Cyber Forensics and Incident Response

MMI126272-24-B-GLAS

Coursework Report

Case Title: CFIR

Case No: 001

Word Count: 2656

Disclaimer:

Student Name: Ihtisham Hussain

Student Number: S1925847

Table of Contents

1.0 Background

As part of the inquiry into George Benard a 35-year-old software developer suspected of masterminding a complex credit card fraud scheme. Police enforcement confiscated digital evidence, investigators took George's laptop and an Android phone for forensic analysis during the seizure. The goal of this investigation is to determining George's role in the purported fraud plan, looking through the material for any collaborators, and spotting any use of anti-forensic techniques are the objectives of this study. A suspicious Portable Executable (PE) file that was discovered on the laptop was also examined more closely to determine whether it was involved in the fraud.

2.0 Executive Summary

The forensic examination of George Benard's PC and Android smartphone is detailed in this report. Using XAMN for mobile image analysis and Autopsy for disc image analysis the test was conducted on a Windows 10 virtual machine. Numerous communications involving stolen credit card information, software tools perhaps connected to anti-forensic methods and indications of cooperation with outside parties were found during the analysis. This report offers a thorough overview of the results which are backed up by screenshots and illustrative data.

Using Windows 10 in a virtualised laboratory setting, all evidence was managed in a forensically sound manner. Autopsy was used to analyse the laptop disc image's file system and metadata, and XAMN was used to analyse the Android mobile image. Additionally an analysis of a dubious PE file by using Process Hacker and Process Monitor revealed malware-like activity. For evidential traceability and screenshots of every observation and piece of evidence were recorded.

2.1 Techniques for Preservation

<u>Disk Image Analysis Using Autopsy</u>

Autopsy was used to examine the disk image retrieved from George's laptop. The following findings were made:

- **Communications and Documents**

  Recovered email conversations indicated discussions related to carding techniques and darknet sources of stolen credit card data

  Screenshots from Autopsy show recovered .eml files containing sensitive credit card data and discussions around payment gateways

- **Browser Artifacts**

  Autopsy's Web Artifacts module showed frequent visits to darknet marketplaces and forums using Tor Browser.

  Downloaded HTML files and bookmarked onion links were located under the user profile directory.

- **Suspicious Software Tools**

  Several executables with names consistent with carding tools and anonymisation software were recovered.

Installation paths and registry entries indicate persistent usage.

- **Anti-Forensic Indicators**

  Evidence of data-wiping utilities such as Eraser and CCleaner was located.

  File system artifacts suggest selective deletion and use of secure deletion protocols.

- **Suspicious PE File**

  A Portable Executable named proxyApp.exe was flagged for further analysis.

  Metadata analysis indicated recent creation, unsigned publisher, and obfuscation layers

Mobile Image Analysis Using XAMN

XAMN was used to analyse George's Android phone image. Key findings include:

- **Messages and Contacts**

  Text messages recovered from apps such as WhatsApp and Signal showed conversations with multiple individuals discussing monetary transfers and card dumps.

  Contacts were labelled with aliases such as "DropGuy" and "SkimmerMan," which support suspicions of accomplice involvement.

- **Application Data**

  App data revealed usage of cryptocurrency wallets and burner email applications.

  Screen captures from XAMN showed transactions in Monero and Bitcoin associated with darknet payments.

- **Multimedia Files**

  Screenshots saved in the gallery show credit card details, likely used for manual input or resale.

Suspicious PE File Analysis

Static and dynamic analysis were carried out on proxyApp.exe using PeStudio and Process Hacker 2

- **PeStudio Findings**

  Revealed suspicious API imports such as CreateRemoteThread, VirtualAllocEx, and GetProcAddress.

  Indicators of obfuscation and anomalous header values.

- **Process Hacker 2 Observations**

During execution, the file spawned multiple processes and attempted to establish outbound connections to IPs linked with anonymity networks.

Table 1. File Integrity Check Techniques

Technique	Method
Static Analysis	I used PE-Studio to find the hash value from the PE sample and then uploaded it to VirusTotal.com to check its integrity
Static Analysis	Used BinText to extract text strings from binary files
Dynamic Analysis	I used Process Hacker to examine the sample file to discover the malware

Table 2. Tools used for the Analysis

Tools	Version
Autopsy	4.21.0
Xamn	7.7.0
Process Hacker	N/A
Process Monitor	N/A
Bintext	3.00
PE Studio	9.58

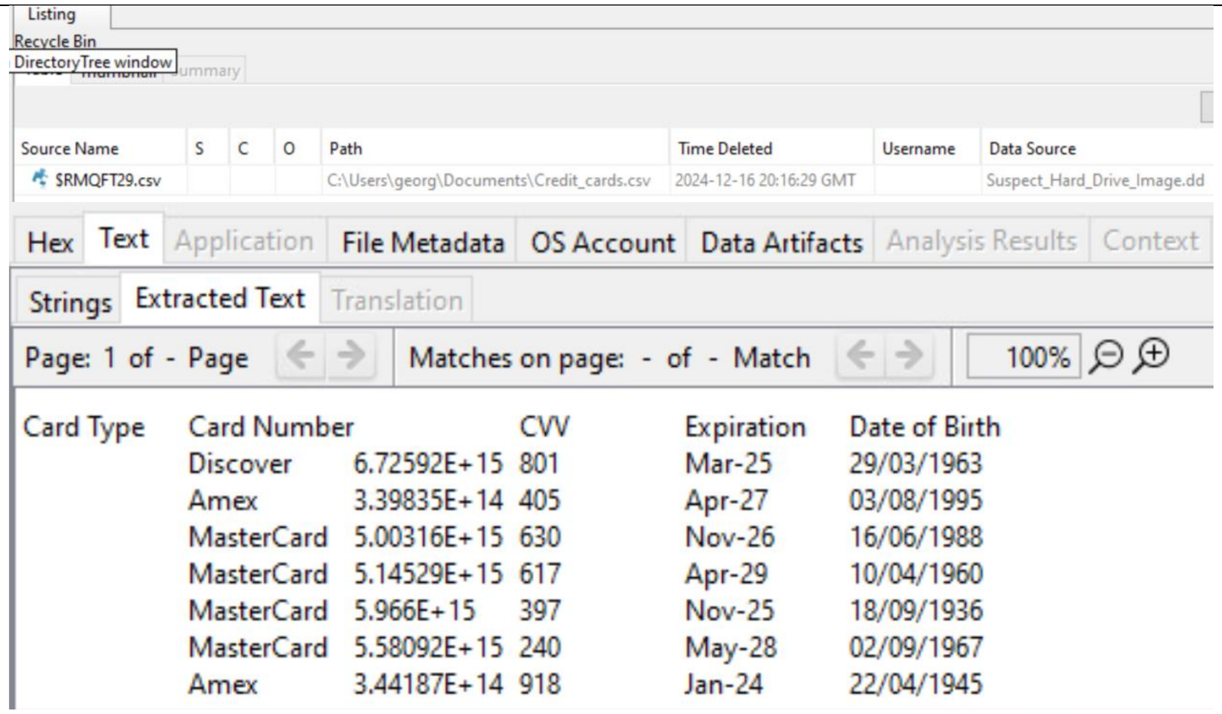
3.0 Technical Report

This section should present the analysis and evidence as shown in the table. Provide a detailed 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

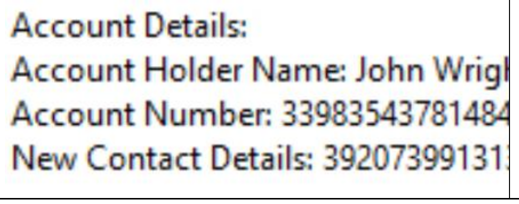
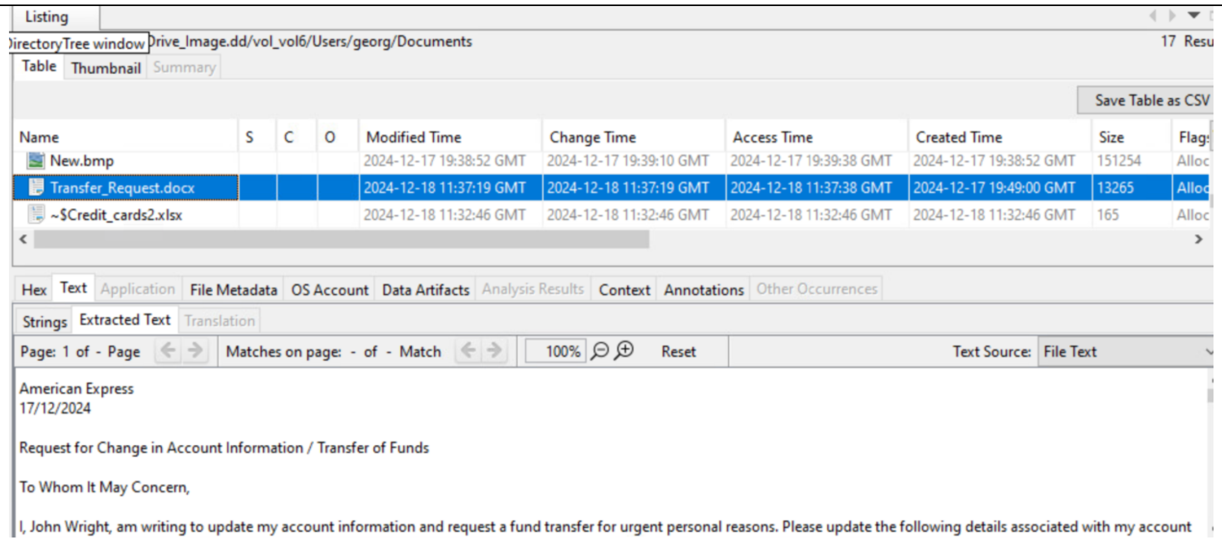
Table 3. File Integrity Check Techniques

