Cyber Forensics and Incident Response

Course code: MMI126272 & MMI125225

Case Title: Digital Forensics Investigation Report

Case Name: Case No. APL-CCF-007

Word count: 2751

Student Name: Siddhi Dilip Ghag

Student Number: S2443066

Disclaimer:

"This piece of coursework is our own original work and has not been submitted elsewhere in fulfillment of the requirement of this or any other award"

Table of Content

1. Background

This document presents the outcomes derived from a digital forensic investigation on George Bernard, a 35-year-old software developer believed to be operating a credit card fraud ring. During an enforcement operation, several items of digital evidence were collected, which comprised a hard drive image (.dd) alongside a mobile phone extraction (.xry) and a suspicious executable file (.exe). This particular examination aimed at analyzing the foregoing artifacts to establish any fraudulent schemes.

2. Executive Summary

Following internationally accepted standards on digital forensic analysis [1], this investigation evaluation document consists of the following findings and evidence in question:

- ***Hard Drive Analysis:*** Retrieved deleted files containing sensitive credit card information, noted installed privacy applications (Tor, VPN), and found evidence of cryptocurrency activities [2]. Hash checksum was obtained during data acquisition.
- ***Mobile Device Analysis:*** Identified communications indicating job sharing with a counterpart ("Danny") along with browsing activity concerning illegal financial activities [3].
- ***Malware Sample:*** The file was identified as a UPX-packed Trojan (Trojan.Zusy), employing process injection for stealthy evasion of detection [4][5].

2.1 Techniques for Preservation

2.1.1. *Table1:File Integrity Check Techniques*

Technique	Method
Hash Verification	Verified file integrity using MD5, SHA1, and SHA256 algorithms [6]
Chain of Custody	Documented every transfer or interaction with evidence to maintain integrity
Read-only Analysis	Ensured analysis tools did not alter original files [1]

2.1.2. *Table 2: Tools used for the Analysis*

Tools	Version	Purpose
Autopsy	4.21.0	Conducted forensic analysis on the hard drive[2]
HashCal	Latest	Used to calculate file hashes[6]
Xamn	7.7.0	Analyzed mobile phone extraction[3]
Process Hacker 2	2.39.124	Carried out static analysis of executable[4]
Pestudio	9.58	Monitored processes during runtime[7]
APIMiner	1.0.0	Tracked API calls for behavioral malware analysis[5]

2.2 Chain of Custody Documentation

Throughout the investigation, all procedures designed to maintain the integrity of custody were followed to ensure that any digital evidence obtained would remain uncontaminated and usable in a court of law. The first step was to obtain the Android model .xry image file, which was precisely described and enclosed. After this, all interactions with the evidence were logged to ensure that no unauthorized actions were performed, and the data was accessed using the Autopsy tool. Interaction with the hard drive image was equally monitored and logged.

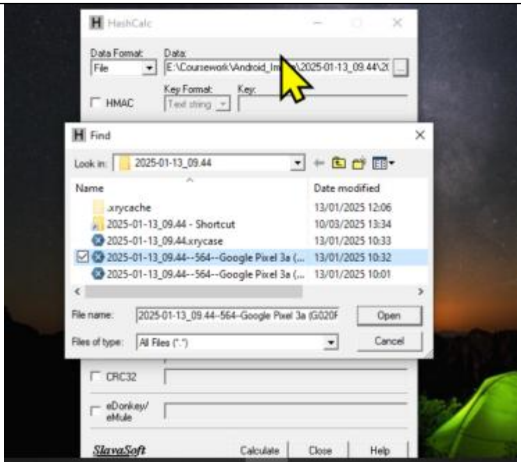
All interactions with devices and databases were passed through the XAMN tool before the evidence was presented regarding the relevant mobile device's data, such as contacts, messages, and browsing history. All examinations performed and actions taken during interactions with the device were logged.

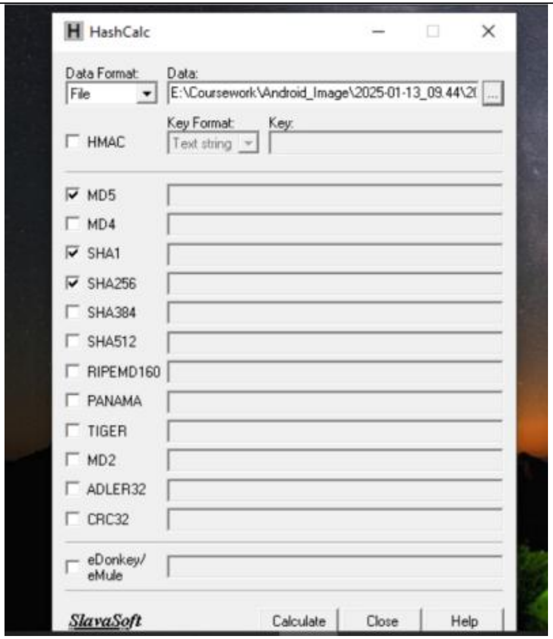
Suspicious PE files were subjected to both static and dynamic analysis where relevant information was collected using read-only modes. Each step taken was precisely timestamped and those responsible for each individual action were logged in detail including the actions they performed, when, and for what reason. Such a detailed approach at each stage of the court presentation and investigation ensures that the evidence is valid and reliable.

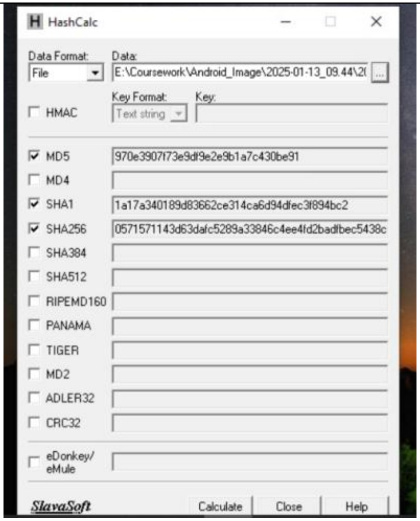
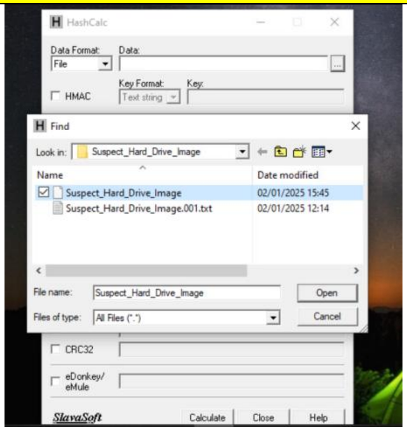
3. Technical Report

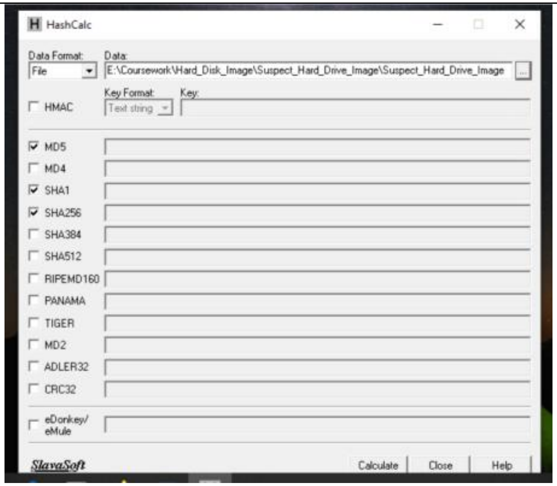
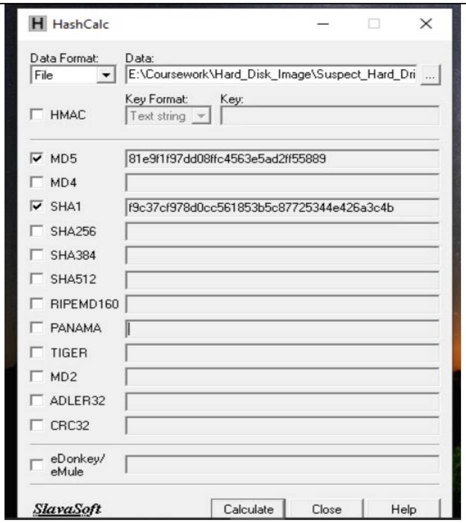
This section present the analysis and evidence as shown in the table. Provide a description of the analysis methods that were used, and also explain the findings of the analysis. Include proof of your findings, such as screenshots and commands (tables make the report more readable and concise). It is important that the evidence provide enough information for the reader to understand the incident completely

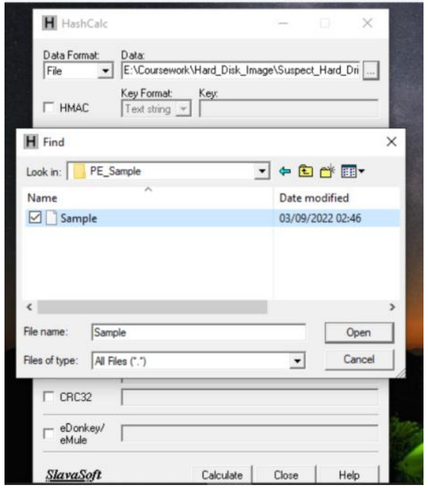
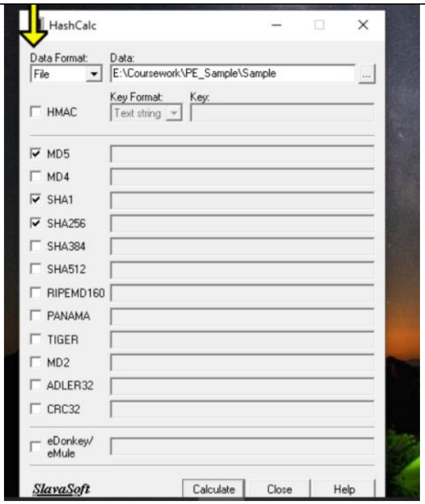
3.1. Table 3: Shows the process used for the Hard drive analysis, PE file and Android Image.*File integrity check using Hashcal*

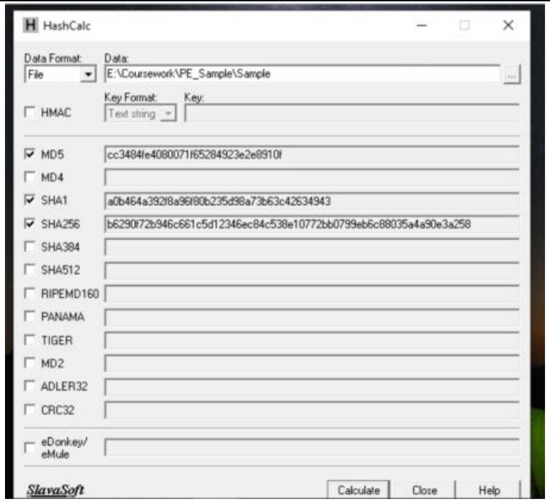
Date/ time	Process	Evidence
Android Image Analysis		
13:34 10-03-2025	Launch Hashcal	
13:41 10-03-2025	Select file format as File	 HashCalc Data Format: File Data: E:\Coursework\Android_Im \2025-01-13_09.44\2(□ HMAC Key Format: Text string Key: Find Look in: 2025-01-13_09.44 Name / Date modified .xrycache 13/01/2025 12:06 2025-01-13_09.44 - Shortcut 10/03/2025 13:34 2025-01-13_09.44.xrycase 13/01/2025 10:33 ☑ 2025-01-13_09.44--564--Google Pixel 3a (... 13/01/2025 10:32 2025-01-13_09.44--564--Google Pixel 3a (... 13/01/2025 10:01 File name: 2025-01-13_09.44--564--Google Pixel 3a (G020F Files of type: All Files (*.*) Open Cancel □ CRC32 □ eDonkey/ eMule SlavaSoft Calculate Close Help
	Upload file in hashcal from location E:\Coursework\Android_Image\2025-01-13_09.44\2025-01-13_09.44--564--Google Pixel 3a (G020F).xry	

13:43 10-03-2025	Select algorithm MD5 , SHA1 and SHA256	 HashCalc Data Format: File Data: E:\Coursework\Android_Image\2025-01-13_09.44\2(□ HMAC Key Format: Text string Key: ☑ MD5 □ MD4 ☑ SHA1 ☑ SHA256 □ SHA384 □ SHA512 □ RIPEMD160 □ PANAMA □ TIGER □ MD2 □ ADLER32 □ CRC32 □ eDonkey/ eMule SlavaSoft Calculate Close Help
	Click on Calculate button	

13:51 10-03-2025	Computed Hash value will be generated MD5: 970e3907f73e9df9e2e9b1a7c430be91 SHA1: 1a17a340189d83662ce314ca6d94dfec3f894bc2 SHA256: 0571571143d63dafc5289a33846c4ee4fd2badfbec5438c5fbed2fbf185b569f	 HashCalc Data Format: File Data: E:\Coursework\Android_Image\2025-01-13_09.44\2(☐ HMAC Key Format: Text string Key: ☑ MD5 970e3907f73e9df9e2e9b1a7c430be91 ☐ MD4 ☑ SHA1 1a17a340189d83662ce314ca6d94dfec3f894bc2 ☑ SHA256 0571571143d63dafc5289a33846c4ee4fd2badfbec5438c ☐ SHA384 ☐ SHA512 ☐ RIPEMD160 ☐ PANAMA ☐ TIGER ☐ MD2 ☐ ADLER32 ☐ CRC32 ☐ eDonkey/ eMule
Hard Drive Image		
13:53 10-03-2025	Select file format as File	 HashCalc Data Format: File Data: ☐ HMAC Key Format: Text string Key: Find Look in: Suspect_Hard_Drive_Image Name / Date modified ☑ Suspect_Hard_Drive_Image 02/01/2025 15:45 Suspect_Hard_Drive_Image.001.txt 02/01/2025 12:14 File name: Suspect_Hard_Drive_Image Files of type: All Files (*.*) ☐ CRC32 ☐ eDonkey/ eMule
	Upload file in hashcal from location E:\Coursework\Hard_Disk_Image\Suspect_Hard_Drive_Image\Suspect_Hard_Drive_Image	

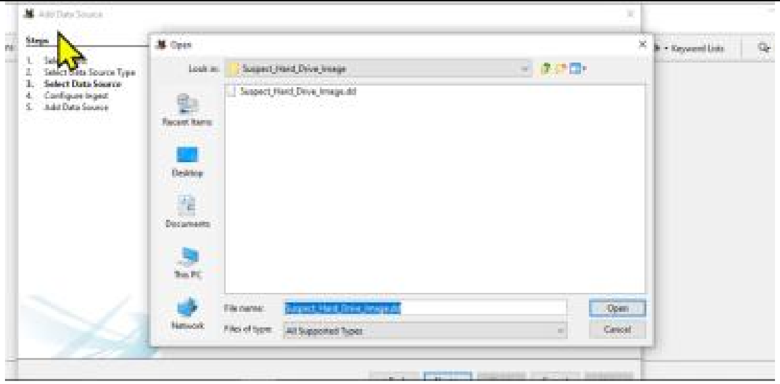
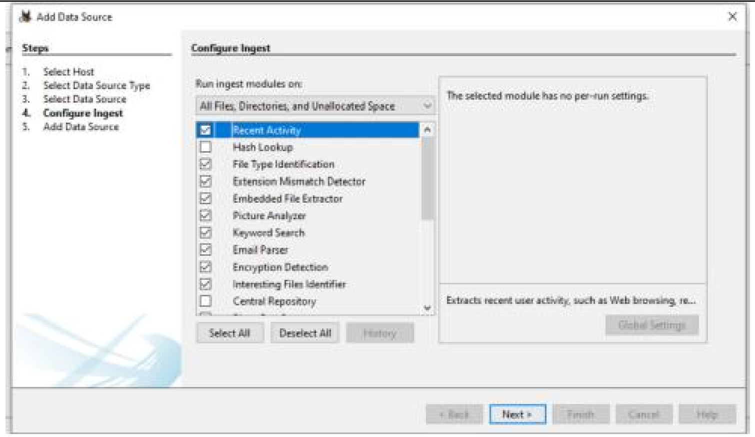
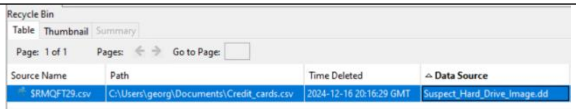
13:55 10-03-2025	Select algorithm MD5 , SHA1 Click on Calculate button	 HashCalc Data Format: File Data: E:\Coursework\Hard_Disk_Image\Suspect_Hard_Drive_Image\Suspect_Hard_Drive_Image ☐ HMAC Key Format: Text string Key: ☑ MD5 ☐ MD4 ☑ SHA1 ☑ SHA256 ☐ SHA384 ☐ SHA512 ☐ RIPEMD160 ☐ PANAMA ☐ TIGER ☐ MD2 ☐ ADLER32 ☐ CRC32 ☐ eDonkey/ eMule
14:15 10-03-2025	Computed Hash value will be generated MD5 checksum: 81e9f1f97dd08ffc4563e5ad2ff55889 SHA1 checksum: f9c37cf978d0cc561853b5c87725344e426a3c4b	 HashCalc Data Format: File Data: E:\Coursework\Hard_Disk_Image\Suspect_Hard_Dri ☐ HMAC Key Format: Text string Key: ☑ MD5 81e9f1f97dd08ffc4563e5ad2ff55889 ☐ MD4 ☑ SHA1 f9c37cf978d0cc561853b5c87725344e426a3c4b ☐ SHA256 ☐ SHA384 ☐ SHA512 ☐ RIPEMD160 ☐ PANAMA ☐ TIGER ☐ MD2 ☐ ADLER32 ☐ CRC32 ☐ eDonkey/ eMule

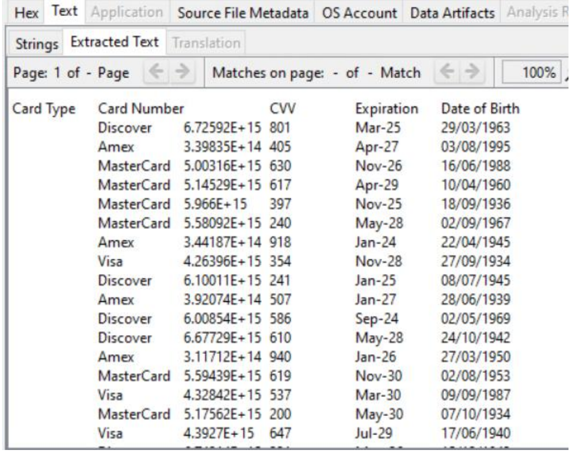
Portable Executable Sample		
14:16 10-03-2025	Select file format as File	 HashCalc Data Format: File Data: E:\Coursework\Hard_Disk_Image\Suspect_Hard_Dri □ HMAC Key Format: Text string Key: Find Look in: PE_Sample Name: ☑ Sample — Date modified: 03/09/2022 02:46 File name: Sample Files of type: All Files (*.*) □ CRC32 □ eDonkey/ eMule
	Upload file in hashcal from location E:\Coursework\PE_Sample\Sample	
14:18 10-03-2025	Select algorithm MD5 , SHA1 and SHA256	 HashCalc Data Format: File Data: E:\Coursework\PE_Sample\Sample □ HMAC Key Format: Text string Key: ☑ MD5 □ MD4 ☑ SHA1 ☑ SHA256 □ SHA384 □ SHA512 □ RIPEMD160 □ PANAMA □ TIGER □ MD2 □ ADLER32 □ CRC32 □ eDonkey/ eMule
	Click on Calculate button	

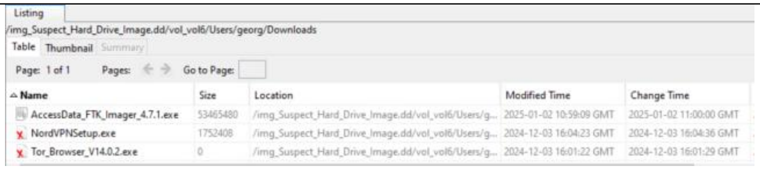
14:20 10-03-2025	Computed Hash value will be generated MD5: cc3484fe4080071f65284923e2e8910f SHA1: a0b464a392f8a96f80b235d98a73b63c42634943 SHA256: b6290f72b946c661c5d12346ec84c538e10772bb0799eb6c88035a4a90e3a258	 HashCalc Data Format: File Data: E:\Coursework\PE_Sample\Sample ☐ HMAC Key Format: Text string Key: ☑ MD5 cc3484fe4080071f65284923e2e8910f ☐ MD4 ☑ SHA1 a0b464a392f8a96f80b235d98a73b63c42634943 ☑ SHA256 b6290f72b946c661c5d12346ec84c538e10772bb0799eb6c88035a4a90e3a258 ☐ SHA384 ☐ SHA512 ☐ RIPEMD160 ☐ PANAMA ☐ TIGER ☐ MD2 ☐ ADLER32 ☐ CRC32 ☐ eDonkey/ eMule SlavaSoft Calculate Close Help

3.2. Table 4: This process show examine a suspect’s storage device *Hard drive image analysis using Autopsy tool* without altering the original data.

