ITIS 5250

Akshay Desai

Graduate Lab Forensics Report (“The Case of Robbin’ Robert”)

04/25/2020

**Overview:**

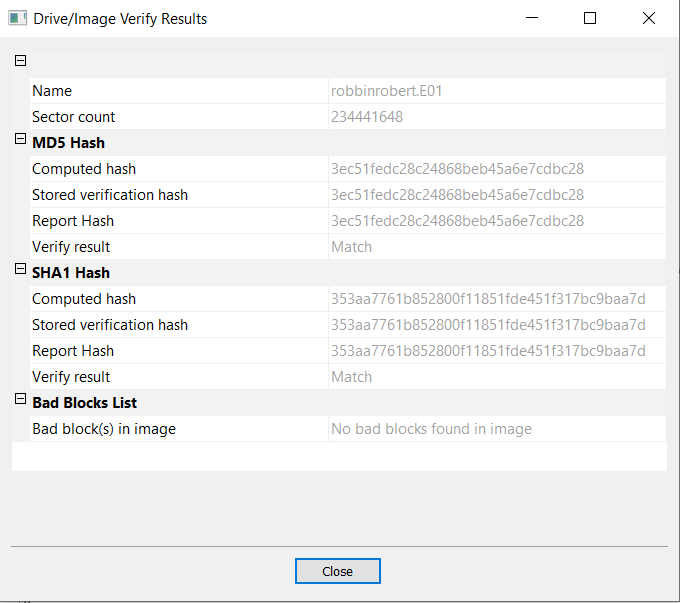
Charlotte’s booming financial infrastructure has suffered a major setback in the past week. A bank robbery took place at the Bank of America Tower in central Charlotte. The heist removed, in totality, $5,000,000 from the tower’s vaults in the form of cash money and other assets such as gold and silver. 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.

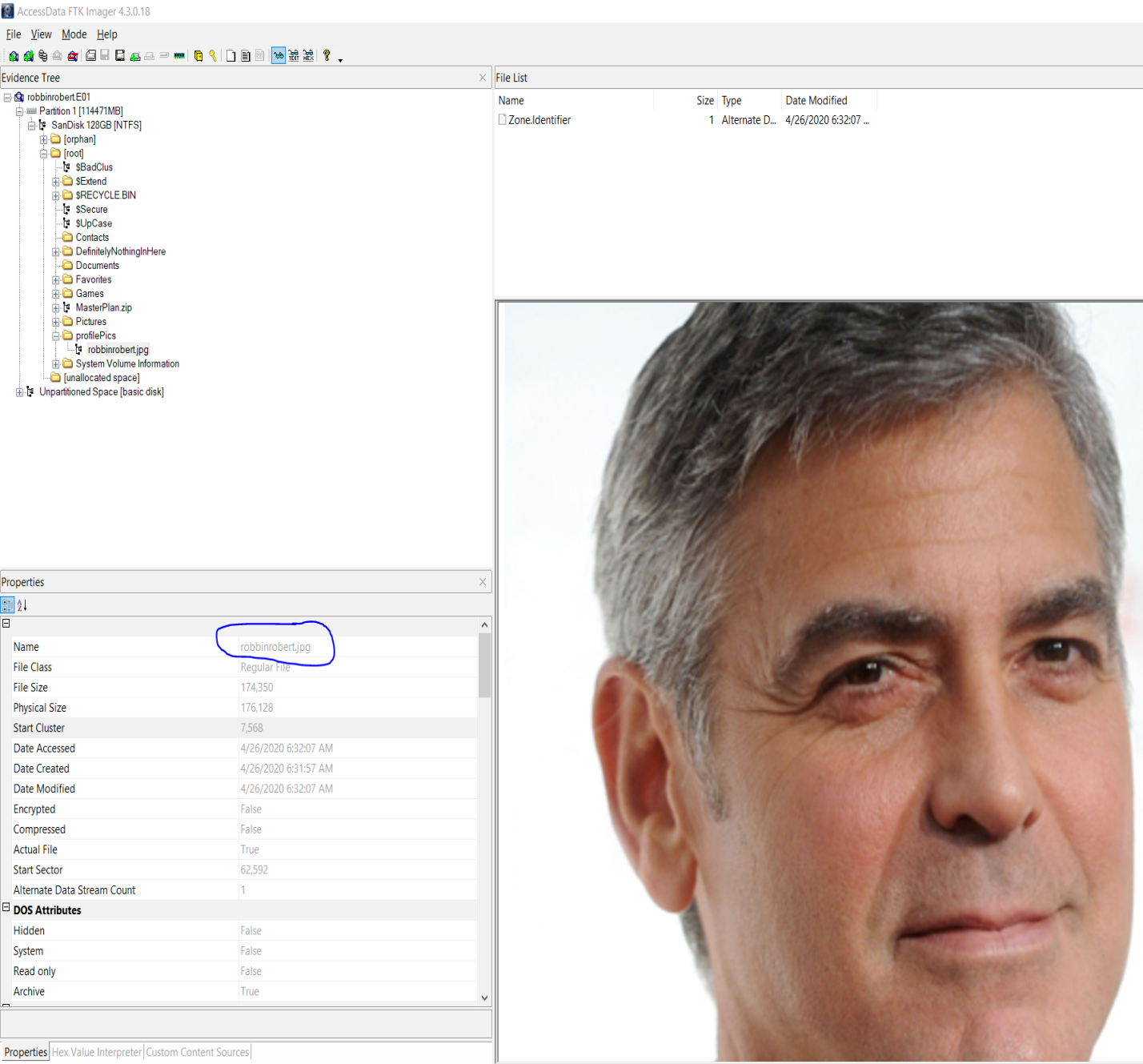
After loading the image file into FTK Imager as an evidence item I found the hash value of *robbinrobert.e01* and verified the image (verification can take a few minutes as the drive imaged is 128GB). The hash value is noted below and in the following screenshot (value is also found in the properties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



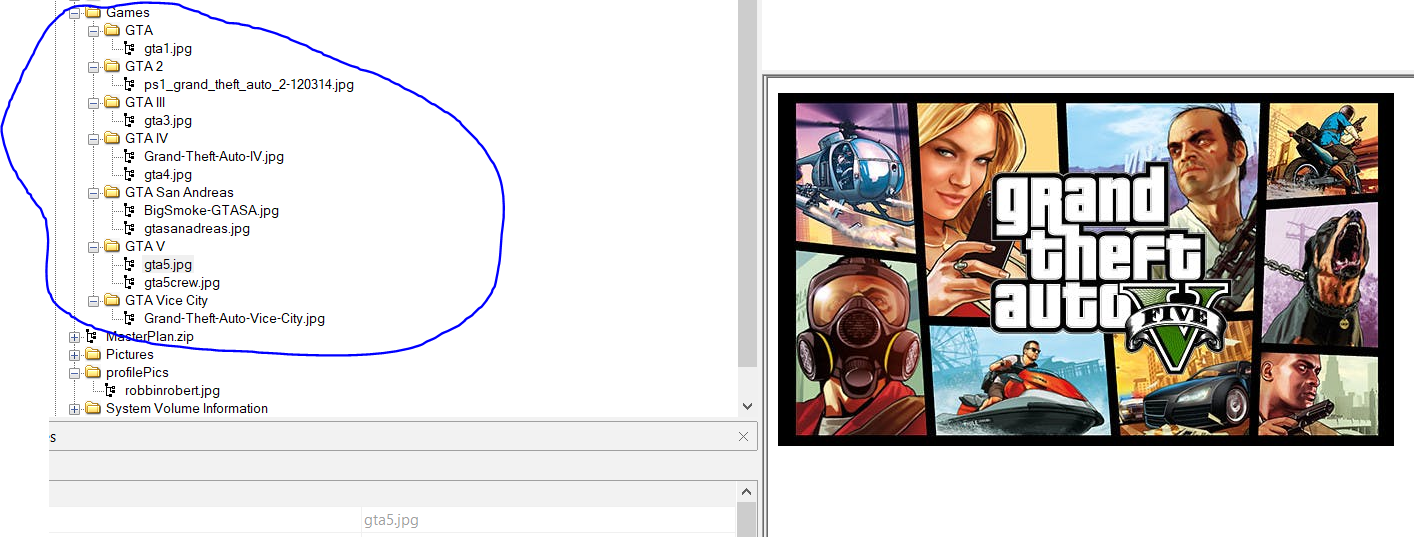
*robbinrobert.e01* MD5 Hash Value: 3ec51fedc28c24868beb45a6e7cdbc28

