ECE 570: Project Report 2

Date: June 22nd, 2024

By: Payton Murdoch, V00904677

&

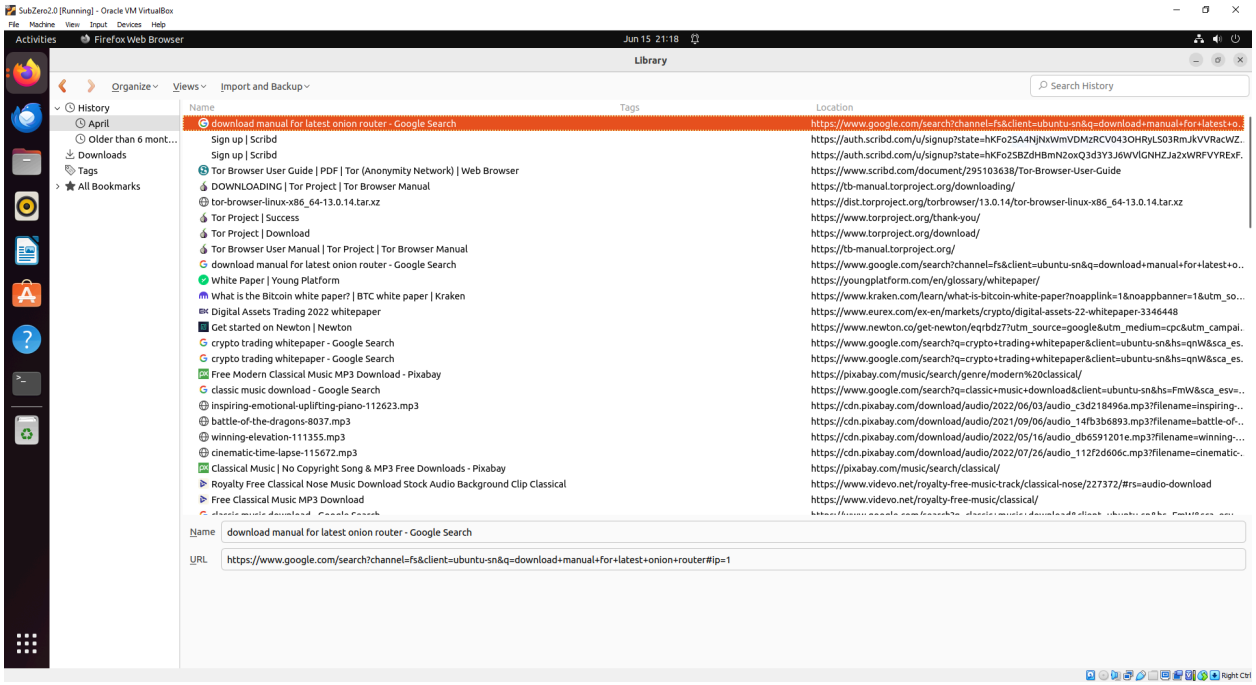
Yun Ma, V01018599

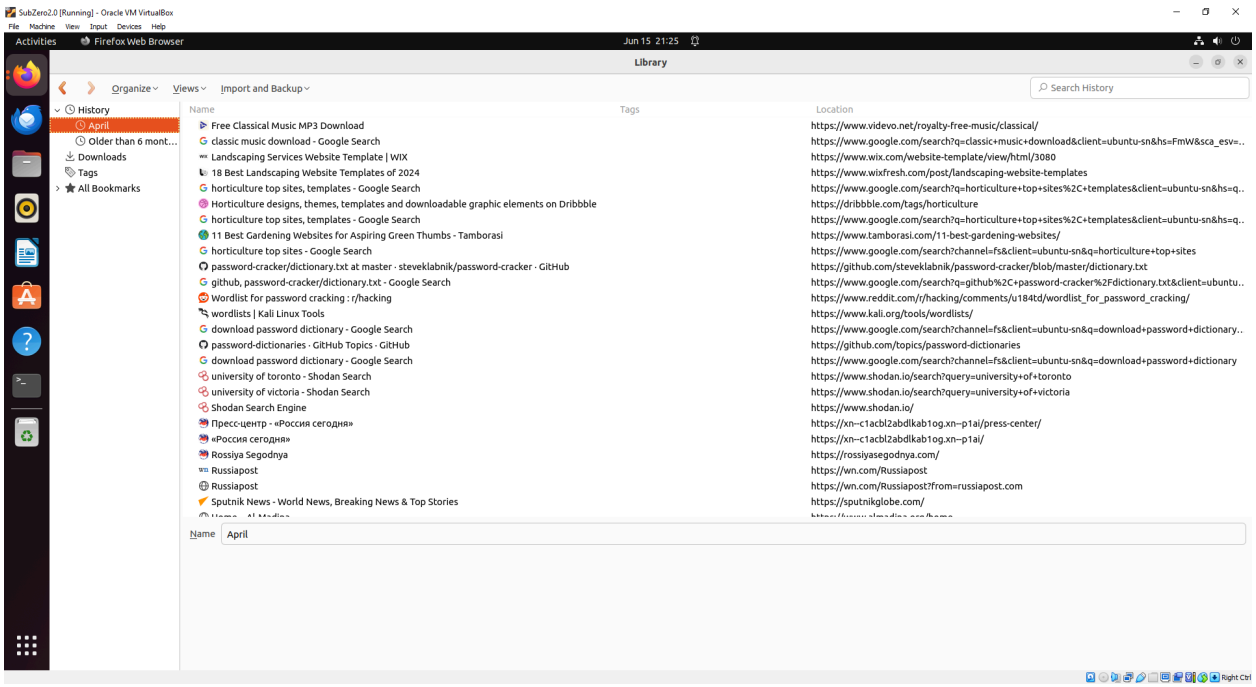
Table of Contents

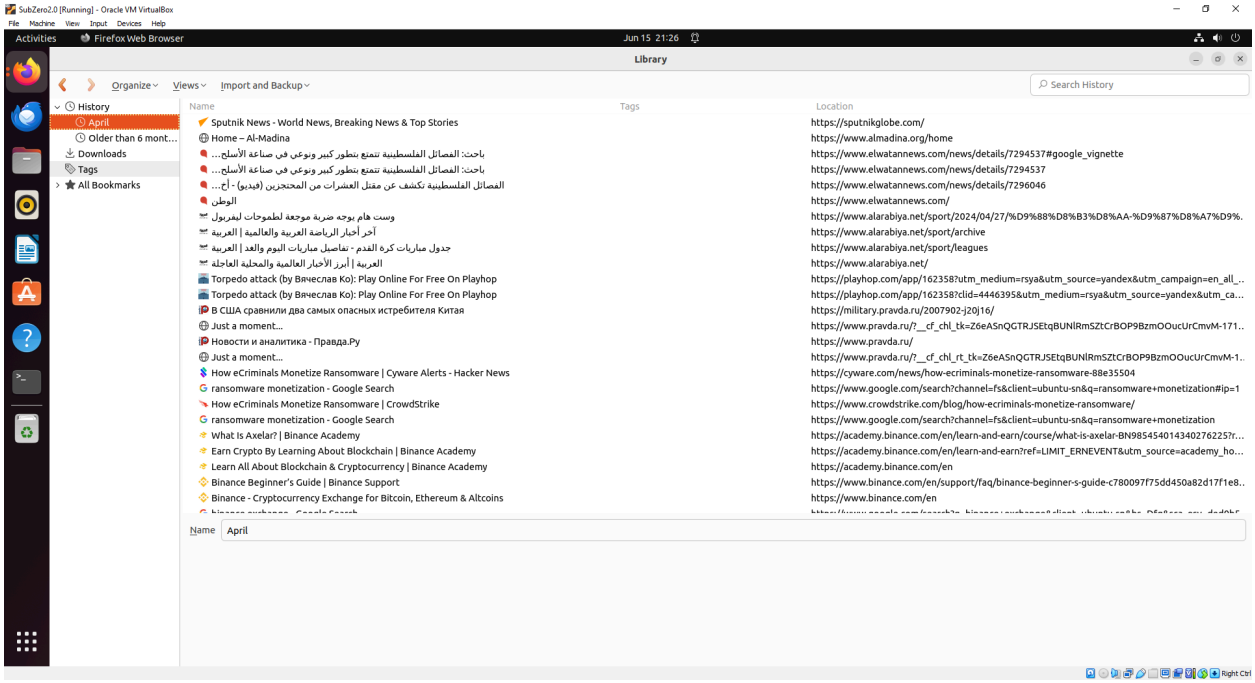
Part 1: VM Investigation

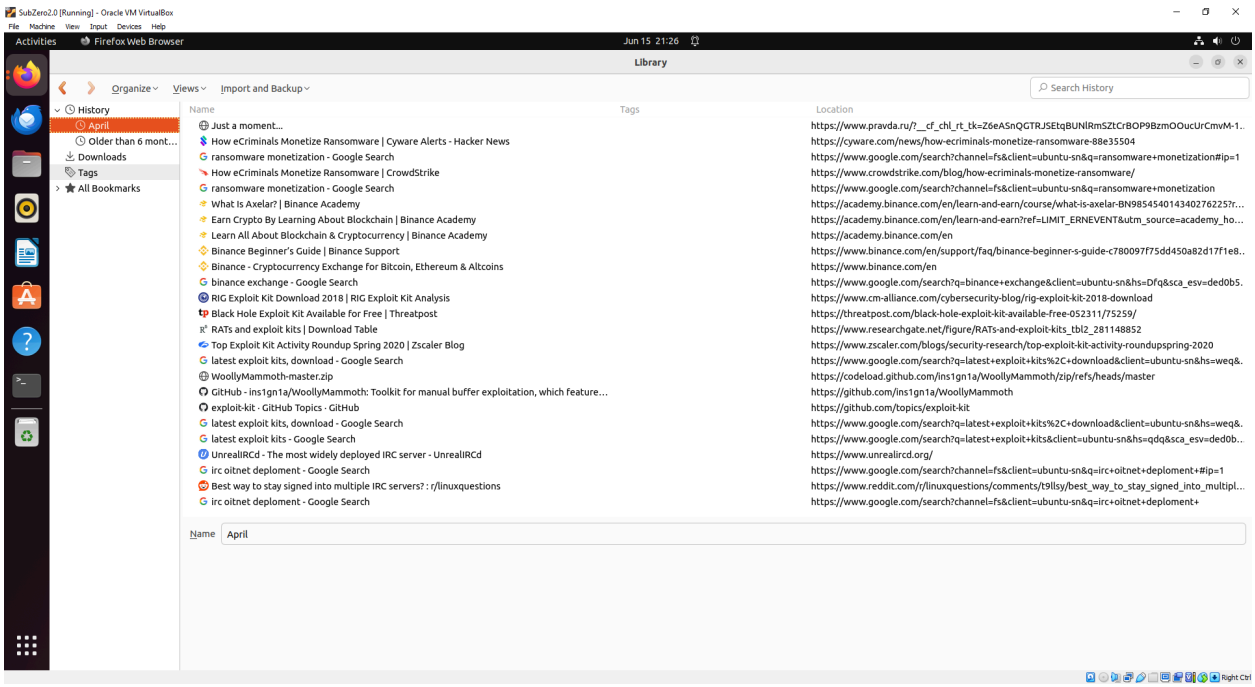
1.1 Suspect Website History.