Date/time	Process	Evidence
18:09 17-03-2025	Open Autopsy	

18:15 17-03-2025	Select the file from E:\Coursework\Hard_Disk_Image\Suspect_Hard_Drive_Image	 Add Data Source Steps 1. Sel 2. Select Data Source Type 3. **Select Data Source** 4. Configure Ingest 5. Add Data Source Open Look in: Suspect_Hard_Drive_Image Suspect_Hard_Drive_Image.dd File name: Suspect_Hard_Drive_Image.dd Files of type: All Supported Types Recent Items Desktop Documents This PC Network Open Cancel Keyword Lists
18:34 17-03-2025	Selected appropriate Configure Ingest	 Add Data Source Steps 1. Select Host 2. Select Data Source Type 3. Select Data Source 4. **Configure Ingest** 5. Add Data Source **Configure Ingest** Run ingest modules on: All Files, Directories, and Unallocated Space ☑ Recent Activity □ Hash Lookup ☑ File Type Identification ☑ Extension Mismatch Detector ☑ Embedded File Extractor ☑ Picture Analyzer ☑ Keyword Search ☑ Email Parser ☑ Encryption Detection ☑ Interesting Files Identifier □ Central Repository The selected module has no per-run settings. Extracts recent user activity, such as Web browsing, re... Select All Deselect All History Global Settings < Back Next > Finish Cancel Help
19:30 17-03-2025	Credit details of all users excel file found in recycle bin	 Recycle Bin Page: 1 of 1 Pages: Go to Page: Source Name | Path | Time Deleted | **Data Source** $RMQFT29.csv | C:\Users\georg\Documents\Credit_cards.csv | 2024-12-16 20:16:29 GMT | Suspect_Hard_Drive_Image.dd

<table>
<tr>
<td></td>
<td>Csv file has user sensitive details like username, credit card type & number, CVV and DOB</td>
<td>


<table>
<tr><th>Card Type</th><th>Card Number</th><th></th><th>CVV</th><th>Expiration</th><th>Date of Birth</th></tr>
<tr><td></td><td>Discover</td><td>6.72592E+15</td><td>801</td><td>Mar-25</td><td>29/03/1963</td></tr>
<tr><td></td><td>Amex</td><td>3.39835E+14</td><td>405</td><td>Apr-27</td><td>03/08/1995</td></tr>
<tr><td></td><td>MasterCard</td><td>5.00316E+15</td><td>630</td><td>Nov-26</td><td>16/06/1988</td></tr>
<tr><td></td><td>MasterCard</td><td>5.14529E+15</td><td>617</td><td>Apr-29</td><td>10/04/1960</td></tr>
<tr><td></td><td>MasterCard</td><td>5.966E+15</td><td>397</td><td>Nov-25</td><td>18/09/1936</td></tr>
<tr><td></td><td>MasterCard</td><td>5.58092E+15</td><td>240</td><td>May-28</td><td>02/09/1967</td></tr>
<tr><td></td><td>Amex</td><td>3.44187E+14</td><td>918</td><td>Jan-24</td><td>22/04/1945</td></tr>
<tr><td></td><td>Visa</td><td>4.26396E+15</td><td>354</td><td>Nov-28</td><td>27/09/1934</td></tr>
<tr><td></td><td>Discover</td><td>6.10011E+15</td><td>241</td><td>Jan-25</td><td>08/07/1945</td></tr>
<tr><td></td><td>Amex</td><td>3.92074E+14</td><td>507</td><td>Jan-27</td><td>28/06/1939</td></tr>
<tr><td></td><td>Discover</td><td>6.00854E+15</td><td>586</td><td>Sep-24</td><td>02/05/1969</td></tr>
<tr><td></td><td>Discover</td><td>6.67729E+15</td><td>610</td><td>May-28</td><td>24/10/1942</td></tr>
<tr><td></td><td>Amex</td><td>3.11712E+14</td><td>940</td><td>Jan-26</td><td>27/03/1950</td></tr>
<tr><td></td><td>MasterCard</td><td>5.59439E+15</td><td>619</td><td>Nov-30</td><td>02/08/1953</td></tr>
<tr><td></td><td>Visa</td><td>4.32842E+15</td><td>537</td><td>Mar-30</td><td>09/09/1987</td></tr>
<tr><td></td><td>MasterCard</td><td>5.17562E+15</td><td>200</td><td>May-30</td><td>07/10/1934</td></tr>
<tr><td></td><td>Visa</td><td>4.3927E+15</td><td>647</td><td>Jul-29</td><td>17/06/1940</td></tr>
</table>
</td>
</tr>
<tr>
<td>19:50 17-03-2025</td>
<td>Evidence found George has downloaded Tor browser, Nord VPN for accessing dark web</td>
<td>


/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Downloads

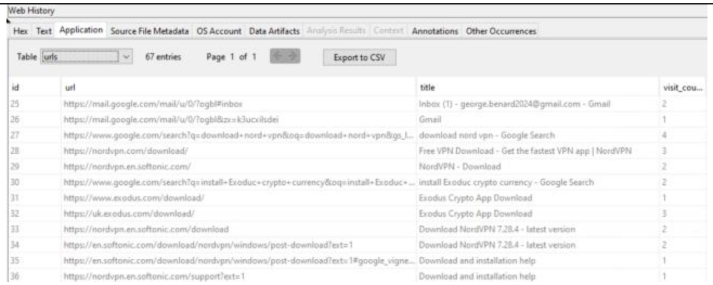
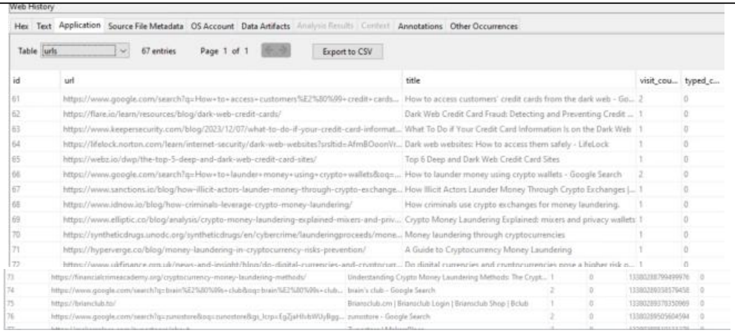
<table>
<tr><th>Name</th><th>Size</th><th>Location</th><th>Modified Time</th><th>Change Time</th></tr>
<tr><td>AccessData_FTK_Imager_4.7.1.exe</td><td>53465480</td><td>/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g...</td><td>2025-01-02 10:59:09 GMT</td><td>2025-01-02 11:00:00 GMT</td></tr>
<tr><td>NordVPNSetup.exe</td><td>1752408</td><td>/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g...</td><td>2024-12-03 16:04:23 GMT</td><td>2024-12-03 16:04:36 GMT</td></tr>
<tr><td>Tor_Browser_V14.0.2.exe</td><td>0</td><td>/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g...</td><td>2024-12-03 16:01:22 GMT</td><td>2024-12-03 16:01:29 GMT</td></tr>
</table>
</td>
</tr>
<tr>
<td>20:15 17-03-2025</td>
<td>Evidence found in web history search on Nord VPN, Exodus (cryptocurrency)</td>
<td>


Table urls 67 entries Page 1 of 1

<table>
<tr><th>id</th><th>url</th><th>title</th><th>visit_cou...</th></tr>
<tr><td>25</td><td>https://mail.google.com/mail/u/0/?ogbl#inbox</td><td>Inbox (1) - george.benard2024@gmail.com - Gmail</td><td>2</td></tr>
<tr><td>26</td><td>https://mail.google.com/mail/u/0/?ogbl&amp;zx=k3ucxilsdei</td><td>Gmail</td><td>1</td></tr>
<tr><td>27</td><td>https://www.google.com/search?q=download+nord+vpn&amp;oq=download+nord+vpn&amp;gs_l...</td><td>download nord vpn - Google Search</td><td>4</td></tr>
<tr><td>28</td><td>https://nordvpn.com/download/</td><td>Free VPN Download - Get the fastest VPN app | NordVPN</td><td>3</td></tr>
<tr><td>29</td><td>https://nordvpn.en.softonic.com/</td><td>NordVPN - Download</td><td>2</td></tr>
<tr><td>30</td><td>https://www.google.com/search?q=install+Exoduc+crypto+currency&amp;oq=install+Exoduc+...</td><td>install Exoduc crypto currency - Google Search</td><td>2</td></tr>
<tr><td>31</td><td>https://www.exodus.com/download/</td><td>Exodus Crypto App Download</td><td>1</td></tr>
<tr><td>32</td><td>https://uk.exodus.com/download/</td><td>Exodus Crypto App Download</td><td>3</td></tr>
<tr><td>33</td><td>https://nordvpn.en.softonic.com/download</td><td>Download NordVPN 7.28.4 - latest version</td><td>2</td></tr>
<tr><td>34</td><td>https://en.softonic.com/download/nordvpn/windows/post-download?ext=1</td><td>Download NordVPN 7.28.4 - latest version</td><td>2</td></tr>
<tr><td>35</td><td>https://en.softonic.com/download/nordvpn/windows/post-download?ext=1#google_vigne...</td><td>Download and installation help</td><td>1</td></tr>
<tr><td>36</td><td>https://nordvpn.en.softonic.com/support?ext=1</td><td>Download and installation help</td><td>1</td></tr>
</table>
</td>
</tr>
</table>

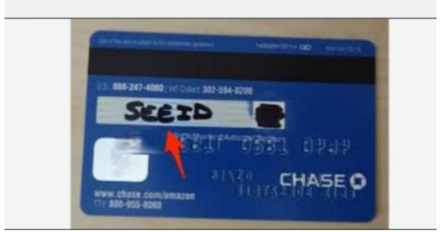
<table>
<tr>
<td>21:00 17-03-2025</td>
<td>Evidence of web history folder where George has made search of money laundry , credit card access , image of leaked credit cards etc.</td>
<td>


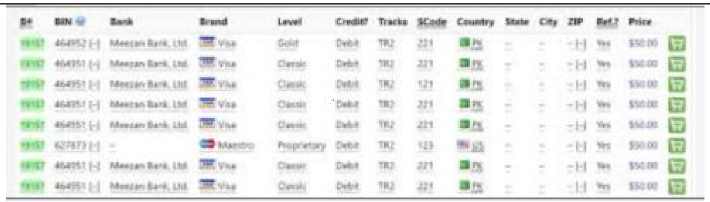
Web History

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

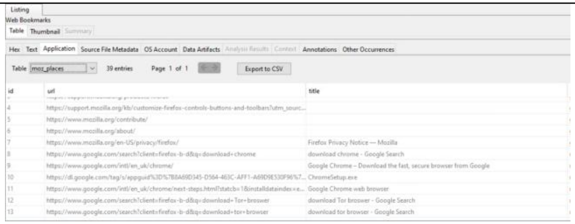
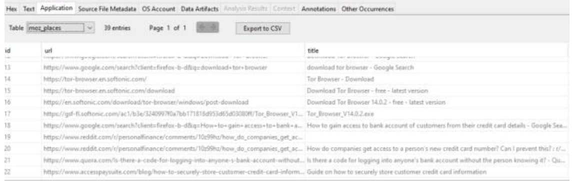
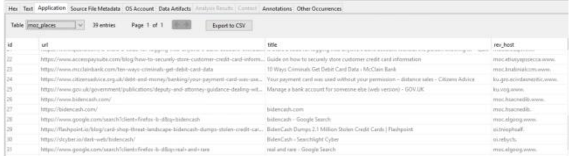
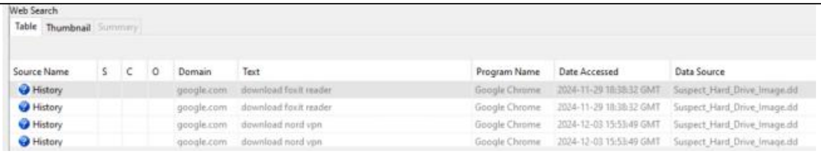
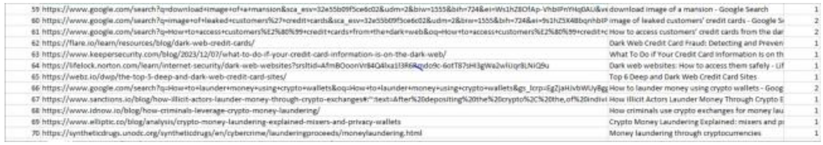
Table urls | 67 entries | Page 1 of 1 | Export to CSV

<table>
<tr><th>id</th><th>url</th><th>title</th><th>visit_cou...</th><th>typed_c...</th></tr>
<tr><td>61</td><td>https://www.google.com/search?q=How+to+access+customers%E2%80%99+credit+cards...</td><td>How to access customers' credit cards from the dark web - Go...</td><td>2</td><td>0</td></tr>
<tr><td>62</td><td>https://flare.io/learn/resources/blog/dark-web-credit-cards/</td><td>Dark Web Credit Card Fraud: Detecting and Preventing Credit ...</td><td>1</td><td>0</td></tr>
<tr><td>63</td><td>https://www.keepersecurity.com/blog/2023/12/07/what-to-do-if-your-credit-card-informat...</td><td>What To Do if Your Credit Card Information Is on the Dark Web</td><td>1</td><td>0</td></tr>
<tr><td>64</td><td>https://lifelock.norton.com/learn/internet-security/dark-web-websites?srsltid=AfmBOoonVr...</td><td>Dark web websites: How to access them safely - LifeLock</td><td>1</td><td>0</td></tr>
<tr><td>65</td><td>https://webz.io/dwp/the-top-5-deep-and-dark-web-credit-card-sites/</td><td>Top 6 Deep and Dark Web Credit Card Sites</td><td>1</td><td>0</td></tr>
<tr><td>66</td><td>https://www.google.com/search?q=How+to+launder+money+using+crypto+wallets&oq=...</td><td>How to launder money using crypto wallets - Google Search</td><td>2</td><td>0</td></tr>
<tr><td>67</td><td>https://www.sanctions.io/blog/how-illicit-actors-launder-money-through-crypto-exchange...</td><td>How Illicit Actors Launder Money Through Crypto Exchanges |...</td><td>1</td><td>0</td></tr>
<tr><td>68</td><td>https://www.idnow.io/blog/how-criminals-leverage-crypto-money-laundering/</td><td>How criminals use crypto exchanges for money laundering.</td><td>1</td><td>0</td></tr>
<tr><td>69</td><td>https://www.elliptic.co/blog/analysis/crypto-money-laundering-explained-mixers-and-priv...</td><td>Crypto Money Laundering Explained: mixers and privacy wallets</td><td>1</td><td>0</td></tr>
<tr><td>70</td><td>https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/mone...</td><td>Money laundering through cryptocurrencies</td><td>1</td><td>0</td></tr>
<tr><td>71</td><td>https://hyperverge.co/blog/money-laundering-in-cryptocurrency-risks-prevention/</td><td>A Guide to Cryptocurrency Money Laundering</td><td>1</td><td>0</td></tr>
<tr><td>72</td><td>https://www.ukfinance.org.uk/news-and-insight/blog/do-digital-currencies-and-cryptocurr...</td><td>Do digital currencies and cryptocurrencies pose a higher risk o...</td><td>1</td><td>0</td></tr>
</table>

<table>
<tr><td>73</td><td>https://financialcrimeacademy.org/cryptocurrency-money-laundering-methods/</td><td>Understanding Crypto Money Laundering Methods: The Crypt...</td><td>1</td><td>0</td><td>13380288799499976</td><td>0</td></tr>
<tr><td>74</td><td>https://www.google.com/search?q=brain%E2%80%99s+club&oq=brain%E2%80%99s+club...</td><td>brain's club - Google Search</td><td>2</td><td>0</td><td>13380289358579458</td><td>0</td></tr>
<tr><td>75</td><td>https://brianclub.to/</td><td>Briansclub.cm | Briansclub Login | Briansclub Shop | Bclub</td><td>1</td><td>0</td><td>13380289378350969</td><td>0</td></tr>
<tr><td>76</td><td>https://www.google.com/search?q=zunostore&oq=zunostore&gs_lcrp=EgZjaHJvbWUyBgg...</td><td>zunostore - Google Search</td><td>2</td><td>0</td><td>13380289505604594</td><td>0</td></tr>
</table>
</td>
</tr>
<tr>
<td>21:30 17-03-2025</td>
<td>Found different credit and debit card images in web cache data, which can be used for purchasing things</td>
<td>


</td>
</tr>
<tr>
<td>22:15 17-03-2025</td>
<td>This image show the George has purchase things from different credit and debit card</td>
<td>


<table>
<tr><th>B#</th><th>BIN</th><th>Bank</th><th>Brand</th><th>Level</th><th>Credit?</th><th>Tracks</th><th>SCode</th><th>Country</th><th>State</th><th>City</th><th>ZIP</th><th>Ref.?</th><th>Price</th><th></th></tr>
<tr><td>[illegible]</td><td>464952 [-]</td><td>Meezan Bank, Ltd</td><td>Visa</td><td>Gold</td><td>Debit</td><td>TR2</td><td>221</td><td>PK</td><td>-</td><td>-</td><td>- [-]</td><td>Yes</td><td>$50.00</td><td></td></tr>
<tr><td>[illegible]</td><td>464951 [-]</td><td>Meezan Bank, Ltd</td><td>Visa</td><td>Classic</td><td>Debit</td><td>TR2</td><td>221</td><td>PK</td><td>-</td><td>-</td><td>- [-]</td><td>Yes</td><td>$50.00</td><td></td></tr>
<tr><td>[illegible]</td><td>464951 [-]</td><td>Meezan Bank, Ltd</td><td>Visa</td><td>Classic</td><td>Debit</td><td>TR2</td><td>121</td><td>PK</td><td>-</td><td>-</td><td>- [-]</td><td>Yes</td><td>$50.00</td><td></td></tr>
<tr><td>[illegible]</td><td>464951 [-]</td><td>Meezan Bank, Ltd</td><td>Visa</td><td>Classic</td><td>Debit</td><td>TR2</td><td>221</td><td>PK</td><td>-</td><td>-</td><td>- [-]</td><td>Yes</td><td>$50.00</td><td></td></tr>
<tr><td>[illegible]</td><td>464951 [-]</td><td>Meezan Bank, Ltd</td><td>Visa</td><td>Classic</td><td>Debit</td><td>TR2</td><td>221</td><td>PK</td><td>-</td><td>-</td><td>- [-]</td><td>Yes</td><td>$50.00</td><td></td></tr>
<tr><td>[illegible]</td><td>627873 [-]</td><td>-</td><td>Maestro</td><td>Proprietary</td><td>Debit</td><td>TR2</td><td>123</td><td>US</td><td>-</td><td>-</td><td>- [-]</td><td>Yes</td><td>$50.00</td><td></td></tr>
<tr><td>[illegible]</td><td>464951 [-]</td><td>Meezan Bank, Ltd</td><td>Visa</td><td>Classic</td><td>Debit</td><td>TR2</td><td>221</td><td>PK</td><td>-</td><td>-</td><td>- [-]</td><td>Yes</td><td>$50.00</td><td></td></tr>
<tr><td>[illegible]</td><td>464951 [-]</td><td>Meezan Bank, Ltd</td><td>Visa</td><td>Classic</td><td>Debit</td><td>TR2</td><td>221</td><td>PK</td><td>-</td><td>-</td><td>- [-]</td><td>Yes</td><td>$50.00</td><td></td></tr>
</table>
</td>
</tr>
</table>

22:30 17-03-2025	This evidence show Mozilla browser sites in Web bookmark folder	  
22:45 17-03-2025	As shown in the both figure of web search where George has search for crypto currency, dark web access, credit cards	 

Listing
Web Bookmarks
Table Thumbnail Summary
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Table moz_places 39 entries Page 1 of 1 Export to CSV

id	url	title
4	https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_sourc...	
5	https://www.mozilla.org/contribute/	
6	https://www.mozilla.org/about/	
7	https://www.mozilla.org/en-US/privacy/firefox/	Firefox Privacy Notice — Mozilla
8	https://www.google.com/search?client=firefox-b-d&q=download+chrome	download chrome - Google Search
9	https://www.google.com/intl/en_uk/chrome/	Google Chrome – Download the fast, secure browser from Google
10	https://dl.google.com/tag/s/appguid%3D%7B8A69D345-D564-463C-AFF1-A69D9E530F96%7...	ChromeSetup.exe
11	https://www.google.com/intl/en_uk/chrome/next-steps.html?statcb=1&installdataindex=e...	Google Chrome web browser
12	https://www.google.com/search?client=firefox-b-d&q=download+Tor+broswer	download Tor broswer - Google Search
13	https://www.google.com/search?client=firefox-b-d&q=download+tor+browser	download tor browser - Google Search

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Table moz_places 39 entries Page 1 of 1 Export to CSV

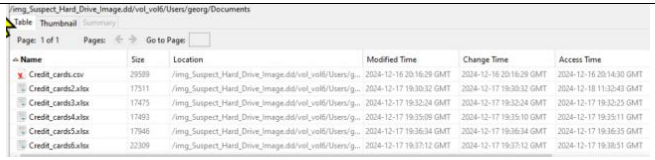
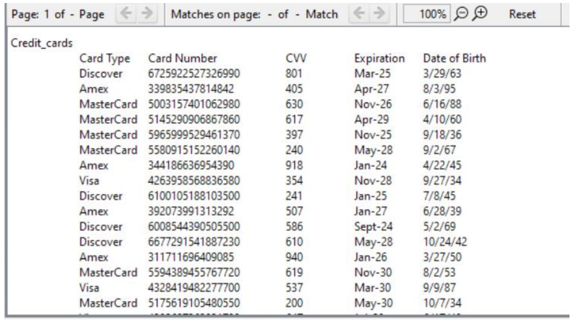
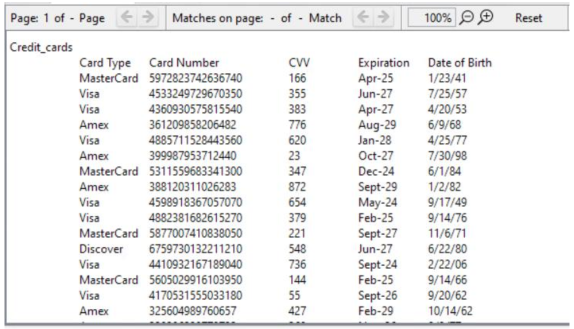
id	url	title
13	https://www.google.com/search?client=firefox-b-d&q=download+tor+browser	download tor browser - Google Search
14	https://tor-browser.en.softonic.com/	Tor Browser - Download
15	https://tor-browser.en.softonic.com/download	Download Tor Browser - free - latest version
16	https://en.softonic.com/download/tor-browser/windows/post-download	Download Tor Browser 14.0.2 - free - latest version
17	https://gsf-fl.softonic.com/ac1/b3e/324099?f0a7bb171818d953d65d03080ff/Tor_Browser_V1...	Tor_Browser_V14.0.2.exe
18	https://www.google.com/search?client=firefox-b-d&q=How+to+gain+access+to+bank+a...	How to gain access to bank account of customers from their credit card details - Google Sea...
19	https://www.reddit.com/r/personalfinance/comments/10z99hz/how_do_companies_get_ac...	
20	https://www.reddit.com/r/personalfinance/comments/10z99hz/how_do_companies_get_ac...	How do companies get access to a person's new credit card number? Can I prevent this? : r/...
21	https://www.quora.com/Is-there-a-code-for-logging-into-anyone-s-bank-account-without...	Is there a code for logging into anyone's bank account without the person knowing it? - Qu...
22	https://www.accesspaysuite.com/blog/how-to-securely-store-customer-credit-card-inform...	Guide on how to securely store customer credit card information

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Table moz_places 39 entries Page 1 of 1 Export to CSV

id	url	title	rev_host
22	https://www.accesspaysuite.com/blog/how-to-securely-store-customer-credit-card-inform...	Guide on how to securely store customer credit card information	moc.etiusyapssecca.www.
23	https://www.mcclainbank.com/ten-ways-criminals-get-debit-card-data	10 Ways Criminals Get Debit Card Data - McClain Bank	moc.knabnialccm.www.
24	https://www.citizensadvice.org.uk/debt-and-money/banking/your-payment-card-was-use...	Your payment card was used without your permission – distance sales - Citizens Advice	ku.gro.ecivdasnezitic.www.
25	https://www.gov.uk/government/publications/deputy-and-attorney-guidance-dealing-wit...	Manage a bank account for someone else (web version) - GOV.UK	ku.vog.www.
26	https://www.bidencash.com/		moc.hsacnedib.www.
27	https://bidencash.com/	bidencash.com	moc.hsacnedib.
28	https://www.google.com/search?client=firefox-b-d&q=bidencash	bidencash - Google Search	moc.elgoog.www.
29	https://flashpoint.io/blog/card-shop-threat-landscape-bidencash-dumps-stolen-credit-car...	BidenCash Dumps 2.1 Million Stolen Credit Cards | Flashpoint	oi.tniophsalf.
30	https://slcyber.io/dark-web/bidencash/	BidenCash - Searchlight Cyber	oi.rebycls.
31	https://www.google.com/search?client=firefox-b-d&q=real+and+rare	real and rare - Google Search	moc.elgoog.www.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	download foxit reader	Google Chrome	2024-11-29 18:38:32 GMT	Suspect_Hard_Drive_Image.dd
History				google.com	download foxit reader	Google Chrome	2024-11-29 18:38:32 GMT	Suspect_Hard_Drive_Image.dd
History				google.com	download nord vpn	Google Chrome	2024-12-03 15:53:49 GMT	Suspect_Hard_Drive_Image.dd
History				google.com	download nord vpn	Google Chrome	2024-12-03 15:53:49 GMT	Suspect_Hard_Drive_Image.dd

59	https://www.google.com/search?q=download+image+of+a+mansion&sca_esv=32e55b09f5ce6c02&udm=2&biw=1555&bih=724&ei=Ws1hZ8OfAp-VhbIPnYHq0AU&ve	download image of a mansion - Google Search	1
60	https://www.google.com/search?q=image+of+leaked+customers%27+credit+cards&sca_esv=32e55b09f5ce6c02&udm=2&biw=1555&bih=724&ei=9s1hZ5X4BbqnhbIP	image of leaked customers' credit cards - Google S	2
61	https://www.google.com/search?q=How+to+access+customers%E2%80%99+credit+cards+from+the+dark+web&oq=How+to+access+customers%E2%80%99+credit+c	How to access customers' credit cards from the dar	2
62	https://flare.io/learn/resources/blog/dark-web-credit-cards/	Dark Web Credit Card Fraud: Detecting and Preven	1
63	https://www.keepersecurity.com/blog/2023/12/07/what-to-do-if-your-credit-card-information-is-on-the-dark-web/	What To Do if Your Credit Card Information Is on th	1
64	https://lifelock.norton.com/learn/internet-security/dark-web-websites?srsltid=AfmBOoonVr84Q4Ixa1I3R6Rqdo9c-6otT87sHI3gWa2wIUqr8LNiQ9u	Dark web websites: How to access them safely - Lif	1
65	https://webz.io/dwp/the-top-5-deep-and-dark-web-credit-card-sites/	Top 6 Deep and Dark Web Credit Card Sites	1
66	https://www.google.com/search?q=How+to+launder+money+using+crypto+wallets&oq=How+to+launder+money+using+crypto+wallets&gs_lcrp=EgZjaHJvbWUyBgg	How to launder money using crypto wallets - Goog	2
67	https://www.sanctions.io/blog/how-illicit-actors-launder-money-through-crypto-exchanges#:~:text=After%20depositing%20the%20crypto%2C%20the,of%20indivi	How Illicit Actors Launder Money Through Crypto E	1
68	https://www.idnow.io/blog/how-criminals-leverage-crypto-money-laundering/	How criminals use crypto exchanges for money lau	1
69	https://www.elliptic.co/blog/analysis/crypto-money-laundering-explained-mixers-and-privacy-wallets	Crypto Money Laundering Explained: mixers and p	1
70	https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html	Money laundering through cryptocurrencies	1