**Findings and Report (Forensic Analysis):**

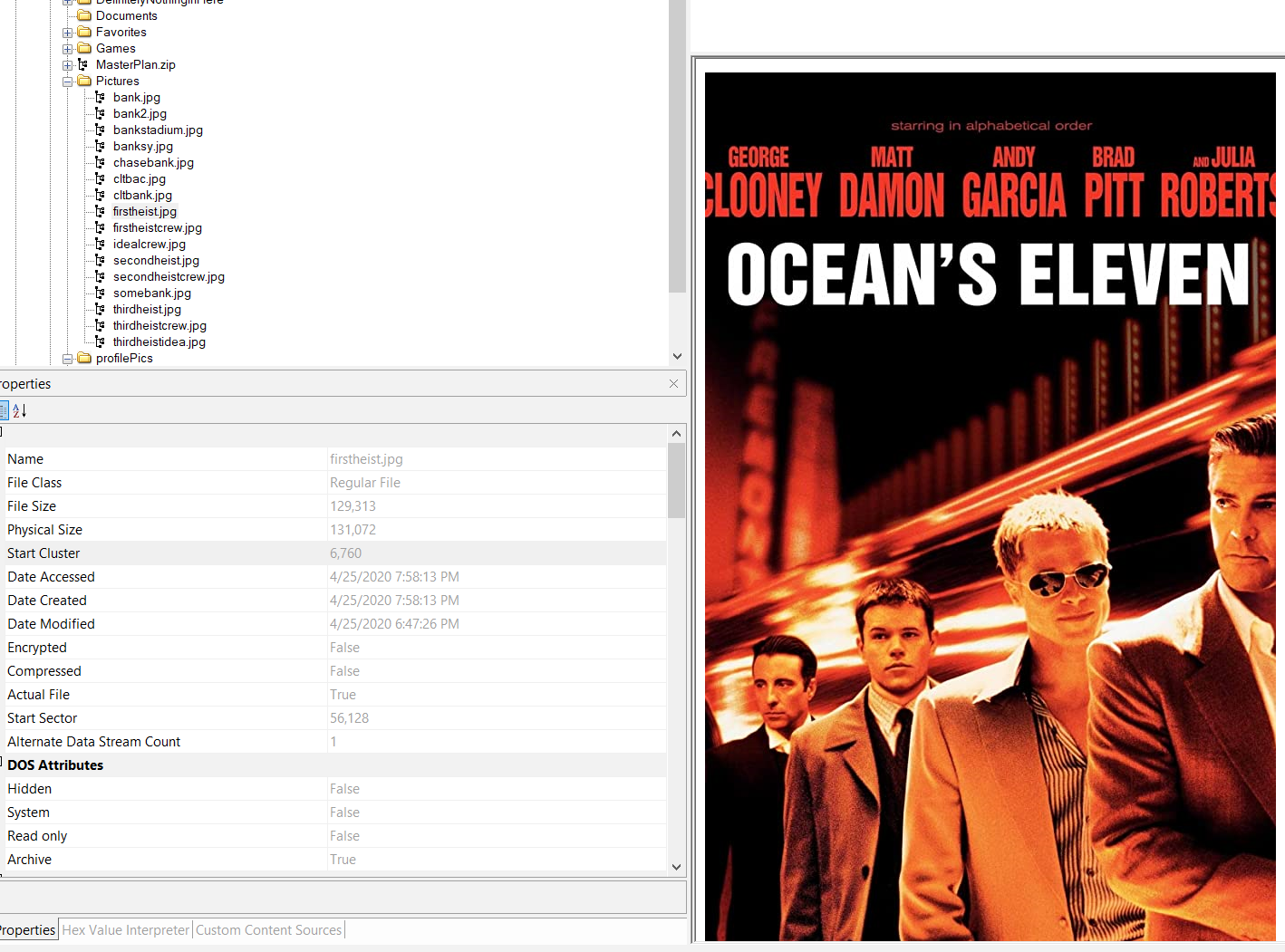
* ***Are there any pictures on the drive that match the description of “Robbin’ Robert”?***
* Yes, “Robbin’ Robert” was described to have a striking resemblance to actor George Clooney. Inside a folder called “profilePics” in the root directory is a single jpg of a man who looks exactly like Georgy Clooney,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

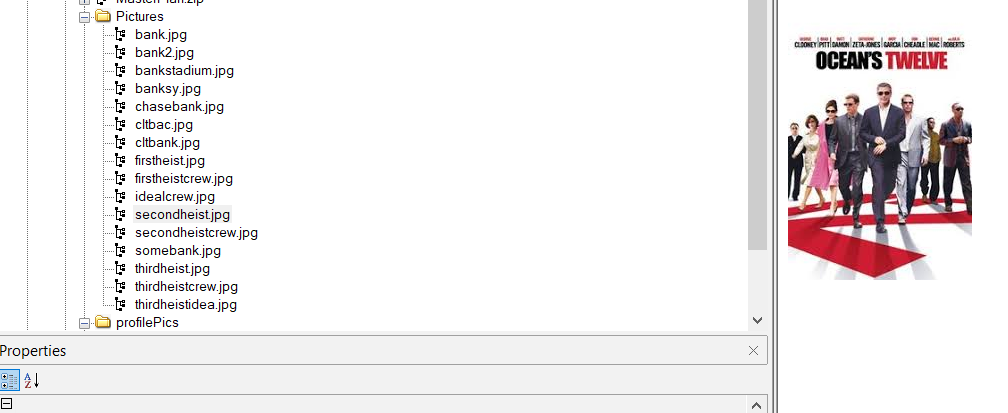


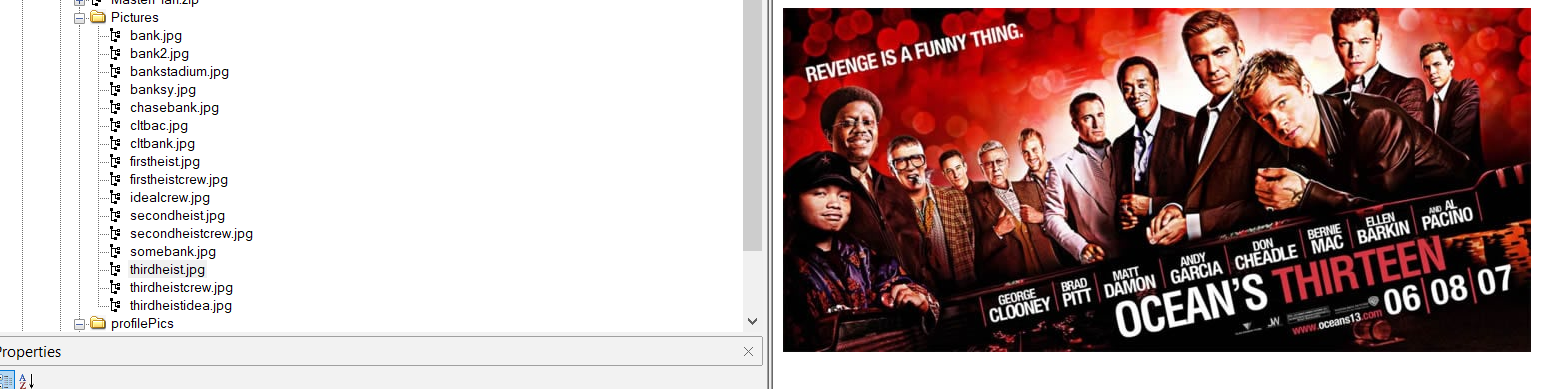
* ***Are there any items on the drive that might allude to heists in general, or any media that involves plans to perform one?***
  + ***Media in terms of video games?***
* Yes, inside the “Games” folder in the root directory lies folders for the games of the “Grand Theft Auto” series by Rockstar. “Grand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