First, working with the Firefox site history shown in Figure 1, we can address relevant sites and Google searches about our investigation as we have information that the suspect is laundering funds through cryptocurrency.






SubZero2.0 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Jun 15 21:26
Library
Organize
Views
Import and Backup
Search History
History
April
Older than 6 mont…
Downloads
Tags
All Bookmarks
Name
Tags
Location
Sputnik News - World News, Breaking News & Top Stories https://sputnikglobe.com/
Home – Al-Madina https://www.almadina.org/home
باحث: الفصائل الفلسطينية تتمتع بتطور كبير ونوعي في صناعة الأسلح… https://www.elwatannews.com/news/details/7294537#google_vignette
باحث: الفصائل الفلسطينية تتمتع بتطور كبير ونوعي في صناعة الأسلح… https://www.elwatannews.com/news/details/7294537
الفصائل الفلسطينية تكشف عن مقتل العشرات من المحتجزين (فيديو) - أ… https://www.elwatannews.com/news/details/7296046
الوطن https://www.elwatannews.com/
وست هام يوجه ضربة موجعة لطموحات ليفربول https://www.alarabiya.net/sport/2024/04/27/%D9%88%D8%B3%D8%AA-%D9%87%D8%A7%D9%.
آخر أخبار الرياضة العربية والعالمية | العربية https://www.alarabiya.net/sport/archive
جدول مباريات كرة القدم - تفاصيل مباريات اليوم والغد | العربية https://www.alarabiya.net/sport/leagues
العربية | أبرز الأخبار العالمية والمحلية العاجلة https://www.alarabiya.net/
Torpedo attack (by Вячеслав Ко): Play Online For Free On Playhop https://playhop.com/app/16235B?utm_medium=rsya&utm_source=yandex&utm_campaign=en_all_…
Torpedo attack (by Вячеслав Ко): Play Online For Free On Playhop https://playhop.com/app/16235B?clid=444639S&utm_medium=rsya&utm_source=yandex&utm_ca…
В США сравнили два самых опасных истребителя Китая https://military.pravda.ru/2007902-j20j16/
Just a moment... https://www.pravda.ru/?__cf_chl_tk=Z6eASnQGTRJSEtqBUNlRmSZtCrBOP9BzmOOucUrCmvM-171…
Новости и аналитика - Правда.Ру https://www.pravda.ru/
Just a moment... https://www.pravda.ru/?__cf_chl_rt_tk=Z6eASnQGTRJSEtqBUNlRmSZtCrBOP9BzmOOucUrCmvM-1…
How eCriminals Monetize Ransomware | Cyware Alerts - Hacker News https://cyware.com/news/how-ecriminals-monetize-ransomware-88e35504
ransomware monetization - Google Search https://www.google.com/search?channel=fs&client=ubuntu-sn&q=ransomware+monetization#ip=1
How eCriminals Monetize Ransomware | CrowdStrike https://www.crowdstrike.com/blog/how-ecriminals-monetize-ransomware/
ransomware monetization - Google Search https://www.google.com/search?channel=fs&client=ubuntu-sn&q=ransomware+monetization
What Is Axelar? | Binance Academy https://academy.binance.com/en/learn-and-earn/course/what-is-axelar-BN985454014340276225?r…
Earn Crypto By Learning About Blockchain | Binance Academy https://academy.binance.com/en/learn-and-earn?ref=LIMIT_ERNEVENT&utm_source=academy_ho…
Learn All About Blockchain & Cryptocurrency | Binance Academy https://academy.binance.com/en
Binance Beginner's Guide | Binance Support https://www.binance.com/en/support/faq/binance-beginner-s-guide-c780097f75dd450a82d17f1e8…
Binance - Cryptocurrency Exchange for Bitcoin, Ethereum & Altcoins https://www.binance.com/en
Name
April
Right Ctrl


SubZero2.0 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Jun 15 21:26
Library
Organize
Views
Import and Backup
Search History
History
April
Older than 6 mont…
Downloads
Tags
All Bookmarks
Name
Tags
Location
Just a moment... https://www.pravda.ru/?__cf_chl_rt_tk=Z6eASnQGTRJSEtqBUNlRmSZtCrBOP9BzmOOucUrCmvM-1…
How eCriminals Monetize Ransomware | Cyware Alerts - Hacker News https://cyware.com/news/how-ecriminals-monetize-ransomware-88e35504
ransomware monetization - Google Search https://www.google.com/search?channel=fs&client=ubuntu-sn&q=ransomware+monetization#ip=1
How eCriminals Monetize Ransomware | CrowdStrike https://www.crowdstrike.com/blog/how-ecriminals-monetize-ransomware/
ransomware monetization - Google Search https://www.google.com/search?channel=fs&client=ubuntu-sn&q=ransomware+monetization
What Is Axelar? | Binance Academy https://academy.binance.com/en/learn-and-earn/course/what-is-axelar-BN985454014340276225?r…
Earn Crypto By Learning About Blockchain | Binance Academy https://academy.binance.com/en/learn-and-earn?ref=LIMIT_ERNEVENT&utm_source=academy_ho…
Learn All About Blockchain & Cryptocurrency | Binance Academy https://academy.binance.com/en
Binance Beginner's Guide | Binance Support https://www.binance.com/en/support/faq/binance-beginner-s-guide-c780097f75dd450a82d17f1e8…
Binance - Cryptocurrency Exchange for Bitcoin, Ethereum & Altcoins https://www.binance.com/en
binance exchange - Google Search https://www.google.com/search?q=binance+exchange&client=ubuntu-sn&hs=Dfq&sca_esv=ded0b5…
RIG Exploit Kit Download 2018 | RIG Exploit Kit Analysis https://www.cm-alliance.com/cybersecurity-blog/rig-exploit-kit-2018-download
Black Hole Exploit Kit Available for Free | Threatpost https://threatpost.com/black-hole-exploit-kit-available-free-052311/75259/
RATs and exploit kits | Download Table https://www.researchgate.net/figure/RATs-and-exploit-kits_tbl2_281148852
Top Exploit Kit Activity Roundup Spring 2020 | Zscaler Blog https://www.zscaler.com/blogs/security-research/top-exploit-kit-activity-roundupspring-2020
latest exploit kits, download - Google Search https://www.google.com/search?q=latest+exploit+kits%2C+download&client=ubuntu-sn&hs=weq&…
WoollyMammoth-master.zip https://codeload.github.com/ins1gn1a/WoollyMammoth/zip/refs/heads/master
GitHub - ins1gn1a/WoollyMammoth: Toolkit for manual buffer exploitation, which feature… https://github.com/ins1gn1a/WoollyMammoth
exploit-kit · GitHub Topics · GitHub https://github.com/topics/exploit-kit
latest exploit kits, download - Google Search https://www.google.com/search?q=latest+exploit+kits%2C+download&client=ubuntu-sn&hs=weq&…
latest exploit kits - Google Search https://www.google.com/search?q=latest+exploit+kits&client=ubuntu-sn&hs=qdq&sca_esv=ded0b…
UnrealIRCd - The most widely deployed IRC server - UnrealIRCd https://www.unrealircd.org/
irc oitnet deployment - Google Search https://www.google.com/search?channel=fs&client=ubuntu-sn&q=irc+oitnet+deployment+#ip=1
Best way to stay signed into multiple IRC servers? : r/linuxquestions https://www.reddit.com/r/linuxquestions/comments/t9llsy/best_way_to_stay_signed_into_multipl…
irc oitnet deployment - Google Search https://www.google.com/search?channel=fs&client=ubuntu-sn&q=irc+oitnet+deployment+
Name
April
Right Ctrl

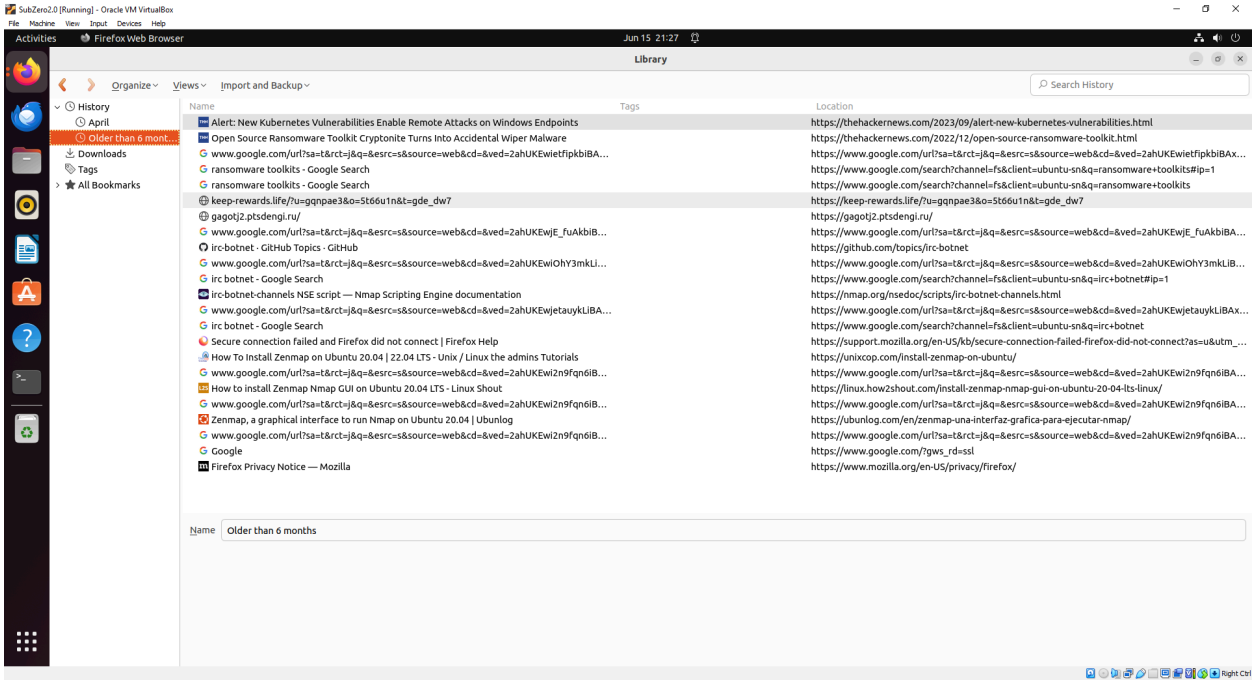


Figure 1: Website Search History.