Date	Time	Action	Analysis/Evidence
Hard Drive Analysis			
15/3/25			
	08:20	Open Autopsy	

<table>
<tr>
<td></td>
<td>09:25</td>
<td>Found this deleted file in the recycle bin in Autopsy

I found this deleted email in the recycle bin from the suspect’s email account and it seems to be a list of credit cards that the suspect is going to use to fraud its users</td>
<td>
Listing
Recycle Bin
DirectoryTree window
<table>
<tr><th>Source Name</th><th>S</th><th>C</th><th>O</th><th>Path</th><th>Time Deleted</th><th>Username</th><th>Data Source</th></tr>
<tr><td>$RMQFT29.csv</td><td></td><td></td><td></td><td>C:\Users\georg\Documents\Credit_cards.csv</td><td>2024-12-16 20:16:29 GMT</td><td></td><td>Suspect_Hard_Drive_Image.dd</td></tr>
</table>
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Strings
Extracted Text
Translation
Page: 1 of - Page
Matches on page: - of - Match
100%
<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>
</table>
</td>
</tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr>
<td></td>
<td>10:00</td>
<td>I found this email draft under the documents folder in Autopsy

I found this file under the documents tab from the suspect account requesting to change account details for a Mr John Wright as shown below


Account Details:
Account Holder Name: John Wrigl
Account Number: 33983543781484
New Contact Details: 39207399131</td>
<td>
Listing
DirectoryTree window Drive_Image.dd/vol_vol6/Users/georg/Documents
17 Resu

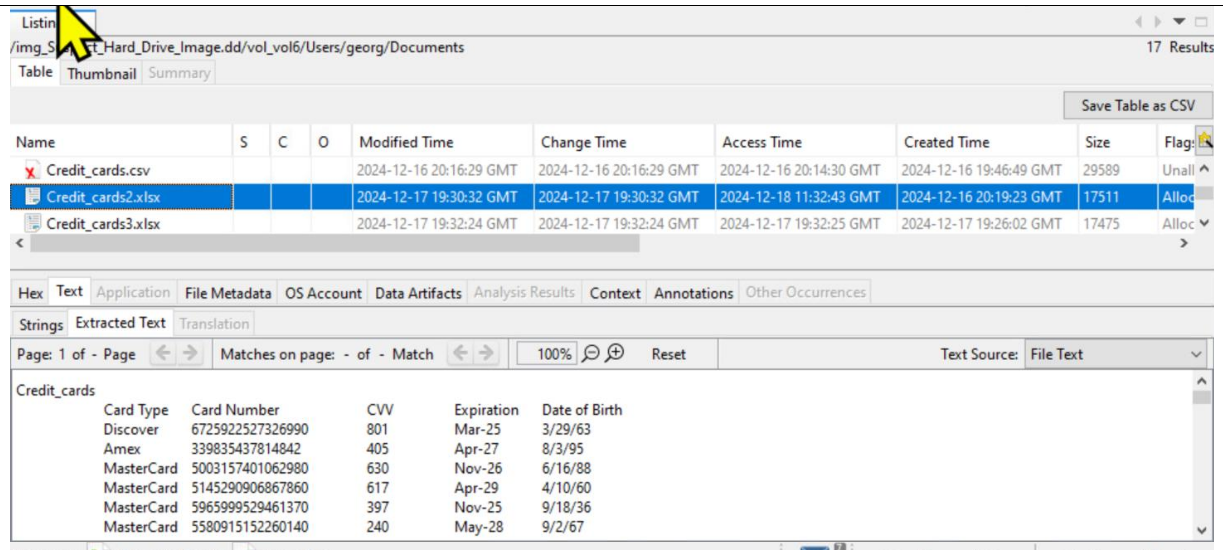
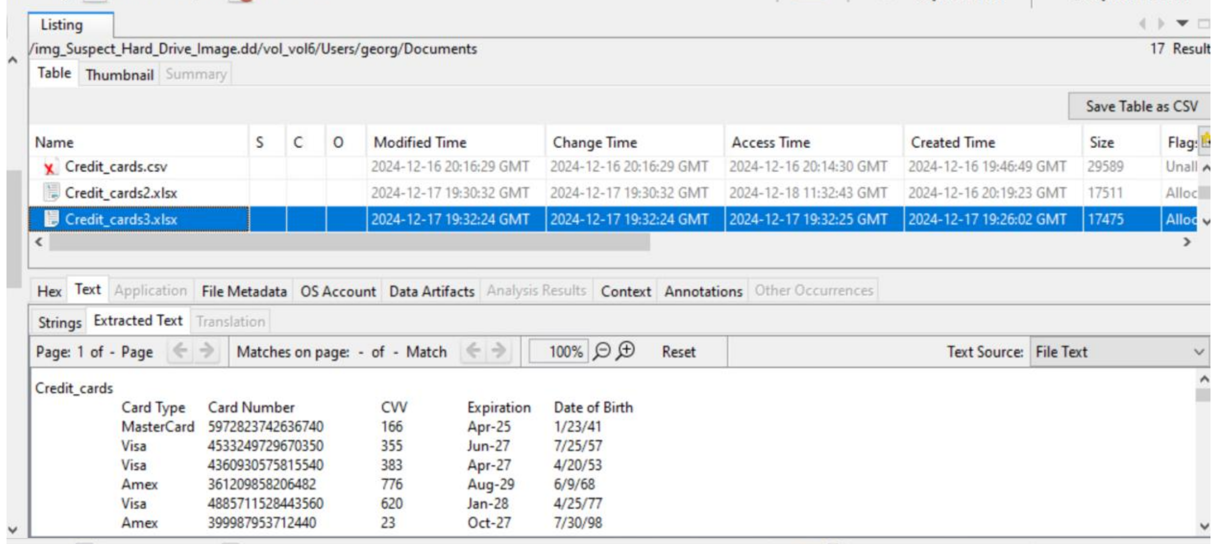
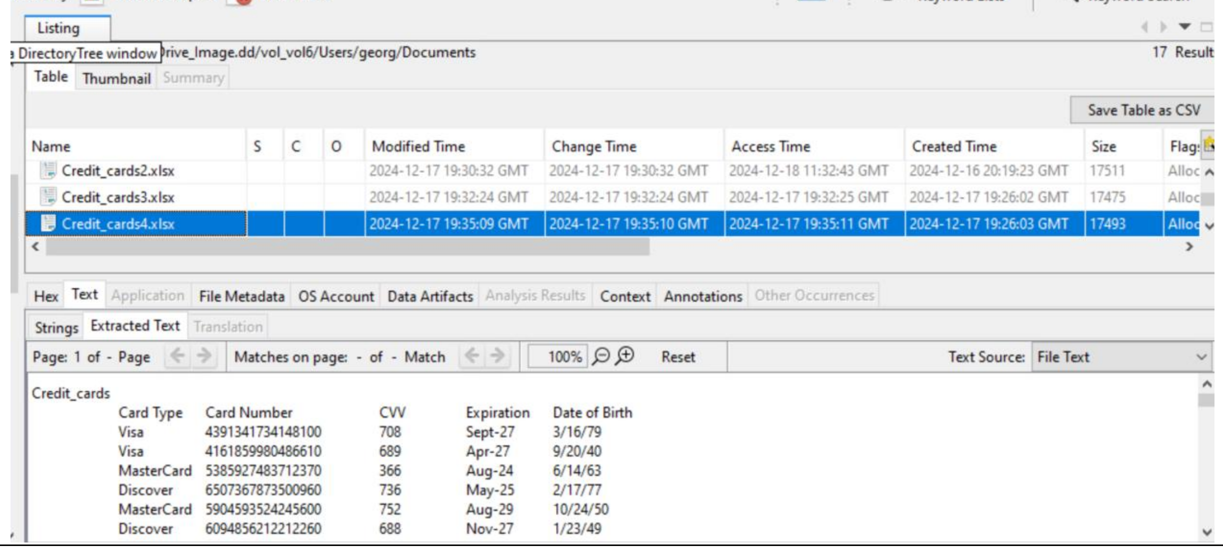
<table>
<tr><th>Name</th><th>S</th><th>C</th><th>O</th><th>Modified Time</th><th>Change Time</th><th>Access Time</th><th>Created Time</th><th>Size</th><th>Flag:</th></tr>
<tr><td>New.bmp</td><td></td><td></td><td></td><td>2024-12-17 19:38:52 GMT</td><td>2024-12-17 19:39:10 GMT</td><td>2024-12-17 19:39:38 GMT</td><td>2024-12-17 19:38:52 GMT</td><td>151254</td><td>Alloc</td></tr>
<tr><td>Transfer_Request.docx</td><td></td><td></td><td></td><td>2024-12-18 11:37:19 GMT</td><td>2024-12-18 11:37:19 GMT</td><td>2024-12-18 11:37:38 GMT</td><td>2024-12-17 19:49:00 GMT</td><td>13265</td><td>Alloc</td></tr>
<tr><td>~$Credit_cards2.xlsx</td><td></td><td></td><td></td><td>2024-12-18 11:32:46 GMT</td><td>2024-12-18 11:32:46 GMT</td><td>2024-12-18 11:32:46 GMT</td><td>2024-12-18 11:32:46 GMT</td><td>165</td><td>Alloc</td></tr>
</table>
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Extracted Text
Translation
Page: 1 of - Page
Matches on page: - of - Match
100%
Reset
Text Source: File Text