23:00 17-03-2025	Evidence of six excel sheets with card details which was found in documents folder	  

/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents

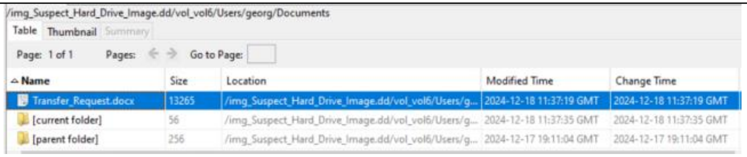
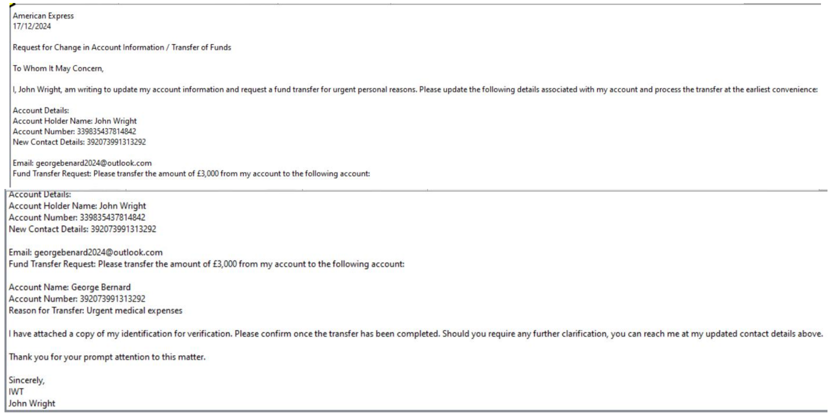
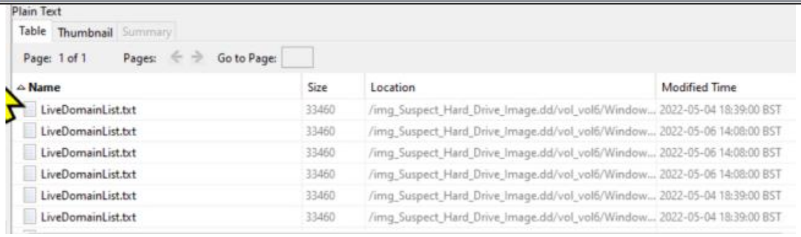
Name	Size	Location	Modified Time	Change Time	Access Time
Credit_cards.csv	29589	/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g...	2024-12-16 20:16:29 GMT	2024-12-16 20:16:29 GMT	2024-12-16 20:14:30 GMT
Credit_cards2.xlsx	17511	/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g...	2024-12-17 19:30:32 GMT	2024-12-17 19:30:32 GMT	2024-12-18 11:32:43 GMT
Credit_cards3.xlsx	17475	/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g...	2024-12-17 19:32:24 GMT	2024-12-17 19:32:24 GMT	2024-12-17 19:32:25 GMT
Credit_cards4.xlsx	17493	/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g...	2024-12-17 19:35:09 GMT	2024-12-17 19:35:10 GMT	2024-12-17 19:35:11 GMT
Credit_cards5.xlsx	17946	/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g...	2024-12-17 19:36:34 GMT	2024-12-17 19:36:34 GMT	2024-12-17 19:36:35 GMT
Credit_cards6.xlsx	22309	/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g...	2024-12-17 19:37:12 GMT	2024-12-17 19:37:12 GMT	2024-12-17 19:38:51 GMT

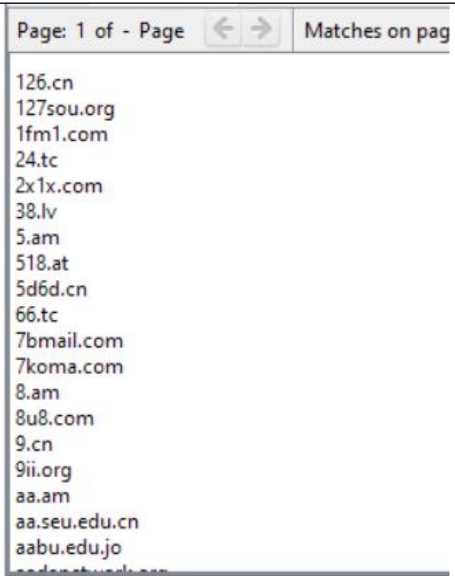
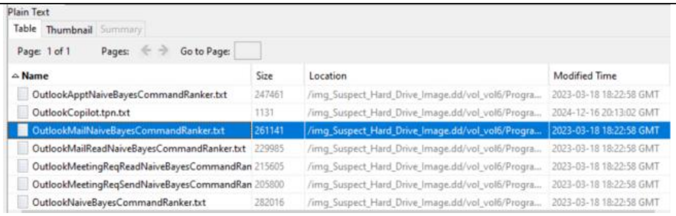
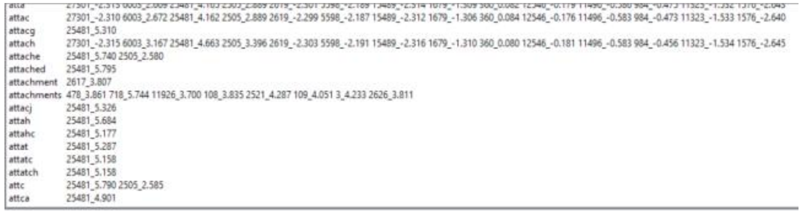
Credit_cards

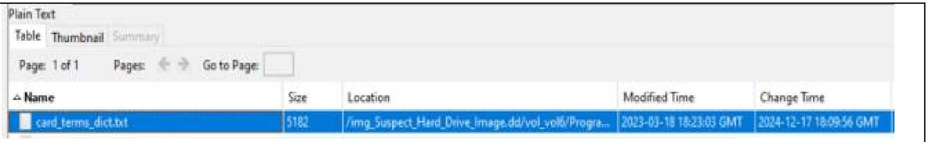
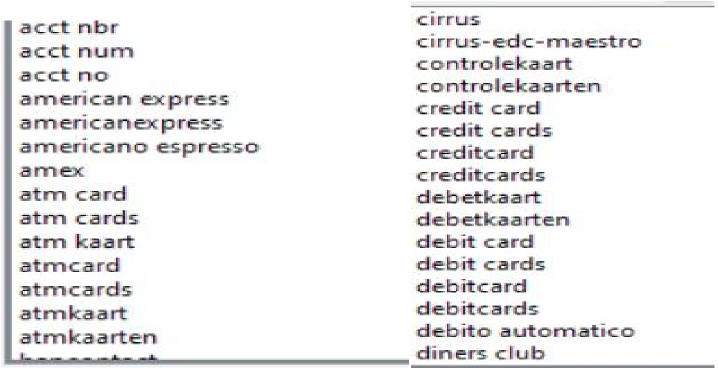
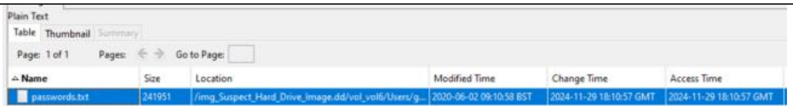
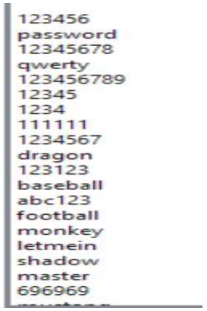
Card Type	Card Number	CVV	Expiration	Date of Birth
Discover	6725922527326990	801	Mar-25	3/29/63
Amex	339835437814842	405	Apr-27	8/3/95
MasterCard	5003157401062980	630	Nov-26	6/16/88
MasterCard	5145290906867860	617	Apr-29	4/10/60
MasterCard	5965999529461370	397	Nov-25	9/18/36
MasterCard	5580915152260140	240	May-28	9/2/67
Amex	344186636954390	918	Jan-24	4/22/45
Visa	4263958568836580	354	Nov-28	9/27/34
Discover	6100105188103500	241	Jan-25	7/8/45
Amex	392073991313292	507	Jan-27	6/28/39
Discover	6008544390505500	586	Sept-24	5/2/69
Discover	6677291541887230	610	May-28	10/24/42
Amex	311711696409085	940	Jan-26	3/27/50
MasterCard	5594389455767720	619	Nov-30	8/2/53
Visa	4328419482277700	537	Mar-30	9/9/87
MasterCard	5175619105480550	200	May-30	10/7/34

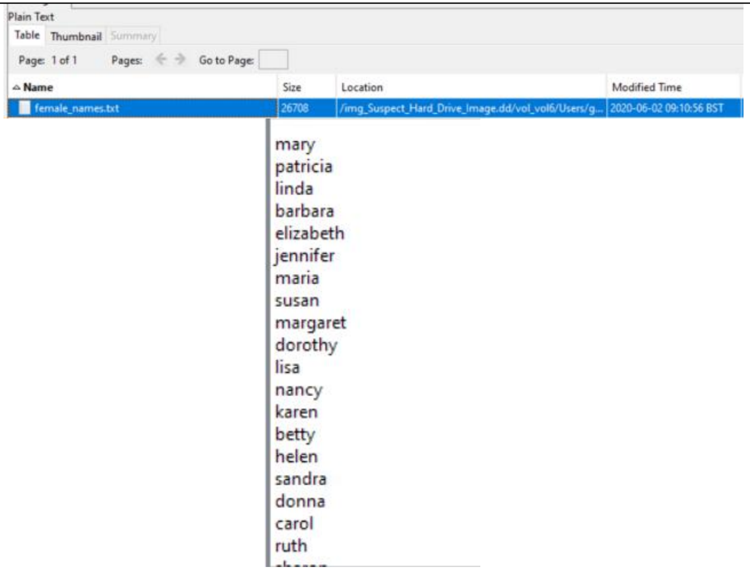
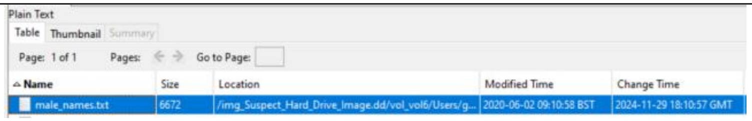
Credit_cards

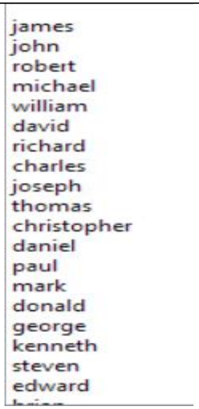
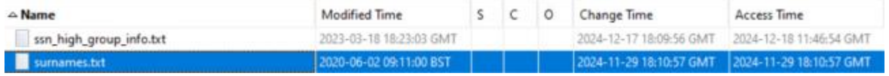
Card Type	Card Number	CVV	Expiration	Date of Birth
MasterCard	5972823742636740	166	Apr-25	1/23/41
Visa	4533249729670350	355	Jun-27	7/25/57
Visa	4360930575815540	383	Apr-27	4/20/53
Amex	361209858206482	776	Aug-29	6/9/68
Visa	4885711528443560	620	Jan-28	4/25/77
Amex	399987953712440	23	Oct-27	7/30/98
MasterCard	5311559683341300	347	Dec-24	6/1/84
Amex	388120311026283	872	Sept-29	1/2/82
Visa	4598918367057070	654	May-24	9/17/49
Visa	4882381682615270	379	Feb-25	9/14/76
MasterCard	5877007410838050	221	Sept-27	11/6/71
Discover	6759730132211210	548	Jun-27	6/22/80
Visa	4410932167189040	736	Sept-24	2/22/06
MasterCard	5605029916103950	144	Feb-25	9/14/66
Visa	4170531555033180	55	Sept-26	9/20/62
Amex	325604989760657	427	Feb-29	10/14/62

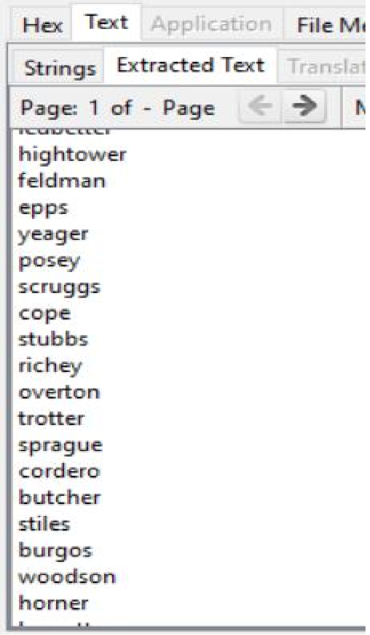
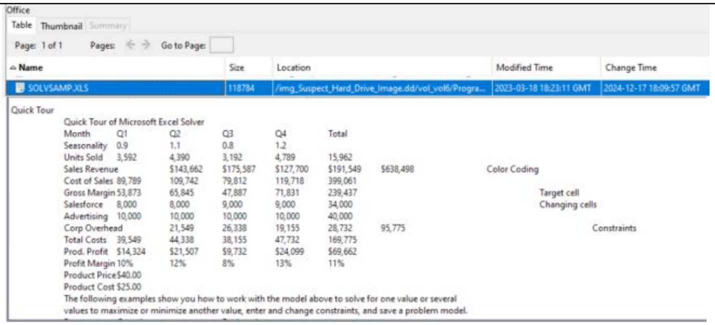
11:00 18-03-2025	Evidence of Transfer request for funds by George was found in Document folder	 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents Table Thumbnail Summary Page: 1 of 1 Pages: Go to Page: Name Size Location Modified Time Change Time Transfer_Request.docx 13265 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g... 2024-12-18 11:37:19 GMT 2024-12-18 11:37:19 GMT [current folder] 56 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g... 2024-12-18 11:37:35 GMT 2024-12-18 11:37:35 GMT [parent folder] 256 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g... 2024-12-17 19:11:04 GMT 2024-12-17 19:11:04 GMT  American Express 17/12/2024 Request for Change in Account Information / Transfer of Funds To Whom It May Concern, I, John Wright, am writing to update my account information and request a fund transfer for urgent personal reasons. Please update the following details associated with my account and process the transfer at the earliest convenience: Account Details: Account Holder Name: John Wright Account Number: 339835437814842 New Contact Details: 392073991313292 Email: georgebenard2024@outlook.com Fund Transfer Request: Please transfer the amount of £3,000 from my account to the following account: Account Details: Account Holder Name: John Wright Account Number: 339835437814842 New Contact Details: 392073991313292 Email: georgebenard2024@outlook.com Fund Transfer Request: Please transfer the amount of £3,000 from my account to the following account: Account Name: George Bernard Account Number: 392073991313292 Reason for Transfer: Urgent medical expenses I have attached a copy of my identification for verification. Please confirm once the transfer has been completed. Should you require any further clarification, you can reach me at my updated contact details above. Thank you for your prompt attention to this matter. Sincerely, IWT John Wright
11:30 18-03-2025	List of Domain names are found in Plain text folder which indicate domains Gorge has access	 Plain Text Table Thumbnail Summary Page: 1 of 1 Pages: Go to Page: Name Size Location Modified Time LiveDomainList.txt 33460 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Window... 2022-05-04 18:39:00 BST LiveDomainList.txt 33460 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Window... 2022-05-06 14:08:00 BST LiveDomainList.txt 33460 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Window... 2022-05-06 14:08:00 BST LiveDomainList.txt 33460 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Window... 2022-05-06 14:08:00 BST LiveDomainList.txt 33460 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Window... 2022-05-04 18:39:00 BST LiveDomainList.txt 33460 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Window... 2022-05-04 18:39:00 BST

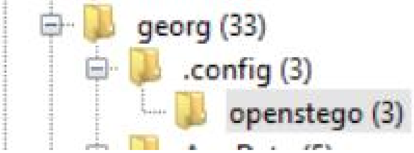
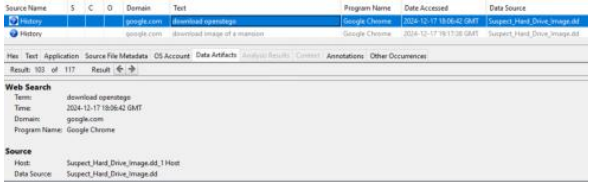
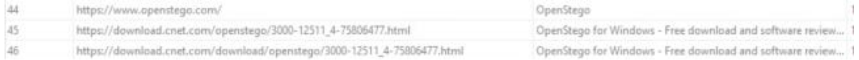
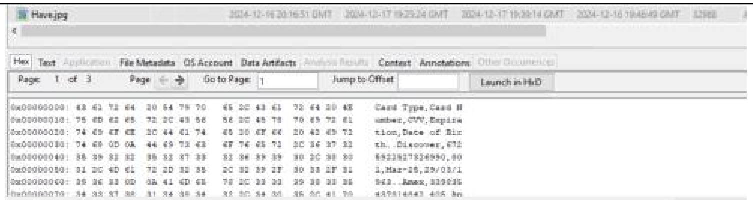
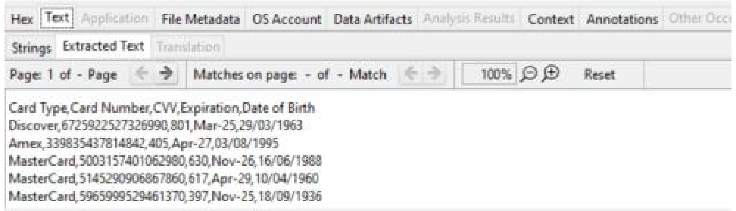
		 Page: 1 of - Page Matches on pag 126.cn 127sou.org 1fm1.com 24.tc 2x1x.com 38.lv 5.am 518.at 5d6d.cn 66.tc 7bmail.com 7koma.com 8.am 8u8.com 9.cn 9ii.org aa.am aa.seu.edu.cn aabu.edu.jo
12:18 18-03-2025	Outloook mail box has request to Naives bay command ranker are found in Plain text folder	 Plain Text Table Thumbnail Summary Page: 1 of 1 Pages: Go to Page: Name | Size | Location | Modified Time OutlookApptNaiveBayesCommandRanker.txt | 247461 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Progra... | 2023-03-18 18:22:58 GMT OutlookCopilot.tpn.txt | 1131 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Progra... | 2024-12-16 20:13:02 GMT OutlookMailNaiveBayesCommandRanker.txt | 261141 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Progra... | 2023-03-18 18:22:58 GMT OutlookMailReadNaiveBayesCommandRanker.txt | 229985 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Progra... | 2023-03-18 18:22:58 GMT OutlookMeetingReqReadNaiveBayesCommandRan | 215605 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Progra... | 2023-03-18 18:22:58 GMT OutlookMeetingReqSendNaiveBayesCommandRan | 205800 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Progra... | 2023-03-18 18:22:58 GMT OutlookNaiveBayesCommandRanker.txt | 282016 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Progra... | 2023-03-18 18:22:58 GMT  atta 27301_-2.315 6003_2.669 25481_4.163 2505_2.889 2619_-2.301 5598_-2.189 15489_-2.314 1679_-1.309 360_0.082 12546_-0.179 11496_-0.580 984_-0.473 11323_-1.532 1576_-2.645 attac 27301_-2.310 6003_2.672 25481_4.162 2505_2.889 2619_-2.299 5598_-2.187 15489_-2.312 1679_-1.306 360_0.084 12546_-0.176 11496_-0.583 984_-0.473 11323_-1.533 1576_-2.640 attacg 25481_5.310 attach 27301_-2.315 6003_3.167 25481_4.663 2505_3.396 2619_-2.303 5598_-2.191 15489_-2.316 1679_-1.310 360_0.080 12546_-0.181 11496_-0.583 984_-0.456 11323_-1.534 1576_-2.645 attache 25481_5.740 2505_2.580 attached 25481_5.795 attachment 2617_3.807 attachments 478_3.861 718_5.744 11926_3.700 108_3.835 2521_4.287 109_4.051 3_4.233 2626_3.811 attacj 25481_5.326 attah 25481_5.684 attahc 25481_5.177 attat 25481_5.287 attatc 25481_5.158 attatch 25481_5.158 attc 25481_5.790 2505_2.585 attca 25481_4.901

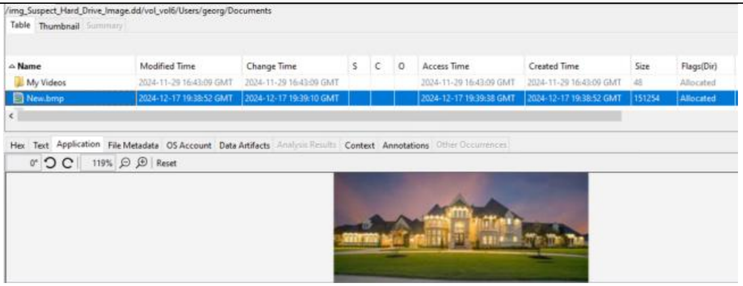
13:26 18-03-2025	Different type of Card names file was found under Plain text folder ,which can be use for selecting different cards on payment page	 Plain Text Table Thumbnail Summary Page: 1 of 1 Pages: Go to Page: Name Size Location Modified Time Change Time card_terms_dict.txt 5182 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Progra... 2023-03-18 18:23:03 GMT 2024-12-17 18:09:56 GMT  acct nbr acct num acct no american express americanexpress americano espresso amex atm card atm cards atm kaart atmcard atmcards atmkaart atmkaarten cirrus cirrus-edc-maestro controlekaart controlekaarten credit card credit cards creditcard creditcards debetkaart debetkaarten debit card debit cards debitcard debitcards debito automatico diners club
14:00 18-03-2025	Password file was found in Documents folder under Plain text which can be use as any file passwords	 Plain Text Table Thumbnail Summary Page: 1 of 1 Pages: Go to Page: Name Size Location Modified Time Change Time Access Time passwords.txt 241951 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g... 2020-06-02 09:10:58 BST 2024-11-29 18:10:57 GMT 2024-11-29 18:10:57 GMT  123456 password 12345678 qwerty 123456789 12345 1234 111111 1234567 dragon 123123 baseball abc123 football monkey letmein shadow master 696969

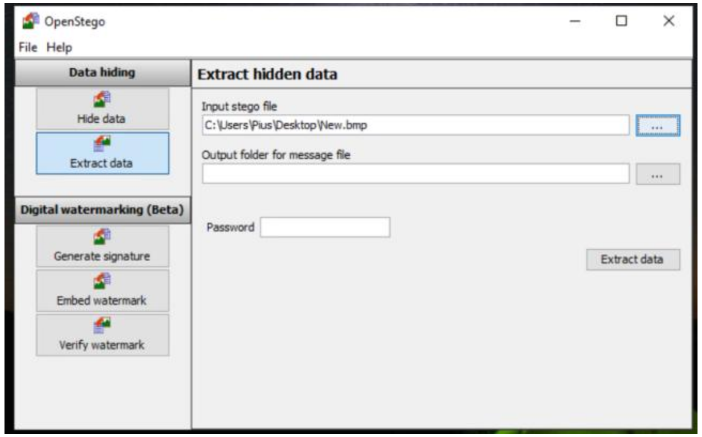
14:39 18-03-2025	Female names file was found in under Plain text folder which can be use as username in card details	 Plain Text Table Thumbnail Summary Page: 1 of 1 Pages: Go to Page: Name | Size | Location | Modified Time female_names.txt | 26708 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g... | 2020-06-02 09:10:56 BST mary patricia linda barbara elizabeth jennifer maria susan margaret dorothy lisa nancy karen betty helen sandra donna carol ruth
14:40 18-03-2025	Male names file was found in under Plain text folder which can be use as username in card details	 Plain Text Table Thumbnail Summary Page: 1 of 1 Pages: Go to Page: Name | Size | Location | Modified Time | Change Time male_names.txt | 6672 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/g... | 2020-06-02 09:10:58 BST | 2024-11-29 18:10:57 GMT

		 james john robert michael william david richard charles joseph thomas christopher daniel paul mark donald george kenneth steven edward
14:50 18-03-2025	Surname names file was found in under Plain text folder which can be use as username in card details	 Name | Modified Time | S | C | O | Change Time | Access Time ssn_high_group_info.txt | 2023-03-18 18:23:03 GMT | | | | 2024-12-17 18:09:56 GMT | 2024-12-18 11:46:54 GMT surnames.txt | 2020-06-02 09:11:00 BST | | | | 2024-11-29 18:10:57 GMT | 2024-11-29 18:10:57 GMT

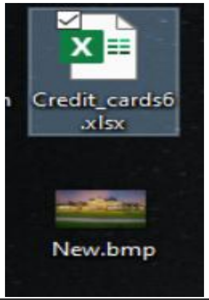
		 Hex Text Application File M Strings Extracted Text Translat Page: 1 of - Pagehightower feldman epps yeager posey scruggs cope stubbs richey overton trotter sprague cordero butcher stiles burgos woodson horner
15:15 18-03-2025	SLOVSAMP.XLS file found in Office folder has financial data about the unit sold , sales revenue	 Office Table Thumbnail Summary Page: 1 of 1 Pages: Go to Page:Name | Size | Location | Modified Time | Change Time SOLVSAMP.XLS | 118784 | /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Progra... | 2023-03-18 18:23:11 GMT | 2024-12-17 18:09:57 GMT Quick Tour Quick Tour of Microsoft Excel Solver Month Q1 Q2 Q3 Q4 Total Seasonality 0.9 1.1 0.8 1.2 Units Sold 3,592 4,390 3,192 4,789 15,962 Sales Revenue $143,662 $175,587 $127,700 $191,549 $638,498 Color Coding Cost of Sales 89,789 109,742 79,812 119,718 399,061 Gross Margin 53,873 65,845 47,887 71,831 239,437 Target cell Salesforce 8,000 8,000 9,000 9,000 34,000 Changing cells Advertising 10,000 10,000 10,000 10,000 40,000 Corp Overhead 21,549 26,338 19,155 28,732 95,775 Constraints Total Costs 39,549 44,338 38,155 47,732 169,775 Prod. Profit $14,324 $21,507 $9,732 $24,099 $69,662 Profit Margin 10% 12% 8% 13% 11% Product Price $40.00 Product Cost $25.00 The following examples show you how to work with the model above to solve for one value or several values to maximize or minimize another value, enter and change constraints, and save a problem model.

