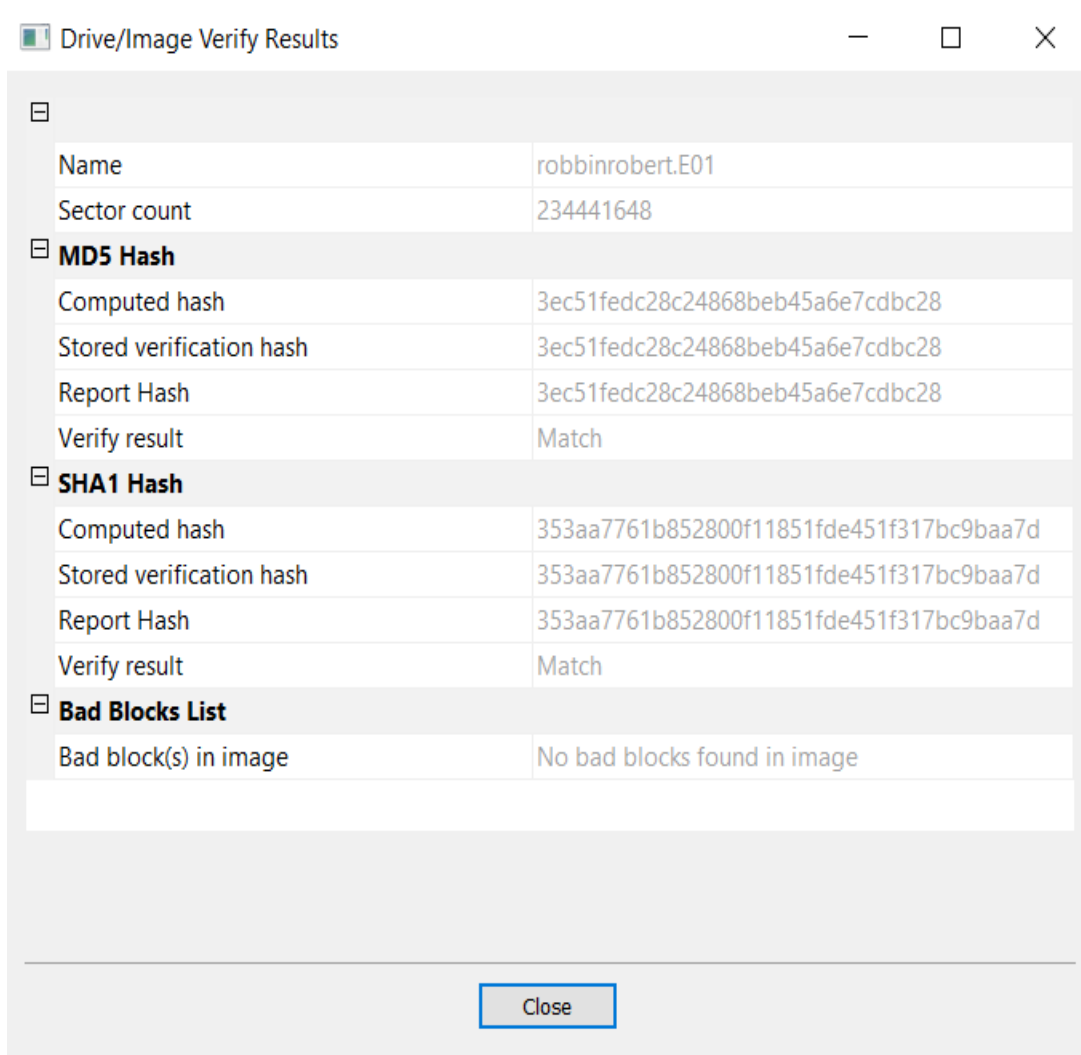
Charlotte’s booming financial infrastructure has suffered a major setback in the past week. A bank robbery took place at the Bank of America Tower in central Charlotte. The heist removed, in total, \$5,000,000 from the tower’s vaults in the form of cash money and other assets such as gold and silver. The heist took place at night on the 47th, 55th, and 60th floors of the building and it is believed to have been committed with a crew of eleven individuals. A suspect has been apprehended who goes by the nickname “Robbin’ Robert” and is believed to have setup this heist with ten other cohorts of crime (the suspect has a striking resemblance to the A-list actor George Clooney). The SATA SSD SanDisk 128GB drive found on his computer has been lawfully retrieved, imaged and sent to myself, a forensic expert, for analysis. The image file, *robbinrobert.e01*, is suspected to have information about the robbery as well as evidence to suggest that the location of the heist was to be the Bank of America tower. Information such as crew contacts, money payouts, and instructional documents are also suspected to be found on the drive.

Forensic Acquisition & Exam Preparation:

First, I created a new folder called “GraduateResearchLab” inside a folder called “ITIS5250” on my desktop and then downloaded and placed the image file and corresponding log text file in the “GraduateResearchLab” folder. The image file *robbinrobert.e01* was downloaded on Google Drive along with the text file *robbinrobert.e01.txt* which provides various information such as drive geometry and MD5 checksum of the image. My forensics environment is a Dell Inspiron 15 7000 series gaming laptop with Windows 10 operating system and 16GB of RAM.

For this lab I used AccessData FTK Imager version 4.3.0.18, Autopsy version 4.14.0, and HxD (a common hex editor) version 2.4.0.0.

After loading the image file into FTK Imager as an evidence item I found the hash value of *robbinrobert.e01* and verified the image (verification can take a few minutes as the drive imaged is 128GB). The hash value is noted below and in the following screenshot (value is also found in the properties section of FTK Imager once image file is loaded).



robbinrobert.e01 MD5 Hash Value: 3ec51fedc28c24868beb45a6e7cdb28

Findings and Report (Forensic Analysis):

- ***Are there any pictures on the drive that match the description of “Robbin’ Robert”?***
- Yes, “Robbin’ Robert” was described to have a striking resemblance to actor George Clooney. Inside a folder called “profilePics” in the root directory is a single jpg of a man who looks exactly like Georgy Clooney, titled “robbinrobert.jpg”. Screenshot:

AccessData FTK Imager 4.3.0.18

File View Mode Help

Evidence Tree

- robbinrobert.E01
 - Partition 1 [114471MB]
 - SanDisk 128GB [NTFS]
 - [orphan]
 - [root]
 - \$BadClus
 - \$Extend
 - \$RECYCLE.BIN
 - \$Secure
 - \$UpCase
 - Contacts
 - DefinitelyNothingHere
 - Documents
 - Favorites
 - Games
 - MasterPlan.zip
 - Pictures
 - profilePics
 - robbinrobert.jpg
 - System Volume Information
 - [unallocated space]


File List

Name	Size	Type	Date Modified
Zone.Identifier	1	Alternate D...	4/26/2020 6:32:07 ...