Let us quickly summarize the notable sites and their influence on this investigation.

- Download for Tor Browser, while not inherently suspicious, allows a user to use services anonymously without being tracked or recorded.[1]
- Google searches for Crypto Trading Whitepapers and sites like kraken.com, eurex.com, and Binance.com imply that the suspect owns crypto.
- Google searches, GitHub and Kali links for password dictionaries imply that the suspect may be utilizing password-cracking software.
- Shodan searches for the University of Victoria and Toronto, which could be possible targets for the suspect.
- Google searches and sites depicting how to monetize ransomware.
- Google searches for the most recent ransomware and Exploit Kits.
- Google searches for IRC botnets.
- Zenmap/Nmap installation guides.

In addition to the suspicious searches and sites, the suspect frequented Russian and Arabic news sites, online games, and royalty-free music sites.

1.2 Recycling Bin.

As shown in Figure 2, only two files are in the recycling bin.

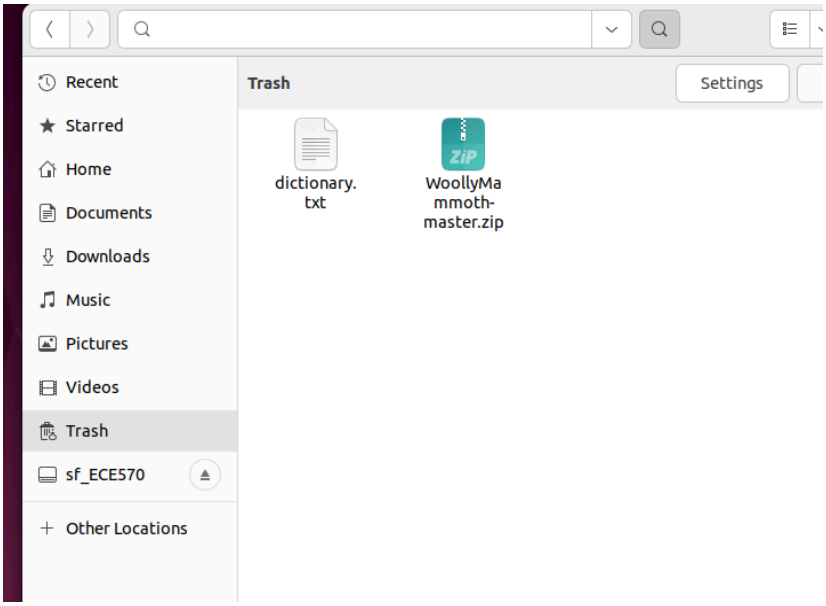


Figure 2: Recycling bin for Suspect Alex.

When files are moved to the recycling bin, they are not deleted in any capacity. They are given an indicator at their memory location, which prepares them for removal. However, the memory will be freed once the user removes it from the trash/recycling bin and can be easily restored. The following Figure 3 shows the contents of these files. First, we have a dictionary.txt containing a list of passwords showing the suspect possibly engaged in brute-force password-cracking methods. Next, we have the WoollyMammoth master zip file, which includes the woollymammoth.py script. This script is a tool which can be used for network fuzzing and exploiting vulnerabilities like buffer overflows and stack carving.[2] Thus, these two packages are incredibly pertinent as they can be used to infer that the suspect is conducting fuzzing attacks or password-cracking attacks against some system.

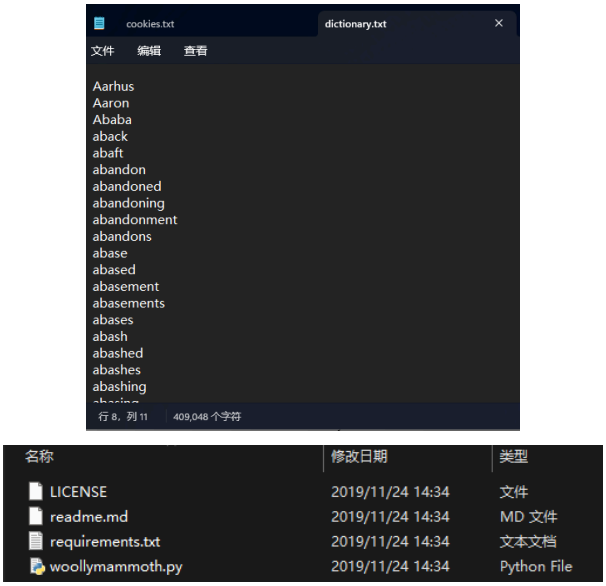


Figure 3: Trash bin file contents.

1.3 Suspects Malicious Software.

Log in to the root, then ‘apt list—installed’ to list all packages on Ubuntu, as shown in Figure 4.

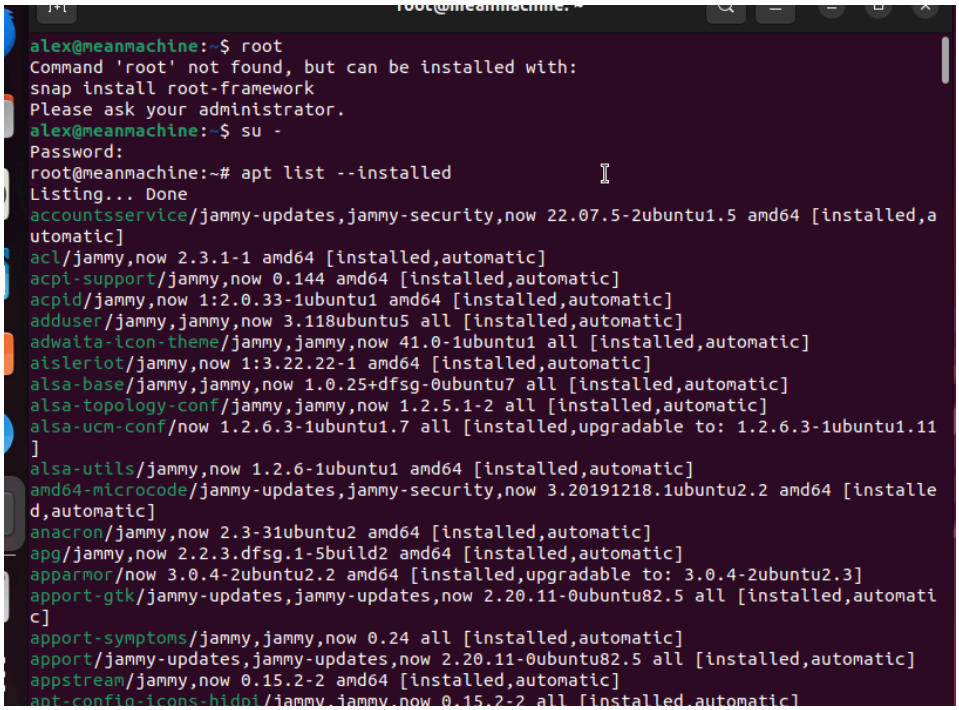


Figure 4: apt list --installed for Alex's system.

Based on our examination of the installed services and knowledge of certain pen-testing tools, we can make inferences about the following programs:

- Hydra: Commonly used for brute-force password cracking attacks to gain unauthorized access to systems through legitimate username and password pairs.
- Ncrack: Commonly used for brute-force password cracking attacks to gain unauthorized access to systems through legitimate username and password pairs.
- Crunch: used to generate custom wordlists for password-cracking services such as Hydra and Ncrack.
- Hping3: Often used for network testing and security auditing, including performing Denial of Service (DoS) attacks.
- Wireshark is often utilized for network testing, logging, and surveillance/verification of network communication. It is not inherently malicious but can be useful for information gathering.
- Tor: A private browser where users can use the internet without tracking.
- Nmap: A port scanning tool which allows

Upon further examination, we can also run the command msfconsole shown in Figure 5, which launches the Metasploit exploit and pen-testing framework, a tool useful for vulnerability scanning and streamlining exploits.

Figure 5: msfconsole running Metasploit on suspect PC.

1.4 Was the machine involved in or prepared to conduct an attack?

Attacks could include unauthorized access through brute force, exploiting software vulnerabilities via buffer overflows, and performing DoS attacks. As shown in Figure 6, looking into the '.bash_history' file for the user Alex, we can see that an actual attempted brute force attack was conducted against a user 'jacobs' over SSH protocols on the IP 142.104.202.14, which was located by port scanning with nmap over the range 142.104.202.0/28.

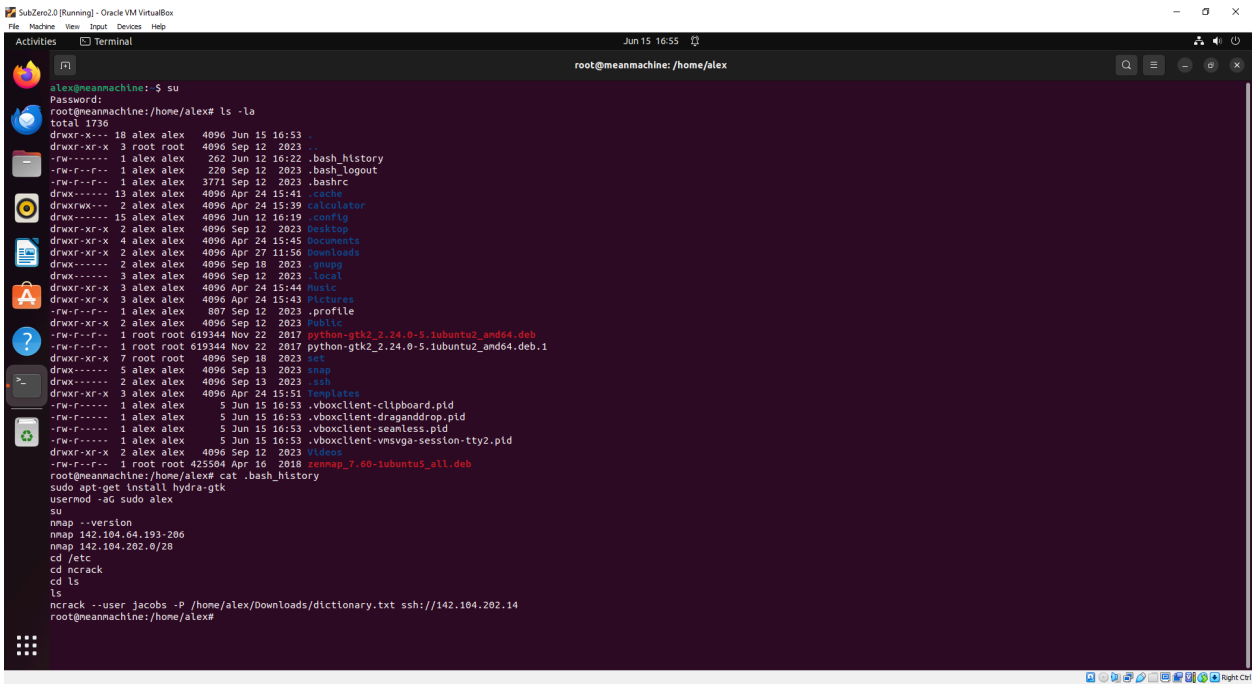


Figure 6: .bash_history of user Alex.