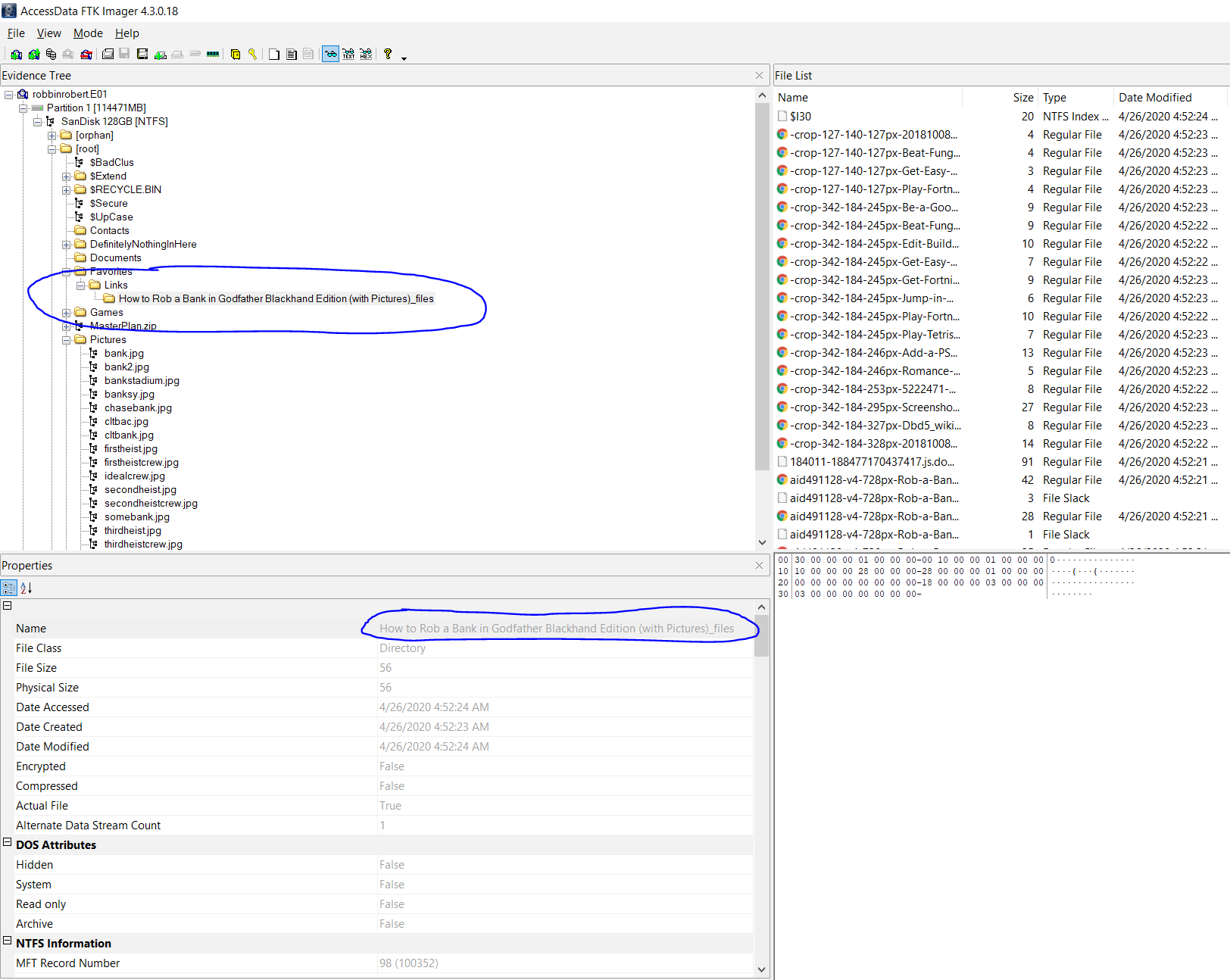
* + ***Media in terms of film?***
* Yes, inside the “Pictures” folder in the root directory lies jpgs for the films of the “Ocean’s” series. Screenshots:



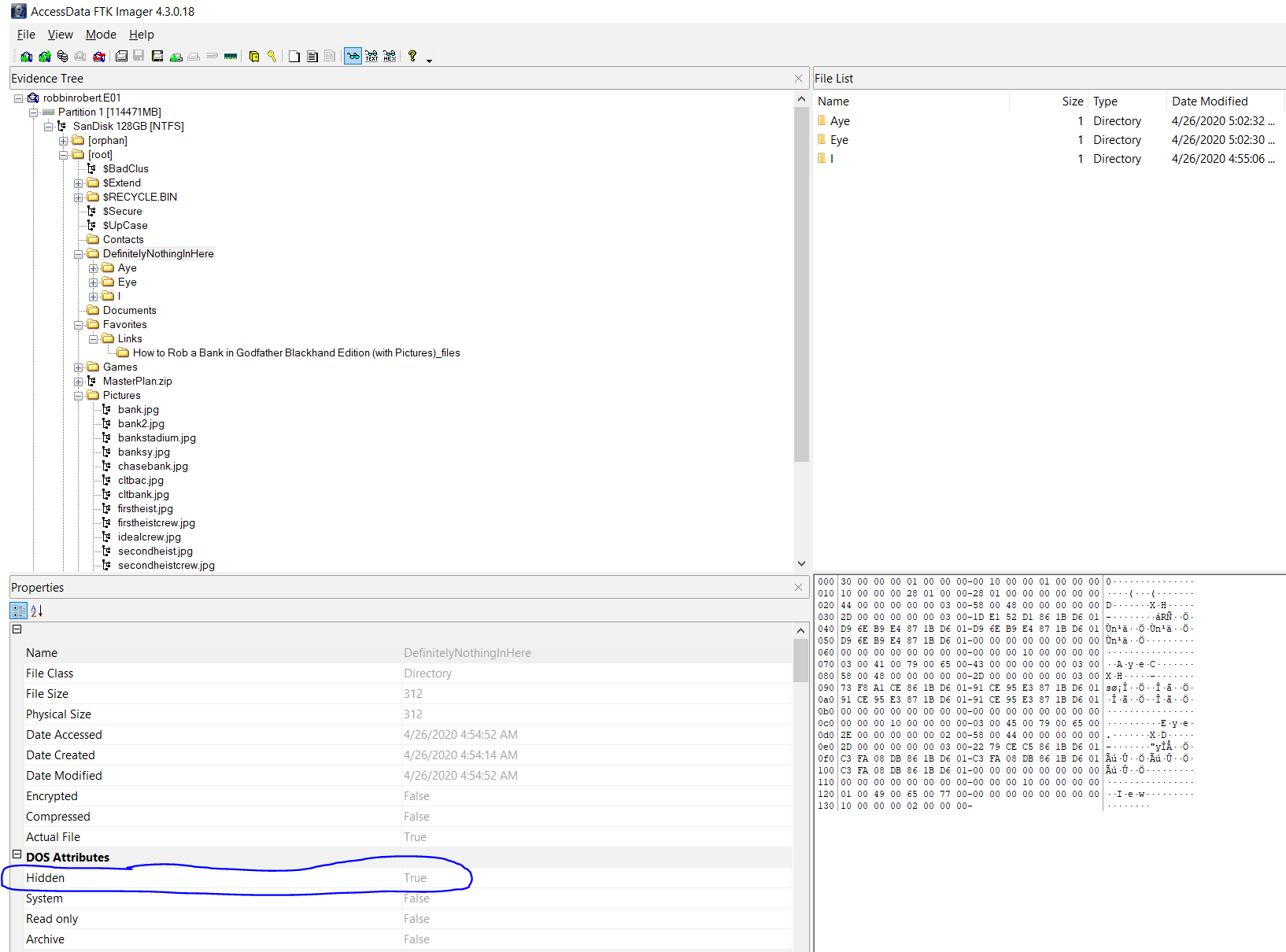


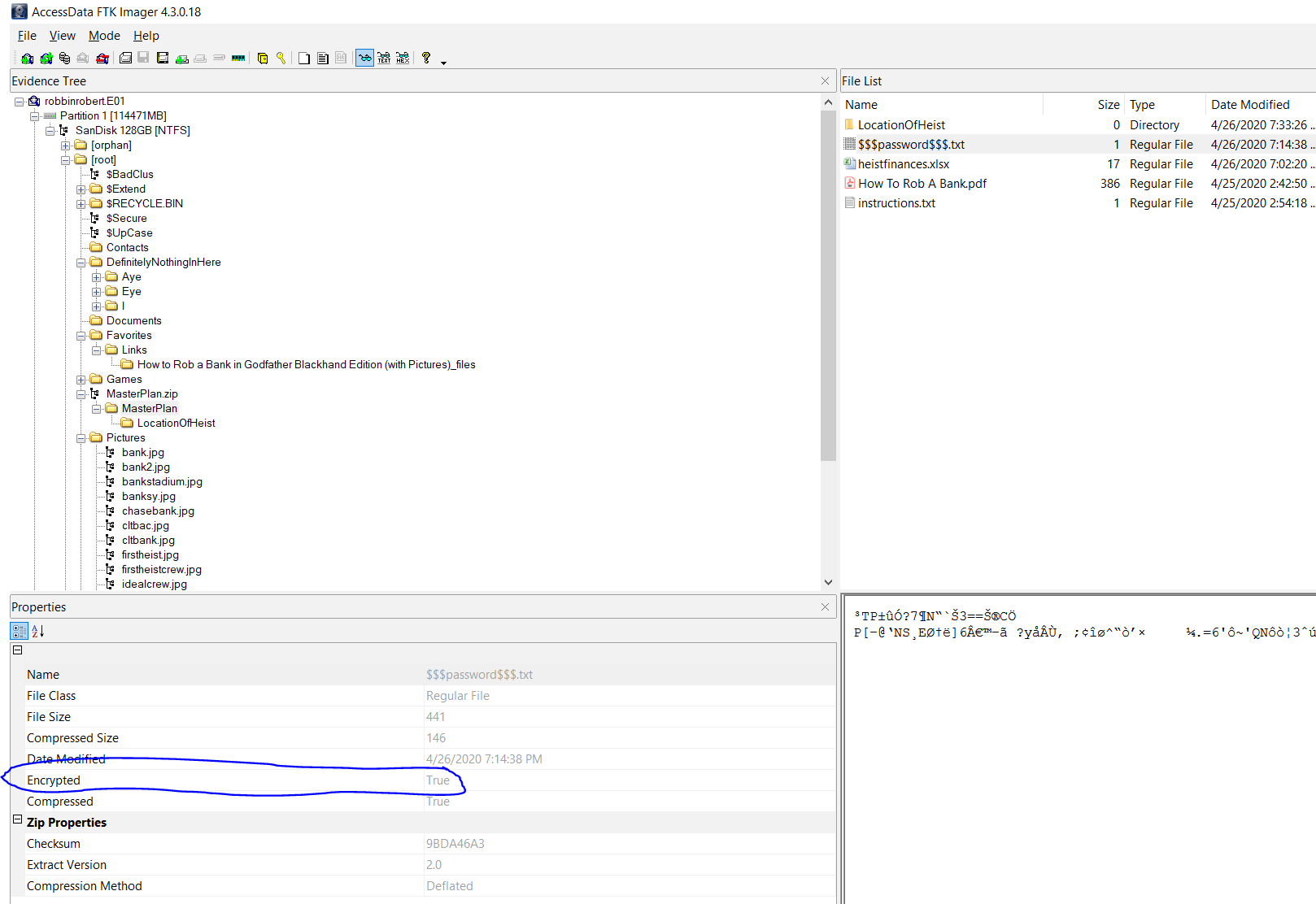


* + ***Media in terms of documents (web, word, etc..)?***
* Yes, inside the “Favorites” folder in the root directory lies a folder for links to a website which is a “how to” on robbing a bank, titled “How to Rob a Bank in Godfather Blackhand Edition (with Pictures)\_files”. Screenshot:

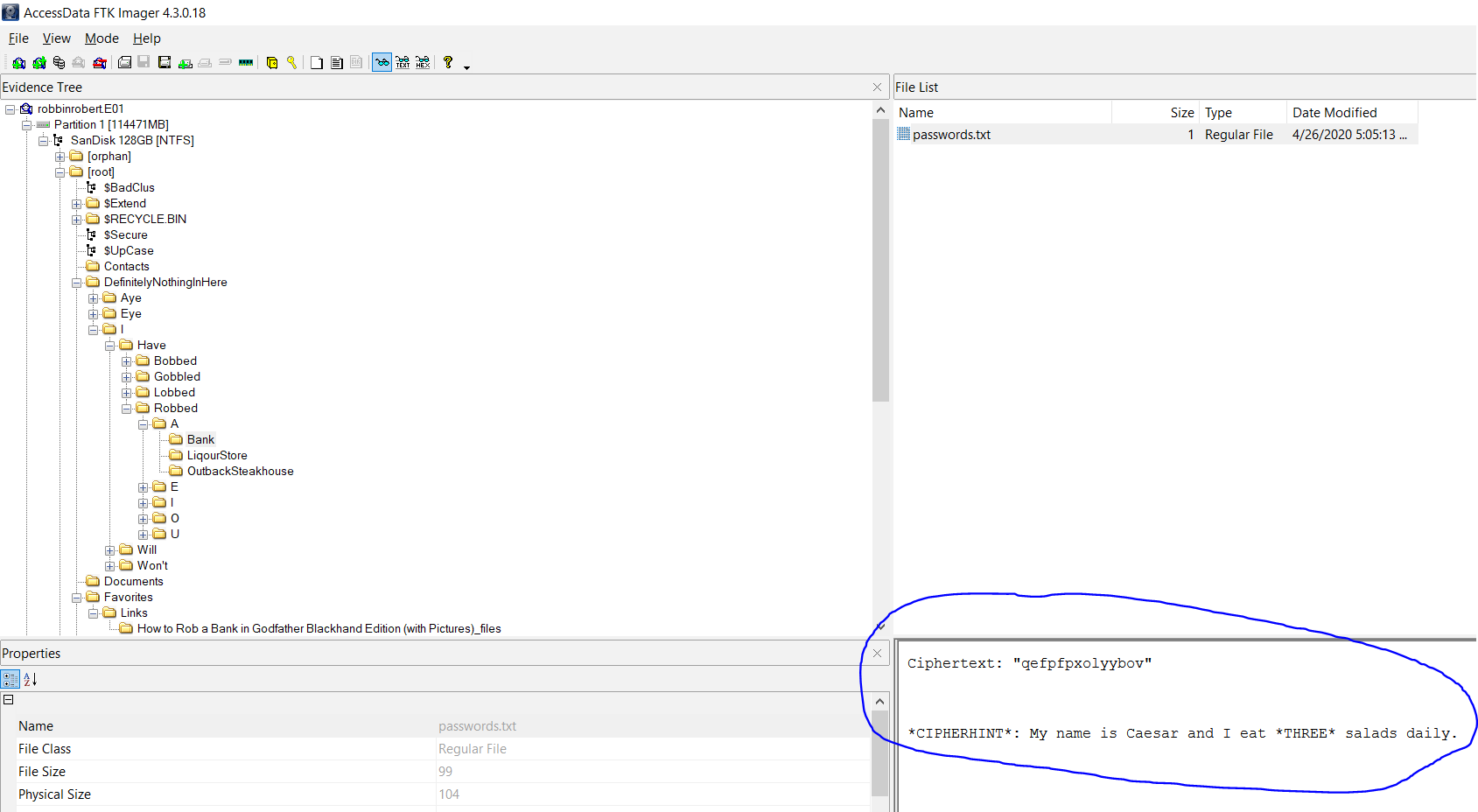


* ***Are there any hidden files/folders on the drive? If so, what are they?***
* Yes. There are two folders on the drive which are hidden, “DefinitelyNothingInHere” and “MasterPlan.zip”. The latter is an encrypted zip folder with password-protected files within. Screenshots:

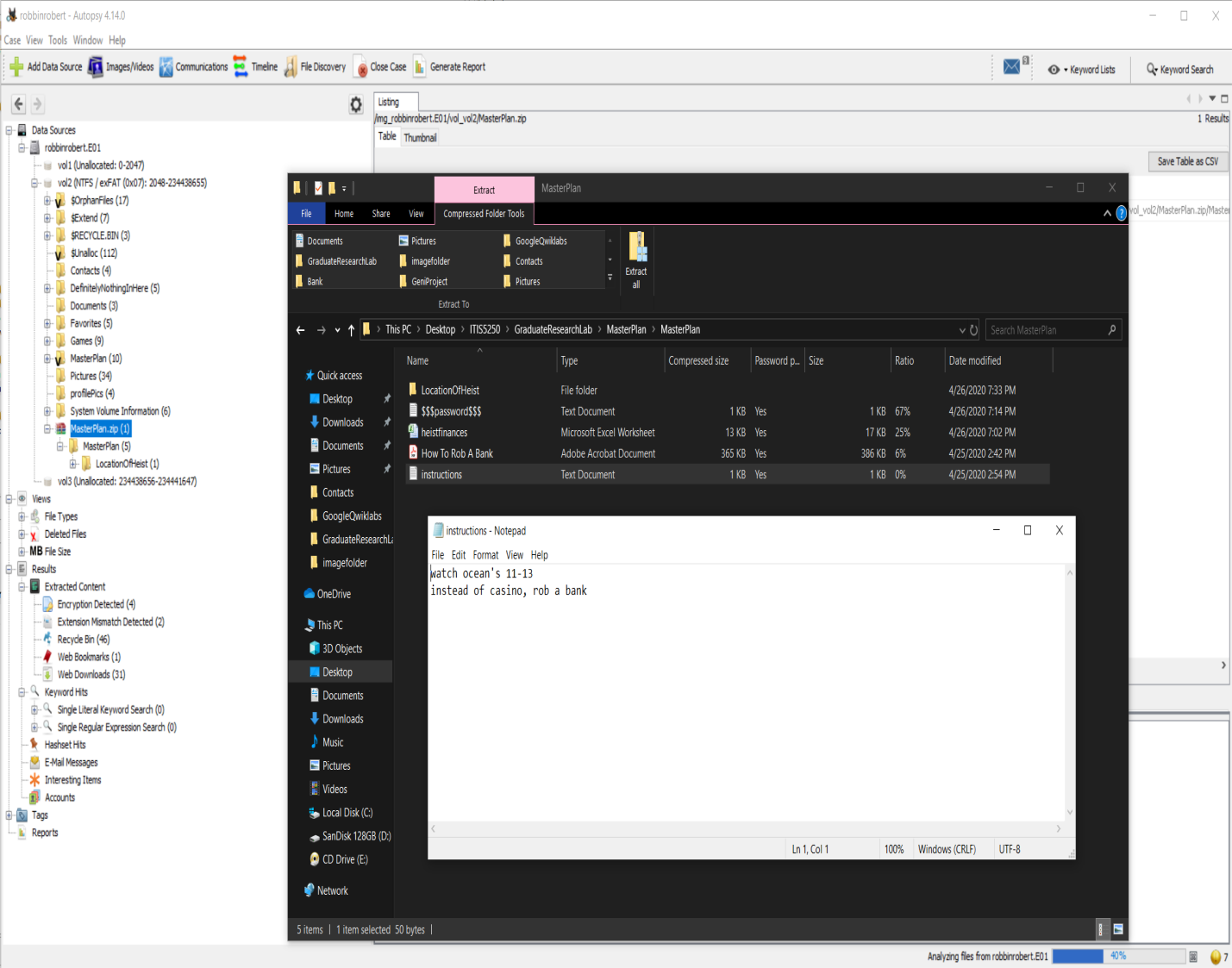


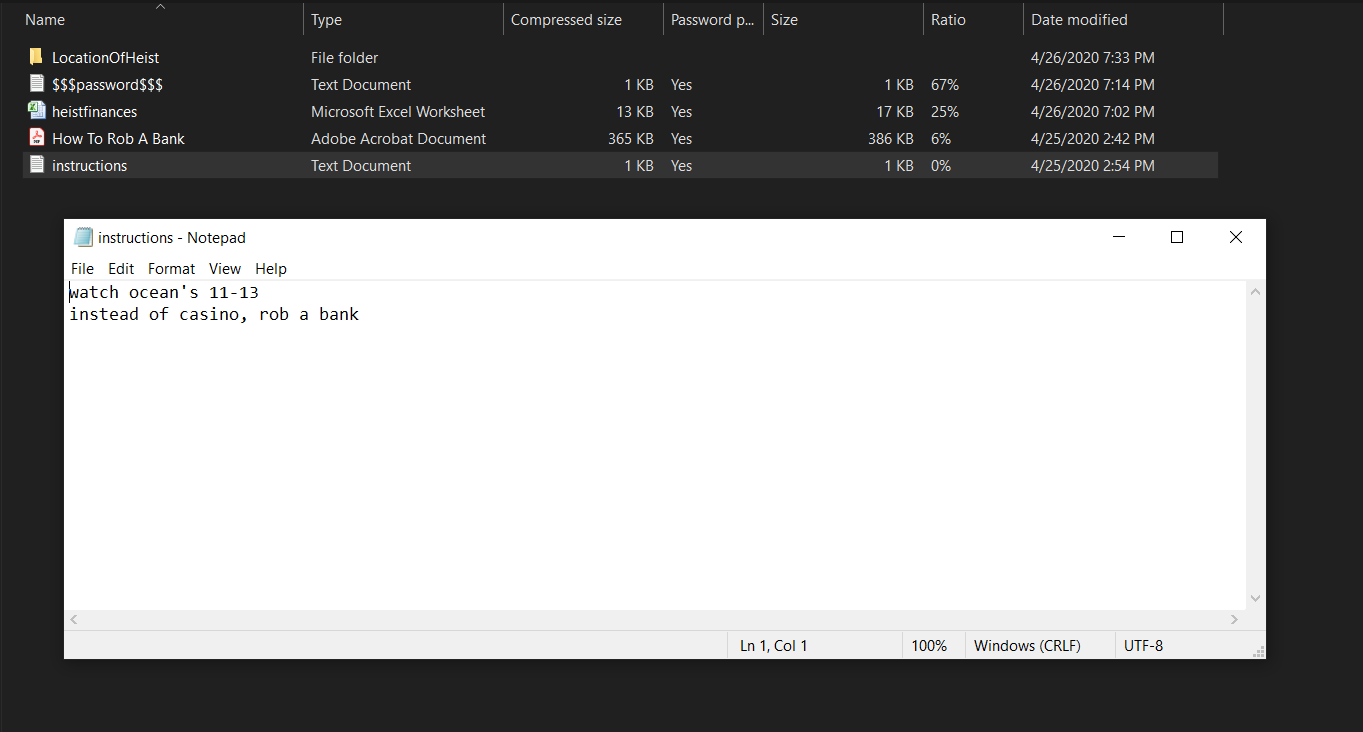


* ***Can you gain access to the encrypted hidden folder, perhaps with information from the other hidden folder?***
* Yes. Although the files in the folder “MasterPlan.zip” are encrypted with passwords, the other folder, “DefinitelyNothingInHere” is unencrypted. Navigating “DefinitelyNothingInHere” through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