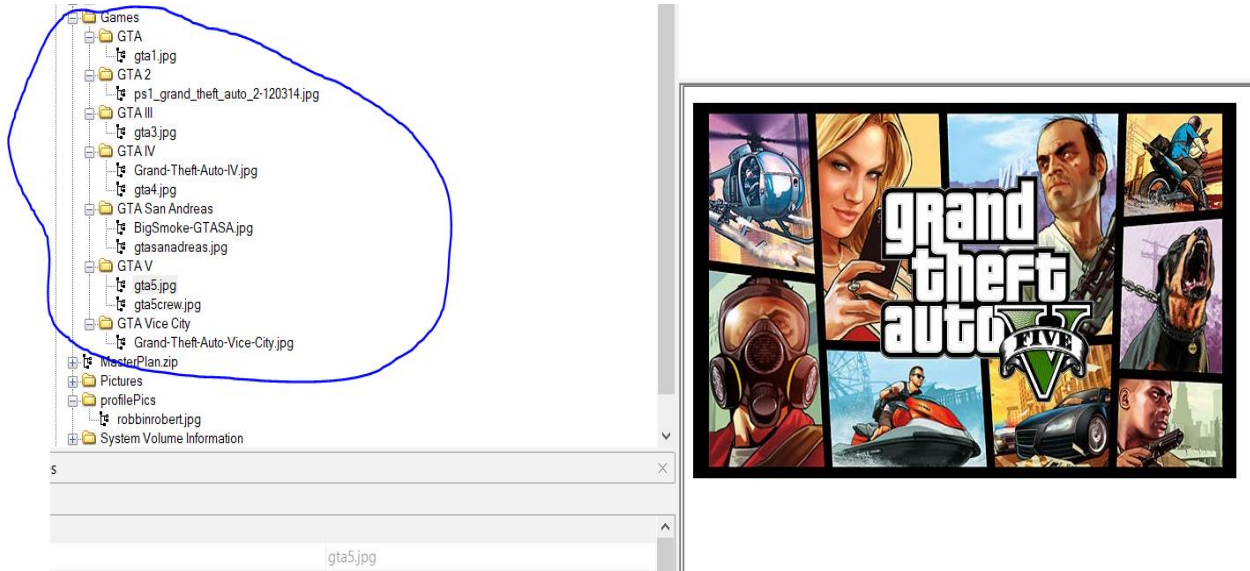
Properties

Name	robbinrobert.jpg
File Class	Regular file
File Size	174,350
Physical Size	176,128
Start Cluster	7,568
Date Accessed	4/26/2020 6:32:07 AM
Date Created	4/26/2020 6:31:57 AM
Date Modified	4/26/2020 6:32:07 AM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	62,592
Alternate Data Stream Count	1
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	True

Properties | Hex Value Interpreter | Custom Content Sources



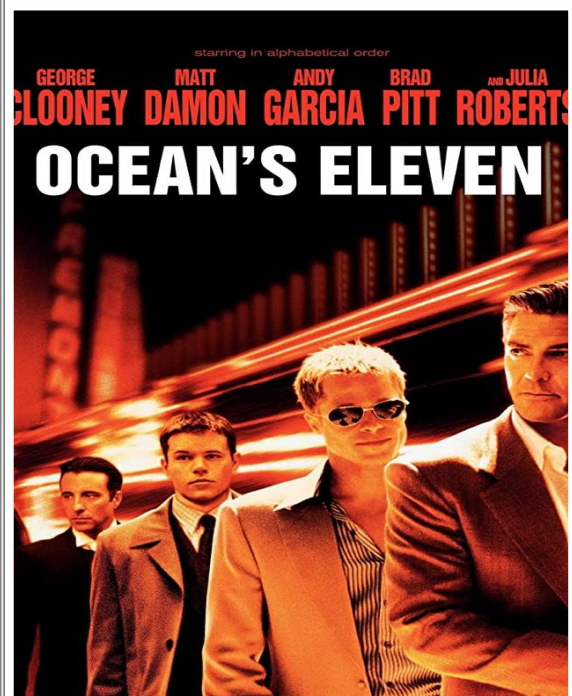
- **Are there any items on the drive that might allude to heists in general, or any media that involves plans to perform one?**
 - **Media in terms of video games?**
- Yes, inside the “Games” folder in the root directory lies folders for the games of the “Grand Theft Auto” series by Rockstar. “Grand Theft Auto V” in particular heavily features heist content. Screenshot:



- **Media in terms of film?**
- Yes, inside the “Pictures” folder in the root directory lies jpgs for the films of the “Ocean’s” series. Screenshots:

Properties window for file **firstheist.jpg**:

Name	firstheist.jpg
File Class	Regular File
File Size	129,313
Physical Size	131,072
Start Cluster	6,760
Date Accessed	4/25/2020 7:58:13 PM
Date Created	4/25/2020 7:58:13 PM
Date Modified	4/25/2020 6:47:26 PM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	56,128
Alternate Data Stream Count	1
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	True



File Explorer view showing the **Pictures** folder contents:

- bank.jpg
- bank2.jpg
- bankstadium.jpg
- banksy.jpg
- chasebank.jpg
- cltbac.jpg
- cltbank.jpg
- firstheist.jpg
- firstheistcrew.jpg
- idealcrew.jpg
- secondheist.jpg
- secondheistcrew.jpg
- somebank.jpg
- thirdheist.jpg
- thirdheistcrew.jpg
- thirdheistidea.jpg
- profilePics



Properties

Properties window for file **firstheist.jpg**:

Name	firstheist.jpg
File Class	Regular File
File Size	129,313
Physical Size	131,072
Start Cluster	6,760
Date Accessed	4/25/2020 7:58:13 PM
Date Created	4/25/2020 7:58:13 PM
Date Modified	4/25/2020 6:47:26 PM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	56,128
Alternate Data Stream Count	1
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	True



○ **Media in terms of documents (web, word, etc..)?**

- Yes, inside the “Favorites” folder in the root directory lies a folder for links to a website which is a “how to” on robbing a bank, titled “How to Rob a Bank in Godfather Blackhand Edition (with Pictures)_files”. Screenshot:

AccessData FTK Imager 4.3.0.18

File View Mode Help

Evidence Tree

robbinrobert.E01

Partition 1 [114471MB]

SanDisk 128GB [NTFS]

[orphan]

[root]