Furthermore, let us return to msfconsole. Luckily, there is a feature within the console where you can call the command history, and as shown in Figure 7, this history shows a search for ‘cve-2014-0160’.

```
msf6 > history
1  help
2  search cve-2014-0160
3  exit
4  quit
5  history
```

Figure 7: msfconsole history.

Upon further investigation, we can see that this CVE corresponds to the HeartBleed exploit, which allows for the leak of target information, as shown in Figure 8. This indicates that the suspect could have performed this attack against a user to leak important information such as user IDs or passwords.

```
msf6 > search cve-2014-0160

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/server/openssl_heartbeat_client_memory  2014-04-07       normal  No     OpenSSL Heartbeat (Heartbleed) Client Memory Exposure
   1  auxiliary/scanner/ssl/openssl_heartbleed          2014-04-07       normal  Yes    OpenSSL Heartbeat (Heartbleed) Information Leak
   2    \_ action: DUMP                                 .                .       .      Dump memory contents to loot
   3    \_ action: KEYS                                 .                .       .      Recover private keys from memory
   4    \_ action: SCAN                                 .                .       .      Check hosts for vulnerability

Interact with a module by name or index. For example info 4, use 4 or use auxiliary/scanner/ssl/openssl_heartbleed
After interacting with a module you can manually set a ACTION with set ACTION 'SCAN'
```

Figure 8: Information for CVE-2014-0160.

1.5 What additional information can you tell about the machine's owner?

Given the following Figure 9, we can infer that the user knows other languages besides English. They would frequent news sites containing Russian and Arabic; thus, we can assume they understand those languages.

Пресс-центр - «Россия сегодня»	https://xn--c1acbl2abdlkab1og.xn--p1ai/press-center/
«Россия сегодня»	https://xn--c1acbl2abdlkab1og.xn--p1ai/
Rossiya Segodnya	https://rossiyasegodnya.com/
Russiapost	https://wn.com/Russiapost
Russiapost	https://wn.com/Russiapost?from=russiapost.com
Sputnik News - World News, Breaking News & Top Stories	https://sputnikglobe.com/
Home – Al-Madina	https://www.almadina.org/home
باحث: الفصائل الفلسطينية تتمتع بتطور كبير ونوعي في صناعة الأسلح...	https://www.elwatannews.com/news/details/7294537#go
باحث: الفصائل الفلسطينية تتمتع بتطور كبير ونوعي في صناعة الأسلح...	https://www.elwatannews.com/news/details/7294537
الفصائل الفلسطينية تكشف عن مقتل العشرات من المحتجزين (فيديو) - أخ...	https://www.elwatannews.com/news/details/7296046
الوطن	https://www.elwatannews.com/
وست هام يوجه ضربة موجعة لطموحات ليفربول	https://www.alarabiya.net/sport/2024/04/27/%D9%88%D
آخر أخبار الرياضة العربية والعالمية | العربية	https://www.alarabiya.net/sport/archive
جدول مباريات كرة القدم - تفاصيل مباريات اليوم والغد | العربية	https://www.alarabiya.net/sport/leagues
العربية | أبرز الأخبار العالمية والمحلية العاجلة	https://www.alarabiya.net/

Figure 9: News Site History.

Figure 10 shows other inferences we can make concerning the machine’s owner's music taste. They frequently look for classical music. Furthermore, we can see that the owner has a passion for horticulture, as they are looking for templates and advice for building a horticulture site.

Free Modern Classical Music MP3 Download - Pixabay
classic music download - Google Search
inspiring-emotional-uplifting-piano-112623.mp3
battle-of-the-dragons-8037.mp3
winning-elevation-111355.mp3
cinematic-time-lapse-115672.mp3
Classical Music | No Copyright Song & MP3 Free Downloads - Pixabay
Royalty Free Classical Nose Music Download Stock Audio Background Clip Classical
Free Classical Music MP3 Download
classic music download - Google Search
Landscaping Services Website Template | WIX
18 Best Landscaping Website Templates of 2024
horticulture top sites, templates - Google Search
Horticulture designs, themes, templates and downloadable graphic elements on Dribbble
horticulture top sites, templates - Google Search
11 Best Gardening Websites for Aspiring Green Thumbs - Tamborasi
horticulture top sites - Google Search

Figure 10: Music and horticulture site history.

Part 2: Raw Image Investigation

2.1 Check the validity of the forensic image.

First, we look at the image to verify that both hashes directly correlate with the hashes.txt file. We use the FTK imager's Drive/Image Verification setting, shown below.

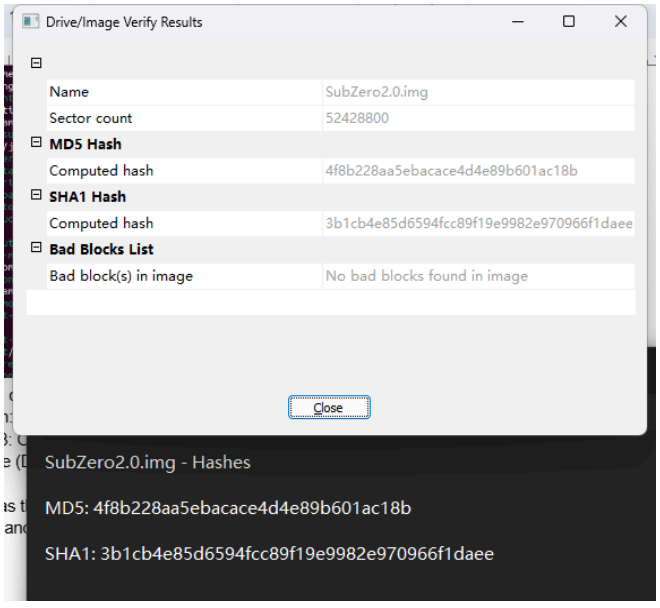


Figure 11: FTK Imager visual hash verification.

With this visual confirmation provided by the FTK imager, we can see that the computed hashes match those enclosed within the text file; thus, our image file is not corrupted.

2.2 Detailed investigation.

To conduct our investigation, we first look at the evidence tree provided by the FTK imager, as shown in the following Figure.

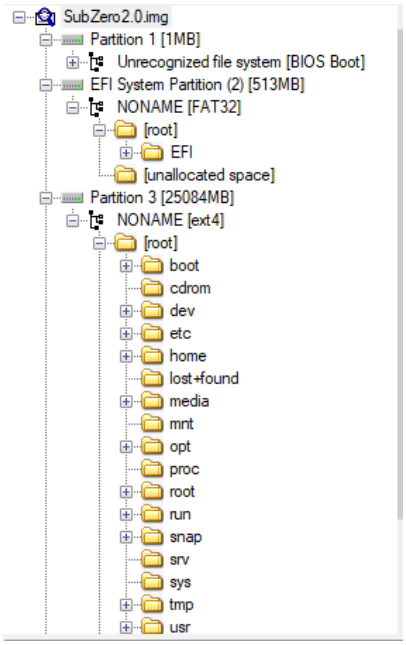


Figure 12: Evidence Tree.

The system is divided into three partitions, with most data resting within Partition 3. As examining the entire file system may be redundant, we will isolate partition 3, which will be the center of our investigation. We will extract the image file as SubZero_P3. Luckily, FTK Imager also computes the hashes for this partition, as shown in the following Figure, to ensure that the files remain uncorrupted once they are examined in Autopsy.

Figure 13: Computed Hash of Partition 3.

Moving onto the Autopsy program on Kali, as shown in the following Figure, we enter the corresponding MD5 Hash and allow the application to verify the hash after importing the file system partition.

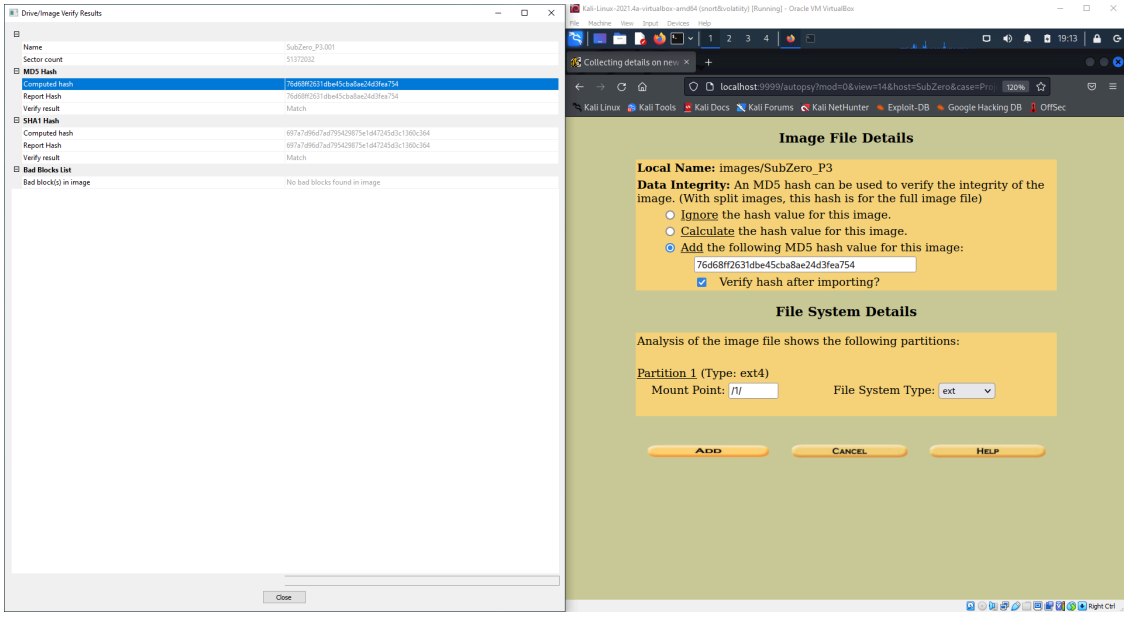


Figure 14: Verify the hash of the image file partition.

Upon completion and verification of the hash, we can begin investigating through file analysis on Autopsy. Autopsy is embedded with a tool that allows us to search and sort files based on their type. This tool also verifies file types, noting that outliers will be sorted into a ‘mismatch.html’ file, as shown in Figure 15.