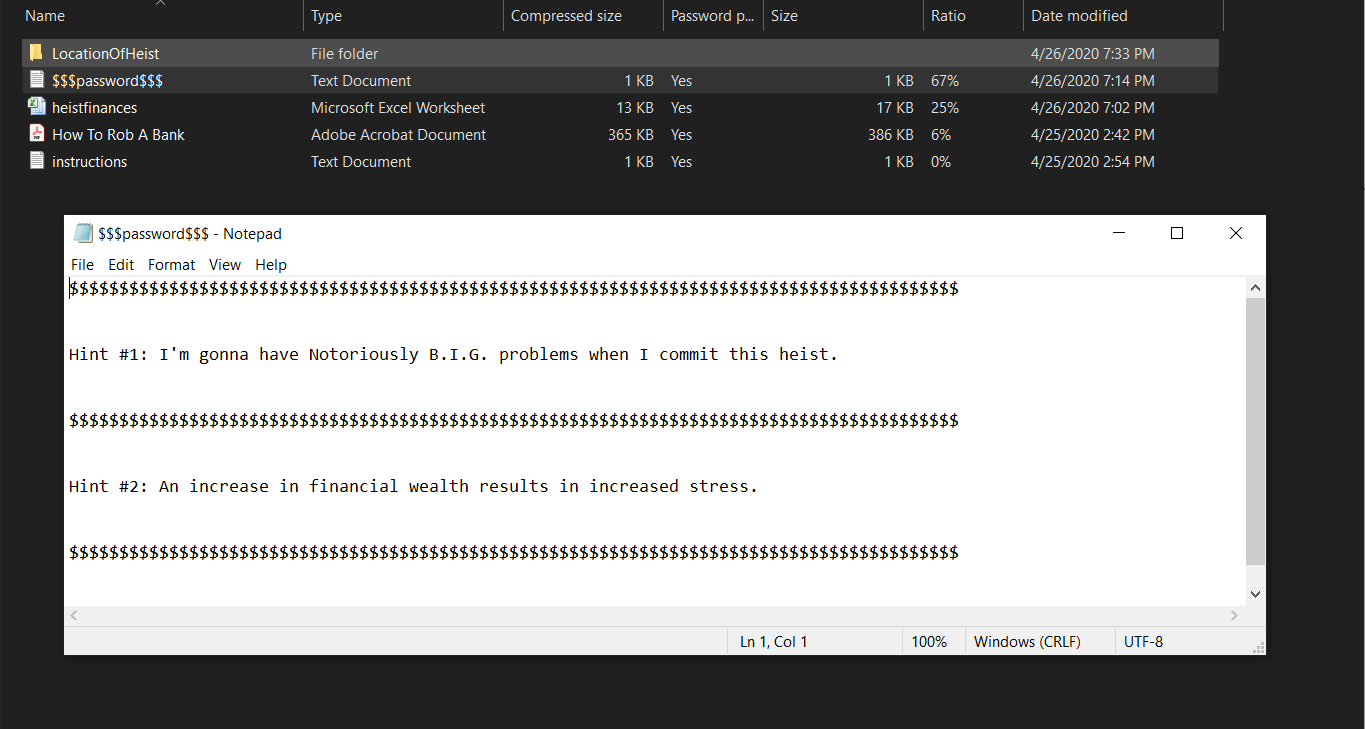


* Which contains a cipher-text, "qefpfpxolyybov", and a hint. The hint reveals the use of a simple Caesar cipher, with an offset of three. Deciphering the cipher-text with this information leads to the text “thisisarobbery”. After exporting the MasterPlan.zip folder using Autopsy, I entered the password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