\$BadClus

\$Extend

\$RECYCLE.BIN

\$Secure

\$UpCase

Contacts

DefinitelyNothingInHere

Documents

Favorites

Links

How to Rob a Bank in Godfather Blackhand Edition (with Pictures)_files

Games

MasterPlan.zip

Pictures

bank.jpg

bank2.jpg

bankstadium.jpg

banksy.jpg

chasebank.jpg

citbac.jpg

citbank.jpg

firstheist.jpg

firstheistcrew.jpg

idealcrew.jpg

secondheist.jpg

secondheistcrew.jpg

somebank.jpg

thirdheist.jpg

thirdheistcrew.jpg

File List

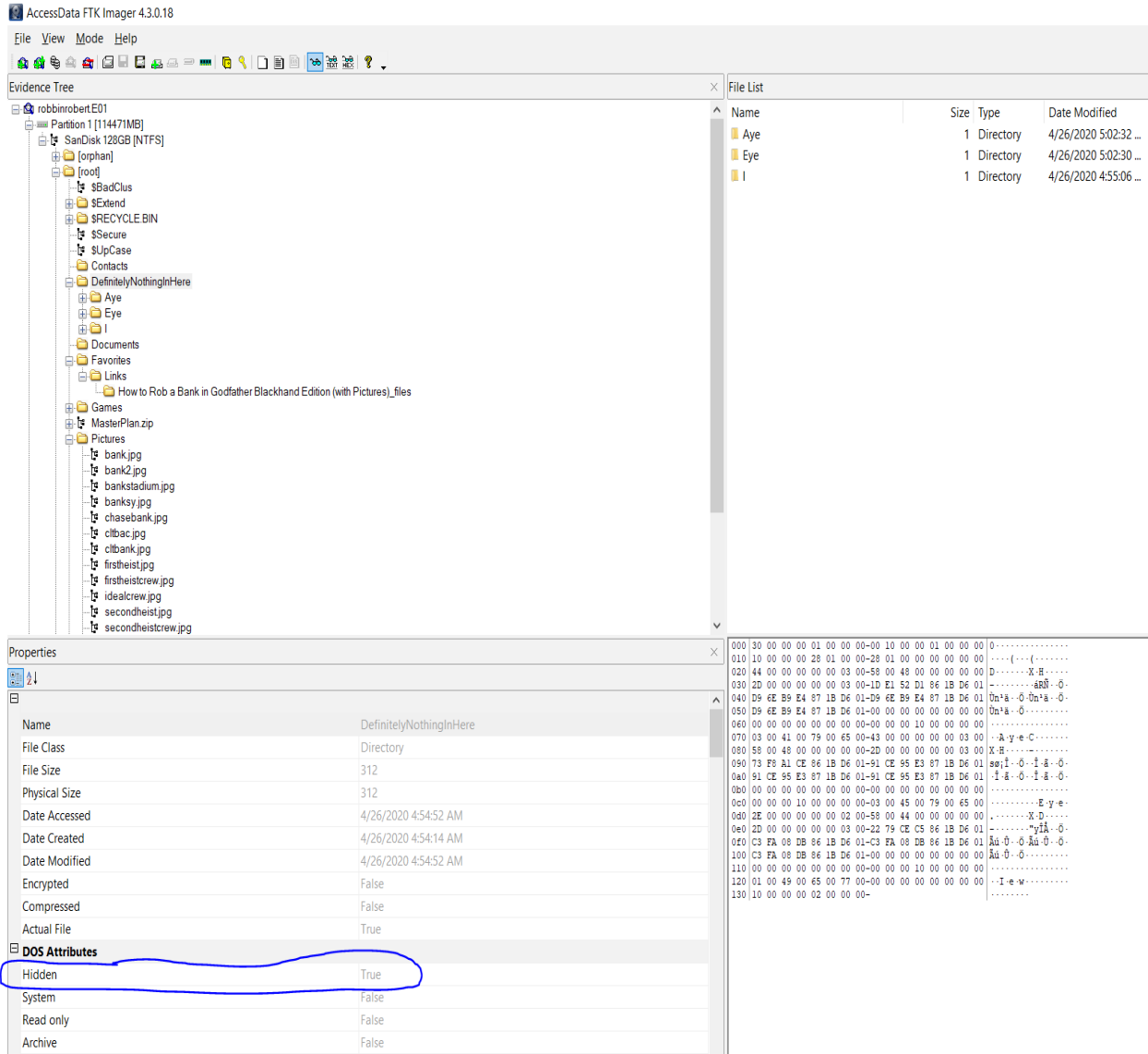
Name	Size	Type	Date Modified
\$I30	20	NTFS Index ...	4/26/2020 4:52:24 ...
-crop-127-140-127px-20181008...	4	Regular File	4/26/2020 4:52:23 ...
-crop-127-140-127px-Beat-Fung...	4	Regular File	4/26/2020 4:52:23 ...
-crop-127-140-127px-Get-Easy...	3	Regular File	4/26/2020 4:52:23 ...
-crop-127-140-127px-Play-Fortn...	4	Regular File	4/26/2020 4:52:23 ...
-crop-342-184-245px-Be-a-Goo...	9	Regular File	4/26/2020 4:52:23 ...
-crop-342-184-245px-Beat-Fung...	9	Regular File	4/26/2020 4:52:22 ...
-crop-342-184-245px-Edit-Build...	10	Regular File	4/26/2020 4:52:22 ...
-crop-342-184-245px-Get-Easy...	7	Regular File	4/26/2020 4:52:22 ...
-crop-342-184-245px-Get-Fortni...	9	Regular File	4/26/2020 4:52:23 ...
-crop-342-184-245px-Jump-in-...	6	Regular File	4/26/2020 4:52:23 ...
-crop-342-184-245px-Play-Fortn...	10	Regular File	4/26/2020 4:52:22 ...
-crop-342-184-245px-Play-Tetris...	7	Regular File	4/26/2020 4:52:23 ...
-crop-342-184-246px-Add-a-PS...	13	Regular File	4/26/2020 4:52:23 ...
-crop-342-184-246px-Romance...	5	Regular File	4/26/2020 4:52:23 ...
-crop-342-184-253px-5222471...	8	Regular File	4/26/2020 4:52:22 ...
-crop-342-184-295px-Screensho...	27	Regular File	4/26/2020 4:52:23 ...
-crop-342-184-327px-Dbd5_wiki...	8	Regular File	4/26/2020 4:52:23 ...
-crop-342-184-328px-20181008...	14	Regular File	4/26/2020 4:52:22 ...
184011-188477170437417.js.do...	91	Regular File	4/26/2020 4:52:21 ...
aid491128-v4-728px-Rob-a-Ban...	42	Regular File	4/26/2020 4:52:21 ...
aid491128-v4-728px-Rob-a-Ban...	3	File Slack	
aid491128-v4-728px-Rob-a-Ban...	28	Regular File	4/26/2020 4:52:21 ...
aid491128-v4-728px-Rob-a-Ban...	1	File Slack	

Properties

How to Rob a Bank in Godfather Blackhand Edition (with Pictures)_files

Name	How to Rob a Bank in Godfather Blackhand Edition (with Pictures)_files
File Class	Directory
File Size	56
Physical Size	56
Date Accessed	4/26/2020 4:52:24 AM
Date Created	4/26/2020 4:52:23 AM
Date Modified	4/26/2020 4:52:24 AM
Encrypted	False
Compressed	False
Actual File	True
Alternate Data Stream Count	1
DOS Attributes	
Hidden	False
System	False
Read only	False
Archive	False
NTFS Information	
MFT Record Number	98 (100352)

- **Are there any hidden files/folders on the drive? If so, what are they?**
- Yes. There are two folders on the drive which are hidden, “DefinitelyNothingInHere” and “MasterPlan.zip”. The latter is an encrypted zip folder with password-protected files within. Screenshots:



AccessData FTK Imager 4.3.0.18

File View Mode Help

Evidence Tree

robbinrobert.E01
Partition 1 [114471MB]
SanDisk 128GB [NTFS]
[orphan]
[root]
\$BadClus
\$Extend
\$RECYCLE.BIN
\$Secure
\$UpCase
Contacts
DefinitelyNothingInHere
Aye
Eye
I
Documents
Favorites
Links
How To Rob a Bank in Godfather Blackhand Edition (with Pictures).files
Games
MasterPlan.zip
MasterPlan
LocationOffHeist
Pictures
bank.jpg
bank2.jpg
bankstadium.jpg
banksy.jpg
chasebank.jpg
cllbac.jpg
cllbak.jpg
firstheist.jpg
firstheistcrew.jpg
idealcrew.jpg

File List

Name	Size	Type	Date Modified
LocationOffHeist	0	Directory	4/26/2020 7:33:26 ..
\$\$\$password\$\$\$txt	1	Regular File	4/26/2020 7:14:38 ..
heistfinances.xlsx	17	Regular File	4/26/2020 7:02:20 ..
How To Rob A Bank.pdf	386	Regular File	4/25/2020 2:42:50 ..
instructions.txt	1	Regular File	4/25/2020 2:54:18 ..