15:50 18-03-2025	Openstego file was found in .config and web history of download	 georg (33) .config (3) openstego (3)  Source Name | S | C | O | Domain | Text | Program Name | Date Accessed | Data Source History | | | | google.com | download openstego | Google Chrome | 2024-12-17 18:06:42 GMT | Suspect_Hard_Drive_Image.dd History | | | | google.com | download image of a mansion | Google Chrome | 2024-12-17 19:17:38 GMT | Suspect_Hard_Drive_Image.dd Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Result: 103 of 117 Result **Web Search** Term: download openstego Time: 2024-12-17 18:06:42 GMT Domain: google.com Program Name: Google Chrome **Source** Host: Suspect_Hard_Drive_Image.dd_1 Host Data Source: Suspect_Hard_Drive_Image.dd  44 | https://www.openstego.com/ | OpenStego 45 | https://download.cnet.com/openstego/3000-12511_4-75806477.html | OpenStego for Windows - Free download and software review... 46 | https://download.cnet.com/download/openstego/3000-12511_4-75806477.html | OpenStego for Windows - Free download and software review...
16:15 18-03-2025	Image Have.jpg is image file but its hex value is different and size of file is also more	 Have.jpg 2024-12-16 20:16:51 GMT 2024-12-17 19:25:24 GMT 2024-12-17 19:39:14 GMT 2024-12-16 19:46:49 GMT 32988 Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Page: 1 of 3 Page Go to Page: 1 Jump to Offset Launch in HxD 0x00000000: 43 61 72 64 20 54 79 70 65 2C 43 61 72 64 20 4E Card Type,Card N 0x00000010: 75 6D 62 65 72 2C 43 56 56 2C 45 78 70 69 72 61 umber,CVV,Expira 0x00000020: 74 69 6F 6E 2C 44 61 74 65 20 6F 66 20 42 69 72 tion,Date of Bir 0x00000030: 74 68 0D 0A 44 69 73 63 6F 76 65 72 2C 36 37 32 th..Discover,672 0x00000040: 35 39 32 32 35 32 37 33 32 36 39 39 30 2C 38 30 5922527326990,80 0x00000050: 31 2C 4D 61 72 2D 32 35 2C 32 39 2F 30 33 2F 31 1,Mar-25,29/03/1 0x00000060: 39 36 33 0D 0A 41 6D 65 78 2C 33 33 39 38 33 35 963..Amex,339835 0x00000070: 34 33 37 38 31 34 38 34 32 2C 34 30 35 2C 41 70 437814842,405,Ap
	When click on text tab the file contain the card details as seen image	 Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occ Strings Extracted Text Translation Page: 1 of - Page Matches on page: - of - Match 100% Reset Card Type,Card Number,CVV,Expiration,Date of Birth Discover,6725922527326990,801,Mar-25,29/03/1963 Amex,339835437814842,405,Apr-27,03/08/1995 MasterCard,5003157401062980,630,Nov-26,16/06/1988 MasterCard,5145290906867860,617,Apr-29,10/04/1960 MasterCard,5965999529461370,397,Nov-25,18/09/1936

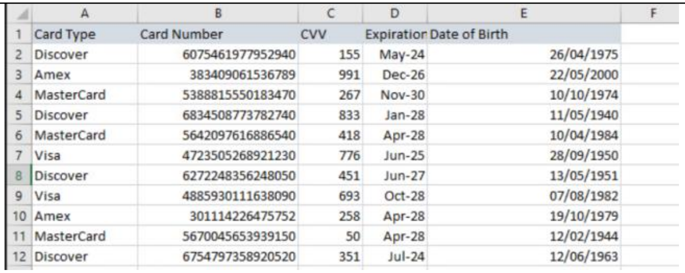
<table>
<tr>
<td>17:15 18-03-2025</td>
<td>New.bmp when data was extracted from it using OpenStego tool , excel sheet with credit cards details where found</td>
<td>

/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents
<table>
<tr><th>Name</th><th>Modified Time</th><th>Change Time</th><th>S</th><th>C</th><th>O</th><th>Access Time</th><th>Created Time</th><th>Size</th><th>Flags(Dir)</th></tr>
<tr><td>My Videos</td><td>2024-11-29 16:43:09 GMT</td><td>2024-11-29 16:43:09 GMT</td><td></td><td></td><td></td><td>2024-11-29 16:43:09 GMT</td><td>2024-11-29 16:43:09 GMT</td><td>48</td><td>Allocated</td></tr>
<tr><td>New.bmp</td><td>2024-12-17 19:38:52 GMT</td><td>2024-12-17 19:39:10 GMT</td><td></td><td></td><td></td><td>2024-12-17 19:39:38 GMT</td><td>2024-12-17 19:38:52 GMT</td><td>151254</td><td>Allocated</td></tr>
</table>
Table Thumbnail Summary
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 119% Reset



Input stego file: C:\Users\Pius\Desktop\New.bmp
Output folder for message file:
Password:

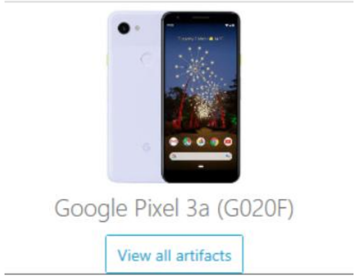


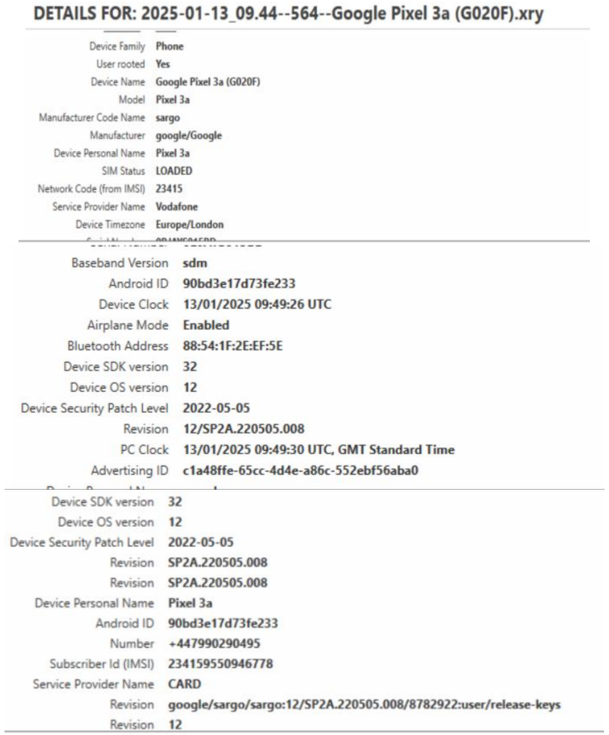
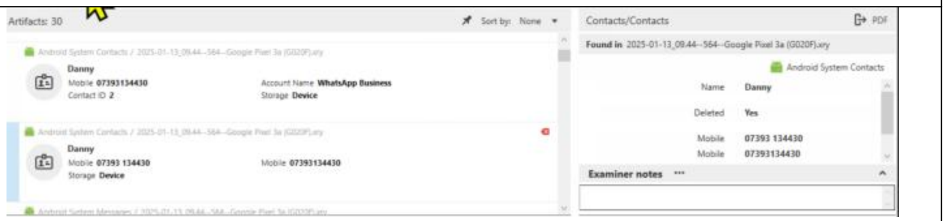
</td>
</tr>
</table>

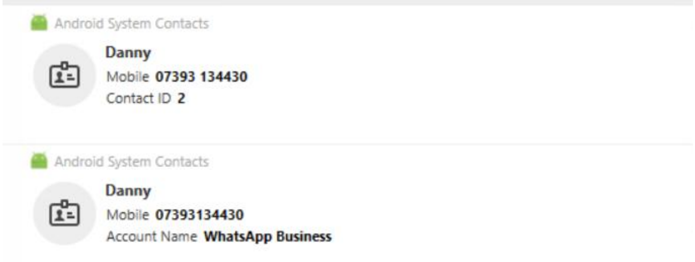
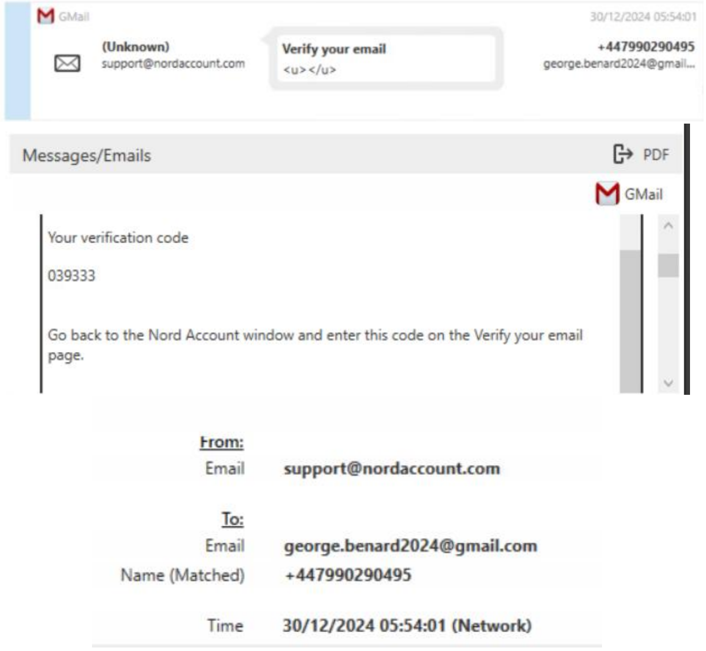
		

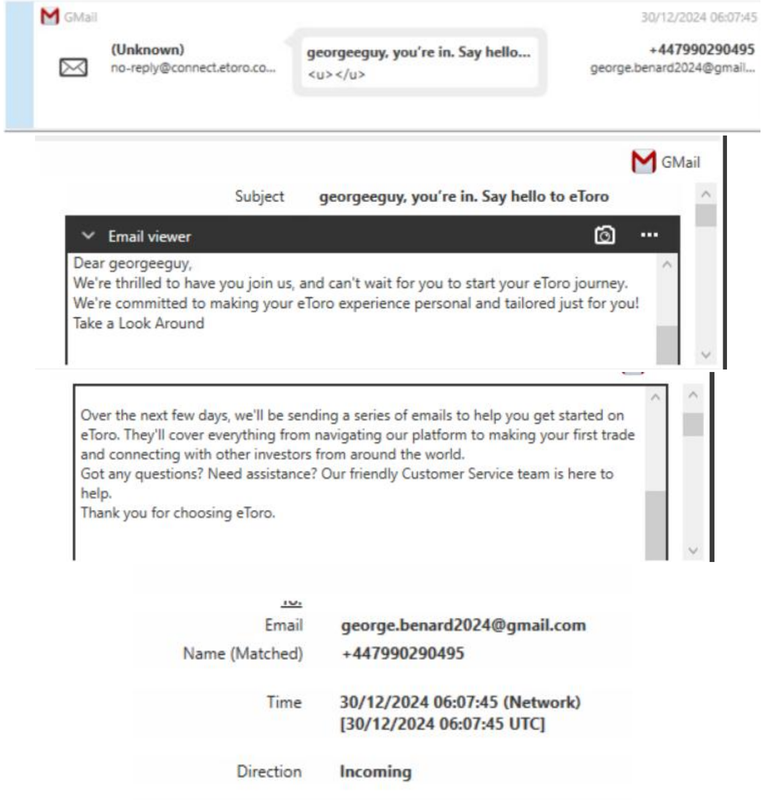
	A	B	C	D	E	F
1	Card Type	Card Number	CVV	Expiratior	Date of Birth	
2	Discover	6075461977952940	155	May-24	26/04/1975	
3	Amex	383409061536789	991	Dec-26	22/05/2000	
4	MasterCard	5388815550183470	267	Nov-30	10/10/1974	
5	Discover	6834508773782740	833	Jan-28	11/05/1940	
6	MasterCard	5642097616886540	418	Apr-28	10/04/1984	
7	Visa	4723505268921230	776	Jun-25	28/09/1950	
8	Discover	6272248356248050	451	Jun-27	13/05/1951	
9	Visa	4885930111638090	693	Oct-28	07/08/1982	
10	Amex	301114226475752	258	Apr-28	19/10/1979	
11	MasterCard	5670045653939150	50	Apr-28	12/02/1944	
12	Discover	6754797358920520	351	Jul-24	12/06/1963	

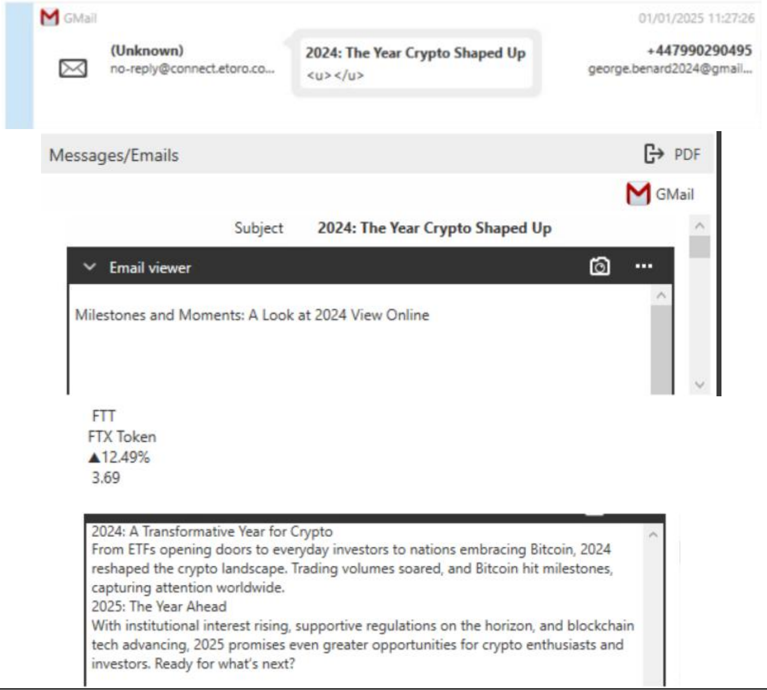
3.3. Table 5: This process show examine a suspect’s *Mobile device analysis using Xamn tool* without altering the original data.

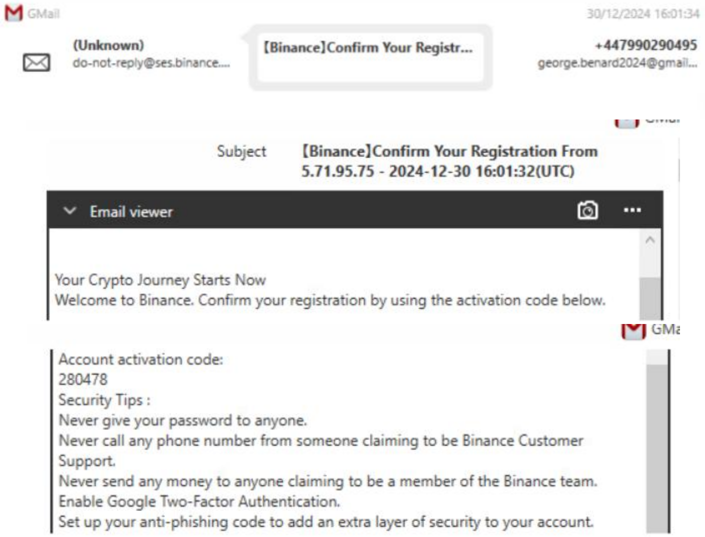
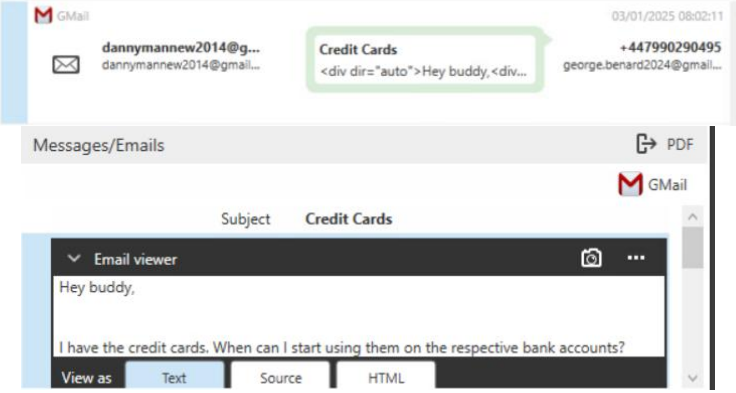
Date/time	Process	Evidence
22:36 22-03-2025	Open Xamn tool	
23:13 22-03-2025	Google Pixel 3a .xry file This are details of device.	

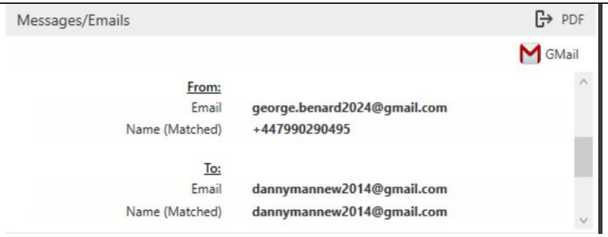
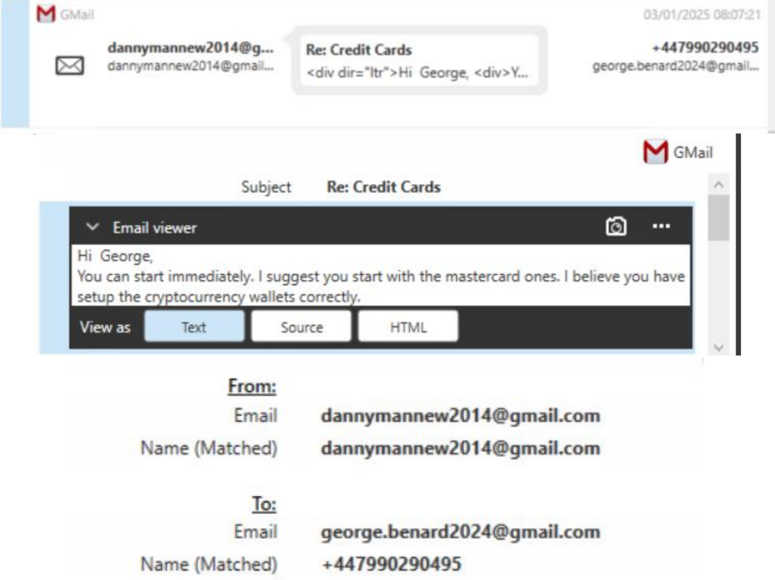
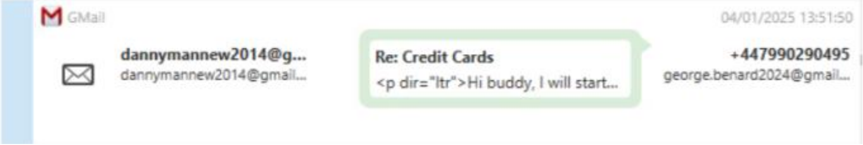
		 DETAILS FOR: 2025-01-13_09.44--564--Google Pixel 3a (G020F).xry Device Family Phone User rooted Yes Device Name Google Pixel 3a (G020F) Model Pixel 3a Manufacturer Code Name sargo Manufacturer google/Google Device Personal Name Pixel 3a SIM Status LOADED Network Code (from IMSI) 23415 Service Provider Name Vodafone Device Timezone Europe/London Baseband Version sdm Android ID 90bd3e17d73fe233 Device Clock 13/01/2025 09:49:26 UTC Airplane Mode Enabled Bluetooth Address 88:54:1F:2E:EF:5E Device SDK version 32 Device OS version 12 Device Security Patch Level 2022-05-05 Revision 12/SP2A.220505.008 PC Clock 13/01/2025 09:49:30 UTC, GMT Standard Time Advertising ID c1a48ffe-65cc-4d4e-a86c-552ebf56aba0 Device SDK version 32 Device OS version 12 Device Security Patch Level 2022-05-05 Revision SP2A.220505.008 Revision SP2A.220505.008 Device Personal Name Pixel 3a Android ID 90bd3e17d73fe233 Number +447990290495 Subscriber Id (IMSI) 234159550946778 Service Provider Name CARD Revision google/sargo/sargo:12/SP2A.220505.008/8782922:user/release-keys Revision 12
23:16 22-03-2025	Evidence indicate Danny contact was deleted from contact list as they did cryptocurrency discussion.	 Artifacts: 30 Sort by: None Android System Contacts / 2025-01-13_09.44--564--Google Pixel 3a (G020F).xry Danny Mobile 07393134430 Contact ID 2 Account Name WhatsApp Business Storage Device Android System Contacts / 2025-01-13_09.44--564--Google Pixel 3a (G020F).xry Danny Mobile 07393 134430 Storage Device Mobile 07393134430 Android System Messages / 2025-01-13_09.44--564--Google Pixel 3a (G020F).xry Contacts/Contacts PDF Found in 2025-01-13_09.44--564--Google Pixel 3a (G020F).xry Android System Contacts Name Danny Deleted Yes Mobile 07393 134430 Mobile 07393134430 Examiner notes