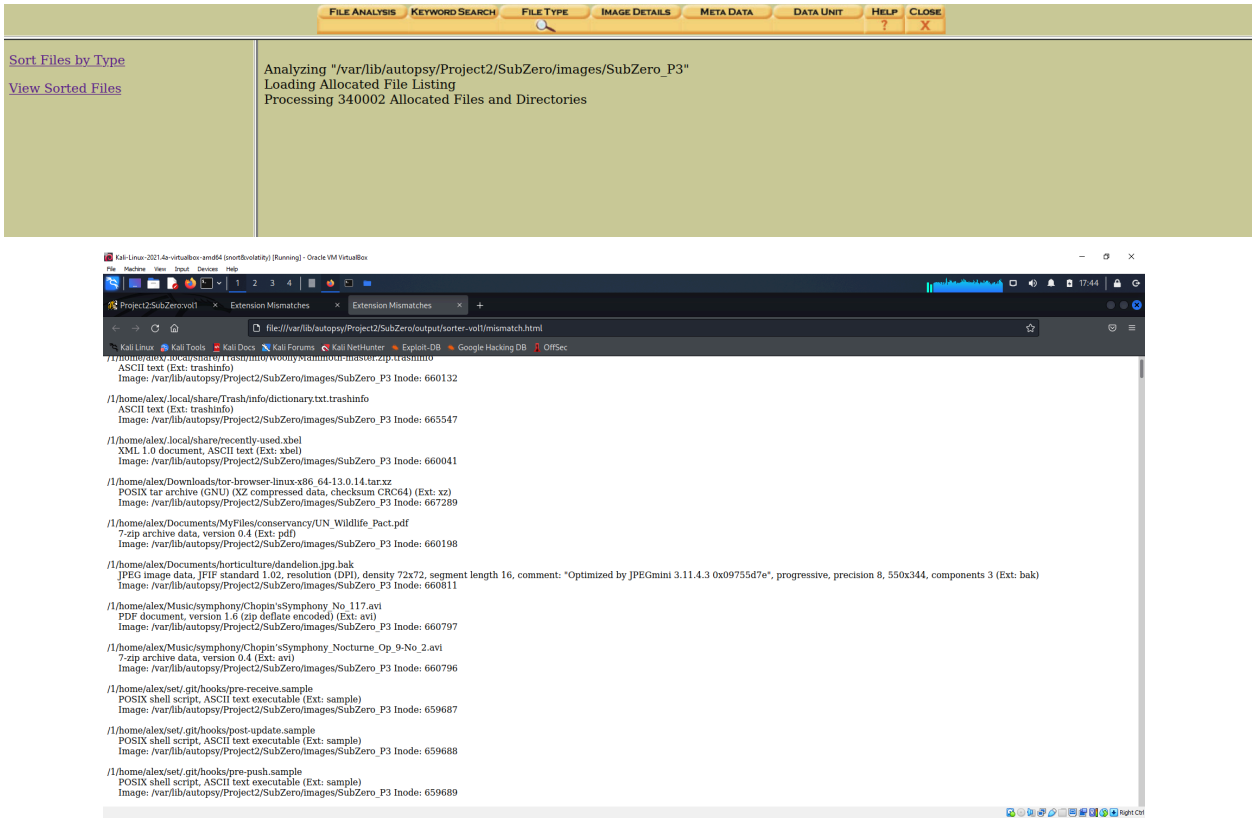


Figure 15: FileType and Mismatch.html file contents.

Therefore, this will be the beginning point of our investigation. In the figure above, four explicit files pique our interest as they are labelled mismatched. These files are UN_Wildlife_Pact.pdf, dandelion.jpg.bak, Chopin'sSymphony_No_117.avi, and Chopin'sSymphony_Nocturne_Op_9-No_2.avi. Considering UN_Wildlife_Pact.pdf, we decided to compare the Hex contents of our suspicious file to the other PDFs in the directory. As shown in Figure 16, we see it begins with the Hex codes 377A BCAF 271C, which we know from [3] represent 7z file formats, further perpetuated by the datatype noted in the mismatch.html file.

```
Hex Contents Of File: /1/home/alex/Documents/MyFiles/conservancy/The Legal Framework of the Endangered Species Act (ESA).pdf


00000000:  2550 4446 2D31 2E35 0D25 E2E3 CFD3 0D0A    %PDF-1.5.%......
00000010:  3538 2030 206F 626A 0D3C 3C2F 4C69 6E65    58 0 obj.<</Line
00000020:  6172 697A 6564 2031 2F4C 2033 3038 3736    arized 1/L 30876
00000030:  392F 4F20 3630 2F45 2031 3533 3531 362F    9/O 60/E 153516/
00000040:  4E20 322F 5420 3330 3834 3337 2F48 205B    N 2/T 308437/H [
00000050:  2034 3938 2032 3134 5D3E 3E0D 656E 646F     498 214]>>.endo
00000060:  626A 0D20 2020 2020 2020 2020 2020 2020    bj.
```

```
Hex Contents Of File: /1/home/alex/Documents/MyFiles/conservancy/UN_Wildlife_Pact.pdf


00000000:  377A BCAF 271C 0004 A868 0267 7818 0600    7z..'....h.gx...
00000010:  0000 0000 2400 0000 0000 0000 AFF2 71E0    ....$.........q.
00000020:  D103 9E79 52FD 97BE 42F8 90A8 9A7C 92E8    ...yR...B....|..
00000030:  B599 25BE 67C8 8CD1 3EEB 6456 B3DA D3C3    ..%.g...>.dV....
00000040:  FCF7 6454 80F1 0540 18EB D837 14C5 0EF4    ..dT...@...7....
00000050:  A065 F281 3AAC 0CF3 BE36 1975 A071 DAE0    .e..:....6.u.q..
00000060:  9003 0718 B0C7 1F8C E106 FB19 4313 D088    ............C...
00000070:  89AF 4AB1 CBB3 56B5 0F25 A5D2 9FF8 4F2A    ..J...V..%....O*
00000080:  5621 4D23 1402 AB26 D514 7DCF C32D DD14    V!M#...&..}..-..
00000090:  D0A7 AFA8 AF13 78D0 BFDA 1E11 9DAD 8D2E    ......x.........
000000A0:  187C 1CE5 1E0F 7567 1797 8A1F 0495 49A8    .|....ug......I.
```

Figure 16: Comparison between Hex Contents of 'UN_Wildlife_Pact.pdf'

In the Music directory, we also found the 7z-encoded file Chopin'sSymphony_Nocturne_Op_9-No_2.avi masking as an AVI file, as shown in Figure 17.

```
Hex Contents Of File: /1/home/alex/Music/symphony/Chopin'sSymphony_Nocturne_Op_9-No_2.avi


00000000:  377A BCAF 271C 0004 951E 9EC1 C87C 0000    7z..'........|..
00000010:  0000 0000 2400 0000 0000 0000 A405 FC53    ....$..........S
00000020:  31A5 B5B2 50FC 49F8 1589 E083 856E 1EC9    1...P.I......n..
00000030:  F448 C824 920D 1111 EA40 5D51 27C4 1203    .H.$.....@]Q'...
00000040:  4A5D 4ABA 08A9 E166 6EDE 5C7C 0F54 AF19    J]J....fn.\|.T..
00000050:  4671 1728 836A C93E 6886 816C FD4E 1E4F    Fq.(.j.>h..l.N.O
00000060:  1C78 12D2 D24D 646F 355C 9A9F 4438 6838    .x...Mdo5\..D8h8
00000070:  517B 1CFE 365F EDFE D819 05A7 9CDA 81E1    Q{..6 ..........
```

Figure 17: 7z file masking as an avi file.

Also, in the music directory, we have 'Chopin'sSymphony_No_117.avi,' noted as a PDF document in the mismatch.html and further perpetuated by Figure 18 showing the file hex contents starting with the PDF magic numbers.

```
Hex Contents Of File: /1/home/alex/Music/symphony/Chopin'sSymphony_No_117.avi


00000000:  2550 4446 2D31 2E36 0D25 E2E3 CFD3 0D0A    %PDF-1.6.%......
00000010:  3331 2030 206F 626A 0D3C 3C2F 4669 6C74    31 0 obj.<</Filt
00000020:  6572 2F46 6C61 7465 4465 636F 6465 2F46    er/FlateDecode/F
00000030:  6972 7374 2035 2F4C 656E 6774 6820 3539    irst 5/Length 59
00000040:  2F4E 2031 2F54 7970 652F 4F62 6A53 746D    /N 1/Type/ObjStm
00000050:  3E3E 7374 7265 616D 0D0A 68DE 3234 5730    >>stream..h.24W0
00000060:  50B0 B1D1 0F28 CA4F 0E4E 2D89 D60F 7071    P....(.O.N-...pq
00000070:  D3F7 CC4D 4C4F 758E D58F F04F CA4A 4D2E    ...MLOu....O.JM.
00000080:  014A 7BE6 1A28 1803 5506 D901 0140 8001    .J{..(..U....@..
00000090:  008E AB0E CE0D 0A65 6E64 7374 7265 616D    .......endstream
000000A0:  0D65 6E64 6F62 6A0D 3332 2030 206F 626A    .endobj.32 0 obj
```

Figure 18: Hex contents of Chopin'sSymphony_No_117.avi.

As we know, we use the magic numbers of the files. We can export them from Autopsy and rename them on our system with the terminator '.7z' and '.pdf' so that they are converted to 7zip compressed files and PDF files and can be opened from our system, as shown in Figure 19.