Properties

\$\$\$password\$\$\$txt

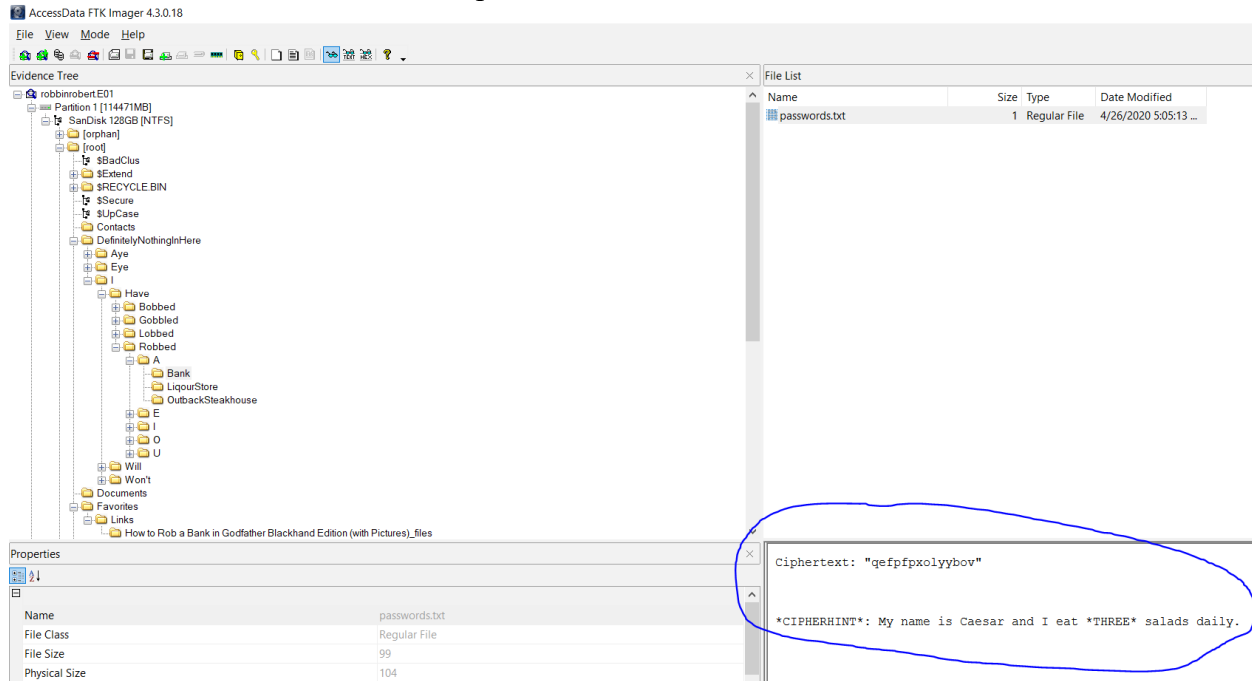
Name	\$\$\$password\$\$\$txt
File Class	Regular File
File Size	441
Compressed Size	146
Date Modified	4/26/2020 7:14:38 PM
Encrypted	True
Compressed	True

Zip Properties

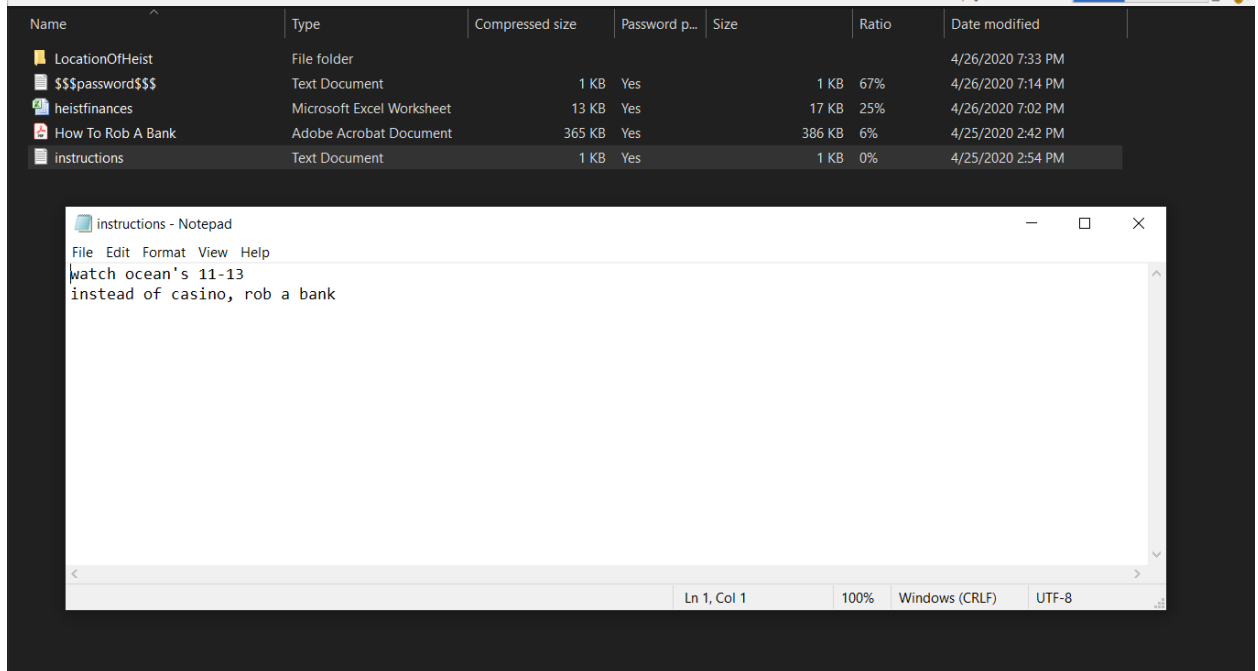
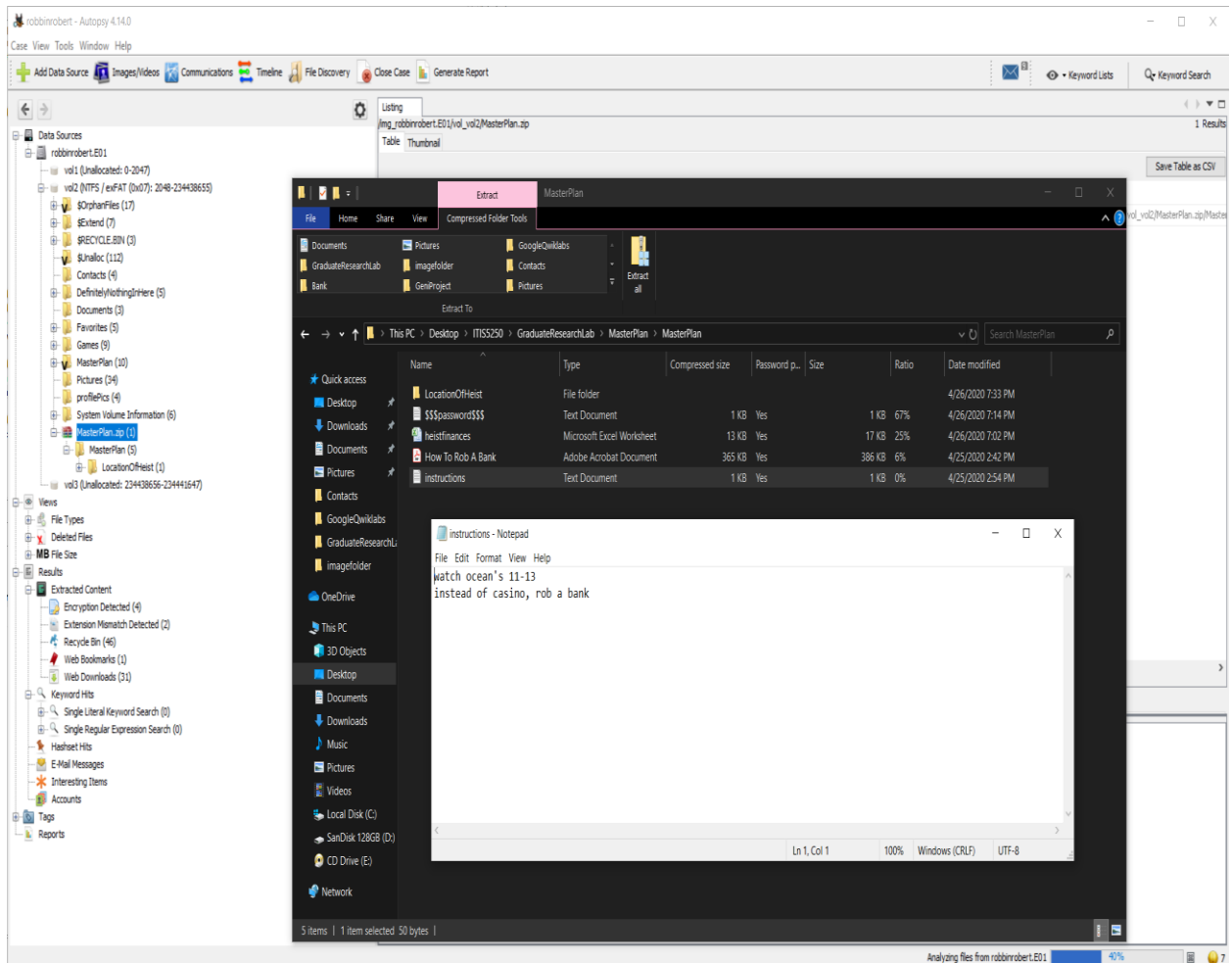
Checksum	9BDA46A3
Extract Version	2.0
Compression Method	Deflated