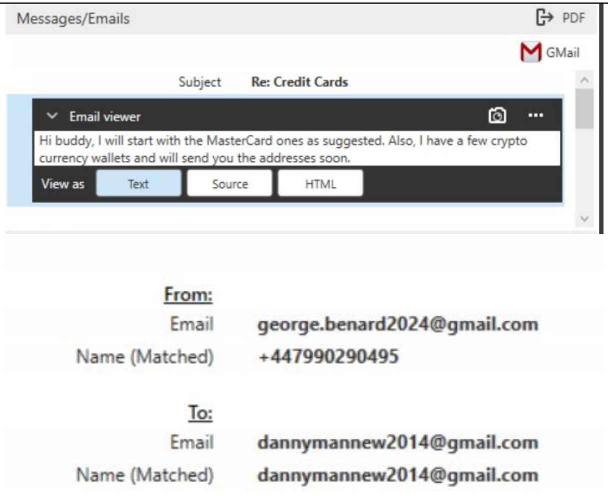
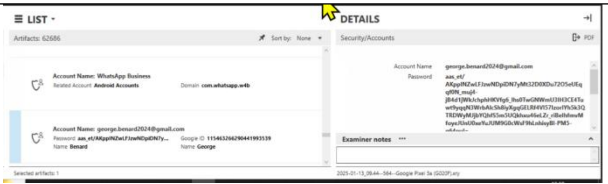
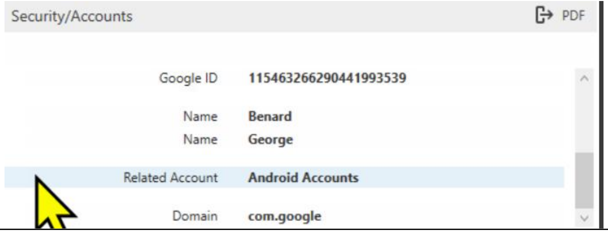
23:20 22-03-2025	Gorge contact list has only Danny’s number	 Android System Contacts Danny Mobile **07393 134430** Contact ID **2** Android System Contacts Danny Mobile **07393134430** Account Name **WhatsApp Business**
13:08 23-03-2025	Verification code of Nord VPN on Gorge phone , downloaded Nord VPN entries where found in hard drive even to access the dark web	 GMail 30/12/2024 05:54:01 **(Unknown)** support@nordaccount.com **Verify your email** <u></u> **+447990290495** george.benard2024@gmail... Messages/Emails PDF GMail Your verification code 039333 Go back to the Nord Account window and enter this code on the Verify your email page. **From:** Email **support@nordaccount.com** **To:** Email **george.benard2024@gmail.com** Name (Matched) **+447990290495** Time **30/12/2024 05:54:01 (Network)**

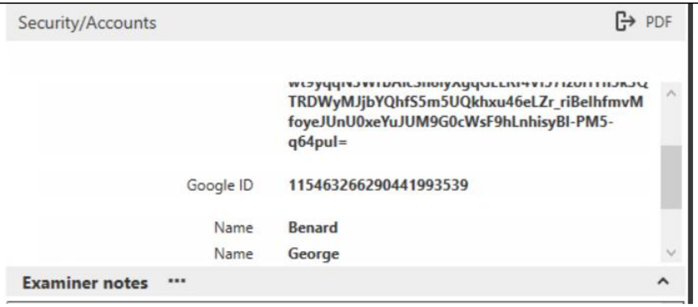
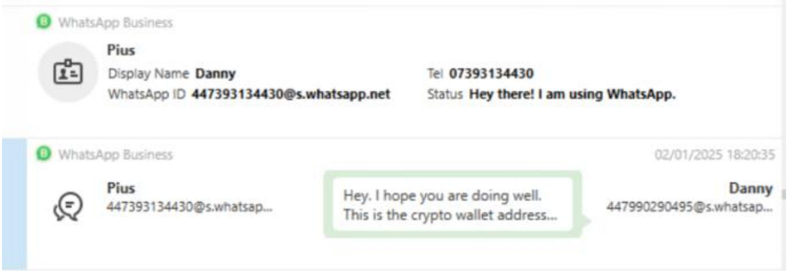
13:17 23-03-2025	In Messages we found George has created the eToro account which is used for trading in cryptocurrency	 GMail 30/12/2024 06:07:45 (Unknown) no-reply@connect.etoro.co... georgeeguy, you're in. Say hello... <u></u> +447990290495 george.benard2024@gmail... GMail Subject georgeeguy, you're in. Say hello to eToro Email viewer Dear georgeeguy, We're thrilled to have you join us, and can't wait for you to start your eToro journey. We're committed to making your eToro experience personal and tailored just for you! Take a Look Around Over the next few days, we'll be sending a series of emails to help you get started on eToro. They'll cover everything from navigating our platform to making your first trade and connecting with other investors from around the world. Got any questions? Need assistance? Our friendly Customer Service team is here to help. Thank you for choosing eToro. To: Email george.benard2024@gmail.com Name (Matched) +447990290495 Time 30/12/2024 06:07:45 (Network) [30/12/2024 06:07:45 UTC] Direction Incoming

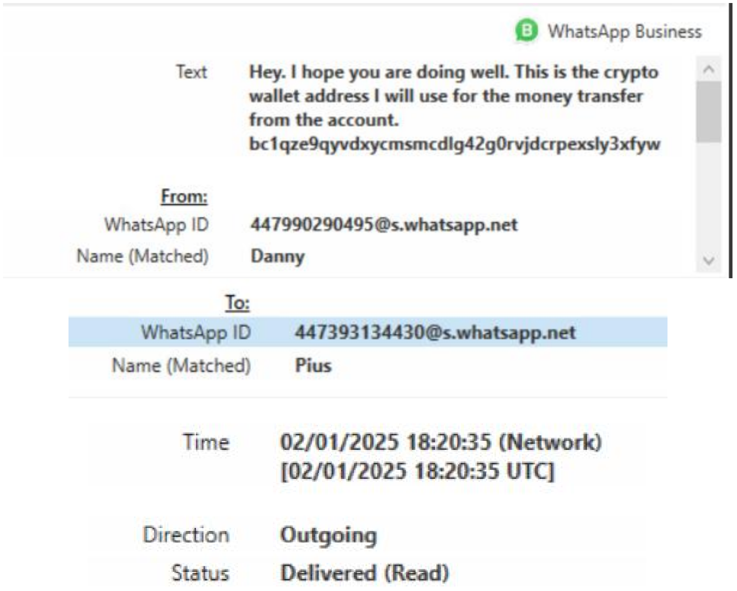
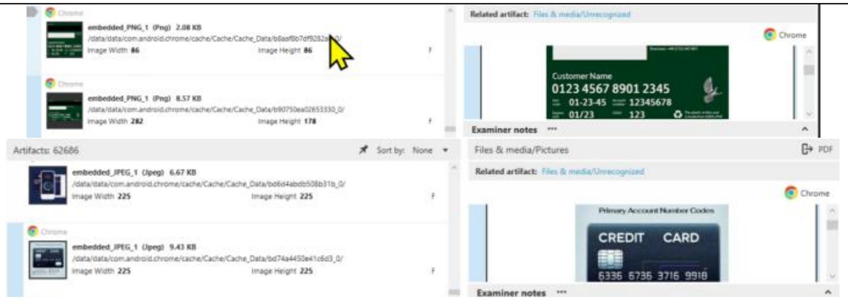
13:19 23-03-2025	In Messages folder we have found that email to George to invest in cryptocurrency trading	 GMail 01/01/2025 11:27:26 (Unknown) no-reply@connect.etoro.co... 2024: The Year Crypto Shaped Up <u></u> +447990290495 george.benard2024@gmail... Messages/Emails Subject 2024: The Year Crypto Shaped Up Milestones and Moments: A Look at 2024 View Online FTT FTX Token ▲12.49% 3.69 2024: A Transformative Year for Crypto From ETFs opening doors to everyday investors to nations embracing Bitcoin, 2024 reshaped the crypto landscape. Trading volumes soared, and Bitcoin hit milestones, capturing attention worldwide. 2025: The Year Ahead With institutional interest rising, supportive regulations on the horizon, and blockchain tech advancing, 2025 promises even greater opportunities for crypto enthusiasts and investors. Ready for what's next?

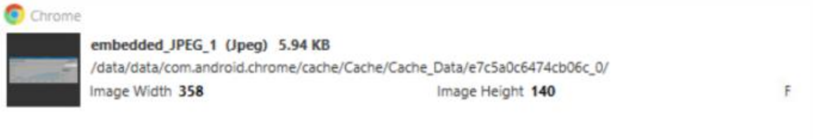
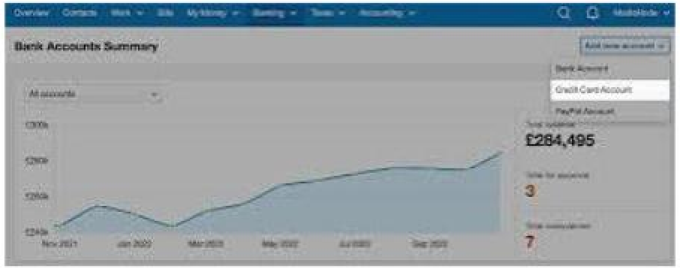
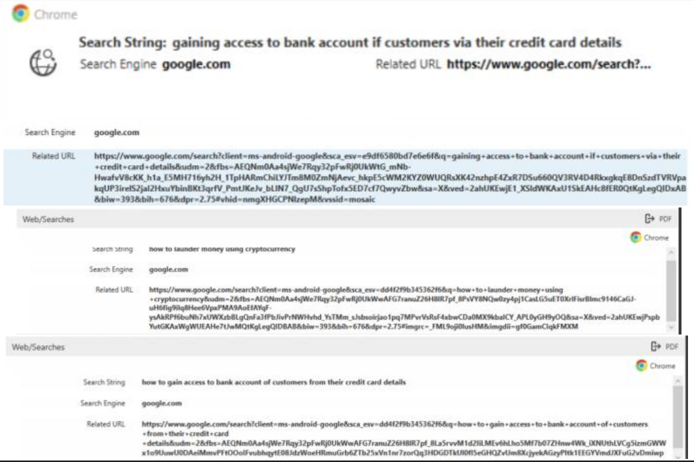
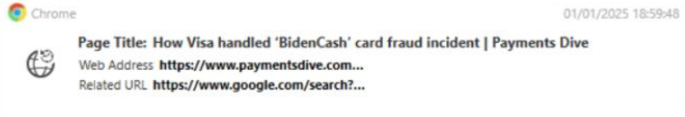
13:25 23-03-2025	In Messages folder we have found that Gorge has registered account in world largest cryptocurrency exchange digital trading	 GMail 30/12/2024 16:01:34 (Unknown) do-not-reply@ses.binance.... 【Binance】Confirm Your Registr... +447990290495 george.benard2024@gmail... Subject 【Binance】Confirm Your Registration From 5.71.95.75 - 2024-12-30 16:01:32(UTC) Email viewer Your Crypto Journey Starts Now Welcome to Binance. Confirm your registration by using the activation code below. Account activation code: 280478 Security Tips : Never give your password to anyone. Never call any phone number from someone claiming to be Binance Customer Support. Never send any money to anyone claiming to be a member of the Binance team. Enable Google Two-Factor Authentication. Set up your anti-phishing code to add an extra layer of security to your account.
13:37 23-03-2025	Email from George has to Danny where George claim to have credit card.	 GMail 03/01/2025 08:02:11 dannymannew2014@g... dannymannew2014@gmail... Credit Cards <div dir="auto">Hey buddy,<div... +447990290495 george.benard2024@gmail... Messages/Emails PDF GMail Subject Credit Cards Email viewer Hey buddy, I have the credit cards. When can I start using them on the respective bank accounts? View as Text Source HTML
	This email where send on 2nd Jan 2025 but email id was wrong. Then on 3rd Jan, 2025 with proper email id of Danny , George has send mail.	

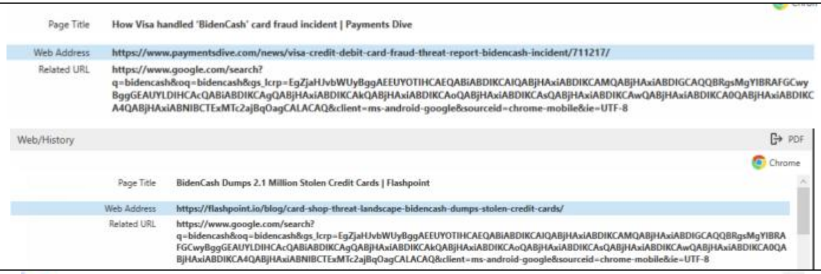
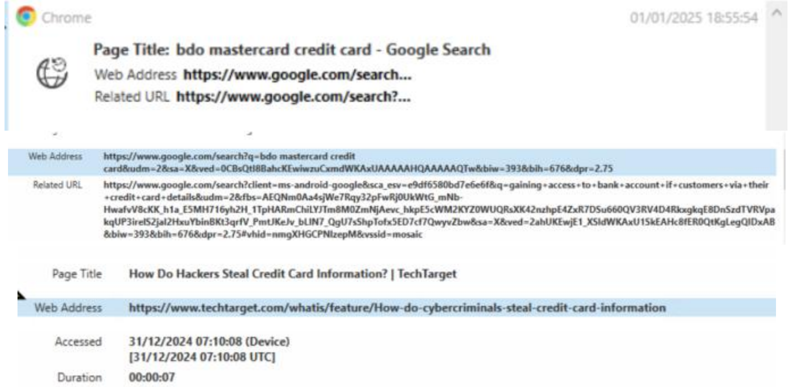
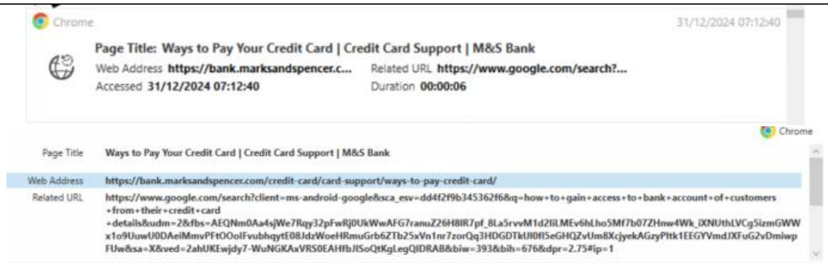
		 Messages/Emails PDF GMail From: Email george.benard2024@gmail.com Name (Matched) +447990290495 To: Email dannymannew2014@gmail.com Name (Matched) dannymannew2014@gmail.com
13:40 23-03-2025	In Emails where George has received the reply from Danny regarding start of using MasterCard with cryptocurrency wallet setup	 GMail 03/01/2025 08:07:21 dannymannew2014@g... dannymannew2014@gmail... Re: Credit Cards <div dir="ltr">Hi George, <div>Y... +447990290495 george.benard2024@gmail... GMail Subject Re: Credit Cards Email viewer Hi George, You can start immediately. I suggest you start with the mastercard ones. I believe you have setup the cryptocurrency wallets correctly. View as Text Source HTML From: Email dannymannew2014@gmail.com Name (Matched) dannymannew2014@gmail.com To: Email george.benard2024@gmail.com Name (Matched) +447990290495
13:47 23-03-2025	Evidence found in Emails where George has replied to Danny	 GMail 04/01/2025 13:51:50 dannymannew2014@g... dannymannew2014@gmail... Re: Credit Cards <p dir="ltr">Hi buddy, I will start... +447990290495 george.benard2024@gmail...

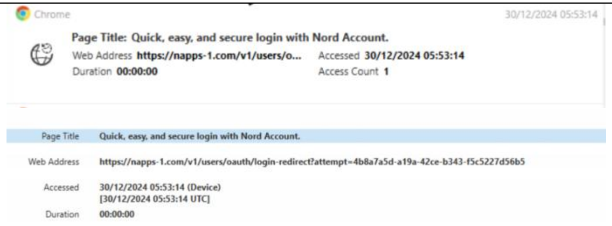
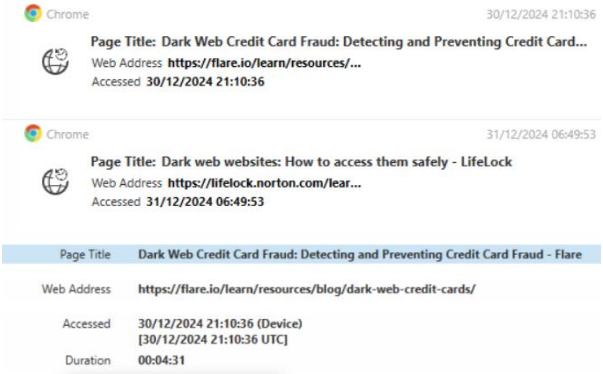
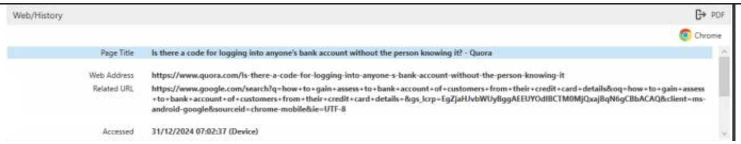
		 Messages/Emails PDF GMail Subject Re: Credit Cards Email viewer Hi buddy, I will start with the MasterCard ones as suggested. Also, I have a few crypto currency wallets and will send you the addresses soon. View as Text Source HTML **From:** Email george.benard2024@gmail.com Name (Matched) +447990290495 **To:** Email dannymannew2014@gmail.com Name (Matched) dannymannew2014@gmail.com
13:50 23-03-2025	George Android account password found in Message folder	 LIST DETAILS Artifacts: 62686 Sort by: None Account Name: WhatsApp Business Related Account Android Accounts Domain com.whatsapp.w4b Account Name: george.benard2024@gmail.com Password aas_et/AKppINZwLFJzwNDpiDN7y... Google ID 115463266290441993539 Name Benard Name George Selected artifacts: 1 Security/Accounts PDF Account Name george.benard2024@gmail.com Password aas_et/AKppINZwLFJzwNDpiDN7yMt32D0XDu72O5eUEq qf0N_muj4-jB4d1jWkJchphHKVfg6_Ihs0TwGNWmU3IH3CE4Tu wt9yqqN3WrbAlcSh8iyXgqGELRf4VI57IzorIYh5k3Q TRDWyMJjbYQhf55m5UQkhau46eLZr_riBelhfmvM foyeJUnU0xeYuJUM9G0cWsF9hLnhisyBI-PM5- Examiner notes 2025-01-13_09.44--564--Google Pixel 5a (G020F).ary  Security/Accounts PDF Google ID 115463266290441993539 Name Benard Name George Related Account Android Accounts Domain com.google

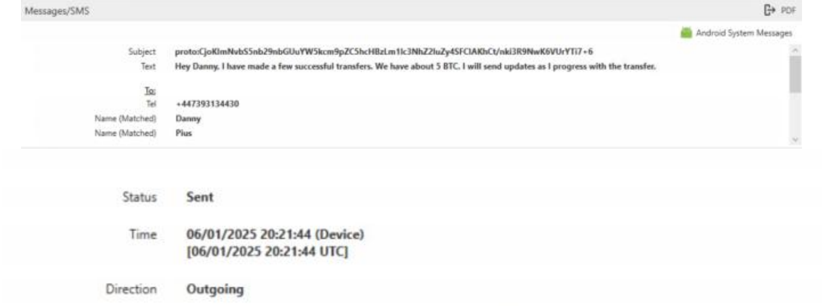
		 Security/Accounts TRDWyMJjbYQhfS5m5UQkhxu46eLZr_riBelhfmvM foyeJUnU0xeYuJUM9G0cWsF9hLnhisyBI-PM5- q64pul= Google ID 115463266290441993539 Name Benard Name George Examiner notes
13:55 23-03-2025	Danny was in contact using whatsapp business.	 WhatsApp Business Pius Display Name Danny WhatsApp ID 447393134430@s.whatsapp.net Tel 07393134430 Status Hey there! I am using WhatsApp. WhatsApp Business 02/01/2025 18:20:35 Pius 447393134430@s.whatsap... Hey. I hope you are doing well. This is the crypto wallet address... Danny 447990290495@s.whatsap...

	Danny is using crypto wallet to transfer the money	 WhatsApp Business Text: Hey. I hope you are doing well. This is the crypto wallet address I will use for the money transfer from the account. bc1qze9qyvdxycmsmcdlg42g0rvjdcrpexsly3xfyw **From:** WhatsApp ID: 447990290495@s.whatsapp.net Name (Matched): Danny **To:** WhatsApp ID: 447393134430@s.whatsapp.net Name (Matched): Pius Time: 02/01/2025 18:20:35 (Network) [02/01/2025 18:20:35 UTC] Direction: Outgoing Status: Delivered (Read)
14:18 23-03-2025	Found credit card phones in media folder	 embedded_PNG_1 (Png) 2.08 KB /data/data/com.android.chrome/cache/Cache/Cache_Data/b8aaf8b7df9282a_0/ Image Width 86 Image Height 86 embedded_PNG_1 (Png) 8.57 KB /data/data/com.android.chrome/cache/Cache/Cache_Data/b90750ea02653330_0/ Image Width 282 Image Height 178 Related artifact: Files & media/Unrecognized Customer Name 0123 4567 8901 2345 01-23-45 12345678 01/23 123 Examiner notes Artifacts: 62686 Sort by: None embedded_JPEG_1 (Jpeg) 6.67 KB /data/data/com.android.chrome/cache/Cache/Cache_Data/bd6d4abdb508b31b_0/ Image Width 225 Image Height 225 embedded_JPEG_1 (Jpeg) 9.43 KB /data/data/com.android.chrome/cache/Cache/Cache_Data/bd74a4450e41c6d3_0/ Image Width 225 Image Height 225 Files & media/Pictures Related artifact: Files & media/Unrecognized Primary Account Number Codes CREDIT CARD 6336 6736 3716 9918 Examiner notes

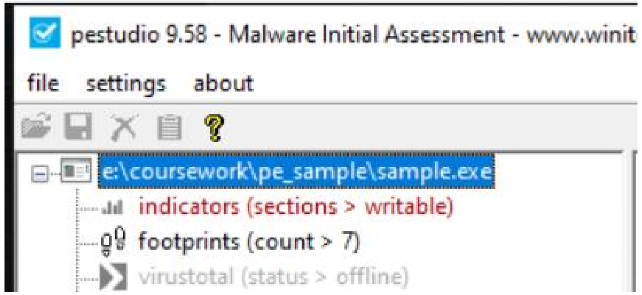
14:26 23-03-2025	Bank account summary details found in Media folder	 Chrome **embedded_JPEG_1 (Jpeg) 5.94 KB** /data/data/com.android.chrome/cache/Cache/Cache_Data/e7c5a0c6474cb06c_0/ Image Width **358** Image Height **140** F  Overview Contacts Bank Accounts Summary Add new account Bank Account Credit Card Account PayPal Account All accounts £284,495 3 7
14:42 23-03-2025	Chrome search history of Gaining access to bank account via credit cards	 Chrome **Search String: gaining access to bank account if customers via their credit card details** Search Engine **google.com** Related URL **https://www.google.com/search?...** Search Engine **google.com** Related URL **https://www.google.com/search?client=ms-android-google&sca_esv=e9df6580bd7e6e6f&q=gaining+access+to+bank+account+if+customers+via+their+credit+card+details&udm=2&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWtG_mNb-HwafvV8cKK_h1a_E5MH716yh2H_1TpHARmChiLYJTm8M0ZmNjAevc_hkpE5cWM2KYZ0WUQRsXK42nzhpE4ZxR7DSu660QV3RV4D4RkxgkqE8DnSzdTVRVpakqUP3irelS2jal2HxuYbinBKt3qrfV_PmtJKeJv_bLIN7_QgU7sShpTofx5ED7cf7QwyvZbw&sa=X&ved=2ahUKEwjE1_XSldWKAxU1SkEAHc8fER0QtKgLegQIDxAB&biw=393&bih=676&dpr=2.75#vhid=nmgXHGCPNlzepM&vssid=mosaic** Web/Searches PDF Chrome Search String **how to launder money using cryptocurrency** Search Engine **google.com** Related URL **https://www.google.com/search?client=ms-android-google&sca_esv=dd4f2f9b345362f6&q=how+to+launder+money+using+cryptocurrency&udm=2&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWwAFG7ranuZ26H8lR7pf_8PsVY8NQw0zy4pj1CasLG5uET0XrlFisrBlmc9146CaGJ-uH6fig9ilq8Hee6VpxPMA9AoEfAYqF-ysAkRPf6buNh7xUWXzbBLgQnFa3fPbJivPrNWHvhd_YsTMm_sJsbsoirjao1pq7MPvrVsRsF4xbwCDa0MX9kbalCY_APL0yGH9yOQ&sa=X&ved=2ahUKEwjPspbYutGKAxWgWUEAHe7tJwMQtKgLegQIDBAB&biw=393&bih=676&dpr=2.75#imgrc=_FML9oji0lusHM&imgdii=gf0GamClqkFMXM** Web/Searches PDF Chrome Search String **how to gain access to bank account of customers from their credit card details** Search Engine **google.com** Related URL **https://www.google.com/search?client=ms-android-google&sca_esv=dd4f2f9b345362f6&q=how+to+gain+access+to+bank+account+of+customers+from+their+credit+card+details&udm=2&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWwAFG7ranuZ26H8lR7pf_8La5rvvM1d2liLMEv6hLho5Mf7b07ZHnw4Wk_iXNUthLVCg5izmGWWx1o9UuwU0DAeiMmvPFtOOolFvubhqytE08JdzWoeHRmuGrb6ZTb25xVn1nr7zorQq3HDGDTkUl0fl5eGHQZvUm8XcjyekAGzyPltk1EEGYVmdJXFuG2vDmiwp**
14:45 23-03-2025	Chrome search history of How to handle BidenCash fraud incident	 Chrome 01/01/2025 18:59:48 **Page Title: How Visa handled 'BidenCash' card fraud incident | Payments Dive** Web Address **https://www.paymentsdive.com...** Related URL **https://www.google.com/search?...**