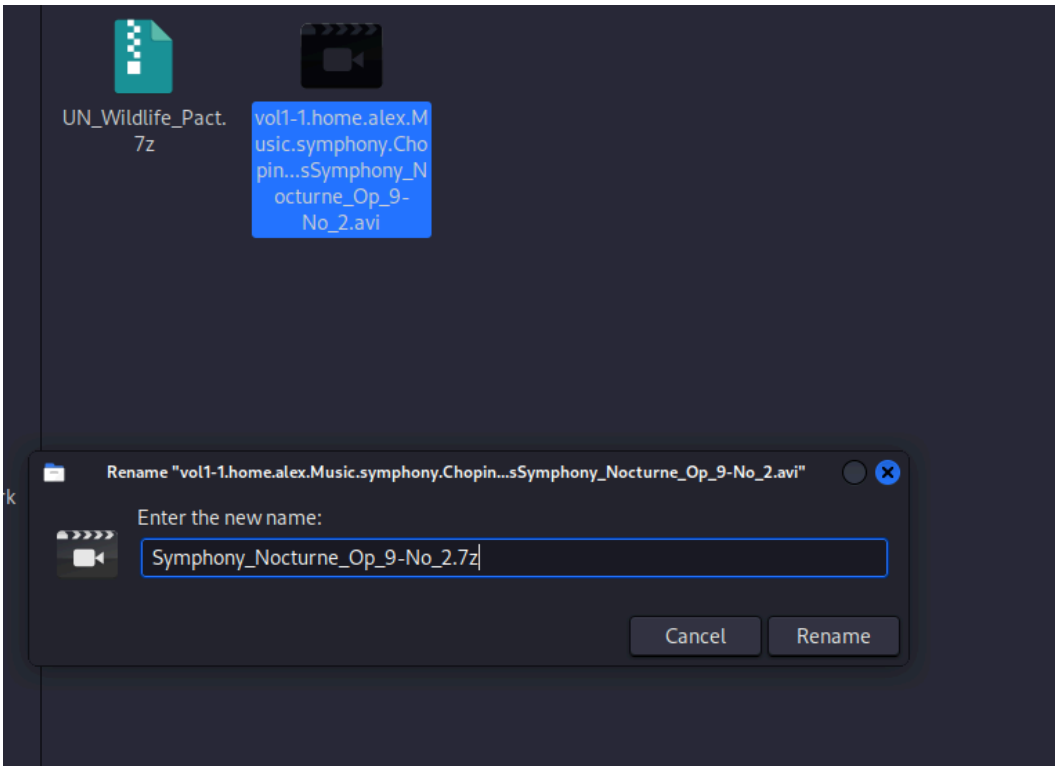


Figure 19: Converting renamed files to 7zip format.

After saving the files, we can investigate them further, as shown in Figure 20. Within the archives, we find a BINANCE account statement PDF and a crypto ledger spreadsheet, both password-locked and unable to be accessed at this investigation stage.

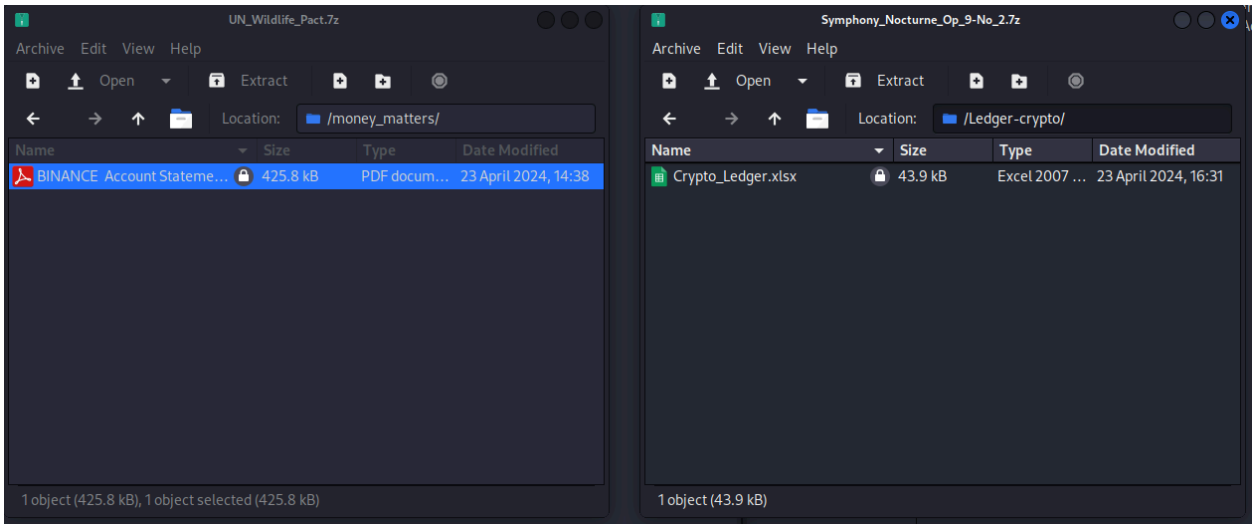


Figure 20: Contents of 7zip files.

Unlike the other two files, the hidden Chopin'sSymphony_No_117.PDF file is not password-locked; therefore, we can see its contents in Figure 21. The figure shows that the PDF contains a simple signature.

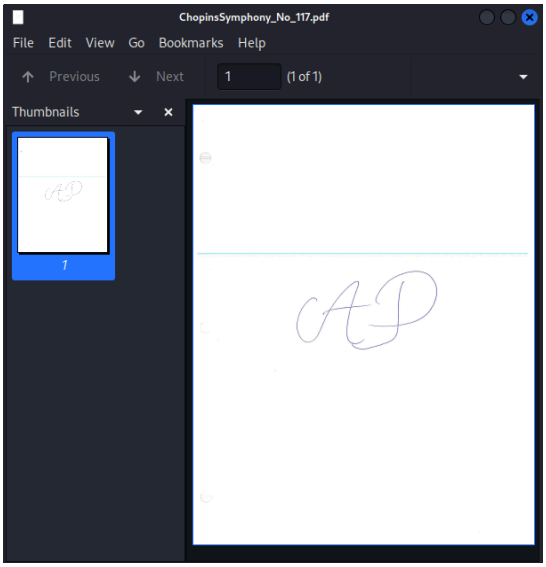


Figure 21: Contents of Chopin'sSymphony_No_117.pdf.

As we do not yet have the passwords for the locked files, we must turn our attention elsewhere to locate them. Returning to our search for files whose magic numbers do not match the file type, we have one more initially suspicious file to examine before searching through our mismatch.html file again. This file is 'dandelion.jpg.bak'. The mismatch.html file only notes that it contains jpg data, which is truthful as it is a backup of an image file. However, we wanted to review the file content to ensure we covered all our bases. In Figure 22, we examine the Hex content of the file with FTKImager, and we notice that appended to the end of it, there is a peculiar string, "C00kstr$$t," which logically does not align with the formatting of JPG imagery. Therefore, we will assume that this string is some kind of password.

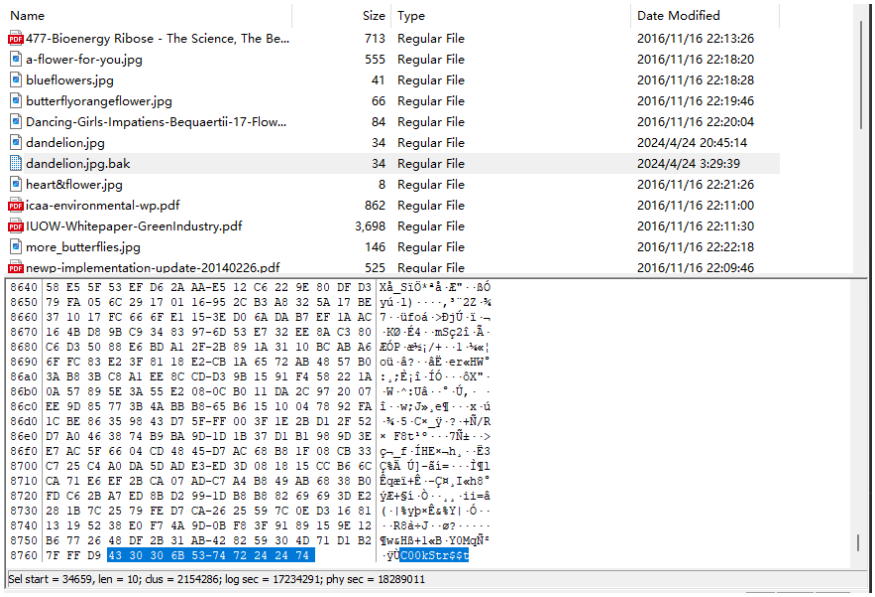


Figure 22: FTKImager view of Hex content for dandelion.jpg.bak.

Assuming the string is a password, we will enter it as a key for the encrypted archives we have accessed. Fortunately, ‘Chopin’sSymphony_Nocturne_Op_9-No_2.7z’ utilized this password, and upon opening it, we can access the Crypto_Ledger.xlsx, as shown in Figure 23. This ledger shows the suspect's transactional history on crypto trading sites, alluding to some money laundering through crypto as the spreadsheet shows large sums of currency being traded.

Figure 23: Crypto ledger Spreadsheet.

Now that we have examined all the initially suspicious files, we return to our ‘mismatch.html’ file type and continue to search through the notable mismatched files to find other suspicious candidates. This leads us to README.txt, as shown in Figure 24, which describes the file content as a tar archive.

/1/home/alex/calculator/README.txt
POSIX tar archive (GNU) (gzip compressed data, from Unix) (Ext: txt)
Image: /var/lib/autopsy/Project2/SubZero/images/SubZero_P3 Inode: 660830

Figure 24: README.txt mismatch info.

Similarly to the prior files, we extract README.txt into a directory on our Kali system, change the file terminator to ‘.tar,’ and see the file's true contents. As shown in Figure 25, we can see that the archive contains a .crypto file encrypted by the MacPaw encrypto application.[4]

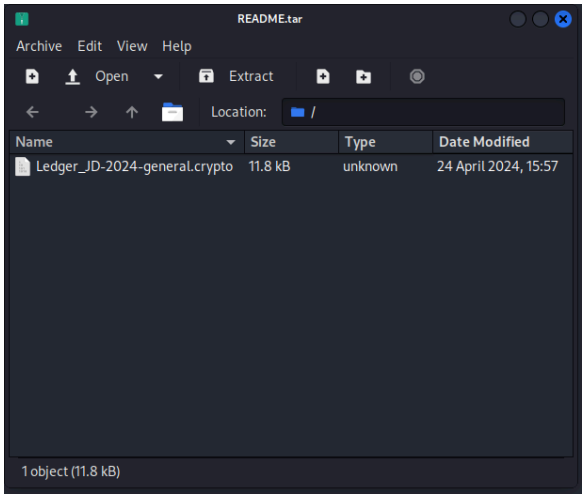


Figure 25: Contents of README.tar

Extracting the .crypto file and moving over to the Encrypto app shown in Figure 26, we can see that there is a hint associated with decrypting the file, which is, in fact, a riddle.