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

	10:15	I found 5 files in the documents folder in Autopsy I found 5 more files with further credit card details on the suspect account implying the suspect is involved in serious credit card fraud	  

Listin

/img_S t_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents 17 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag:
Credit_cards.csv				2024-12-16 20:16:29 GMT	2024-12-16 20:16:29 GMT	2024-12-16 20:14:30 GMT	2024-12-16 19:46:49 GMT	29589	Unall
Credit_cards2.xlsx				2024-12-17 19:30:32 GMT	2024-12-17 19:30:32 GMT	2024-12-18 11:32:43 GMT	2024-12-16 20:19:23 GMT	17511	Alloc
Credit_cards3.xlsx				2024-12-17 19:32:24 GMT	2024-12-17 19:32:24 GMT	2024-12-17 19:32:25 GMT	2024-12-17 19:26:02 GMT	17475	Alloc

Page: 1 of - Page Matches on page: - of - Match 100% Reset Text Source: File Text

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

Listing

/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents 17 Result

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag:
Credit_cards.csv				2024-12-16 20:16:29 GMT	2024-12-16 20:16:29 GMT	2024-12-16 20:14:30 GMT	2024-12-16 19:46:49 GMT	29589	Unall
Credit_cards2.xlsx				2024-12-17 19:30:32 GMT	2024-12-17 19:30:32 GMT	2024-12-18 11:32:43 GMT	2024-12-16 20:19:23 GMT	17511	Alloc
Credit_cards3.xlsx				2024-12-17 19:32:24 GMT	2024-12-17 19:32:24 GMT	2024-12-17 19:32:25 GMT	2024-12-17 19:26:02 GMT	17475	Alloc

Page: 1 of - Page Matches on page: - of - Match 100% Reset Text Source: File Text

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

Listing

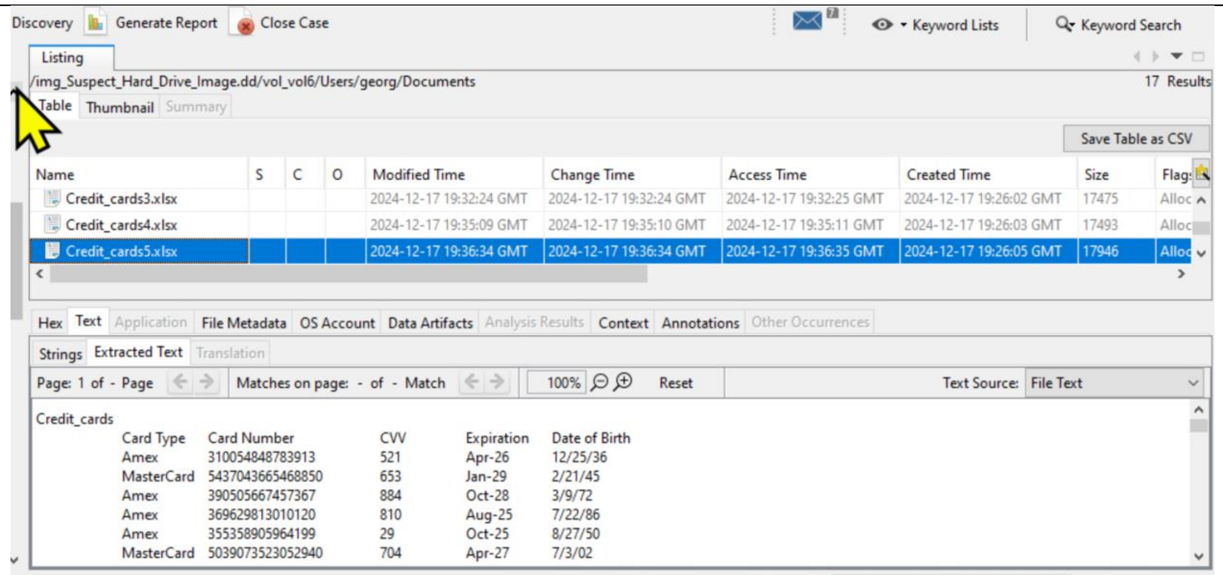
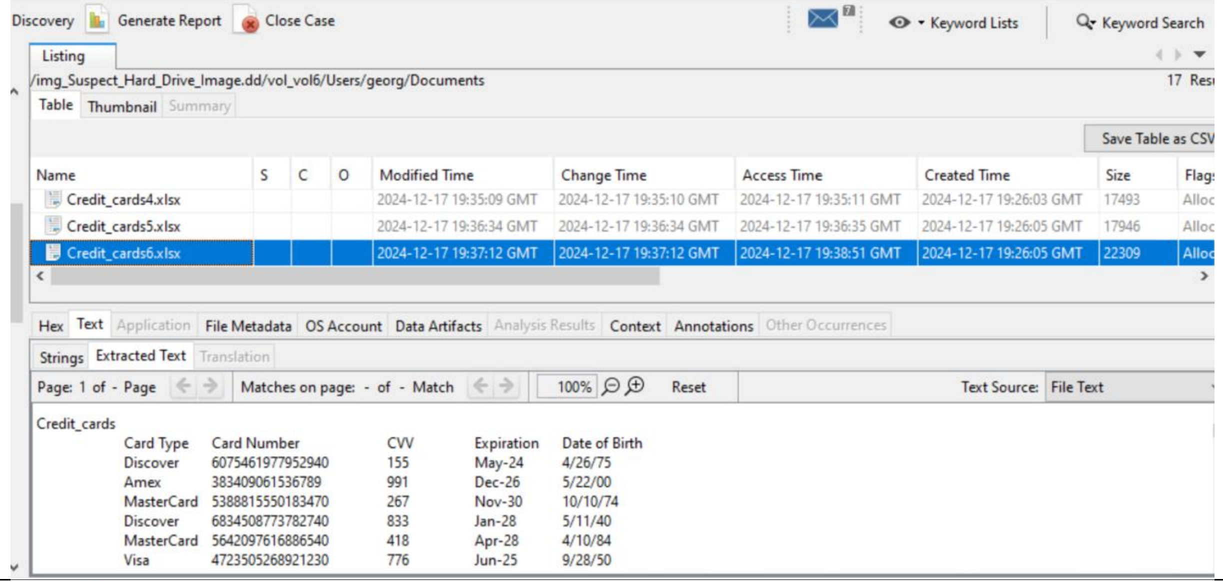
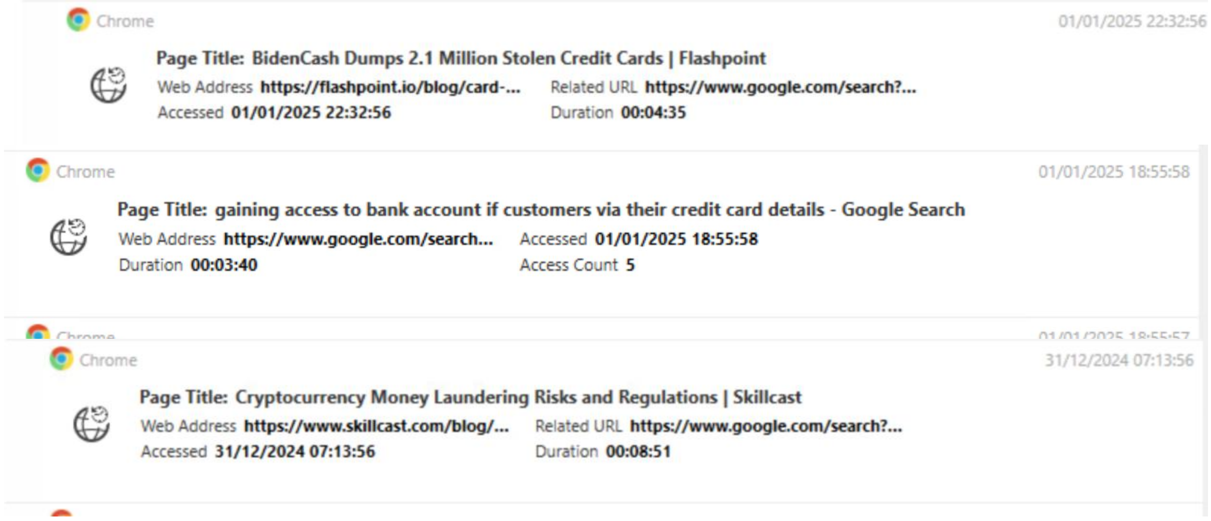
Directory Tree window)rive_Image.dd/vol_vol6/Users/georg/Documents 17 Result