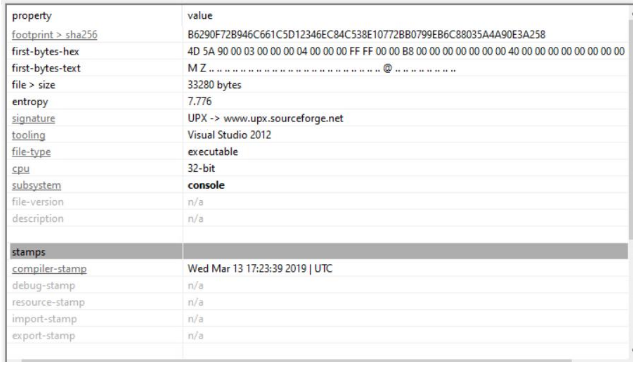
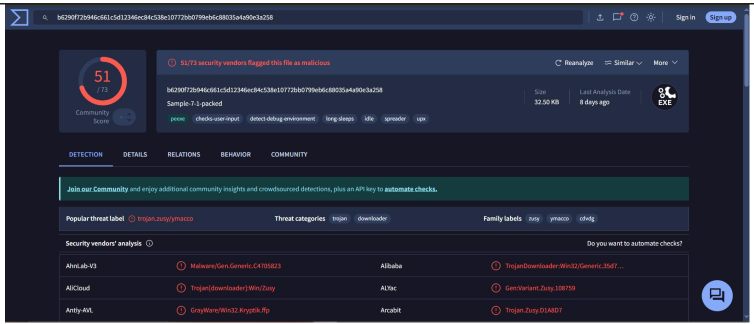
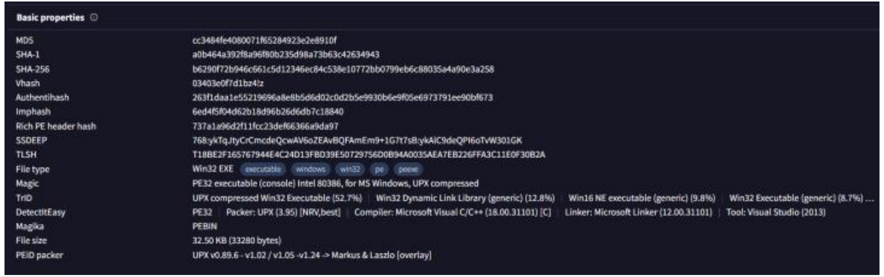
		 Page Title How Visa handled 'BidenCash' card fraud incident | Payments Dive Web Address https://www.paymentsdive.com/news/visa-credit-debit-card-fraud-threat-report-bidencash-incident/711217/ Related URL https://www.google.com/search?q=bidencash&oq=bidencash&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQABiABDIKCAIQABjHAxiABDIKCAMQABjHAxiABDIGCAQQBRgsMgYIBRAFGCwyBggGEAUYLDIHCAcQABiABDIKCAgQABjHAxiABDIKCAkQABjHAxiABDIKCAoQABjHAxiABDIKCAsQABjHAxiABDIKCAwQABjHAxiABDIKCA0QABjHAxiABDIKCA4QABjHAxiABNIBCTExMTc2ajBqOagCALACAQ&client=ms-android-google&sourceid=chrome-mobile&ie=UTF-8 Web/History Chrome Page Title BidenCash Dumps 2.1 Million Stolen Credit Cards | Flashpoint Web Address https://flashpoint.io/blog/card-shop-threat-landscape-bidencash-dumps-stolen-credit-cards/ Related URL https://www.google.com/search?q=bidencash&oq=bidencash&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQABiABDIKCAIQABjHAxiABDIKCAMQABjHAxiABDIGCAQQBRgsMgYIBRAFGCwyBggGEAUYLDIHCAcQABiABDIKCAgQABjHAxiABDIKCAkQABjHAxiABDIKCAoQABjHAxiABDIKCAsQABjHAxiABDIKCAwQABjHAxiABDIKCA0QABjHAxiABDIKCA4QABjHAxiABNIBCTExMTc2ajBqOagCALACAQ&client=ms-android-google&sourceid=chrome-mobile&ie=UTF-8
14:50 23-03-2025	Chrome search history of Steal credit card information	 Chrome 01/01/2025 18:55:54 Page Title: bdo mastercard credit card - Google Search Web Address https://www.google.com/search... Related URL https://www.google.com/search?... Web Address https://www.google.com/search?q=bdo mastercard credit card&udm=2&sa=X&ved=0CBsQtI8BahcKEwiwzuCxmdWKAxUAAAAAHQAAAAAQTw&biw=393&bih=676&dpr=2.75 Related URL https://www.google.com/search?client=ms-android-google&sca_esv=e9df6580bd7e6e6f&q=gaining+access+to+bank+account+if+customers+via+their+credit+card+details&udm=2&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWtG_mNb-HwafvV8cKK_h1a_E5MH716yh2H_1TpHARmChiLYJTm8M0ZmNjAevc_hkpE5cWM2KYZ0WUQRsXK42nzhpE4ZxR7DSu660QV3RV4D4RkxgkqE8DnSzdTVRVpakqUP3irelS2jal2HxuYbinBKt3qrfV_PmtJKeJv_bLIN7_QgU7sShpTofx5ED7cf7QwyvZbw&sa=X&ved=2ahUKEwjE1_XSldWKAxU1SkEAHc8fER0QtKgLegQIDxAB&biw=393&bih=676&dpr=2.75#vhid=nmgXHGCPNlzepM&vssid=mosaic Page Title How Do Hackers Steal Credit Card Information? | TechTarget Web Address https://www.techtarget.com/whatis/feature/How-do-cybercriminals-steal-credit-card-information Accessed 31/12/2024 07:10:08 (Device) [31/12/2024 07:10:08 UTC] Duration 00:00:07
14:43 23-03-2025	Chrome search history of Credit payment to M&S bank	 Chrome 31/12/2024 07:12:40 Page Title: Ways to Pay Your Credit Card | Credit Card Support | M&S Bank Web Address https://bank.marksandspencer.c... Related URL https://www.google.com/search?... Accessed 31/12/2024 07:12:40 Duration 00:00:06 Chrome Page Title Ways to Pay Your Credit Card | Credit Card Support | M&S Bank Web Address https://bank.marksandspencer.com/credit-card/card-support/ways-to-pay-credit-card/ Related URL https://www.google.com/search?client=ms-android-google&sca_esv=dd4f2f9b345362f6&q=how+to+gain+access+to+bank+account+of+customers+from+their+credit+card+details&udm=2&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWwAFG7ranuZ26H8IR7pf_8La5rvvM1d2liLMEv6hLho5Mf7b07ZHnw4Wk_iXNUthLVCg5izmGWWx1o9UuwU0DAeiMmvPFtOOolFvubhqytE08JdzWoeHRmuGrb6ZTb25xVn1nr7zorQq3HDGDTkUl0fI5eGHQZvUm8XcjyekAGzyPltk1EEGYVmdJXFuG2vDmiwpFUw&sa=X&ved=2ahUKEwjdy7-WuNGKAxVRS0EAHfbJISoQtKgLegQIDRAB&biw=393&bih=676&dpr=2.75#ip=1

14:58 23-03-2025	Chrome search history of opening Nord account for using VPN	 Chrome 30/12/2024 05:53:14 Page Title: Quick, easy, and secure login with Nord Account. Web Address https://napps-1.com/v1/users/o... Accessed 30/12/2024 05:53:14 Duration 00:00:00 Access Count 1 Page Title Quick, easy, and secure login with Nord Account. Web Address https://napps-1.com/v1/users/oauth/login-redirect?attempt=4b8a7a5d-a19a-42ce-b343-f5c5227d56b5 Accessed 30/12/2024 05:53:14 (Device) [30/12/2024 05:53:14 UTC] Duration 00:00:00
15:00 23-03-2025	Chrome search history of Accessing Dark web for credit card fraud	 Chrome 30/12/2024 21:10:36 Page Title: Dark Web Credit Card Fraud: Detecting and Preventing Credit Card... Web Address https://flare.io/learn/resources/... Accessed 30/12/2024 21:10:36 Chrome 31/12/2024 06:49:53 Page Title: Dark web websites: How to access them safely - LifeLock Web Address https://lifelock.norton.com/lear... Accessed 31/12/2024 06:49:53 Page Title Dark Web Credit Card Fraud: Detecting and Preventing Credit Card Fraud - Flare Web Address https://flare.io/learn/resources/blog/dark-web-credit-cards/ Accessed 30/12/2024 21:10:36 (Device) [30/12/2024 21:10:36 UTC] Duration 00:04:31
15:02 23-03-2025	Chrome search history of code to logging in anyone bank account	 Web/History PDF Chrome Page Title Is there a code for logging into anyone's bank account without the person knowing it? - Quora Web Address https://www.quora.com/Is-there-a-code-for-logging-into-anyone-s-bank-account-without-the-person-knowing-it Related URL https://www.google.com/search?q=how+to+gain+assess+to+bank+account+of+customers+from+their+credit+card+details&oq=how+to+gain+assess+to+bank+account+of+customers+from+their+credit+card+details+&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCTM0MjQxajBqN6gCBbACAQ&client=ms-android-google&sourceid=chrome-mobile&ie=UTF-8 Accessed 31/12/2024 07:02:37 (Device)

15:20 23-03-2025	Message found money transfer by George to Danny	 Messages/SMS PDF Android System Messages Subject proto:CjoKlmNvbS5nb29nbGUuYW5kcm9pZC5hcHBzLm1lc3NhZ2luZy4SFClAKhCt/nki3R9NwK6VUrYTi7+6 Text Hey Danny. I have made a few successful transfers. We have about 5 BTC. I will send updates as I progress with the transfer. To: Tel +447393134430 Name (Matched) Danny Name (Matched) Plus Status Sent Time 06/01/2025 20:21:44 (Device) [06/01/2025 20:21:44 UTC] Direction Outgoing

3.4. Table 6: This process show performing the *Static analysis* on PE sample using *Pestudio tool*

Date/ time	Process	Evidence
21:00 23-03-2025	Open Pestudio	
21:05 23-03-2025	Entropy is 7.776 which is very high. It indicate the data has been compressed, encrypted, or obfuscated. "4D 5A" value in the first-byte-hexadecimal and the "M Z" string in the first-byte-text, it confirms it is a portable executable file (.exe).	 pestudio 9.58 - Malware Initial Assessment - www.winit e:\coursework\pe_sample\sample.exe indicators (sections > writable) footprints (count > 7) virustotal (status > offline)

	UPX, a popular packer for compression look like to have been used to pack t he file.	
21:10 23-03-2025	Copy the hash code	 
	Paste in Virus total	
	Family it below to is trojan.zusy/ymacco	

property	value
footprint > sha256	B6290F72B946C661C5D12346EC84C538E10772BB0799EB6C88035A4A90E3A258
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file > size	33280 bytes
entropy	7.776
signature	UPX -> www.upx.sourceforge.net
tooling	Visual Studio 2012
file-type	executable
cpu	32-bit
subsystem	**console**
file-version	n/a
description	n/a
stamps	
compiler-stamp	Wed Mar 13 17:23:39 2019 | UTC
debug-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a

b6290f72b946c661c5d12346ec84c538e10772bb0799eb6c88035a4a90e3a258
Sign in
Sign up
51
/ 73
Community Score

51/73 security vendors flagged this file as malicious

b6290f72b946c661c5d12346ec84c538e10772bb0799eb6c88035a4a90e3a258
Sample-7-1-packed

peexe checks-user-input detect-debug-environment long-sleeps idle spreader upx

Size 32.50 KB

Last Analysis Date 8 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.zusy/ymacco

Threat categories trojan downloader

Family labels zusy ymacco cdvdg

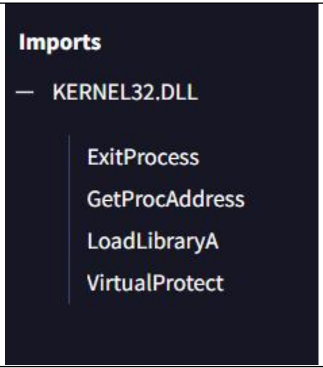
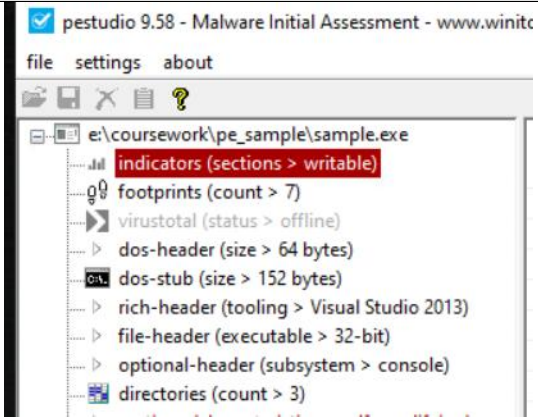
Security vendors' analysis

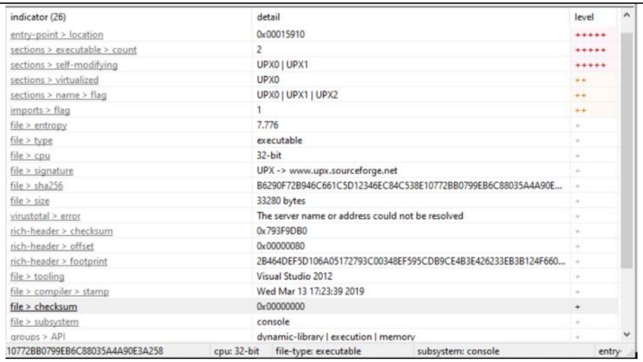
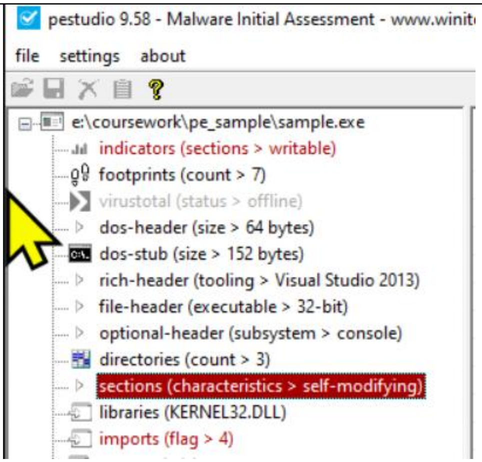
Do you want to automate checks?

AhnLab-V3	Malware/Gen.Generic.C4705823	Alibaba	TrojanDownloader:Win32/Generic.35d7...
AliCloud	Trojan[downloader]:Win/Zusy	ALYac	Gen:Variant.Zusy.108759
Antiy-AVL	GrayWare/Win32.Kryptik.ffp	Arcabit	Trojan.Zusy.D1A8D7

Basic properties

MD5	cc3484fe4080071f65284923e2e8910f
SHA-1	a0b464a392f8a96f80b235d98a73b63c42634943
SHA-256	b6290f72b946c661c5d12346ec84c538e10772bb0799eb6c88035a4a90e3a258
Vhash	03403e0f7d1bz4!z
Authentihash	263f1daa1e55219696a8e8b5d6d02c0d2b5e9930b6e9f05e6973791ee90bf673
Imphash	6ed4f5f04d62b18d96b26d6db7c18840
Rich PE header hash	737a1a96d2f11fcc23def66366a9da97
SSDEEP	768:ykTqJtyCrCmcdeQcwAV6oZEAvBQFAmEm9+1G7t7sB:ykAlC9deQPI6oTvW301GK
TLSH	T18BE2F165767944E4C24D13FBD39E50729756D0B94A0035AEA7EB226FFA3C11E0F30B2A
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (console) Intel 80386, for MS Windows, UPX compressed
TrID	UPX compressed Win32 Executable (52.7%) | Win32 Dynamic Link Library (generic) (12.8%) | Win16 NE executable (generic) (9.8%) | Win32 Executable (generic) (8.7%) ...
DetectItEasy	PE32 | Packer: UPX (3.95) [NRV,best] | Compiler: Microsoft Visual C/C++ (18.00.31101) [C] | Linker: Microsoft Linker (12.00.31101) | Tool: Visual Studio (2013)
Magika	PEBIN
File size	32.50 KB (33280 bytes)
PEiD packer	UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus & Laszlo [overlay]

		 Imports — KERNEL32.DLL ExitProcess GetProcAddress LoadLibraryA VirtualProtect
21:20 23-03-2025	Sections >> writable and self-modifying, a behavior commonly found in malware to evade detection.	 pestudio 9.58 - Malware Initial Assessment - www.winitc file settings about e:\coursework\pe_sample\sample.exe indicators (sections > writable) footprints (count > 7) virustotal (status > offline) dos-header (size > 64 bytes) dos-stub (size > 152 bytes) rich-header (tooling > Visual Studio 2013) file-header (executable > 32-bit) optional-header (subsystem > console) directories (count > 3)
	The file is UPX-packed (UPX0 | UPX1 | UPX2), often used to obfuscate malicious code.	
	Kernel32.dll is imported, commonly used for system-level API calls, including process injection or privilege escalation.	

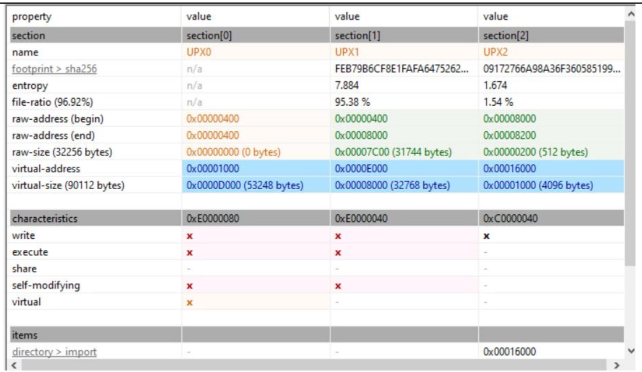
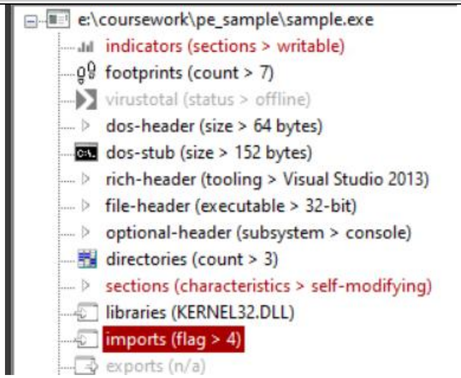
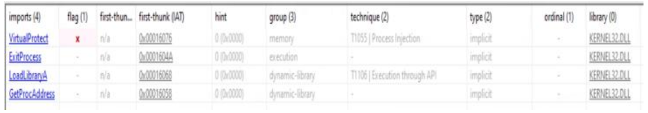
	virtualization -> UPX0 suggests further obfuscation techniques	
	The checksum is 0x0000000, which may indicate tampering.	
21:40 23-03-2025	Go to section	
	Section shows the file is UPX-packed (UPX0 | UPX1 | UPX2) with each entropy and dile-ratio and in which UPX1 entropy is very high	

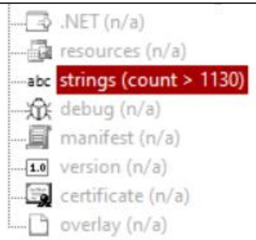
indicator (26)	detail	level
entry-point > location	0x00015910	+++++
sections > executable > count	2	+++++
sections > self-modifying	UPX0 | UPX1	+++++
sections > virtualized	UPX0	++
sections > name > flag	UPX0 | UPX1 | UPX2	++
imports > flag	1	++
file > entropy	7.776	+
file > type	executable	+
file > cpu	32-bit	+
file > signature	UPX -> www.upx.sourceforge.net	+
file > sha256	B6290F72B946C661C5D12346EC84C538E10772BB0799EB6C88035A4A90E...	+
file > size	33280 bytes	+
virustotal > error	The server name or address could not be resolved	+
rich-header > checksum	0x793F9DB0	+
rich-header > offset	0x00000080	+
rich-header > footprint	2B464DEF5D106A05172793C00348EF595CDB9CE4B3E426233EB3B124F660...	+
file > tooling	Visual Studio 2012	+
file > compiler > stamp	Wed Mar 13 17:23:39 2019	+
file > checksum	0x00000000	+
file > subsystem	console	+
groups > API	dynamic-library | execution | memory	+

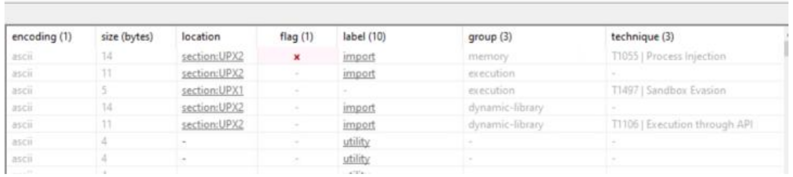
10772BB0799EB6C88035A4A90E3A258 cpu: 32-bit file-type: executable subsystem: console entry-

pestudio 9.58 - Malware Initial Assessment - www.winit

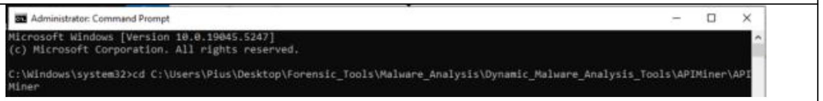
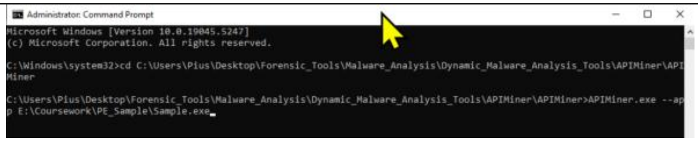
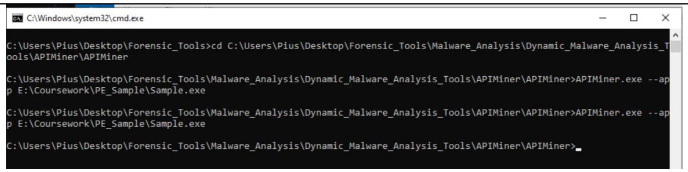
```
e:\coursework\pe_sample\sample.exe
    indicators (sections > writable)
    footprints (count > 7)
    virustotal (status > offline)
    dos-header (size > 64 bytes)
    dos-stub (size > 152 bytes)
    rich-header (tooling > Visual Studio 2013)
    file-header (executable > 32-bit)
    optional-header (subsystem > console)
    directories (count > 3)
    sections (characteristics > self-modifying)
    libraries (KERNEL32.DLL)
    imports (flag > 4)
```