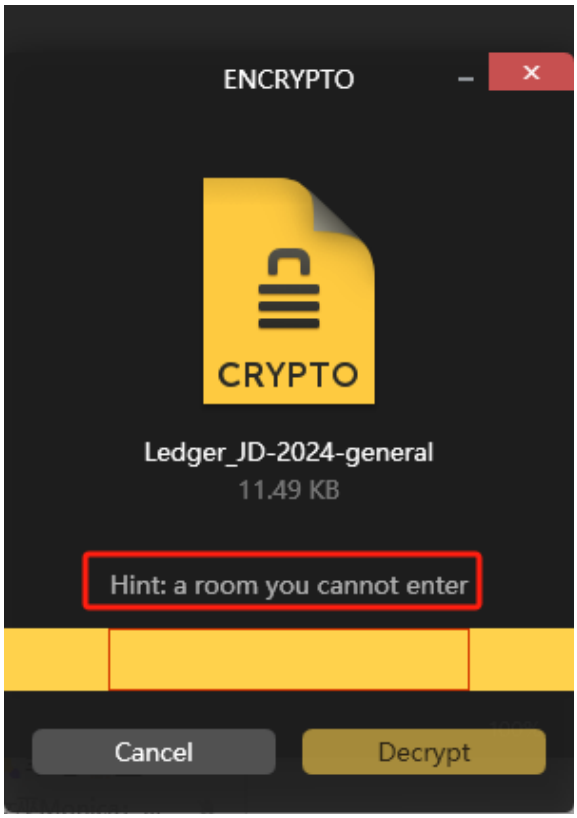


Figure 26: Encrypto app with hint.

We can solve this riddle by simply entering a Google search. As shown in [5], the answer is mushroom. By entering this into the app and selecting decrypt, we can see, as shown in Figure 27, a ledger recording ransom payments, payments for various services and the distribution of shares between accomplices.

JD LEDGER
Jan 1, 2023 - Apr 01,2024

Opening Balance: $350,000.00

Date	Reference	Account	Explanation	Credit	Debit	Balance
				##########	##########	$611,651.00
1/1/2023	1021	Revenue	Ransom payment - LiveLong Hospit	$337,952.00		$687,952.00
1/2/2023	1621	Liabilities	Yuri's share		$160,000.00	$527,952.00
1/3/2023	1002	Expenses	Evgenys's share		$150,000.00	$377,952.00
1/4/2023	210	Assets	Ransom payment - Dreamware App	$213,423.00		$591,375.00
1/5/2023	200	Liabilities	Hosting services		$90,000.00	$501,375.00
1-6-2023	1021	Revenue	Ransom payment - BetaKits	$209,806.00		$711,181.00
1-7-2023	1002	Expenses	Supply - Butagogo		$250,000.00	$461,181.00
1-9-2023	1002	Expenses	Supply - Amazon RF		$80,000.00	$381,181.00
1-11-2021	1021	Revenue	Ransom payment - Uniform Bank	$384,330.00		$765,511.00
1-12-2023	1621	Liabilities	Yuri's share		$180,000.00	$585,511.00
1/1/2024	1002	Liabilities	Evgeny's share		$150,000.00	$435,511.00
2/1/2024	1005	Liabilities	Ransom payment - Jam Hydro	$386,140.00		$821,651.00
3/1/2024	1003	Liabilities	Sapienza's share		$100,000.00	$721,651.00
4/1/2024	200	Liabilities	Hosting services		$110,000.00	

Types of Account	DR/CR
Assets	DR
Liabilities	DR
Revenue	CR
Expenses	DR
Capital	CR

2024/4/1

Figure 27: Ledger_JD-2024-general contents.

After this point, we have no more pertinent information relative to the ‘mismatch.html’ file. Therefore, we must pursue different methods to uncover any remaining hidden files and the final password for the encrypted PDF document in ‘UN_Wildlife_Pact.7z’. Given the sheer volume of images in the Alex/documents/horticulture/ and Alex/Pictures/nature/ directories, we are to assume some steganographic hidden message may be embedded within the pictures. This suspicion is further perpetuated by the suspect looking into creating a horticulture-based website and uploading images with embedded messages to that site, which could be an effective means of communication. Using FTKimager to download each of the photos and QuickStego, as shown in Figure 28, we were able to siphon through all of the images, and all were clear except for ‘Iguazu-Falls.bmp,’ which contains within it the hint message associated with the .crypto file found in the earlier paragraphs.

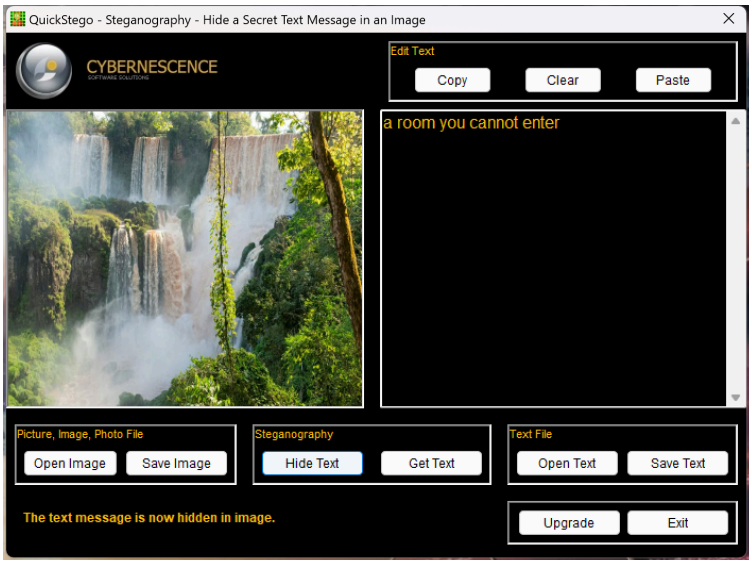


Figure 28: QuickStego of Iguazu-Falls.bmp.

As this yielded no additional passwords, we moved on to a different method. While we have truthfully exhausted the file type search using ‘mismatch.html,’ we have another file we can search through, shown in Figure 29, depicting the ‘unknown.html’ file type search.

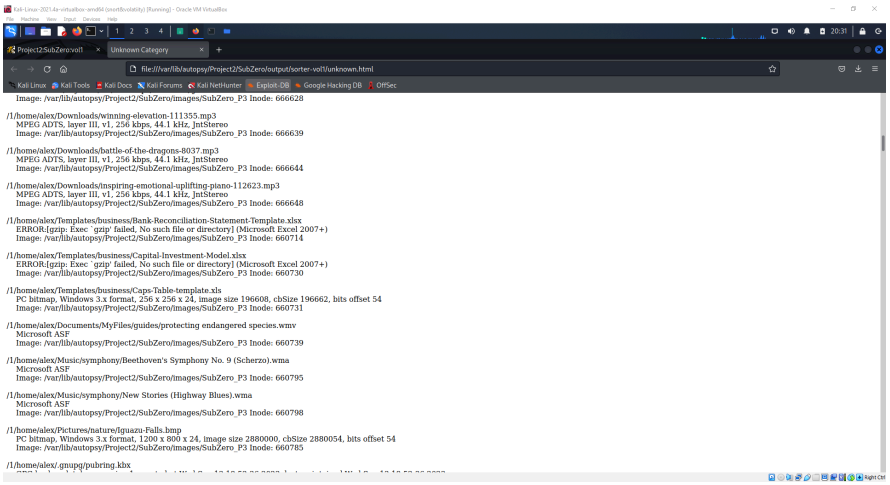


Figure 29: ‘unknown.html’ file type search document.

While performing this exhaustive search, we were trying to locate any unknown files whose file terminator does not match the file type noted. While searching, as shown in Figure 30, we found a peculiar instance. In the directory /Alex/Templates/business/, there is a file Caps-Table-template.xls, which has been noted to contain a PC bitmap. Yet the image Iguazu-Falls.bmp is also reported as a PC bitmap in the Figure. Given that these two files have different file terminators, and we know that Iguazu-Falls is a readable image as shown above through QuickStego, we can assume that Caps-Table-template.xls is incorrectly labelled and is truthfully a ‘.bmp’ file.

```
/1/home/alex/Templates/business/Caps-Table-template.xls
   PC bitmap, Windows 3.x format, 256 x 256 x 24, image size 196608, cbSize 196662, bits offset 54
   Image: /var/lib/autopsy/Project2/SubZero/images/SubZero_P3 Inode: 660731

/1/home/alex/Documents/MyFiles/guides/protecting endangered species.wmv
   Microsoft ASF
   Image: /var/lib/autopsy/Project2/SubZero/images/SubZero_P3 Inode: 660739

/1/home/alex/Music/symphony/Beethoven's Symphony No. 9 (Scherzo).wma
   Microsoft ASF
   Image: /var/lib/autopsy/Project2/SubZero/images/SubZero_P3 Inode: 660795

/1/home/alex/Music/symphony/New Stories (Highway Blues).wma
   Microsoft ASF
   Image: /var/lib/autopsy/Project2/SubZero/images/SubZero_P3 Inode: 660798

/1/home/alex/Pictures/nature/Iguazu-Falls.bmp
   PC bitmap, Windows 3.x format, 1200 x 800 x 24, image size 2880000, cbSize 2880054, bits offset 54
   Image: /var/lib/autopsy/Project2/SubZero/images/SubZero_P3 Inode: 660785
```

Figure 30: ‘Unknown.html’ contents with peculiar file data.

Exporting and renaming ‘Caps-Table-template.xls’ to ‘Caps-Table-template.bmp’ reveals an image as shown in Figure 31.

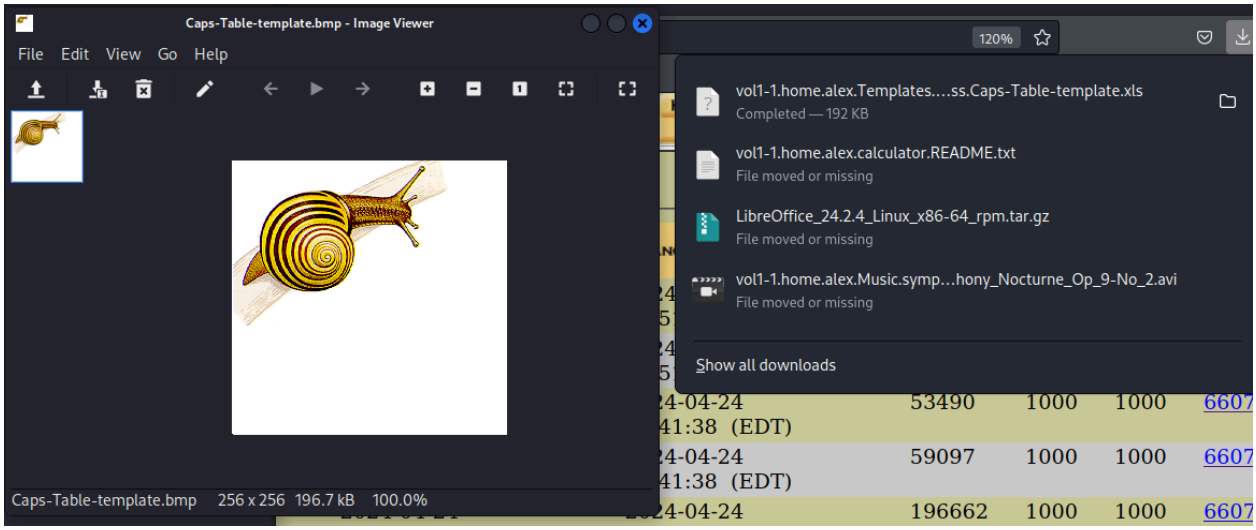


Figure 31: bmp image contents.