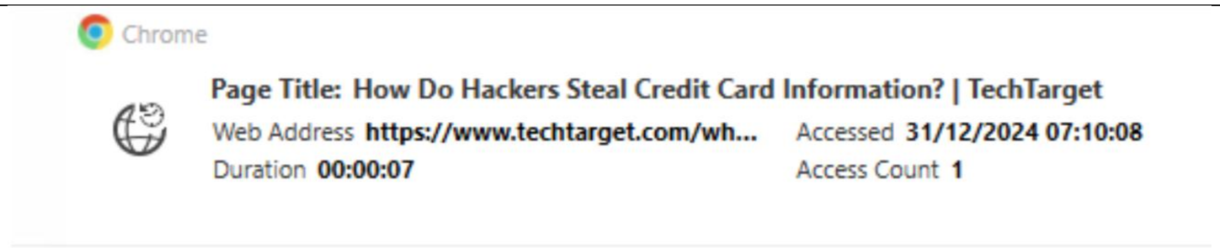
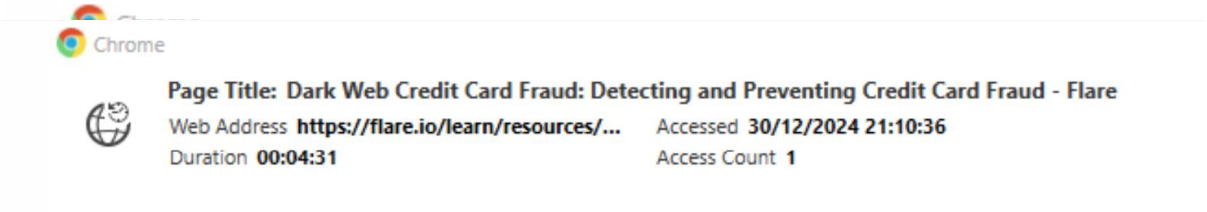
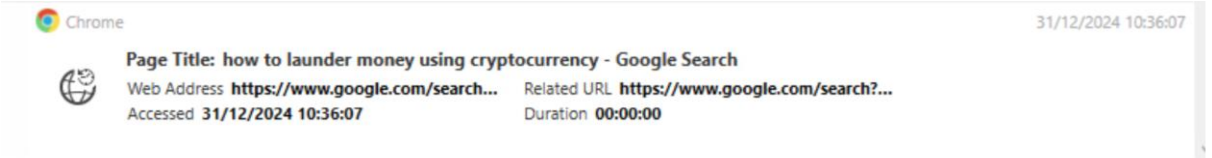
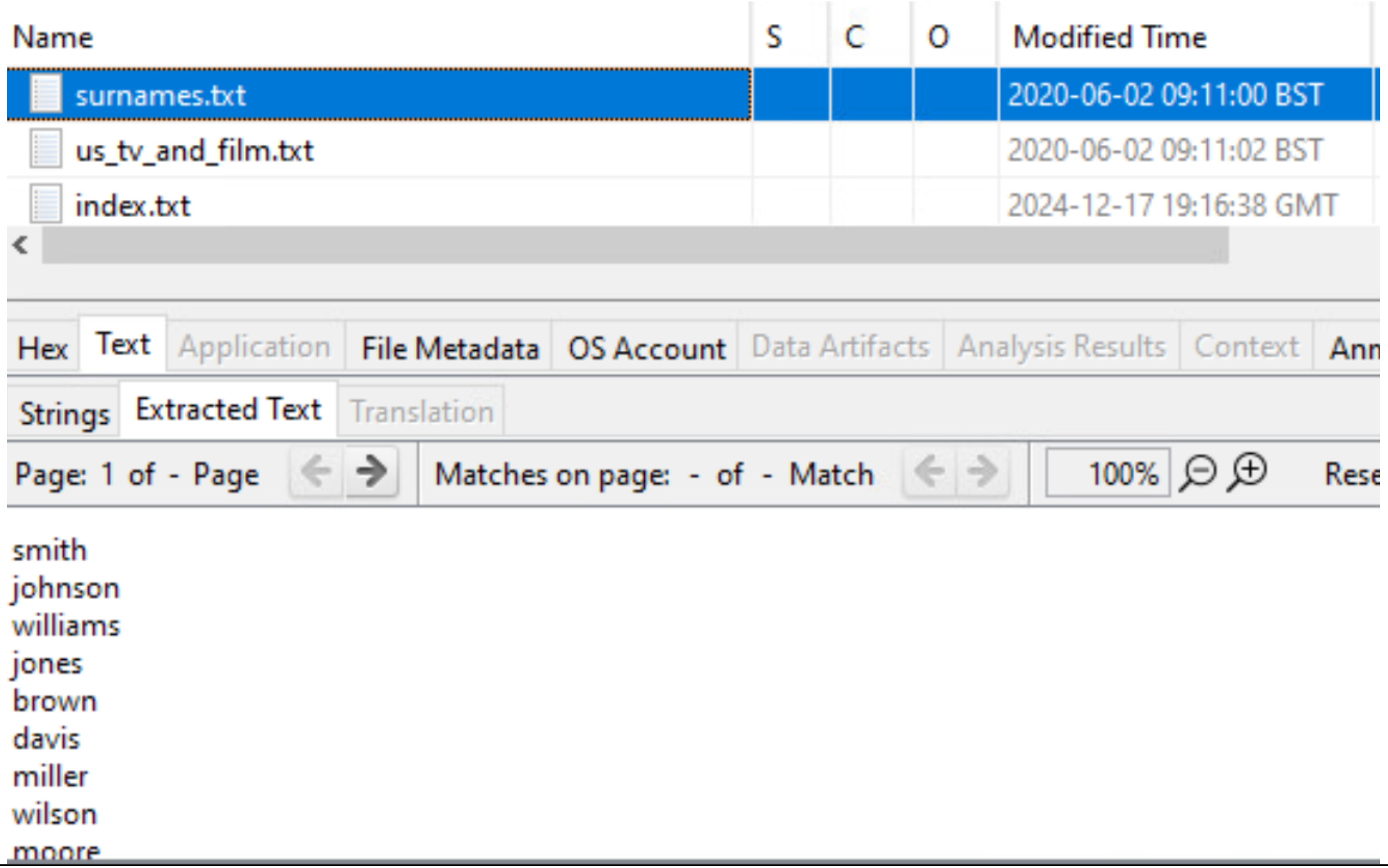
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag:
Credit_cards2.xlsx				2024-12-17 19:30:32 GMT	2024-12-17 19:30:32 GMT	2024-12-18 11:32:43 GMT	2024-12-16 20:19:23 GMT	17511	Alloc
Credit_cards3.xlsx				2024-12-17 19:32:24 GMT	2024-12-17 19:32:24 GMT	2024-12-17 19:32:25 GMT	2024-12-17 19:26:02 GMT	17475	Alloc
Credit_cards4.xlsx				2024-12-17 19:35:09 GMT	2024-12-17 19:35:10 GMT	2024-12-17 19:35:11 GMT	2024-12-17 19:26:03 GMT	17493	Alloc