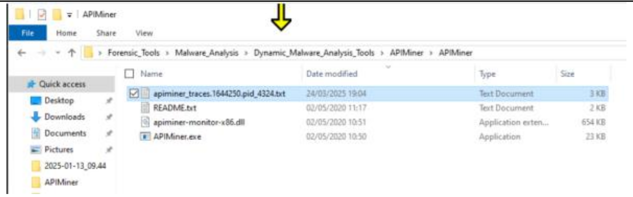
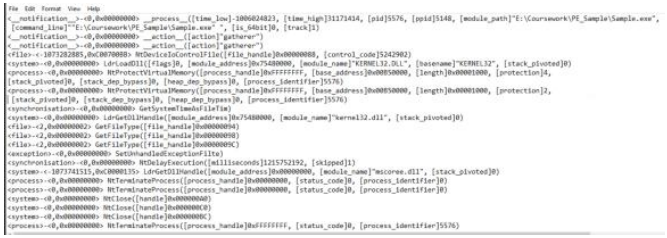
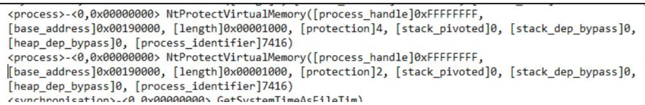
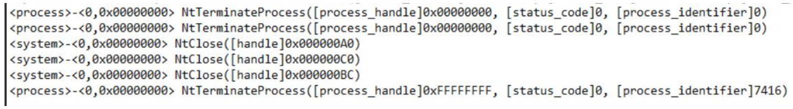
<table>
<tr>
<td></td>
<td>As seen in Characteristics UPX1 has all RWX rights
UPX1 and UPX2 have execution permissions, meaning they will run code after unpacking.</td>
<td>
<table>
<tr><th>property</th><th>value</th><th>value</th><th>value</th></tr>
<tr><td>section</td><td>section[0]</td><td>section[1]</td><td>section[2]</td></tr>
<tr><td>name</td><td>UPX0</td><td>UPX1</td><td>UPX2</td></tr>
<tr><td>footprint > sha256</td><td>n/a</td><td>FEB79B6CF8E1FAFA6475262...</td><td>09172766A98A36F360585199...</td></tr>
<tr><td>entropy</td><td>n/a</td><td>7.884</td><td>1.674</td></tr>
<tr><td>file-ratio (96.92%)</td><td>n/a</td><td>95.38 %</td><td>1.54 %</td></tr>
<tr><td>raw-address (begin)</td><td>0x00000400</td><td>0x00000400</td><td>0x00008000</td></tr>
<tr><td>raw-address (end)</td><td>0x00000400</td><td>0x00008000</td><td>0x00008200</td></tr>
<tr><td>raw-size (32256 bytes)</td><td>0x00000000 (0 bytes)</td><td>0x00007C00 (31744 bytes)</td><td>0x00000200 (512 bytes)</td></tr>
<tr><td>virtual-address</td><td>0x00001000</td><td>0x0000E000</td><td>0x00016000</td></tr>
<tr><td>virtual-size (90112 bytes)</td><td>0x0000D000 (53248 bytes)</td><td>0x00008000 (32768 bytes)</td><td>0x00001000 (4096 bytes)</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>characteristics</td><td>0xE0000080</td><td>0xE0000040</td><td>0xC0000040</td></tr>
<tr><td>write</td><td>x</td><td>x</td><td>x</td></tr>
<tr><td>execute</td><td>x</td><td>x</td><td>-</td></tr>
<tr><td>share</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>self-modifying</td><td>x</td><td>x</td><td>-</td></tr>
<tr><td>virtual</td><td>x</td><td>-</td><td>-</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>items</td><td></td><td></td><td></td></tr>
<tr><td>directory > import</td><td>-</td><td>-</td><td>0x00016000</td></tr>
</table>
</td>
</tr>
<tr>
<td rowspan="3">22:00 23-03-2025</td>
<td>Go to imports
(flag > 4)</td>
<td rowspan="3">
e:\coursework\pe_sample\sample.exe
indicators (sections > writable)
footprints (count > 7)
virustotal (status > offline)
dos-header (size > 64 bytes)
dos-stub (size > 152 bytes)
rich-header (tooling > Visual Studio 2013)
file-header (executable > 32-bit)
optional-header (subsystem > console)
directories (count > 3)
sections (characteristics > self-modifying)
libraries (KERNEL32.DLL)
imports (flag > 4)
exports (n/a)

<table>
<tr><th>imports (4)</th><th>flag (1)</th><th>first-thun...</th><th>first-thunk (IAT)</th><th>hint</th><th>group (3)</th><th>technique (2)</th><th>type (2)</th><th>ordinal (1)</th><th>library (0)</th></tr>
<tr><td>VirtualProtect</td><td>x</td><td>n/a</td><td>0x00016076</td><td>0 (0x0000)</td><td>memory</td><td>T1055 | Process Injection</td><td>implicit</td><td>-</td><td>KERNEL32.DLL</td></tr>
<tr><td>ExitProcess</td><td>-</td><td>n/a</td><td>0x0001604A</td><td>0 (0x0000)</td><td>execution</td><td>-</td><td>implicit</td><td>-</td><td>KERNEL32.DLL</td></tr>
<tr><td>LoadLibraryA</td><td>-</td><td>n/a</td><td>0x00016068</td><td>0 (0x0000)</td><td>dynamic-library</td><td>T1106 | Execution through API</td><td>implicit</td><td>-</td><td>KERNEL32.DLL</td></tr>
<tr><td>GetProcAddress</td><td>-</td><td>n/a</td><td>0x00016058</td><td>0 (0x0000)</td><td>dynamic-library</td><td>-</td><td>implicit</td><td>-</td><td>KERNEL32.DLL</td></tr>
</table>
</td>
</tr>
<tr>
<td>VirtualProtect (Process Injection - T1055)
Used to change memory protection (e.g., making code writable/executable).</td>
</tr>
<tr>
<td>LoadLibraryA & GetProcAddress (T1106 - Execution via API)
Malware can load additional malicious modules at runtime.</td>
</tr>
</table>

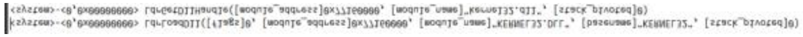
<table>
<tr>
<td rowspan="4">22:05 23-03-2025</td>
<td>VirtualProtect code injection (e.g., modifying memory permissions to execute injected shellcode).</td>
<td rowspan="4">


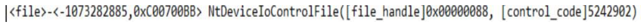

<table>
<tr><th>encoding (1)</th><th>size (bytes)</th><th>location</th><th>flag (1)</th><th>label (10)</th><th>group (3)</th><th>technique (3)</th></tr>
<tr><td>ascii</td><td>14</td><td>section:UPX2</td><td>×</td><td>import</td><td>memory</td><td>T1055 | Process Injection</td></tr>
<tr><td>ascii</td><td>11</td><td>section:UPX2</td><td>-</td><td>import</td><td>execution</td><td>-</td></tr>
<tr><td>ascii</td><td>5</td><td>section:UPX1</td><td>-</td><td>-</td><td>execution</td><td>T1497 | Sandbox Evasion</td></tr>
<tr><td>ascii</td><td>14</td><td>section:UPX2</td><td>-</td><td>import</td><td>dynamic-library</td><td>-</td></tr>
<tr><td>ascii</td><td>11</td><td>section:UPX2</td><td>-</td><td>import</td><td>dynamic-library</td><td>T1106 | Execution through API</td></tr>
<tr><td>ascii</td><td>4</td><td>-</td><td>-</td><td>utility</td><td>-</td><td>-</td></tr>
<tr><td>ascii</td><td>4</td><td>-</td><td>-</td><td>utility</td><td>-</td><td>-</td></tr>
</table>
</td>
</tr>
<tr>
<td>ExitProcess → Execution Control
May indicate anti-analysis behavior terminating execution under specific conditions.</td>
</tr>
<tr>
<td>Sleep → (T1497 | Sandbox Evasion)
Could be delaying execution to evade detection in sandboxes.</td>
</tr>
<tr>
<td>GetProcAddress & LoadLibrary → (T1106 | Execution through API)
Used for dynamically resolving function addresses (common in malware to hide API calls).</td>
</tr>
</table>

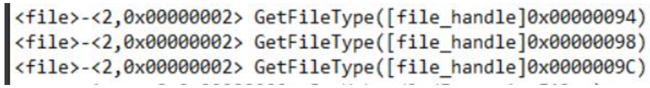
3.5. Table 7: This process show *Dynamic Analysis using API miner tool* examine a API calls without altering the original data.

Date/ Time	Process	Evidence
19:00 24-03-2025	Open API Miner	
19:01 24-03-2025	Open CMD >> Run as administrator	
19:02 24-03-2025	Write below command cd C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_tools\APIMiner\APIMiner	 Administrator: Command Prompt Microsoft Windows [Version 10.0.19045.5247] (c) Microsoft Corporation. All rights reserved. C:\Windows\system32>cd C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_Tools\APIMiner\API Miner
	Hit Enter	
19:05 24-03-2025	Write command APIMiner.exe --app E:\Coursework\PE_Sample\Sample.exe	 Administrator: Command Prompt Microsoft Windows [Version 10.0.19045.5247] (c) Microsoft Corporation. All rights reserved. C:\Windows\system32>cd C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_Tools\APIMiner\API Miner C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_Tools\APIMiner\APIMiner>APIMiner.exe --ap p E:\Coursework\PE_Sample\Sample.exe
19:07 24-03-2025	Hit Enter Sample.exe file will run	 C:\Windows\system32\cmd.exe C:\Users\Pius\Desktop\Forensic_Tools>cd C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_T ools\APIMiner\APIMiner C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_Tools\APIMiner\APIMiner>APIMiner.exe --ap p E:\Coursework\PE_Sample\Sample.exe C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_Tools\APIMiner\APIMiner>APIMiner.exe --ap p E:\Coursework\PE_Sample\Sample.exe C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_Tools\APIMiner\APIMiner>

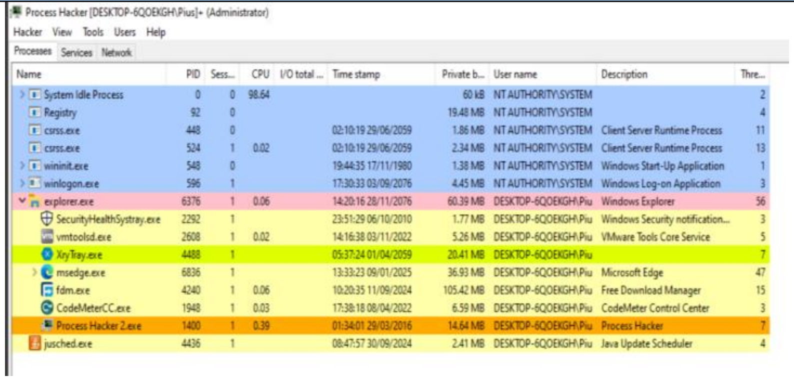
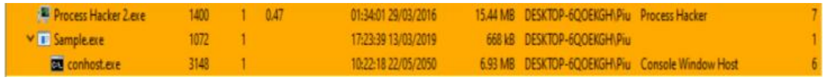
19:08 24-03-2025	Go to APIMiner apiminer_traces.1782031.pid_7416.txt is generated	 APIMiner File Home Share View Forensic_Tools › Malware_Analysis › Dynamic_Malware_Analysis_Tools › APIMiner › APIMiner Quick access Desktop Downloads Documents Pictures 2025-01-13_09.44 APIMiner Name Date modified Type Size ☑ apiminer_traces.1644250.pid_4324.txt 24/03/2025 19:04 Text Document 3 KB README.txt 02/05/2020 11:17 Text Document 2 KB apiminer-monitor-x86.dll 02/05/2020 10:51 Application exten... 654 KB APIMiner.exe 02/05/2020 10:50 Application 23 KB
19:09 24-03-2025	Open file apiminer_traces.1782031.pid_7416.txt User can check the API logs	 File Edit Format View Help <__notification__>-<0,0x00000000> __process__([time_low]-1006024823, [time_high]31171414, [pid]5576, [ppid]5148, [module_path]"E:\Coursework\PE_Sample\Sample.exe", [command_line]""E:\Coursework\PE_Sample\Sample.exe" ", [is_64bit]0, [track]1) <__notification__>-<0,0x00000000> __action__([action]"gatherer") <__notification__>-<0,0x00000000> __action__([action]"gatherer") <file>-<-1073282885,0xC0070088> NtDeviceIoControlFile([file_handle]0x00000088, [control_code]5242902) <system>-<0,0x00000000> LdrLoadDll([flags]0, [module_address]0x75480000, [module_name]"KERNEL32.DLL", [basename]"KERNEL32", [stack_pivoted]0) <process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x00850000, [length]0x00001000, [protection]4, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0, [process_identifier]5576) <process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x00850000, [length]0x00001000, [protection]2, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0, [process_identifier]5576) <synchronisation>-<0,0x00000000> GetSystemTimeAsFileTim) <system>-<0,0x00000000> LdrGetDllHandle([module_address]0x75480000, [module_name]"kernel32.dll", [stack_pivoted]0) <file>-<2,0x00000002> GetFileType([file_handle]0x00000094) <file>-<2,0x00000002> GetFileType([file_handle]0x00000098) <file>-<2,0x00000002> GetFileType([file_handle]0x0000009C) <exception>-<0,0x00000000> SetUnhandledExceptionFilte) <synchronisation>-<0,0x00000000> NtDelayExecution([milliseconds]1215752192, [skipped]1) <system>-<-1073741515,0xC0000135> LdrGetDllHandle([module_address]0x00000000, [module_name]"mscoree.dll", [stack_pivoted]0) <process>-<0,0x00000000> NtTerminateProcess([process_handle]0x00000000, [status_code]0, [process_identifier]0) <process>-<0,0x00000000> NtTerminateProcess([process_handle]0x00000000, [status_code]0, [process_identifier]0) <system>-<0,0x00000000> NtClose([handle]0x000000A0) <system>-<0,0x00000000> NtClose([handle]0x000000C0) <system>-<0,0x00000000> NtClose([handle]0x000000BC) <process>-<0,0x00000000> NtTerminateProcess([process_handle]0xFFFFFFFF, [status_code]0, [process_identifier]5576)
19:12 24-03-2025	NtProtectVirtualMemory is used twice, modifying memory protections at base_address 0x00190000 with protection values 4 and 2.	 <process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x00190000, [length]0x00001000, [protection]4, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0, [process_identifier]7416) <process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x00190000, [length]0x00001000, [protection]2, [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0, [process_identifier]7416) <synchronisation>-<0,0x00000000> GetSystemTimeAsFileTim)
	Changing memory protections can indicate code injection, unpacking, or evasion techniques.	
19:15 24-03-2025	Multiple calls to NtTerminateProcess, potentially trying to evade analysis or terminate security tools.	 <process>-<0,0x00000000> NtTerminateProcess([process_handle]0x00000000, [status_code]0, [process_identifier]0) <process>-<0,0x00000000> NtTerminateProcess([process_handle]0x00000000, [status_code]0, [process_identifier]0) <system>-<0,0x00000000> NtClose([handle]0x000000A0) <system>-<0,0x00000000> NtClose([handle]0x000000C0) <system>-<0,0x00000000> NtClose([handle]0x000000BC) <process>-<0,0x00000000> NtTerminateProcess([process_handle]0xFFFFFFFF, [status_code]0, [process_identifier]7416)

19:16 24-03-2025	LdrLoadDll loads KERNEL32.DLL, which is a standard Windows DLL but is commonly abused in process hollowing or DLL injection.	
		`<system>-<0,0x00000000> LdrGetDllHandle([module_address]0x77100000, [module_name]"kernel32.dll", [stack_pivoted]0)`
		`<system>-<0,0x00000000> LdrLoadDll([flags]0, [module_address]0x77100000, [module_name]"KERNEL32.DLL", [basename]"KERNEL32", [stack_pivoted]0)`

19:20 24-03-2025	NtDeviceIoControlFile is seen with control code 5242902. This might be interacting with a driver, possibly indicating rootkit-like behavior.	 `<file>-<-1073282885,0xC00700BB> NtDeviceIoControlFile([file_handle]0x00000088, [control_code]5242902)`

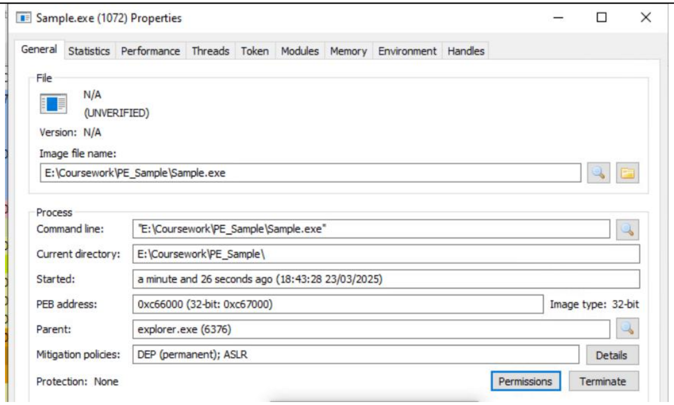
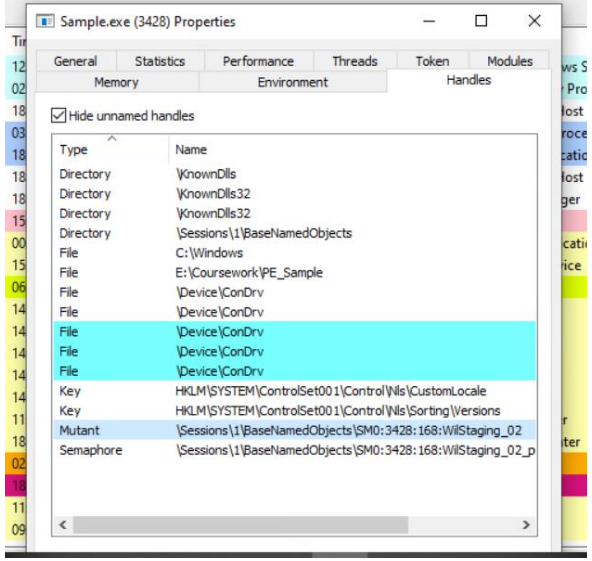
19:25 24-03-2025	GetFileType is used multiple times, likely checking for the existence of files before execution.	
		`<file>-<2,0x00000002> GetFileType([file_handle]0x00000094)`
		`<file>-<2,0x00000002> GetFileType([file_handle]0x00000098)`
		`<file>-<2,0x00000002> GetFileType([file_handle]0x0000009C)`

3.6. Table 8: This process show examine a *PE sample file using Process hacker tool* without altering the original data.

Date/ Time	**Process**	**Evidence**
20:05 24-03-2025	Open Process Hacker	
20:08 24-03-2025	Run file Sample.exe from E:\Coursework\PE_Sample folder	

Name	PID	Sess...	CPU	I/O total ...	Time stamp	Private b...	User name	Description	Thre...
System Idle Process	0	0	98.64			60 kB	NT AUTHORITY\SYSTEM		2
Registry	92	0				19.48 MB	NT AUTHORITY\SYSTEM		4
csrss.exe	448	0			02:10:19 29/06/2059	1.86 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process	11
csrss.exe	524	1	0.02		02:10:19 29/06/2059	2.34 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process	13
wininit.exe	548	0			19:44:35 17/11/1980	1.38 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application	1
winlogon.exe	596	1			17:30:33 03/09/2076	4.45 MB	NT AUTHORITY\SYSTEM	Windows Log-on Application	3
explorer.exe	6376	1	0.06		14:20:16 28/11/2076	60.39 MB	DESKTOP-6QOEKGH\Piu	Windows Explorer	56
SecurityHealthSystray.exe	2292	1			23:51:29 06/10/2010	1.77 MB	DESKTOP-6QOEKGH\Piu	Windows Security notification...	3
vmtoolsd.exe	2608	1	0.02		14:16:38 03/11/2022	5.26 MB	DESKTOP-6QOEKGH\Piu	VMware Tools Core Service	5
XryTray.exe	4488	1			05:37:24 01/04/2059	20.41 MB	DESKTOP-6QOEKGH\Piu		7
msedge.exe	6836	1			13:33:23 09/01/2025	36.93 MB	DESKTOP-6QOEKGH\Piu	Microsoft Edge	47
fdm.exe	4240	1	0.06		10:20:35 11/09/2024	105.42 MB	DESKTOP-6QOEKGH\Piu	Free Download Manager	15
CodeMeterCC.exe	1948	1	0.03		17:38:18 08/04/2022	6.59 MB	DESKTOP-6QOEKGH\Piu	CodeMeter Control Center	3
Process Hacker 2.exe	1400	1	0.39		01:34:01 29/03/2016	14.64 MB	DESKTOP-6QOEKGH\Piu	Process Hacker	7
jusched.exe	4436	1			08:47:57 30/09/2024	2.41 MB	DESKTOP-6QOEKGH\Piu	Java Update Scheduler	4

Process Hacker 2.exe	1400	1	0.47	01:34:01 29/03/2016	15.44 MB	DESKTOP-6QOEKGH\Piu	Process Hacker	7
Sample.exe	1072	1		17:23:39 13/03/2019	668 kB	DESKTOP-6QOEKGH\Piu		1
conhost.exe	3148	1		10:22:18 22/05/2050	6.93 MB	DESKTOP-6QOEKGH\Piu	Console Window Host	6

20:10 24-03-2025	No verified signature	
21:15 24-03-2025	Double-click on sample.exe	
	Click on Handles	
	Mutant are found in file	

Sample.exe (1072) Properties

File

N/A
(UNVERIFIED)

Version: N/A

Image file name:
E:\Coursework\PE_Sample\Sample.exe

Process

Command line: "E:\Coursework\PE_Sample\Sample.exe"

Current directory: E:\Coursework\PE_Sample\

Started: a minute and 26 seconds ago (18:43:28 23/03/2025)

PEB address: 0xc66000 (32-bit: 0xc67000) Image type: 32-bit

Parent: explorer.exe (6376)

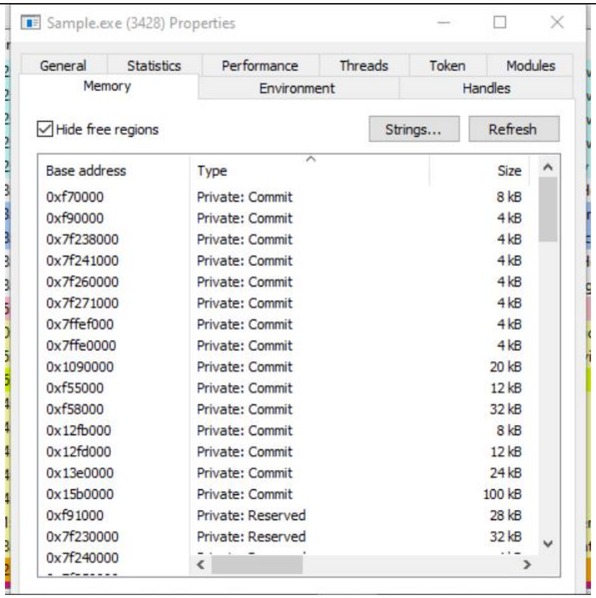
Mitigation policies: DEP (permanent); ASLR

Protection: None

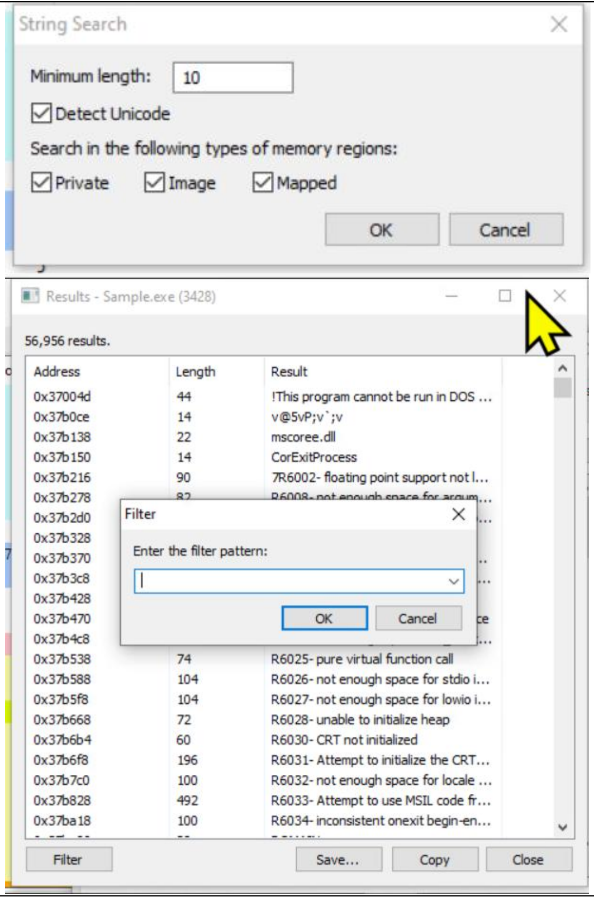
Sample.exe (3428) Properties

☑ Hide unnamed handles

Type	Name
Directory	\KnownDlls
Directory	\KnownDlls32
Directory	\KnownDlls32
Directory	\Sessions\1\BaseNamedObjects
File	C:\Windows
File	E:\Coursework\PE_Sample
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Mutant	\Sessions\1\BaseNamedObjects\SM0:3428:168:WilStaging_02
Semaphore	\Sessions\1\BaseNamedObjects\SM0:3428:168:WilStaging_02_p

	Mutant are object used by windows to ensure that only one instance of application is running at time	
22:00 24-03-2025	Click on memory>> strings	
	In string search select all	
	Filter the strings and try to find unusual strings and search on google about it	

Base address	Type	Size
0xf70000	Private: Commit	8 kB
0xf90000	Private: Commit	4 kB
0x7f238000	Private: Commit	4 kB
0x7f241000	Private: Commit	4 kB
0x7f260000	Private: Commit	4 kB
0x7f271000	Private: Commit	4 kB
0x7ffef000	Private: Commit	4 kB
0x7ffe0000	Private: Commit	4 kB
0x1090000	Private: Commit	20 kB
0xf55000	Private: Commit	12 kB
0xf58000	Private: Commit	32 kB
0x12fb000	Private: Commit	8 kB
0x12fd000	Private: Commit	12 kB
0x13e0000	Private: Commit	24 kB
0x15b0000	Private: Commit	100 kB
0xf91000	Private: Reserved	28 kB
0x7f230000	Private: Reserved	32 kB
0x7f240000		

	In this case no unusual string was found		

String Search

Minimum length: 10

☑ Detect Unicode

Search in the following types of memory regions:

☑ Private ☑ Image ☑ Mapped

Results - Sample.exe (3428)

56,956 results.