*TF±ûó?79N``š3==š0C0
P[-@'NS,E0†e]6Æe~ã ?ydÂû, ;c1ø^"ò'× ¼.=6'ò~'QNôò;3^û

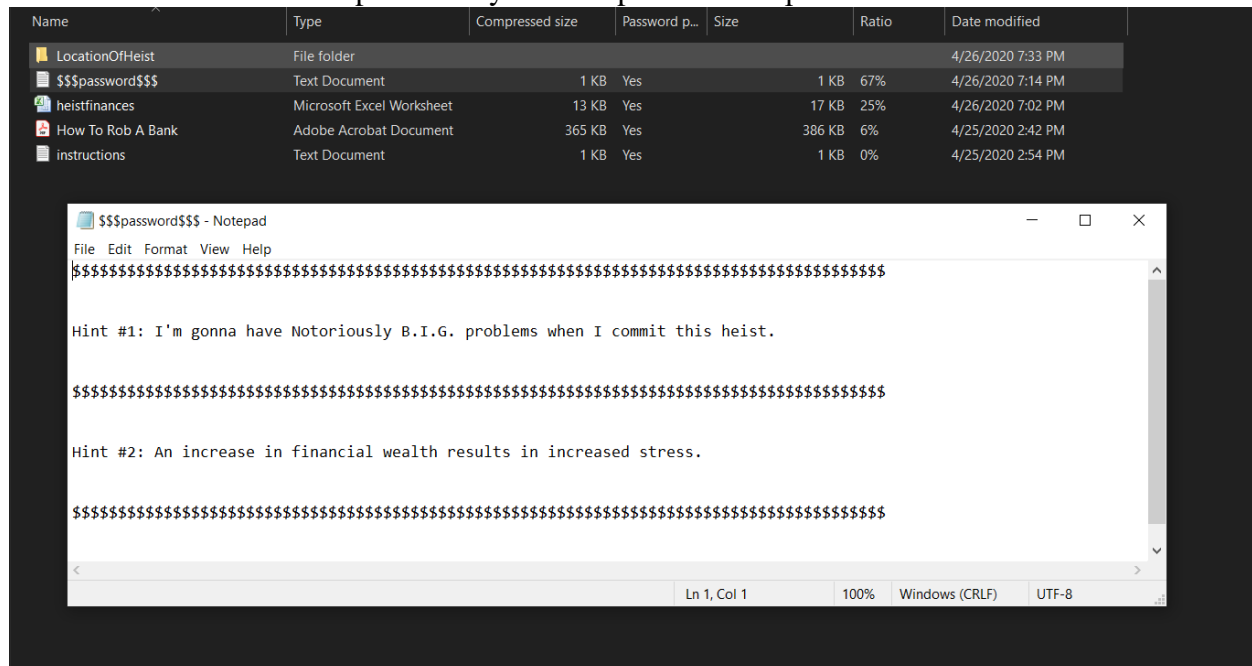
- **Can you gain access to the encrypted hidden folder, perhaps with information from the other hidden folder?**
- Yes. Although the files in the folder “MasterPlan.zip” are encrypted with passwords, the other folder, “DefinitelyNothingInHere” is unencrypted. Navigating “DefinitelyNothingInHere” through the folders “I > Have > Robbed > A > Bank” leads to a text file titled “password.txt”. Screenshot:



- Which contains a cipher-text, "qefpfpxolyb", and a hint. The hint reveals the use of a simple Caesar cipher, with an offset of three. Deciphering the cipher-text with this information leads to the text “thisisarobbery”. After exporting the MasterPlan.zip folder using Autopsy, I entered the password and unlocked the files in the MasterPlan folder. Screenshots:



- ***A heist of \$5,000,000 doesn't happen without financial planning. Can you find a document related to the finances of the heist? Can it be accessed?***
- Yes, once I gained access to the files in the “MasterPlan” folder, I could see an Excel Spreadsheet titled “heistfinances.xlsx”. The spreadsheet, however, was password-protected. Another file in the “MasterPlan” folder titled “\$\$\$password\$\$\$.txt” contained hints presumably for the spreadsheet’s password. Screenshot:



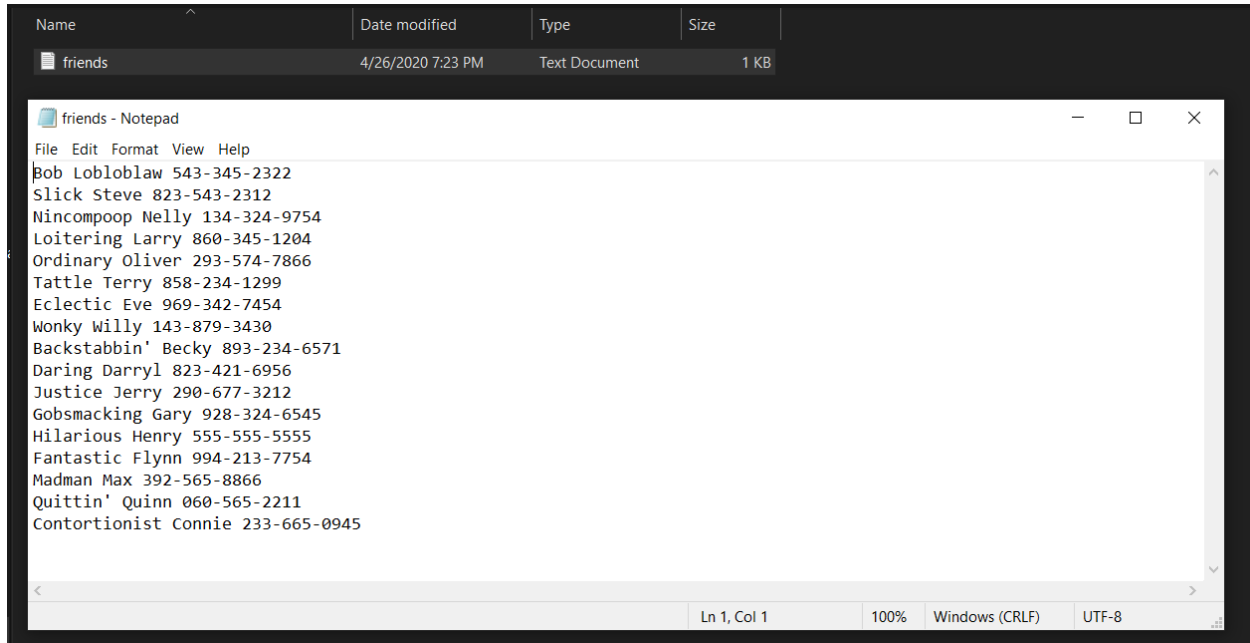
- The password was determined to be “momoneymoproblems” and leads to all the finances of a “Bank of America” heist noted in the spreadsheet. Screenshot of spreadsheet:

heistfinances [Read-Only] - Microsoft Excel

	A	B	C	D	E	F	G	H	I	J
1	Bank of America Heist									
2										
3										
4	Expenditures:	<u>Item</u>	<u>Cost</u>		Payout:	<u>Crew Member</u>	<u>Bank Account #</u>	<u>\$Payout</u>		
5		Guns	\$5,000			Bob Loblaw	5011769150	\$200,000		
6		Ammunition	\$2,000			Slick Steve	5037899478	\$200,000		
7		Vehicles	\$10,000			Loitering Larry	4509331471	\$200,000		
8		Police payoffs	\$100,000			Tattle Terry	2997389363	\$200,000		
9		Surveillance Equipment	\$30,000			Backstabbin' Becky	9298971593	\$200,000		
10		Total Expense	\$147,000			Daring Darryl	1722323851	\$200,000		
11						Gobsmacking Gary	4736758851	\$200,000		
12						Hilarious Henry	2251875495	\$200,000		
13						Madman Max	9546695609	\$200,000		
14						Contortionist Connie	3576872794	\$200,000		
15	Gains:	<u>Item</u>	<u>\$Gain</u>				Total Payout		\$2,000,000	
16		Cash	\$3,000,000							
17		Gold	\$1,500,000							
18		Silver	\$500,000							
19		Total Gain	\$5,000,000							
20						MORE FOR ME: \$\$\$				
21							\$5,000,000			
22							(\$2,000,000)			
23							(\$147,000)			
24						Total \$\$\$ for ME!!!	\$2,853,000			
25										

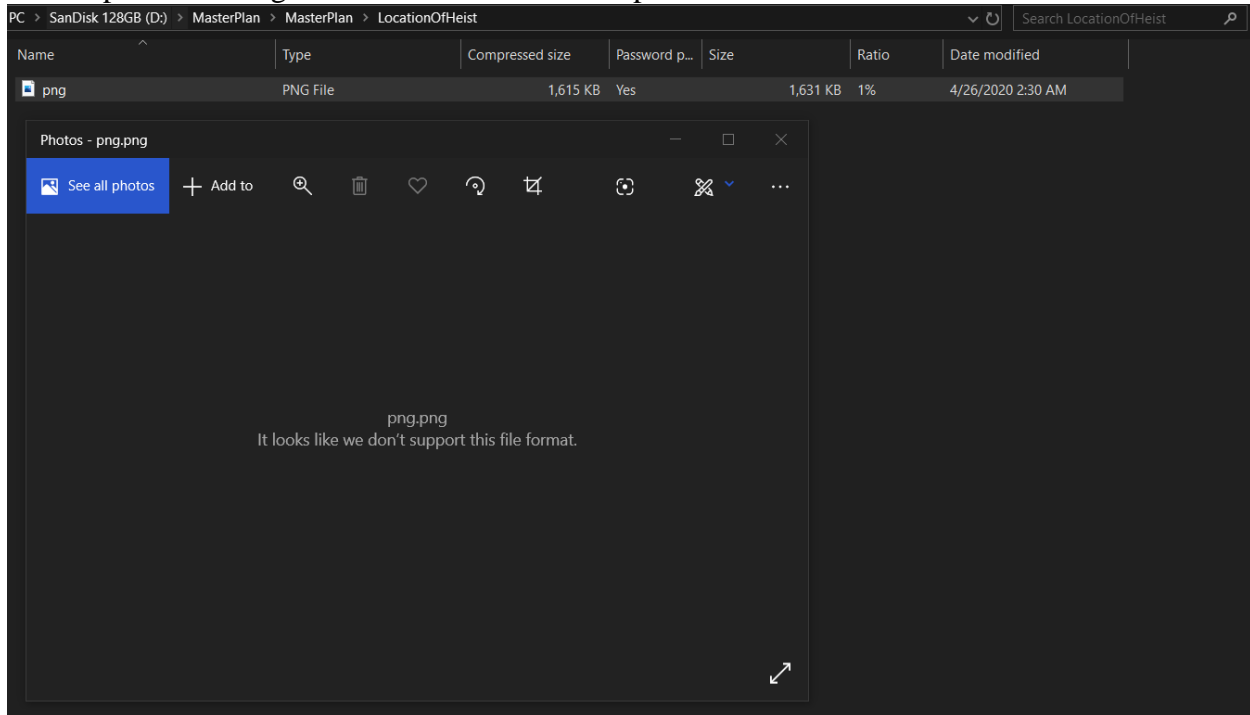
- **Can you identify the expenditures of the heist?**
- Dollar values for heist expenditures: \$5,000 on guns, \$2,000 on ammunition, \$10,000 on vehicles, \$100,000 on police payoffs, and \$30,000 on surveillance equipment.
- **Can you identify the payouts to the crew members?**
- Dollar value of payouts: \$200,000 to each of 10 crew members to their corresponding bank accounts (bank account #'s provided in spreadsheet).
- **Can you identify the financial gain of the materials from the heist, and the financial gain for the last crew member after expenditures?**
- Total financial gains from heist is \$5,000,000: \$3,000,000 in cash, \$1,500,000 in gold, \$500,000 in silver. Financial gain for last crew member after expenditures: \$2,853,000.