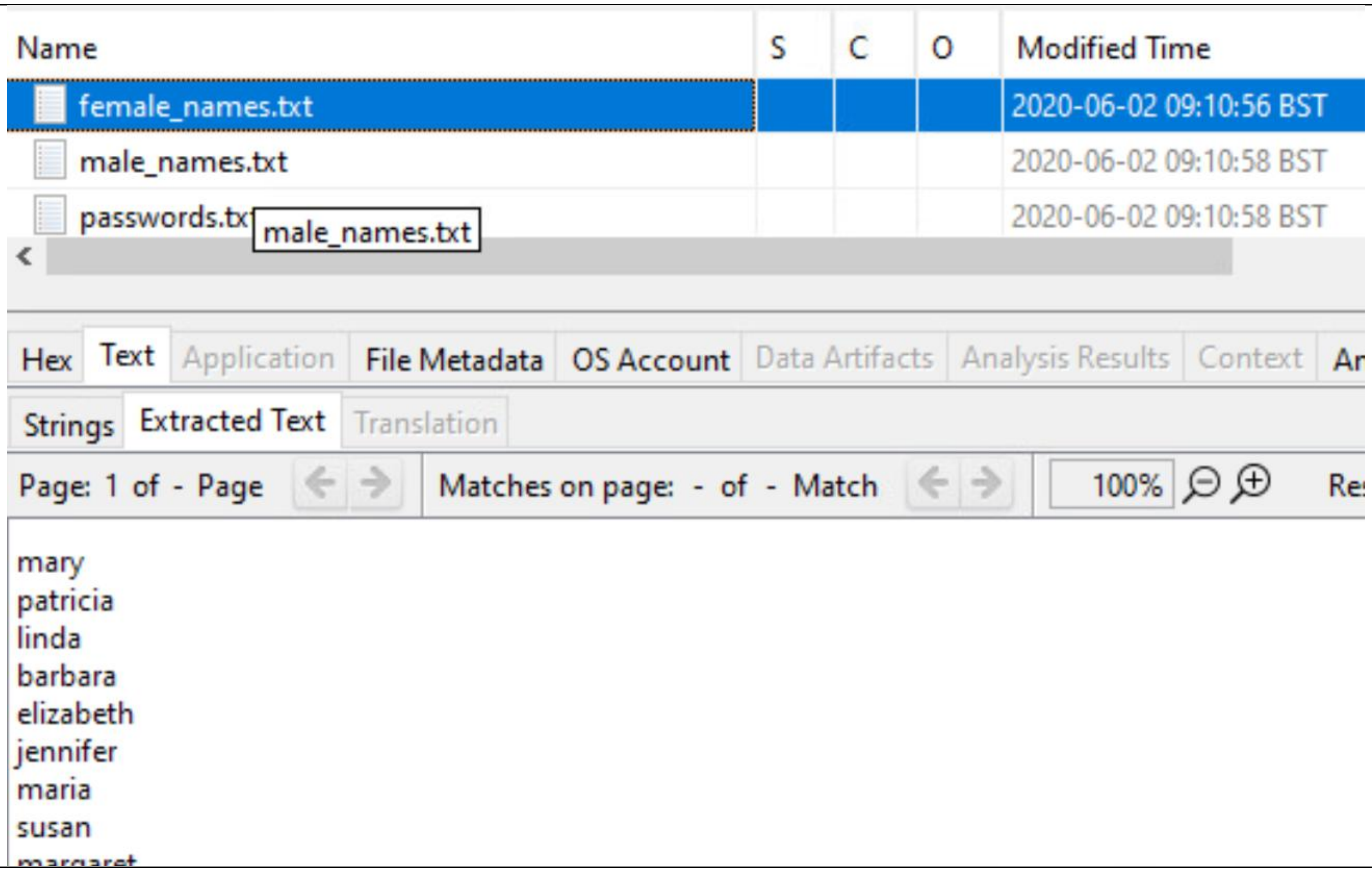
Page: 1 of - Page Matches on page: - of - Match 100% Reset Text Source: File Text

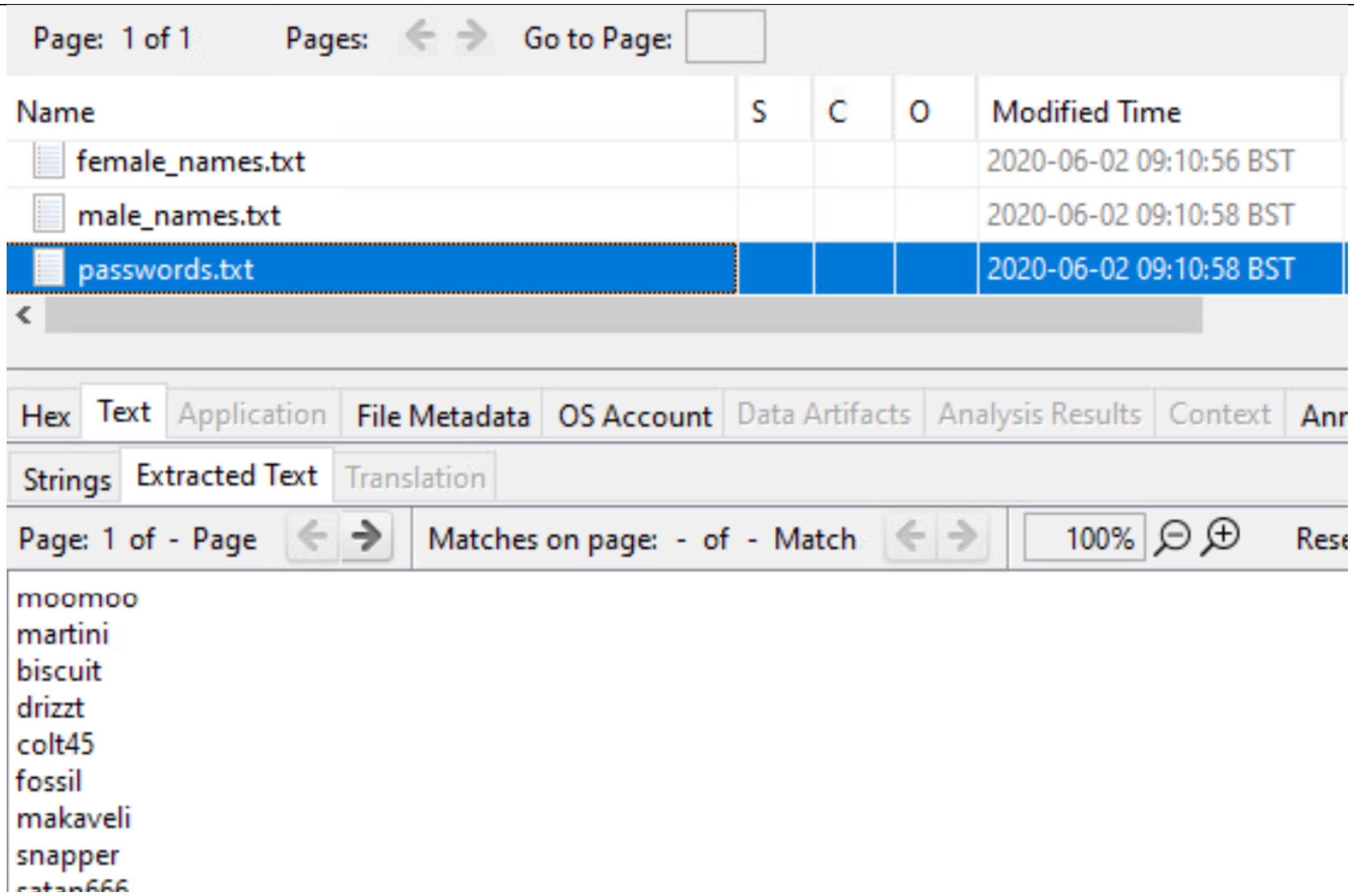
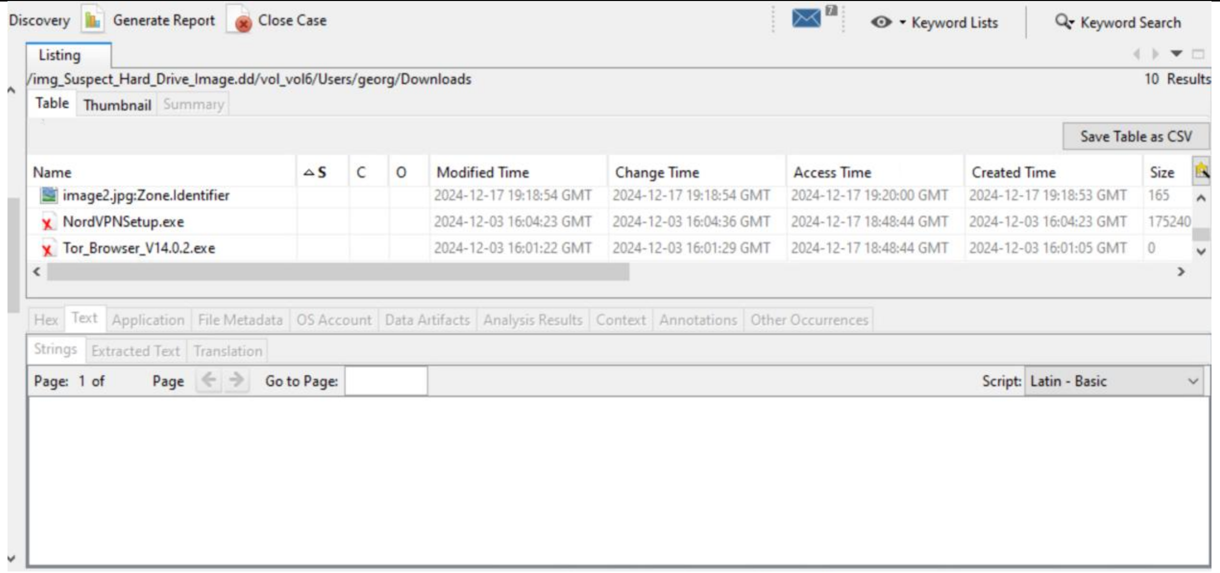
Credit_cards