Address	Length	Result
0x37004d	44	!This program cannot be run in DOS ...
0x37b0ce	14	v@5vP;v`;v
0x37b138	22	mscoree.dll
0x37b150	14	CorExitProcess
0x37b216	90	7R6002- floating point support not l...
0x37b278	82	R6008- not enough space for argum...
0x37b2d0		...
0x37b328		
0x37b370		..
0x37b3c8		...
0x37b428		
0x37b470		ce
0x37b4c8		...
0x37b538	74	R6025- pure virtual function call
0x37b588	104	R6026- not enough space for stdio i...
0x37b5f8	104	R6027- not enough space for lowio i...
0x37b668	72	R6028- unable to initialize heap
0x37b6b4	60	R6030- CRT not initialized
0x37b6f8	196	R6031- Attempt to initialize the CRT...
0x37b7c0	100	R6032- not enough space for locale ...
0x37b828	492	R6033- Attempt to use MSIL code fr...
0x37ba18	100	R6034- inconsistent onexit begin-en...

Filter

Enter the filter pattern:

4. Conclusion

Following are the conclusion drawn from forensic examination of each file.

- Hard-drive: Evidence found in George Bernard hard drive are files that had been purged from the recycle bin were restored, revealing critical data including credit card details, CVV codes, and personal identifiers. The use of privacy tools, Tor and NordVPN, indicated attempts to conceal online activities, while browsing history and downloads suggested the suspect engaged in cryptocurrency dealings and dark web surfing. The sophisticated methods of information concealment employed in this operation were further revealed by the presence of credit card information that had been steganographically encoded within image files.

- Mobile Device : Through the Xamn tool mobile device examination, several communications, as well as contacts alongside data, reaffirmed the suspect's active engagement in activities. Suspect's calls and messages gave the indication of coordinating with fellow named Danny with cryptocurrency trading and account setups on several trading platforms. Furthermore, the device was stored with images of several credit cards, and Chrome history pertaining to credit card scams. These results, in addition to corroborating the digital traces observed from the hard disk, also gave momentary views of the fraudulent activities and alliances the suspect was executing.

- PE Sample :The comprehensive analysis both static and dynamic of the suspicious PE executable confirmed it is indeed a malicious file whose nature is identified as a UPX-packed Trojan.Zusy. Employment of Pestudio and API Miner highlighted the presence of malware attributes which include, but are not limited to, high entropy values, self-modifying algorithms, code harvesting, and the application of obscurantism. The executable made use of Windows API functions related to sandbox evasion and code injection. Moreover, Process Hacker displayed active manipulation at the system level with Mutex objects, string memory, and other regions that are not available to public viewing which further strengthens the suspicion that the file was designed for stealthy persistence exploits of sensitive channels siphoning confidential financial information or maintain accessibility to compromised devices..

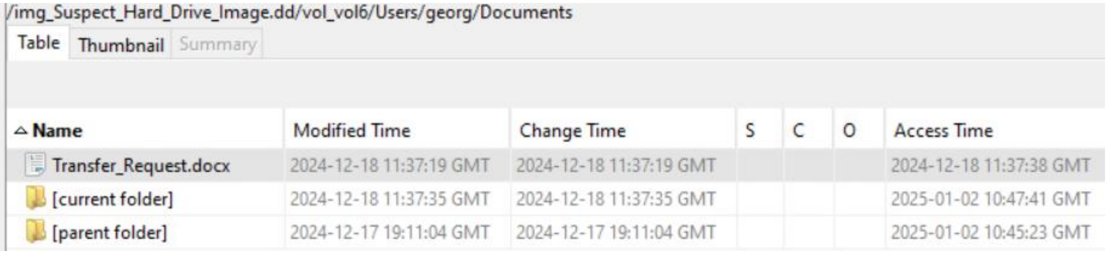
All forensic activities were conducted with the protocols of the relevant accepted practices and would withstand scrutiny for accuracy, reproducibility, and court admission.

5. Reference

[1] ISO/IEC, Guidelines for digital evidence preservation, ISO/IEC 27037:2012, 2012.
[2] NIST, Secure Hash Standard (SHS), FIPS PUB 180-4, 2015.
[3] [5] B. Carrier, “Autopsy Digital Forensics Tool,” 2025. [Online]. Available: https://www.autopsy.com/. Accessed: Mar. 23, 2025.
[4] MSAB, XAMN Forensic Software, 2025. [Online]. Available: https://www.msab.com/products/xamn/.
[5] PeStudio, Malware Initial Assessment, 2025. [Online]. Available: https://www.winitor.com/.
[6] MITRE, ATT&CK Framework: Process Injection (T1055), 2025. [Online]. Available: https://attack.mitre.org/.
[7] APIMiner, Dynamic Analysis Documentation, 2025. [Online]. Available: https://apiminer.com/docs.

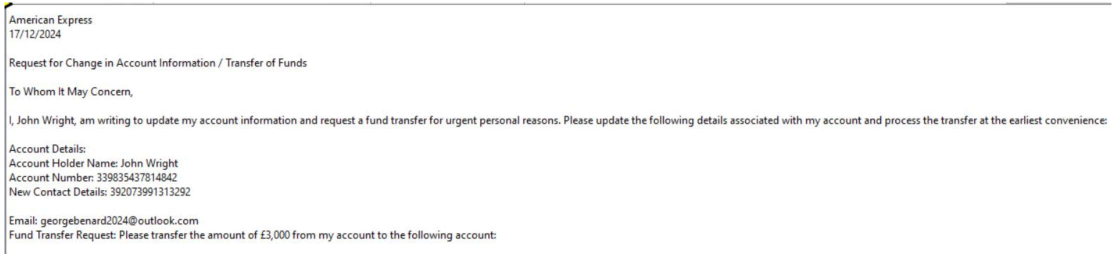
6. Appendix

Transfer request image



/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents
Table
Thumbnail
Summary

Name	Modified Time	Change Time	S	C	O	Access Time
Transfer_Request.docx	2024-12-18 11:37:19 GMT	2024-12-18 11:37:19 GMT				2024-12-18 11:37:38 GMT
[current folder]	2024-12-18 11:37:35 GMT	2024-12-18 11:37:35 GMT				2025-01-02 10:47:41 GMT
[parent folder]	2024-12-17 19:11:04 GMT	2024-12-17 19:11:04 GMT				2025-01-02 10:45:23 GMT



American Express
17/12/2024

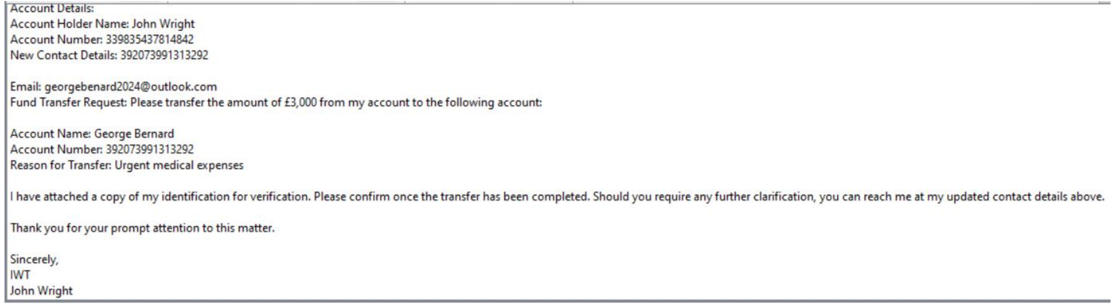
Request for Change in Account Information / Transfer of Funds

To Whom It May Concern,

I, John Wright, am writing to update my account information and request a fund transfer for urgent personal reasons. Please update the following details associated with my account and process the transfer at the earliest convenience:

Account Details:
Account Holder Name: John Wright
Account Number: 339835437814842
New Contact Details: 392073991313292

Email: georgebenard2024@outlook.com
Fund Transfer Request: Please transfer the amount of £3,000 from my account to the following account:



Account Details:
Account Holder Name: John Wright
Account Number: 339835437814842
New Contact Details: 392073991313292

Email: georgebenard2024@outlook.com
Fund Transfer Request: Please transfer the amount of £3,000 from my account to the following account:

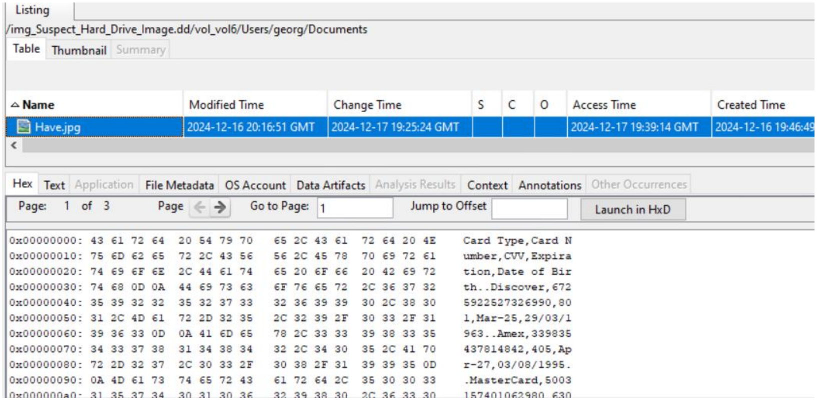
Account Name: George Bernard
Account Number: 392073991313292
Reason for Transfer: Urgent medical expenses

I have attached a copy of my identification for verification. Please confirm once the transfer has been completed. Should you require any further clarification, you can reach me at my updated contact details above.

Thank you for your prompt attention to this matter.

Sincerely,
IWT
John Wright

Stegno image

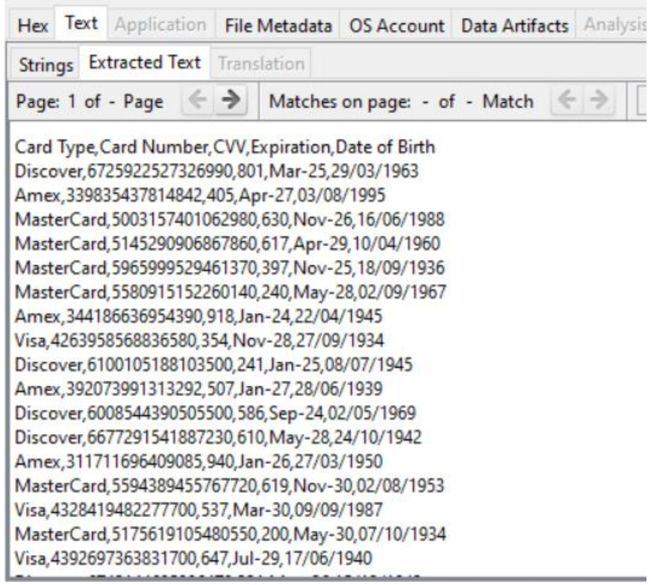


/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents

Name	Modified Time	Change Time	S	C	O	Access Time	Created Time
Have.jpg	2024-12-16 20:16:51 GMT	2024-12-17 19:25:24 GMT				2024-12-17 19:39:14 GMT	2024-12-16 19:46:49

Page: 1 of 3 Page Go to Page: 1 Jump to Offset

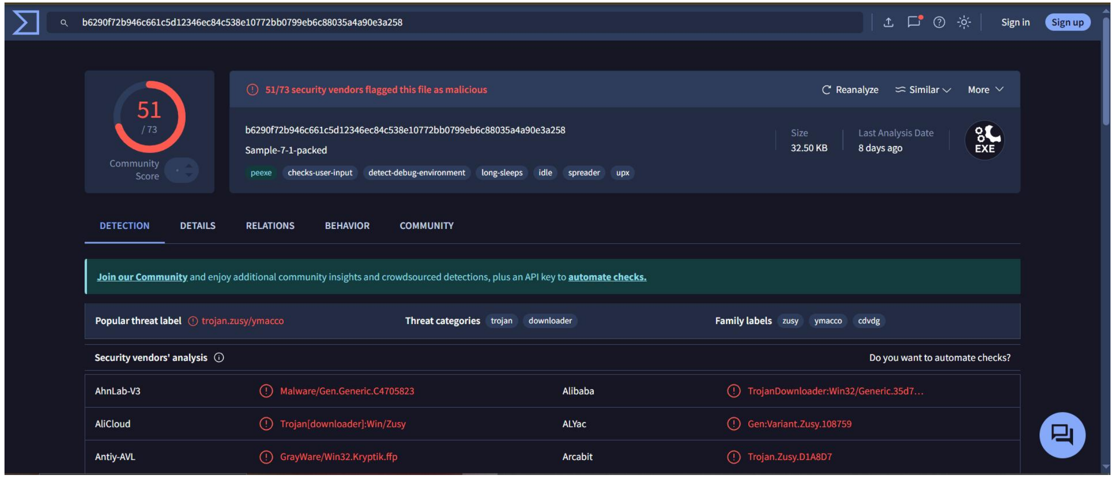
```
0x00000000: 43 61 72 64  20 54 79 70  65 2C 43 61  72 64 20 4E   Card Type,Card N
0x00000010: 75 6D 62 65  72 2C 43 56  56 2C 45 78  70 69 72 61   umber,CVV,Expira
0x00000020: 74 69 6F 6E  2C 44 61 74  65 20 6F 66  20 42 69 72   tion,Date of Bir
0x00000030: 74 68 0D 0A  44 69 73 63  6F 76 65 72  2C 36 37 32   th..Discover,672
0x00000040: 35 39 32 32  35 32 37 33  32 36 39 39  30 2C 38 30   5922527326990,80
0x00000050: 31 2C 4D 61  72 2D 32 35  2C 32 39 2F  30 33 2F 31   1,Mar-25,29/03/1
0x00000060: 39 36 33 0D  0A 41 6D 65  78 2C 33 33  39 38 33 35   963..Amex,339835
0x00000070: 34 33 37 38  31 34 38 34  32 2C 34 30  35 2C 41 70   437814842,405,Ap
0x00000080: 72 2D 32 37  2C 30 33 2F  30 38 2F 31  39 39 35 0D   r-27,03/08/1995.
0x00000090: 0A 4D 61 73  74 65 72 43  61 72 64 2C  35 30 30 33   .MasterCard,5003
0x000000a0: 31 35 37 34  30 31 30 36  32 39 38 30  2C 36 33 30   157401062980,630
```



Page: 1 of - Page Matches on page: - of - Match

```
Card Type,Card Number,CVV,Expiration,Date of Birth
Discover,6725922527326990,801,Mar-25,29/03/1963
Amex,339835437814842,405,Apr-27,03/08/1995
MasterCard,5003157401062980,630,Nov-26,16/06/1988
MasterCard,5145290906867860,617,Apr-29,10/04/1960
MasterCard,5965999529461370,397,Nov-25,18/09/1936
MasterCard,5580915152260140,240,May-28,02/09/1967
Amex,344186636954390,918,Jan-24,22/04/1945
Visa,4263958568836580,354,Nov-28,27/09/1934
Discover,6100105188103500,241,Jan-25,08/07/1945
Amex,392073991313292,507,Jan-27,28/06/1939
Discover,6008544390505500,586,Sep-24,02/05/1969
Discover,6677291541887230,610,May-28,24/10/1942
Amex,311711696409085,940,Jan-26,27/03/1950
MasterCard,5594389455767720,619,Nov-30,02/08/1953
Visa,4328419482277700,537,Mar-30,09/09/1987
MasterCard,5175619105480550,200,May-30,07/10/1934
Visa,4392697363831700,647,Jul-29,17/06/1940
```

Virus total - Malware family name



b6290f72b946c661c5d12346ec84c538e10772bb0799eb6c88035a4a90e3a258

51 / 73

Community Score

51/73 security vendors flagged this file as malicious

b6290f72b946c661c5d12346ec84c538e10772bb0799eb6c88035a4a90e3a258

Sample-7-1-packed

peexe checks-user-input detect-debug-environment long-sleeps idle spreader upx

Size 32.50 KB

Last Analysis Date 8 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.zusy/ymacco

Threat categories trojan downloader

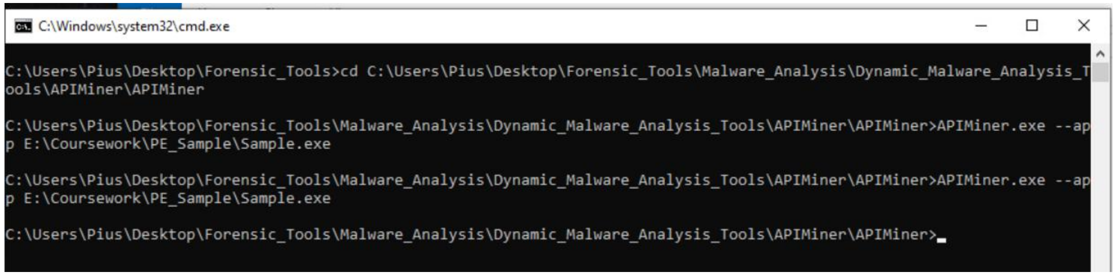
Family labels zusy ymacco cdvdg

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Gen.Generic.C4705823	Alibaba	TrojanDownloader:Win32/Generic.35d7...
AliCloud	Trojan[downloader]:Win/Zusy	ALYac	Gen:Variant.Zusy.108759
Antiy-AVL	GrayWare/Win32.Kryptik.ffp	Arcabit	Trojan.Zusy.D1A8D7

API file

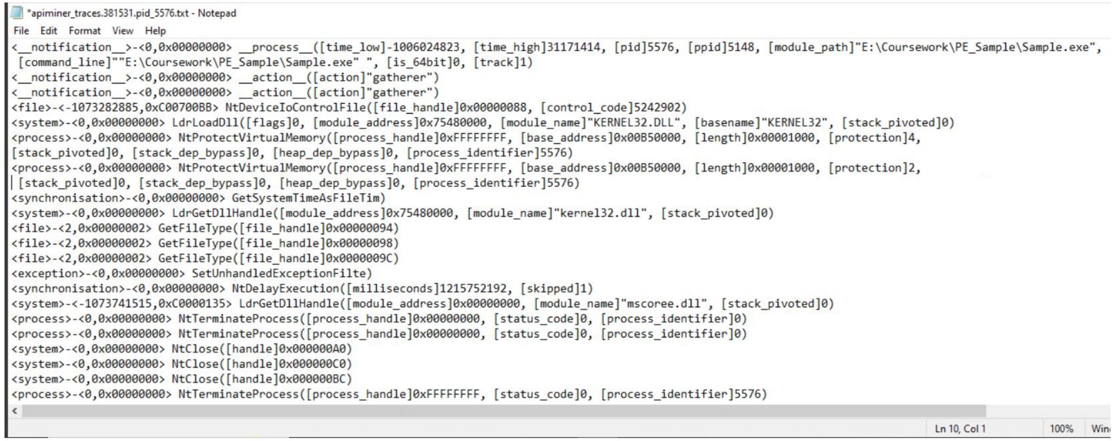


```
C:\Users\Pius\Desktop\Forensic_Tools>cd C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_T
ools\APIMiner\APIMiner

C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_Tools\APIMiner\APIMiner>APIMiner.exe --ap
p E:\Coursework\PE_Sample\Sample.exe

C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_Tools\APIMiner\APIMiner>APIMiner.exe --ap
p E:\Coursework\PE_Sample\Sample.exe

C:\Users\Pius\Desktop\Forensic_Tools\Malware_Analysis\Dynamic_Malware_Analysis_Tools\APIMiner\APIMiner>_
```



*apiminer_traces.381531.pid_5576.txt - Notepad
File Edit Format View Help
Ln 10, Col 1
100%
Win

```
<__notification__>-<0,0x00000000> __process__([time_low]-1006024823, [time_high]31171414, [pid]5576, [ppid]5148, [module_path]"E:\Coursework\PE_Sample\Sample.exe",
 [command_line]""E:\Coursework\PE_Sample\Sample.exe" ", [is_64bit]0, [track]1)
<__notification__>-<0,0x00000000> __action__([action]"gatherer")
<__notification__>-<0,0x00000000> __action__([action]"gatherer")
<file>-<-1073282885,0xC00700BB> NtDeviceIoControlFile([file_handle]0x00000088, [control_code]5242902)
<system>-<0,0x00000000> LdrLoadDll([flags]0, [module_address]0x75480000, [module_name]"KERNEL32.DLL", [basename]"KERNEL32", [stack_pivoted]0)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x00B50000, [length]0x00001000, [protection]4,
[stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0, [process_identifier]5576)
<process>-<0,0x00000000> NtProtectVirtualMemory([process_handle]0xFFFFFFFF, [base_address]0x00B50000, [length]0x00001000, [protection]2,
 [stack_pivoted]0, [stack_dep_bypass]0, [heap_dep_bypass]0, [process_identifier]5576)
<synchronisation>-<0,0x00000000> GetSystemTimeAsFileTim)
<system>-<0,0x00000000> LdrGetDllHandle([module_address]0x75480000, [module_name]"kernel32.dll", [stack_pivoted]0)
<file>-<2,0x00000002> GetFileType([file_handle]0x00000094)
<file>-<2,0x00000002> GetFileType([file_handle]0x00000098)
<file>-<2,0x00000002> GetFileType([file_handle]0x0000009C)
<exception>-<0,0x00000000> SetUnhandledExceptionFilte)
<synchronisation>-<0,0x00000000> NtDelayExecution([milliseconds]1215752192, [skipped]1)
<system>-<-1073741515,0xC0000135> LdrGetDllHandle([module_address]0x00000000, [module_name]"mscoree.dll", [stack_pivoted]0)
<process>-<0,0x00000000> NtTerminateProcess([process_handle]0x00000000, [status_code]0, [process_identifier]0)
<process>-<0,0x00000000> NtTerminateProcess([process_handle]0x00000000, [status_code]0, [process_identifier]0)
<system>-<0,0x00000000> NtClose([handle]0x000000A0)
<system>-<0,0x00000000> NtClose([handle]0x000000C0)
<system>-<0,0x00000000> NtClose([handle]0x000000BC)
<process>-<0,0x00000000> NtTerminateProcess([process_handle]0xFFFFFFFF, [status_code]0, [process_identifier]5576)
```