The image alone does not reveal any additional information. However, given that steganographic messages can be embedded within any image, we can use QuickStego again to reveal hidden messages. Therefore, as shown in Figure 32, this image has a message embedded within it: ‘H@z$l&P!ckle,’ which may be the last remaining password needed to complete our investigation.

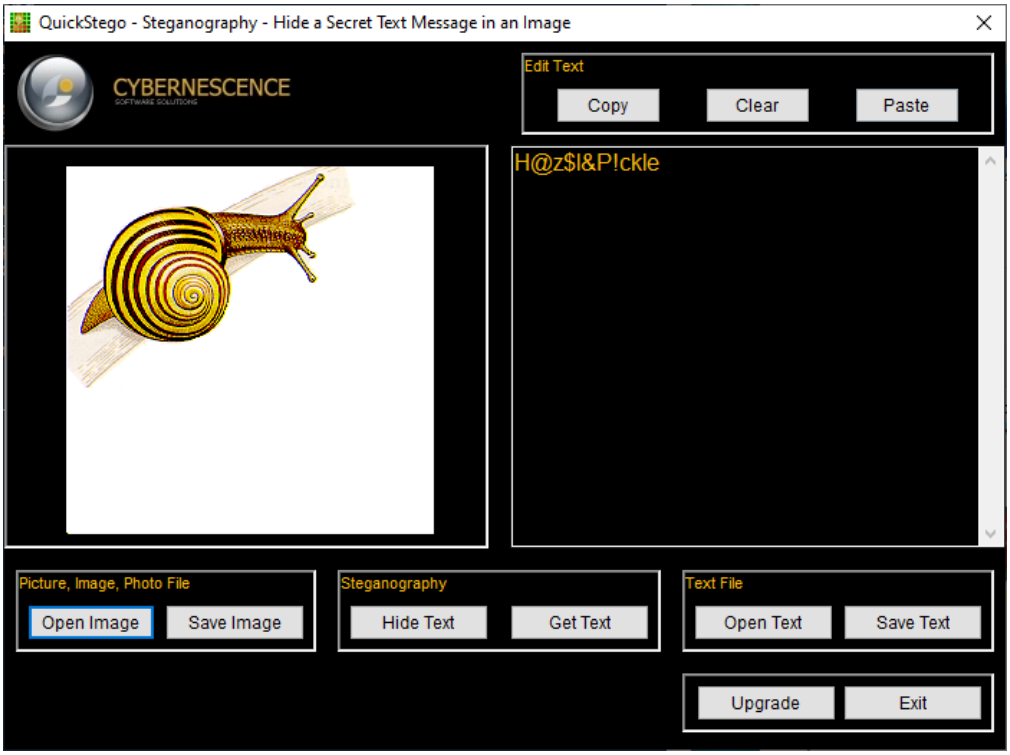


Figure 32: QuickStego revealing the assumed password.

Fortunately, our assumptions are correct again. Entering this password into the archive extracts the contents, revealing the unencrypted Binance account statement, as shown in Figure 33. Thus, we can decrypt all files we have received.

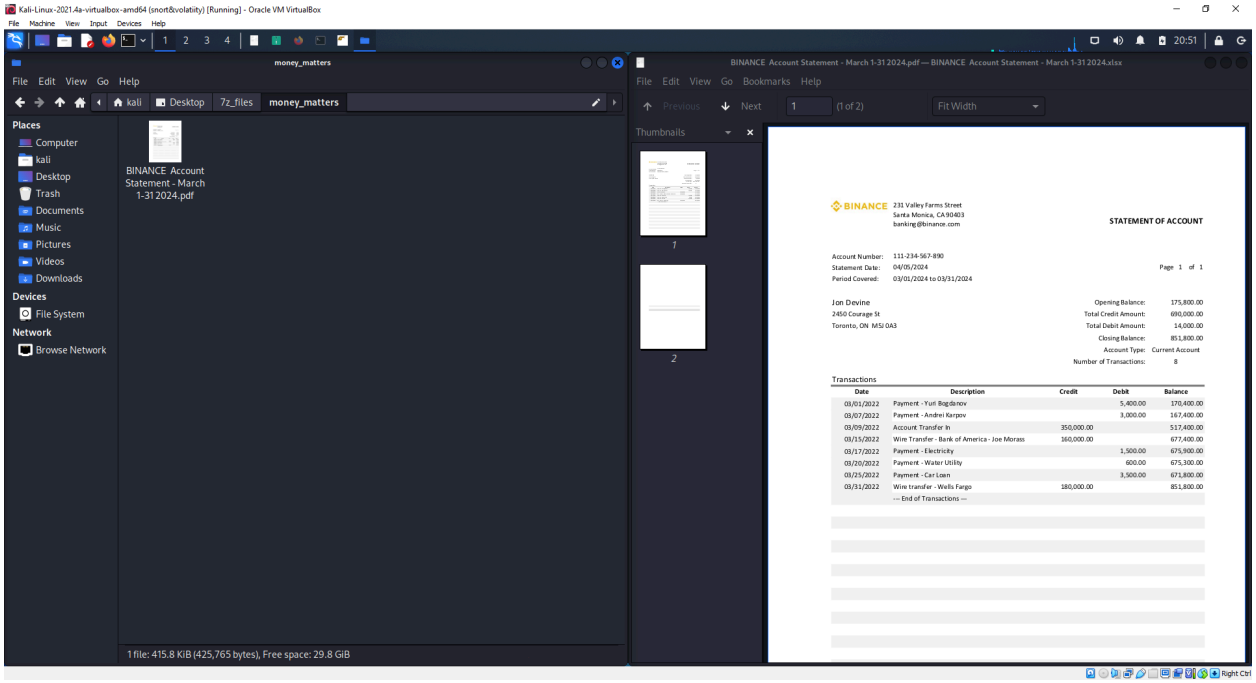


Figure 33: Decrypted archive and financial statement.

BINANCE 231 Valley Farms Street
Santa Monica, CA 90403
banking@binance.com

STATEMENT OF ACCOUNT

Account Number: 111-234-567-890
Statement Date: 04/05/2024
Period Covered: 03/01/2024 to 03/31/2024

Page 1 of 1

Jon Devine
2450 Courage St
Toronto, ON M5J 0A3

Opening Balance:	175,800.00
Total Credit Amount:	690,000.00
Total Debit Amount:	14,000.00
Closing Balance:	851,800.00
Account Type:	Current Account
Number of Transactions:	8

Transactions

Date	Description	Credit	Debit	Balance
03/01/2022	Payment - Yuri Bogdanov		5,400.00	170,400.00
03/07/2022	Payment - Andrei Karpov		3,000.00	167,400.00
03/09/2022	Account Transfer In	350,000.00		517,400.00
03/15/2022	Wire Transfer - Bank of America - Joe Morass	160,000.00		677,400.00
03/17/2022	Payment - Electricity		1,500.00	675,900.00
03/20/2022	Payment - Water Utility		600.00	675,300.00
03/25/2022	Payment - Car Loan		3,500.00	671,800.00
03/31/2022	Wire transfer - Wells Fargo	180,000.00		851,800.00
	--- End of Transactions ---			

Figure 34: Statement of Account close-up.

2.3 Investigation Outcome.

Let us recount the evidence we have discovered throughout our investigation, from examining the PC itself to the memory forensics investigation. Upon reviewing the suspect's computer, we noted the peculiar elements in their Firefox search history, alluding to the possession of Bitcoin and installation of root and exploit kits. We also found programs like Nmap, Metasploit, fuzzing tools and brute-force password-cracking algorithms. However, this history is not definitive proof of the suspect's guilt as the history and programs do not actively show an exploit occurring. Moving on from this, we can see the user bash history showing an attempted Ncrack brute-force attack against a user named ‘jacobs.’ Suppose the suspect has no relation to this user and no explicit permission from the entity using this user ID and the associated IP. In that case, this violation can be utilized in a court of law to allude to their blackmail scams as it is a clear attempt to access someone unethically else's property.

The logs and traces we found while examining the PC are also contained within the Disc Image. Therefore, we have an untempered system whose contents can be recorded as evidence. As we investigated the Disc Image, we recovered three archived and locked files whose passwords were hidden throughout the memory. After some sleuthing, we were able to locate the passwords. These three files were a Binance bank account statement, a crypto trading/exchange spreadsheet ledger and a transaction history spreadsheet ledger. These three documents can link the suspect to blackmailing scams and laundering through crypto. For example, we know from the transaction history spreadsheet that there was a ransom payment for a company called Dreamware on April 1st, 2023, for the cost of $213,423.00. Looking at the Crypto trading ledger, we can see a transaction to sell Bitcoin for the same price, acquiring the suspect and their accomplices the ransom funds on the same date. This is further perpetuated by the Binance account statement. While this statement is dated outside the range for the spreadsheets and ledgers, we can see a payment to a suspected accomplice named Yuri Bogdanov, which may be the same Yuri addressed in the transaction history document, although this is pure speculation.

Given this evidence of logs, transaction histories and statements, we have a substantial case against the suspect. Suppose this evidence were to be submitted to a court of law. In that case, we believe it would lead to a conviction of the suspect as we have found detailed accounts of the actions taken by the suspect concerning crypto laundering and blackmailing/hacking scams. Of course, this information could be further perpetuated by additional evidence, such as reports from the companies the suspect targeted stating the exact monetary amounts they were required to pay and methods used to submit them in hopes of forming an additional paper trail back to the suspect and their strategies for exploiting businesses.

References

[1] "The Tor Project: Privacy & Freedom Online," Tor Project | Anonymity Online, https://www.torproject.org/ (accessed Jun. 21, 2024).

[2] ins1gn1a, "INS1GN1A/Woollymammoth: Toolkit for manual buffer exploitation, which features a basic network socket fuzzer, offset pattern generator and detector, bad character identifier, Shellcode Carver, and a vanilla eip exploiter," GitHub, https://github.com/ins1gn1a/WoollyMammoth/tree/master (accessed Jun. 21, 2024).

[3] Ph. D. Gary C. Kessler, File signatures, https://www.garykessler.net/library/file_sigs.html (accessed Jun. 21, 2024).

[4] "Encrypto: Encrypt your files before sending them to friends or coworkers," MacPaw, https://macpaw.com/encrypto (accessed Jun. 21, 2024).

[5] R/dmacademy on Reddit: "You cannot enter this room" - riddles: Easy for kids, hard for adults., https://www.reddit.com/r/DMAcademy/comments/o5c1m4/you_cannot_enter_this_room_riddles_easy_for_kids/ (accessed Jun. 21, 2024).