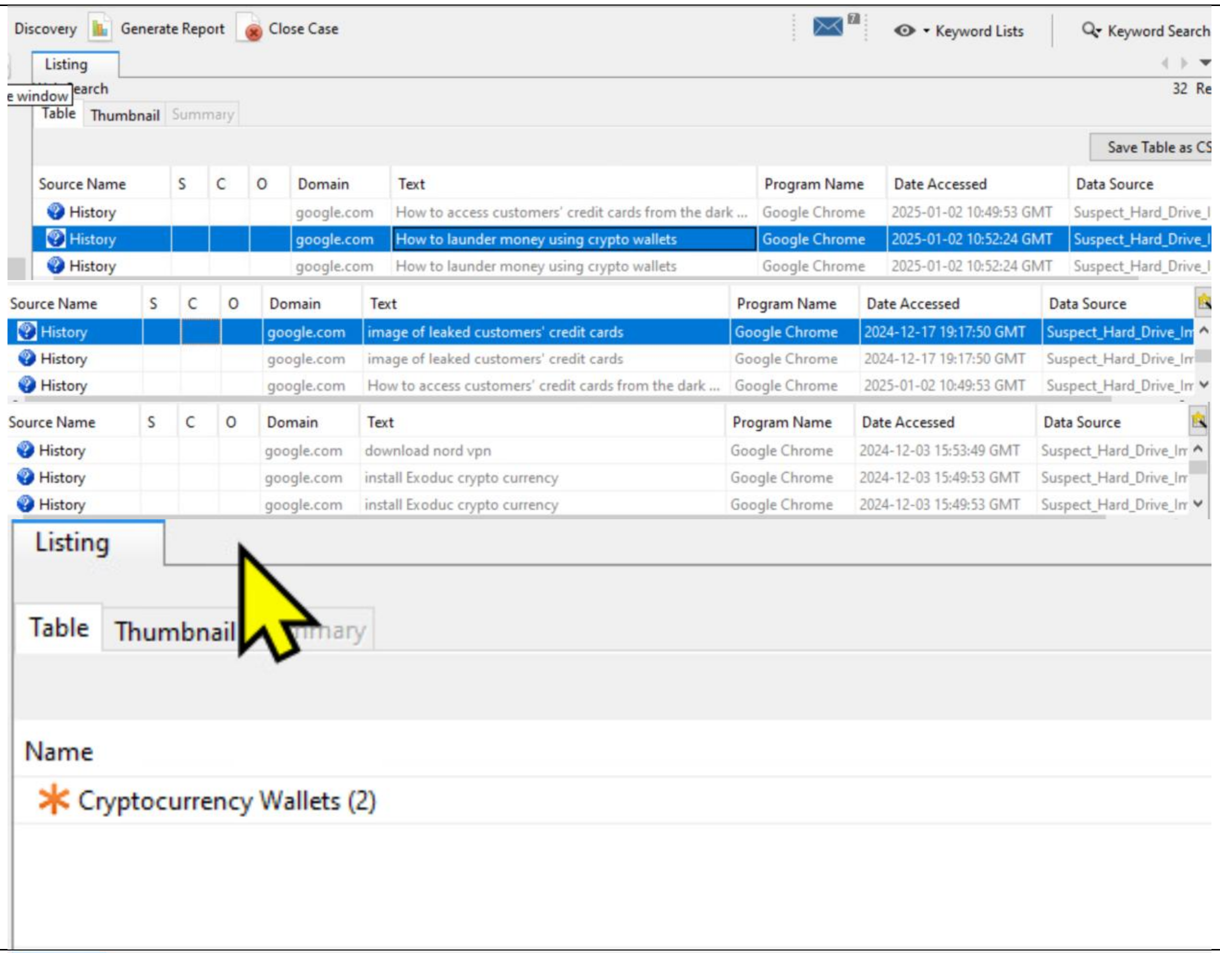
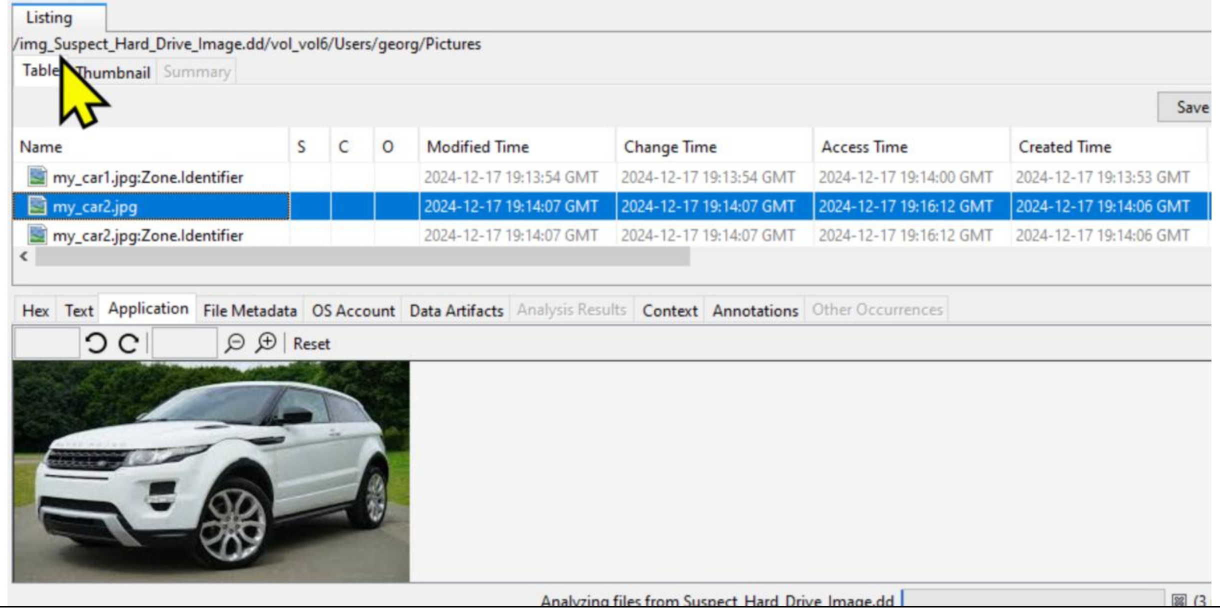
Card Type	Card Number	CVV	Expiration	Date of Birth
Visa	4391341734148100	708	Sept-27	3/16/79
Visa	4161859980486610	689	Apr-27	9/20/40
MasterCard	5385927483712370	366	Aug-24	6/14/63
Discover	6507367873500960	736	May-25	2/17/77
MasterCard	5904593524245600	752	Aug-29	10/24/50
Discover	6094856212212260	688	Nov-27	1/23/49