- **Can you now retrieve any possible names and contact information of the heist crew?**
- Yes, in a folder titled “Contacts” in the root directory sits a single text file titled “friends.txt”. Inside are names and numbers of different people, 10 of which have names which correspond to those in the “heistfinances.xlsx” spreadsheet. Screenshot of “friends.txt”:

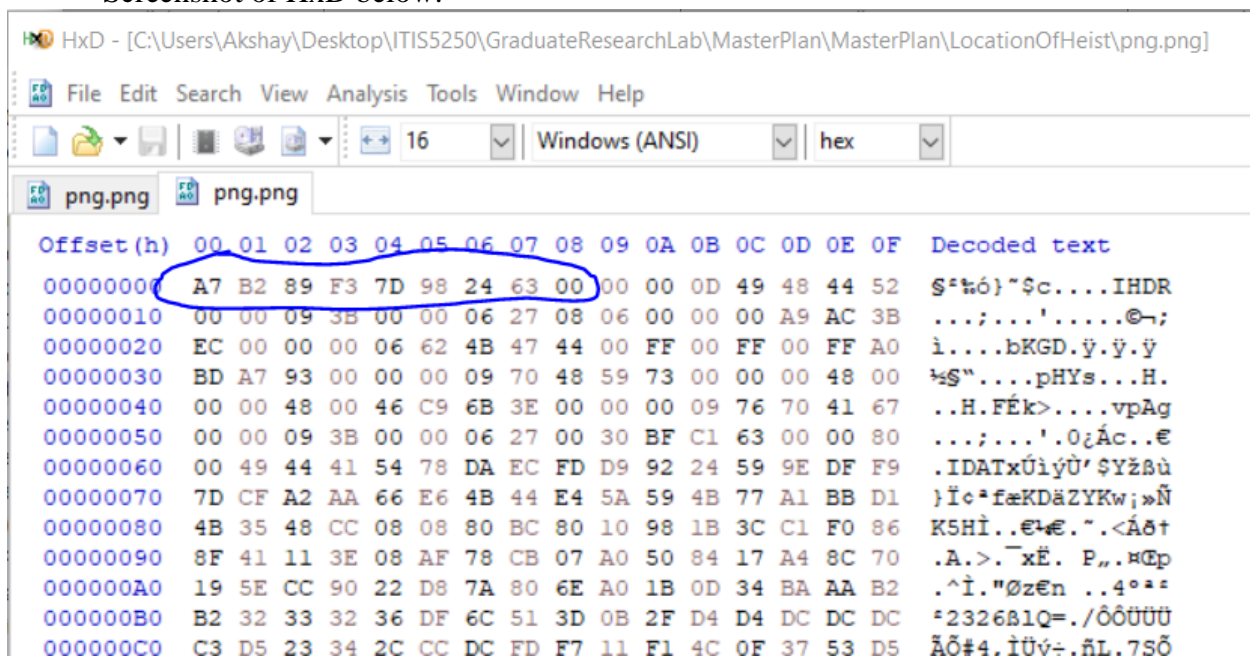


- 10 cross-referenced names between text file and spreadsheet (name & phone number from “friends.txt”):
 - Bob Loblaw 543-345-2322
 - Slick Steve 823-543-2312
 - Loitering Larry 860-345-1204
 - Tattle Terry 858-234-1299
 - Backstabbin' Becky 893-234-6571
 - Daring Darryl 823-421-6956
 - Gobsmacking Gary 928-324-6545
 - Hilarious Henry 555-555-5555
 - Madman Max 392-565-8866
 - Contortionist Connie 233-665-0945

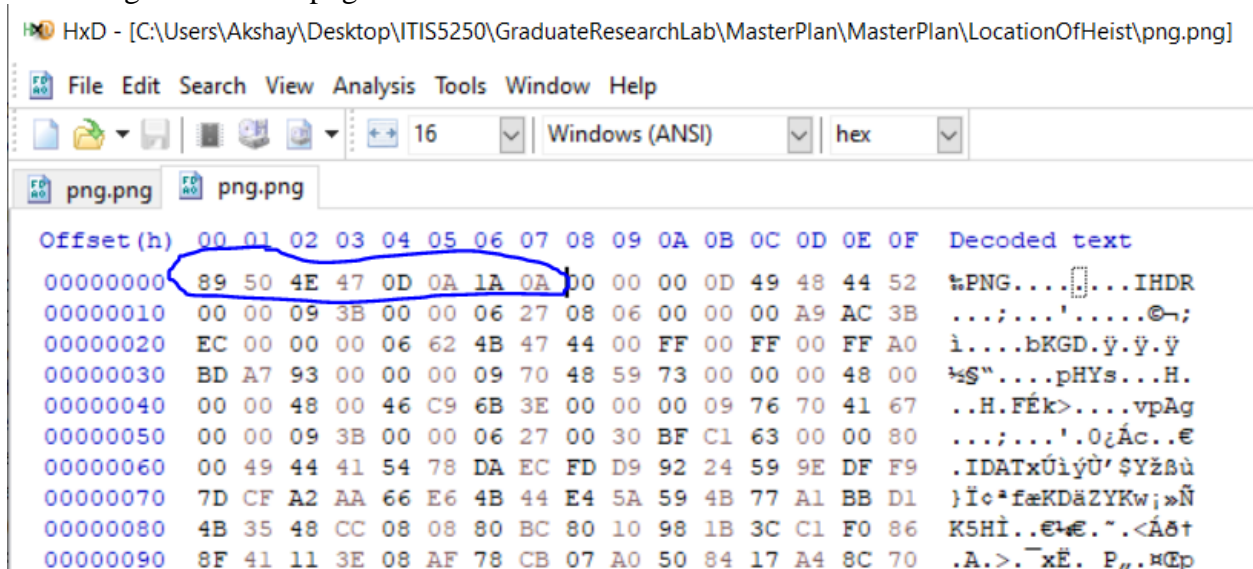
- **Can you find any evidence that the heist was planned to take place at the Bank of America tower on the 47th, 55th, and 60th floors?**
- Yes, inside the “MasterPlan” folder is another folder titled “LocationOfHeist”. Inside of that, there is a single png file titled “png.png” which is unable to be opened by Windows 10 Photos due to file format. However, png file formats are easily opened by regular photo viewing software. This file is corrupt. Screenshot:



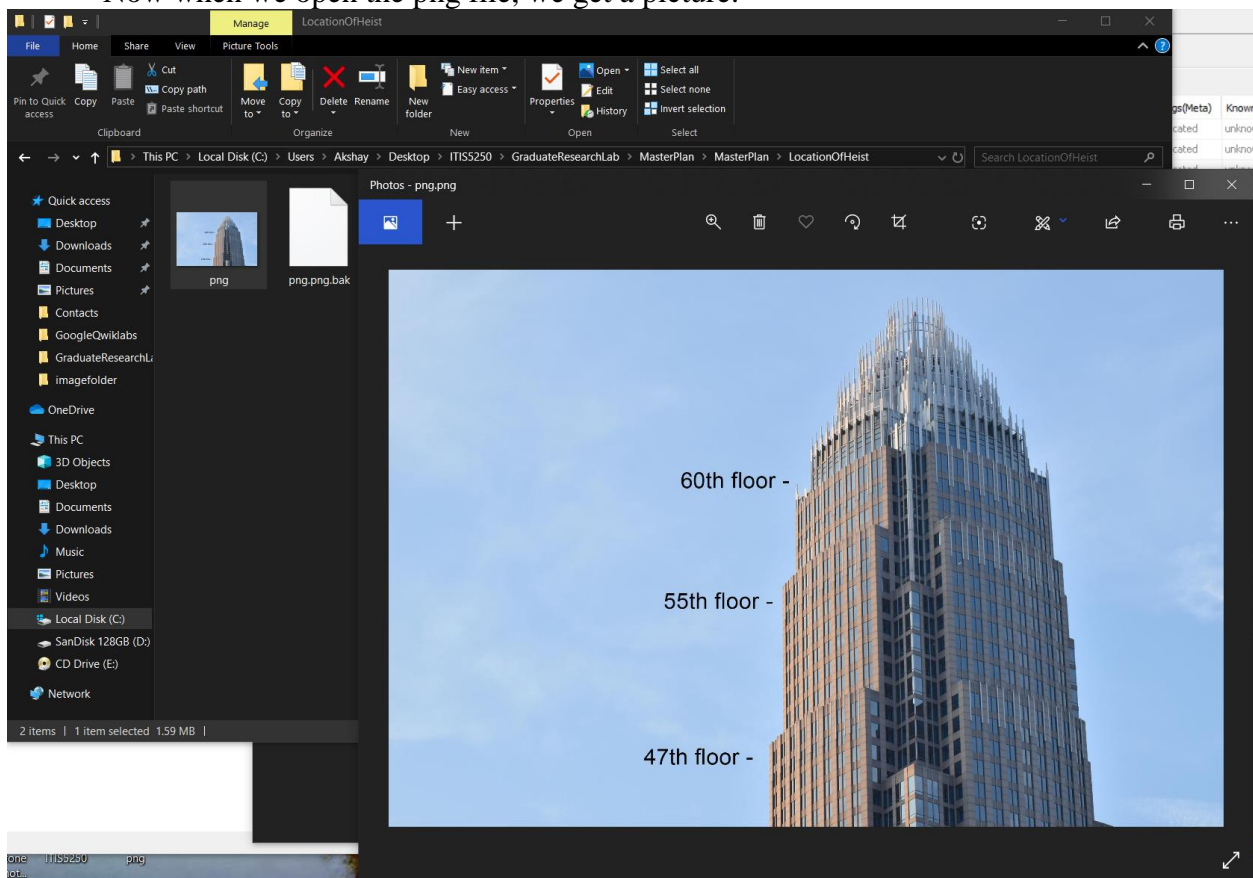
- We can look at the hex content of the file using FTK Imager or a hex editor like HxD. Screenshot of HxD below:



- The opening file signature for a png file is “89 50 4E 47 0D 0A 1A 0A”. Fixing the file signature of the png file results in HxD screenshot:



- Now when we open the png file, we get a picture:



- Which features the Charlotte Bank of America building, with text showing the 47th, 55th, and 60th floors.

Conclusion:

Screenshot of verification provided below. Shows initial verification and final verification.

```
robbinrobert.E01 - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 4.3.0.18

Case Information:
Acquired using: ADI4.3.0.18
Case Number: 1
Evidence Number: 1
Unique description: Robbin Robert's SATA SSD (128GB)
Examiner: Akshay Desai
Notes: contains possible important information on charlotte bank of america robbery
-----

Information for C:\Users\Akshay\Desktop\ITIS5250\GraduateResearchLab\imagefolder\robb

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 14,593
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 234,441,648
[Physical Drive Information]
Drive Model: SanDisk SDSSDX120GG25
Drive Serial Number: 124279400953
Drive Interface Type: IDE
Removable drive: False
Source data size: 114473 MB
Sector count: 234441648
[Computed Hashes]
MD5 checksum: 3ec51fedc28c24868beb45a6e7cdabc28
SHA1 checksum: 353aa7761b852800f11851fde451f317bc9baa7d

Image Information:
Acquisition started: Sun Apr 26 21:18:49 2020
Acquisition finished: Sun Apr 26 21:25:25 2020
Segment list:
C:\Users\Akshay\Desktop\ITIS5250\GraduateResearchLab\imagefolder\robbinrobert.E01

Image Verification Results:
Verification started: Sun Apr 26 21:25:25 2020
Verification finished: Sun Apr 26 21:30:36 2020
MD5 checksum: 3ec51fedc28c24868beb45a6e7cdabc28 : verified
SHA1 checksum: 353aa7761b852800f11851fde451f317bc9baa7d : verified

Image Verification Results:
Verification started: Sun Apr 26 22:05:06 2020
Verification finished: Sun Apr 26 22:10:13 2020
MD5 checksum: 3ec51fedc28c24868beb45a6e7cdabc28 : verified
SHA1 checksum: 353aa7761b852800f11851fde451f317bc9baa7d : verified
```

(robbinrobert.e01 log file), MD5 checksum: 3ec51fedc28c24868beb45a6e7cdabc2

The image file *robbinrobert.e01* contains a picture matching the description provided of “Robbin’ Robert. There are plenty of items, of or relating to, planning heists and/or executing them. Of these items found were game of the “Grand Theft Auto” series, images from the “Ocean’s” heist films, and documents relating to instructions on completing heists. Further inspection of the drive revealed two hidden files, “DefinitelyNothingInHere” and an encrypted zip file “MasterPlan.zip”, the latter of which contained files encrypted with a password. By deciphering a cipher-text (using a Caesar cipher with an offset of three) gathered from a text file deep in the other hidden folder, “DefinitelyNothingInHere”, the password was determined to be “thisisarobbery”.

Inside the “MasterPlan” were many items relating the planning/execution of a heist. The files were “\$\$\$password\$\$\$.txt”, “heistfinances.xlsx”, “How to Rob a Bank.pdf”, “instructions.txt”, and a folder titled “LocationOfHeist”. The file “\$\$\$passwords\$\$\$.txt” contained information on the password to unlock the spreadsheet “heistfinances.xlsx”, and that password was found to be “momoneymoproblems”. The spreadsheet “heistfinances.xlsx” revealed a slew of information of the financials of a “Bank of America” heist. Inside were dollar values of expenditures (total \$147,000), gains (total \$5,000,000 in cash, gold and silver), and payouts to 10 crew members (of \$200,000 each), along with a value titled “MORE FOR ME \$\$\$” (\$2,853,000 to the last member of the crew). Cross-referencing the list of crew members in the spreadsheet with the list of people found in the “friends.txt” file in the “Contacts” folder of the root directory led to the name and number of ten possible crew members.

Finally, within the “LocationOfHeist” folder was a single corrupted png file titled “png.png”. After manipulating the hex of the file signature to be that of a png file, the picture was opened which featured the Charlotte Bank of America tower with the floors 47, 55, and 60 marked on the tower.