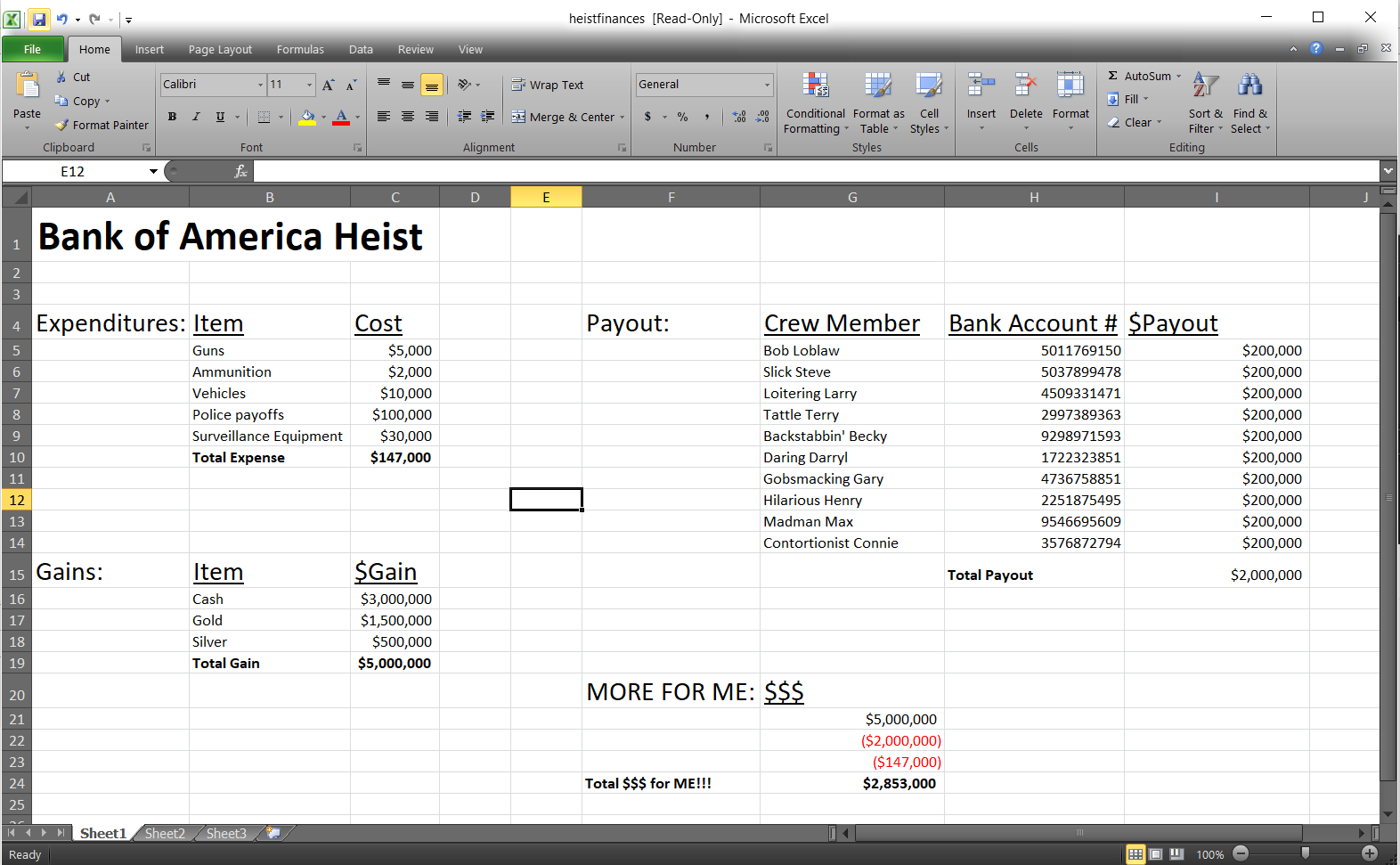




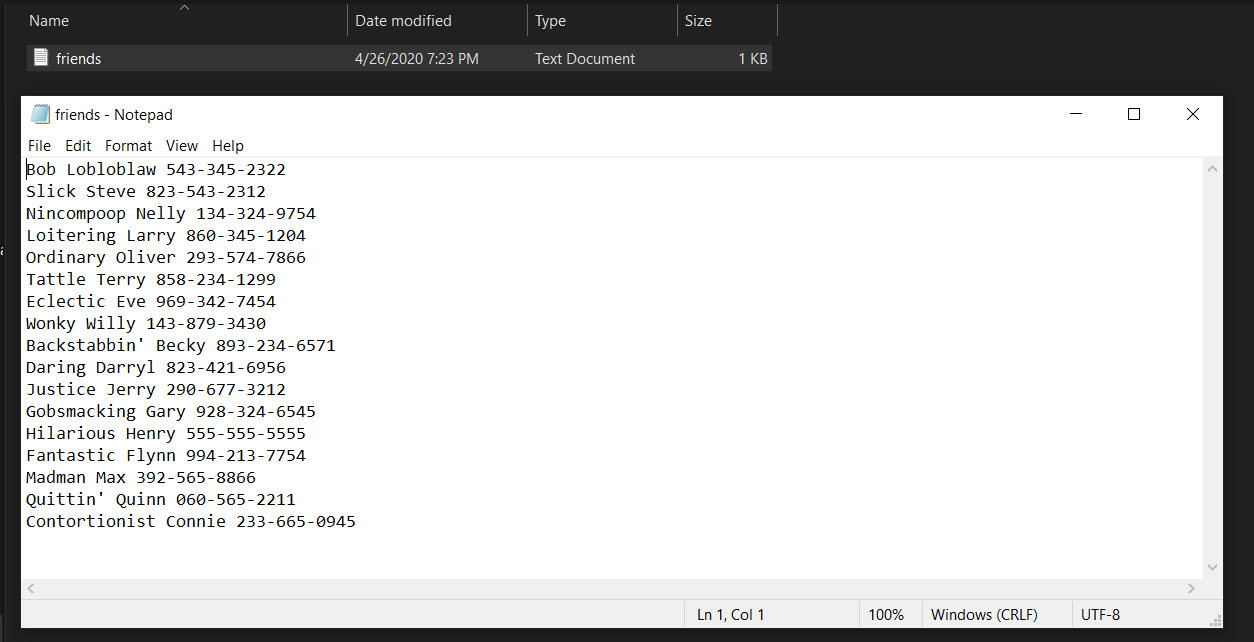
* ***A heist of $5,000,000 doesn’t happen without financial planning. Can you find a document related to the finances of the heist? Can it be accessed?***
* Yes, once I gained access to the files in the “MasterPlan” folder, I could see an Excel Spreadsheet titled “heistfinances.xlsx”. The spreadsheet, 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:



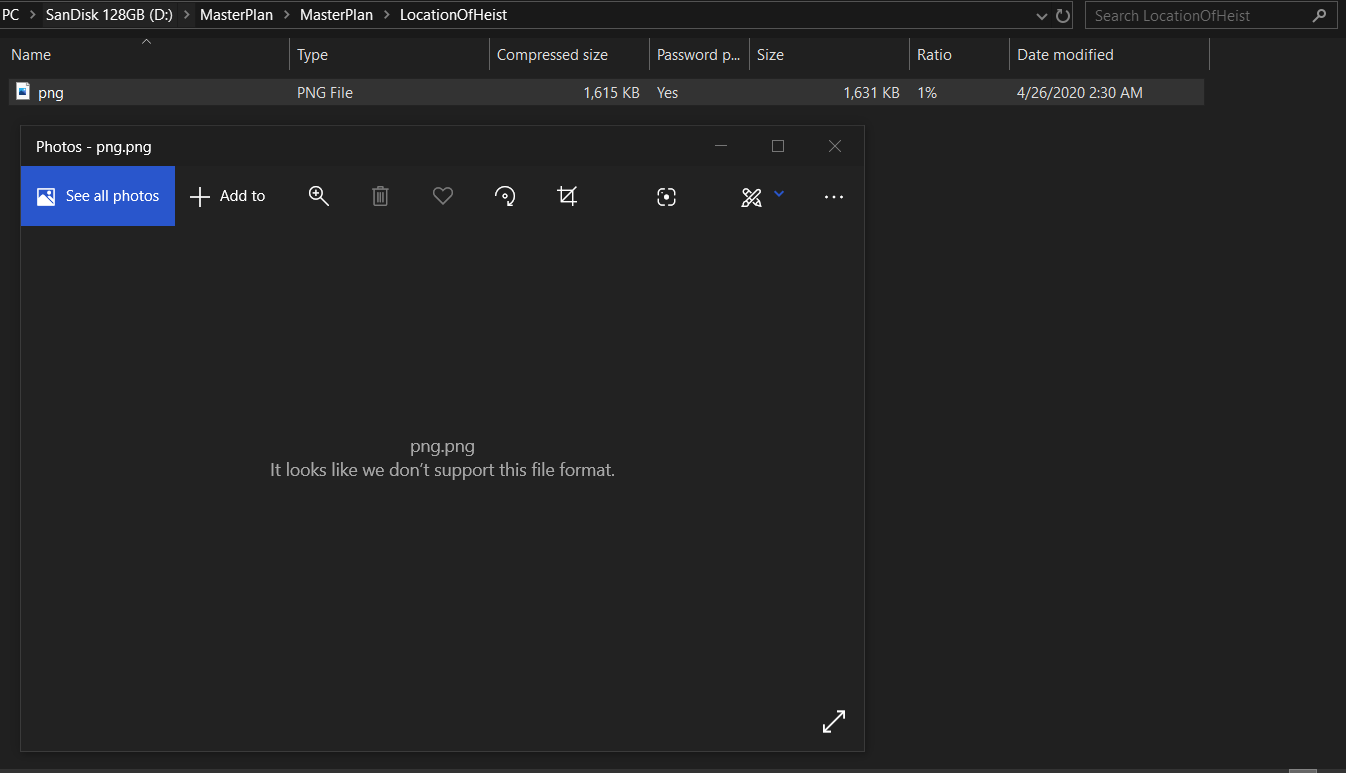
* ***Can you identify the expenditures of the heist?***
* Dollar values for heist expenditures: $5,000 on guns, $2,000 on ammunition, $10,000 on vehicles, $100,000 on police payoffs, and $30,000 on surveillance equipment.
* ***Can you identify the payouts to the crew members?***
* Dollar value of payouts: $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 |

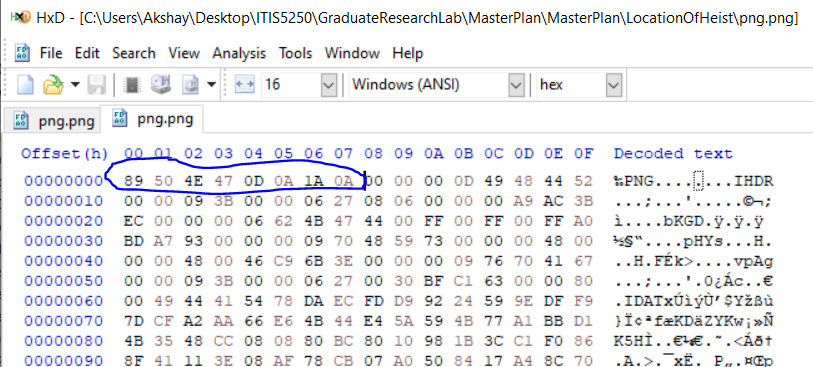
* ***Can you find any evidence that the heist was planned to take place at the Bank of America tower on the 47th, 55th, and 60th floors?***
* Yes, inside the “MasterPlan” folder is another folder titled “LocationOfHeist”. Inside of that, there is a single png file titled “png.png” which is unable to 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:



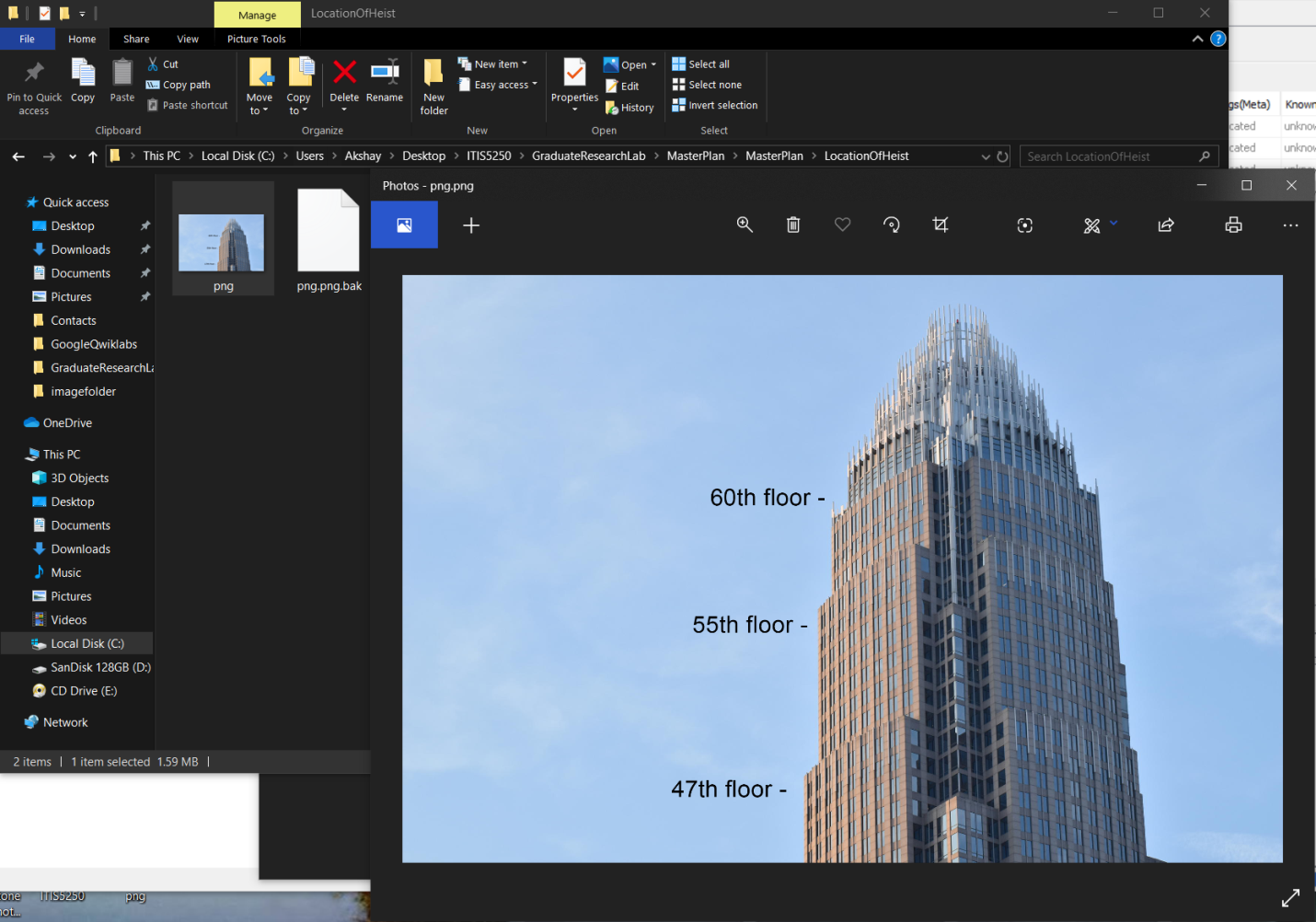
* We can look at the hex content of the file using FTK Imager or a hex editor like HxD. Screenshot of HxD below:



* 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:



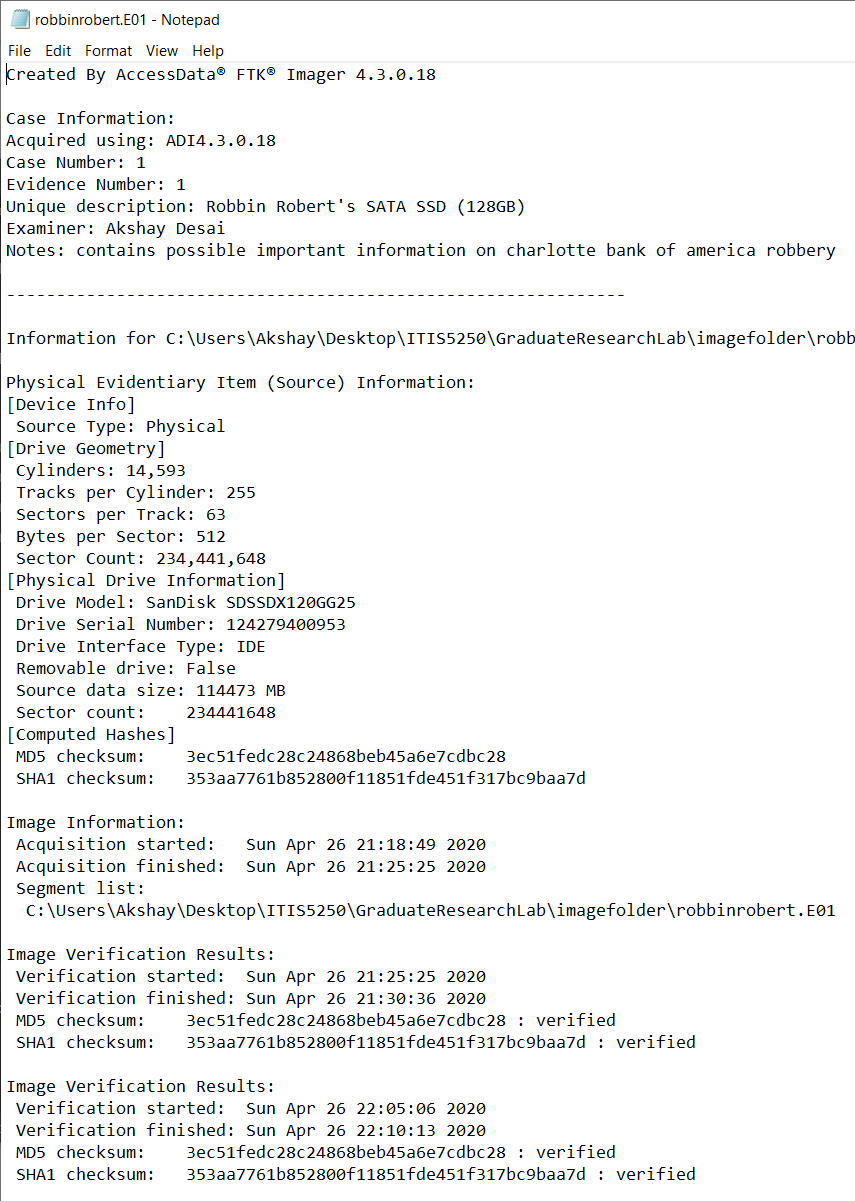
* Now when we open the png file, we get a picture:



* 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* log file), MD5 checksum: 3ec51fedc28c24868beb45a6e7cdbc2

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.