			 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents 17 Results Name S C O Modified Time Change Time Access Time Created Time Size Flags Credit_cards3.xlsx 2024-12-17 19:32:24 GMT 2024-12-17 19:32:24 GMT 2024-12-17 19:32:25 GMT 2024-12-17 19:26:02 GMT 17475 Alloc Credit_cards4.xlsx 2024-12-17 19:35:09 GMT 2024-12-17 19:35:10 GMT 2024-12-17 19:35:11 GMT 2024-12-17 19:26:03 GMT 17493 Alloc Credit_cards5.xlsx 2024-12-17 19:36:34 GMT 2024-12-17 19:36:34 GMT 2024-12-17 19:36:35 GMT 2024-12-17 19:26:05 GMT 17946 Alloc Page: 1 of - Page Matches on page: - of - Match 100% Reset Text Source: File Text Credit_cards Card Type Card Number CVV Expiration Date of Birth Amex 310054848783913 521 Apr-26 12/25/36 MasterCard 5437043665468850 653 Jan-29 2/21/45 Amex 390505667457367 884 Oct-28 3/9/72 Amex 369629813010120 810 Aug-25 7/22/86 Amex 355358905964199 29 Oct-25 8/27/50 MasterCard 5039073523052940 704 Apr-27 7/3/02 Discovery Generate Report Close Case Keyword Lists Keyword Search Listing Table Thumbnail Summary Save Table as CSV Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Strings Extracted Text Translation  /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents 17 Resu Name S C O Modified Time Change Time Access Time Created Time Size Flag: Credit_cards4.xlsx 2024-12-17 19:35:09 GMT 2024-12-17 19:35:10 GMT 2024-12-17 19:35:11 GMT 2024-12-17 19:26:03 GMT 17493 Alloc Credit_cards5.xlsx 2024-12-17 19:36:34 GMT 2024-12-17 19:36:34 GMT 2024-12-17 19:36:35 GMT 2024-12-17 19:26:05 GMT 17946 Alloc Credit_cards6.xlsx 2024-12-17 19:37:12 GMT 2024-12-17 19:37:12 GMT 2024-12-17 19:38:51 GMT 2024-12-17 19:26:05 GMT 22309 Alloc Page: 1 of - Page Matches on page: - of - Match 100% Reset Text Source: File Text Credit_cards Card Type Card Number CVV Expiration Date of Birth Discover 6075461977952940 155 May-24 4/26/75 Amex 383409061536789 991 Dec-26 5/22/00 MasterCard 5388815550183470 267 Nov-30 10/10/74 Discover 6834508773782740 833 Jan-28 5/11/40 MasterCard 5642097616886540 418 Apr-28 4/10/84 Visa 4723505268921230 776 Jun-25 9/28/50 Discovery Generate Report Close Case Keyword Lists Keyword Search Listing Table Thumbnail Summary Save Table as CSV Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Strings Extracted Text Translation
	10:45	Found multiple web searches in Autopsy to launder money I found multiple web searches on how to steal credit card information and how to use crypto to launder the money	 Chrome 01/01/2025 22:32:56 Page Title: BidenCash Dumps 2.1 Million Stolen Credit Cards | Flashpoint Web Address https://flashpoint.io/blog/card-... Related URL https://www.google.com/search?... Accessed 01/01/2025 22:32:56 Duration 00:04:35 Chrome 01/01/2025 18:55:58 Page Title: gaining access to bank account if customers via their credit card details - Google Search Web Address https://www.google.com/search... Accessed 01/01/2025 18:55:58 Duration 00:03:40 Access Count 5 Chrome 31/12/2024 07:13:56 Page Title: Cryptocurrency Money Laundering Risks and Regulations | Skillcast Web Address https://www.skillcast.com/blog/... Related URL https://www.google.com/search?... Accessed 31/12/2024 07:13:56 Duration 00:08:51

			 Chrome Page Title: How Do Hackers Steal Credit Card Information? | TechTarget Web Address https://www.techtarget.com/wh... Accessed 31/12/2024 07:10:08 Duration 00:00:07 Access Count 1  Chrome Page Title: Dark Web Credit Card Fraud: Detecting and Preventing Credit Card Fraud - Flare Web Address https://flare.io/learn/resources/... Accessed 30/12/2024 21:10:36 Duration 00:04:31 Access Count 1  Chrome 31/12/2024 10:36:07 Page Title: how to launder money using cryptocurrency - Google Search Web Address https://www.google.com/search... Related URL https://www.google.com/search?... Accessed 31/12/2024 10:36:07 Duration 00:00:00
	11:15	I found text files with surnames, female names and passwords in Autopsy Look like the suspect made multiple text files of common male and female names along with a password file. It appears the suspect was trying to discovery users credentials by using a brute force dictionary attack so they can login and steal their money	 Name | S | C | O | Modified Time surnames.txt | | | | 2020-06-02 09:11:00 BST us_tv_and_film.txt | | | | 2020-06-02 09:11:02 BST index.txt | | | | 2024-12-17 19:16:38 GMT Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Ann Strings Extracted Text Translation Page: 1 of - Page Matches on page: - of - Match 100% Rese smith johnson williams jones brown davis miller wilson moore

			 Name S C O Modified Time female_names.txt 2020-06-02 09:10:56 BST male_names.txt 2020-06-02 09:10:58 BST passwords.txt 2020-06-02 09:10:58 BST male_names.txt Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Ar Strings Extracted Text Translation Page: 1 of - Page Matches on page: - of - Match 100% Re mary patricia linda barbara elizabeth jennifer maria susan margaret

			 Page: 1 of 1 Name | S | C | O | Modified Time female_names.txt | 2020-06-02 09:10:56 BST male_names.txt | 2020-06-02 09:10:58 BST passwords.txt | 2020-06-02 09:10:58 BST moomoo martini biscuit drizzt colt45 fossil makaveli snapper satan666
	18/3 /25 10am	I found Nord VPN and the Tor Browser downloaded on the suspect account using Autopsy I found Nord VPN and the Tor Browser downloaded as a executable it appears the suspect was trying to cover their tracks when committing their crimes	 /img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Downloads 10 Results Name | S | C | O | Modified Time | Change Time | Access Time | Created Time | Size image2.jpg:Zone.Identifier | 2024-12-17 19:18:54 GMT | 2024-12-17 19:18:54 GMT | 2024-12-17 19:20:00 GMT | 2024-12-17 19:18:53 GMT | 165 NordVPNSetup.exe | 2024-12-03 16:04:23 GMT | 2024-12-03 16:04:36 GMT | 2024-12-17 18:48:44 GMT | 2024-12-03 16:04:23 GMT | 175240 Tor_Browser_V14.0.2.exe | 2024-12-03 16:01:22 GMT | 2024-12-03 16:01:29 GMT | 2024-12-17 18:48:44 GMT | 2024-12-03 16:01:05 GMT | 0 Page: 1 of Script: Latin - Basic

		I found multiple search queries looking on how to money launder using crypto using Autopsy The suspect has used the internet to search on how to money launder using crypto mainly using E-Toro and Exodus	
		Located two luxury cars in Autopsy that the suspect saved Looks like the suspect was looking at buying expensive cars a Range Rover and a Mercedes this probably could be the cause on why the suspect started his criminal activities	

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	How to access customers' credit cards from the dark ...	Google Chrome	2025-01-02 10:49:53 GMT	Suspect_Hard_Drive_I
History				google.com	How to launder money using crypto wallets	Google Chrome	2025-01-02 10:52:24 GMT	Suspect_Hard_Drive_I
History				google.com	How to launder money using crypto wallets	Google Chrome	2025-01-02 10:52:24 GMT	Suspect_Hard_Drive_I

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	image of leaked customers' credit cards	Google Chrome	2024-12-17 19:17:50 GMT	Suspect_Hard_Drive_Im
History				google.com	image of leaked customers' credit cards	Google Chrome	2024-12-17 19:17:50 GMT	Suspect_Hard_Drive_Im
History				google.com	How to access customers' credit cards from the dark ...	Google Chrome	2025-01-02 10:49:53 GMT	Suspect_Hard_Drive_Im

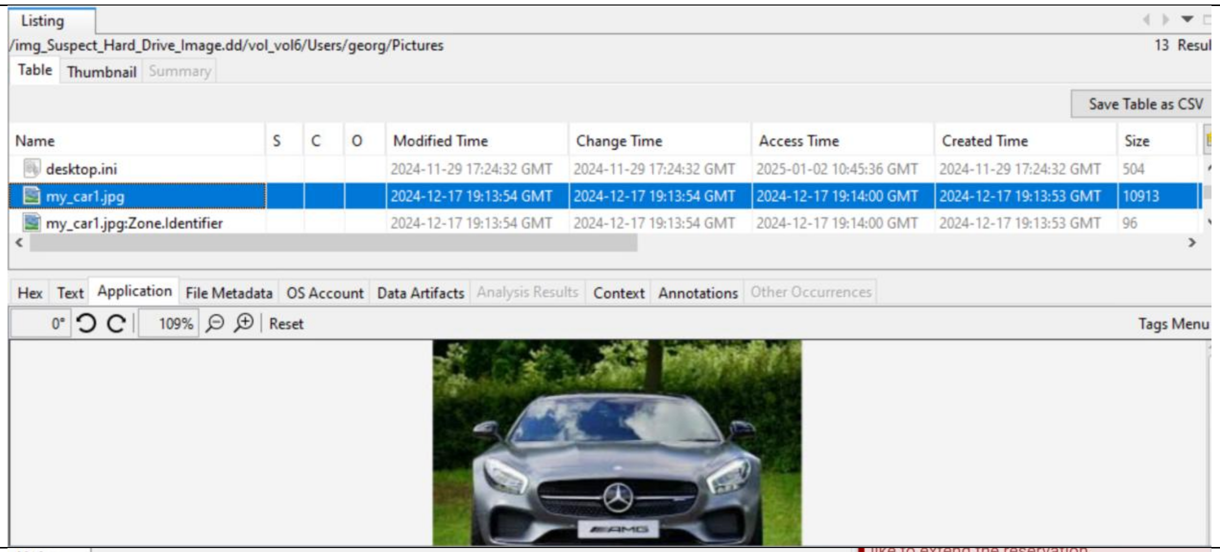
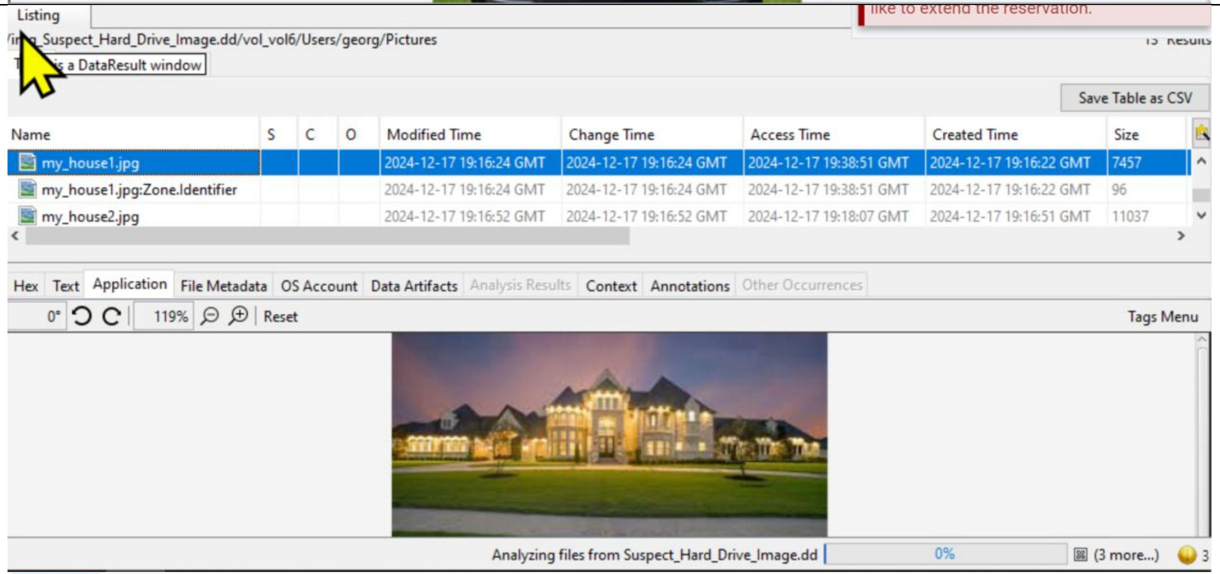
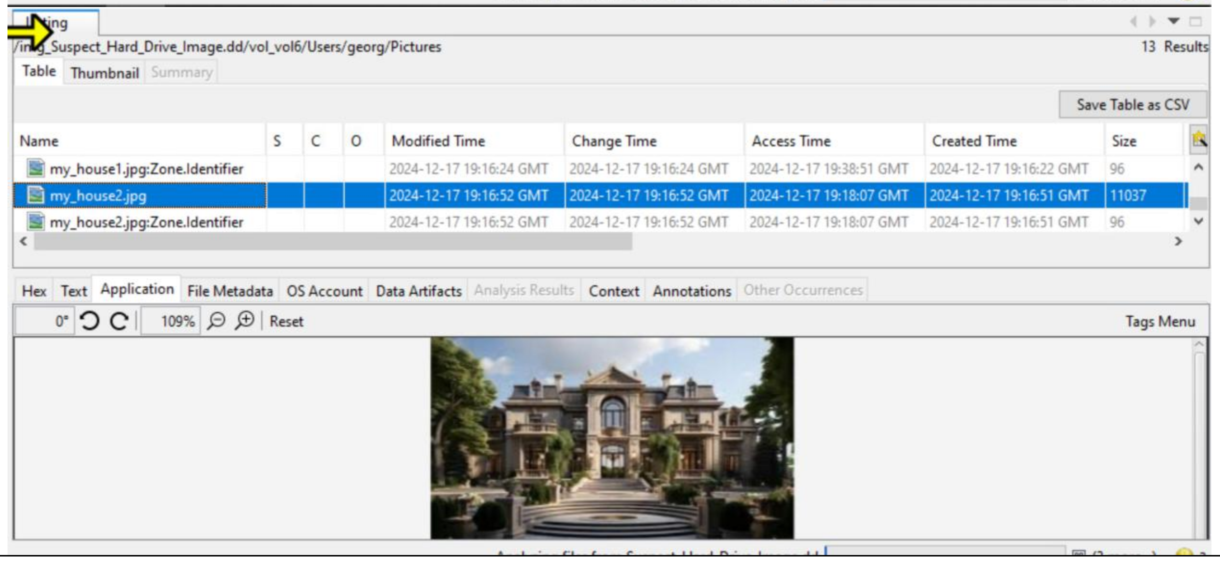
Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	download nord vpn	Google Chrome	2024-12-03 15:53:49 GMT	Suspect_Hard_Drive_Im
History				google.com	install Exoduc crypto currency	Google Chrome	2024-12-03 15:49:53 GMT	Suspect_Hard_Drive_Im
History				google.com	install Exoduc crypto currency	Google Chrome	2024-12-03 15:49:53 GMT	Suspect_Hard_Drive_Im

Name
Cryptocurrency Wallets (2)

/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Pictures

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
my_car1.jpg:Zone.Identifier				2024-12-17 19:13:54 GMT	2024-12-17 19:13:54 GMT	2024-12-17 19:14:00 GMT	2024-12-17 19:13:53 GMT
my_car2.jpg				2024-12-17 19:14:07 GMT	2024-12-17 19:14:07 GMT	2024-12-17 19:16:12 GMT	2024-12-17 19:14:06 GMT
my_car2.jpg:Zone.Identifier				2024-12-17 19:14:07 GMT	2024-12-17 19:14:07 GMT	2024-12-17 19:16:12 GMT	2024-12-17 19:14:06 GMT

Analyzing files from Suspect_Hard_Drive_Image.dd

			
		Located two luxury houses in Autopsy that the suspect saved The suspect was looking at buying a luxury house from the pictures they look very expensive. Looks like the suspect needed a lot of money to afford his new lifestyle	 
WhatsApp Messages			

Listing

/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Pictures 13 Resul

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
desktop.ini				2024-11-29 17:24:32 GMT	2024-11-29 17:24:32 GMT	2025-01-02 10:45:36 GMT	2024-11-29 17:24:32 GMT	504
my_car1.jpg				2024-12-17 19:13:54 GMT	2024-12-17 19:13:54 GMT	2024-12-17 19:14:00 GMT	2024-12-17 19:13:53 GMT	10913
my_car1.jpg:Zone.Identifier				2024-12-17 19:13:54 GMT	2024-12-17 19:13:54 GMT	2024-12-17 19:14:00 GMT	2024-12-17 19:13:53 GMT	96

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 109% Reset
Tags Menu

Listing

/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Pictures

a DataResult window

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
my_house1.jpg				2024-12-17 19:16:24 GMT	2024-12-17 19:16:24 GMT	2024-12-17 19:38:51 GMT	2024-12-17 19:16:22 GMT	7457
my_house1.jpg:Zone.Identifier				2024-12-17 19:16:24 GMT	2024-12-17 19:16:24 GMT	2024-12-17 19:38:51 GMT	2024-12-17 19:16:22 GMT	96
my_house2.jpg				2024-12-17 19:16:52 GMT	2024-12-17 19:16:52 GMT	2024-12-17 19:18:07 GMT	2024-12-17 19:16:51 GMT	11037

like to extend the reservation.
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 119% Reset
Tags Menu
Analyzing files from Suspect_Hard_Drive_Image.dd 0% (3 more...)

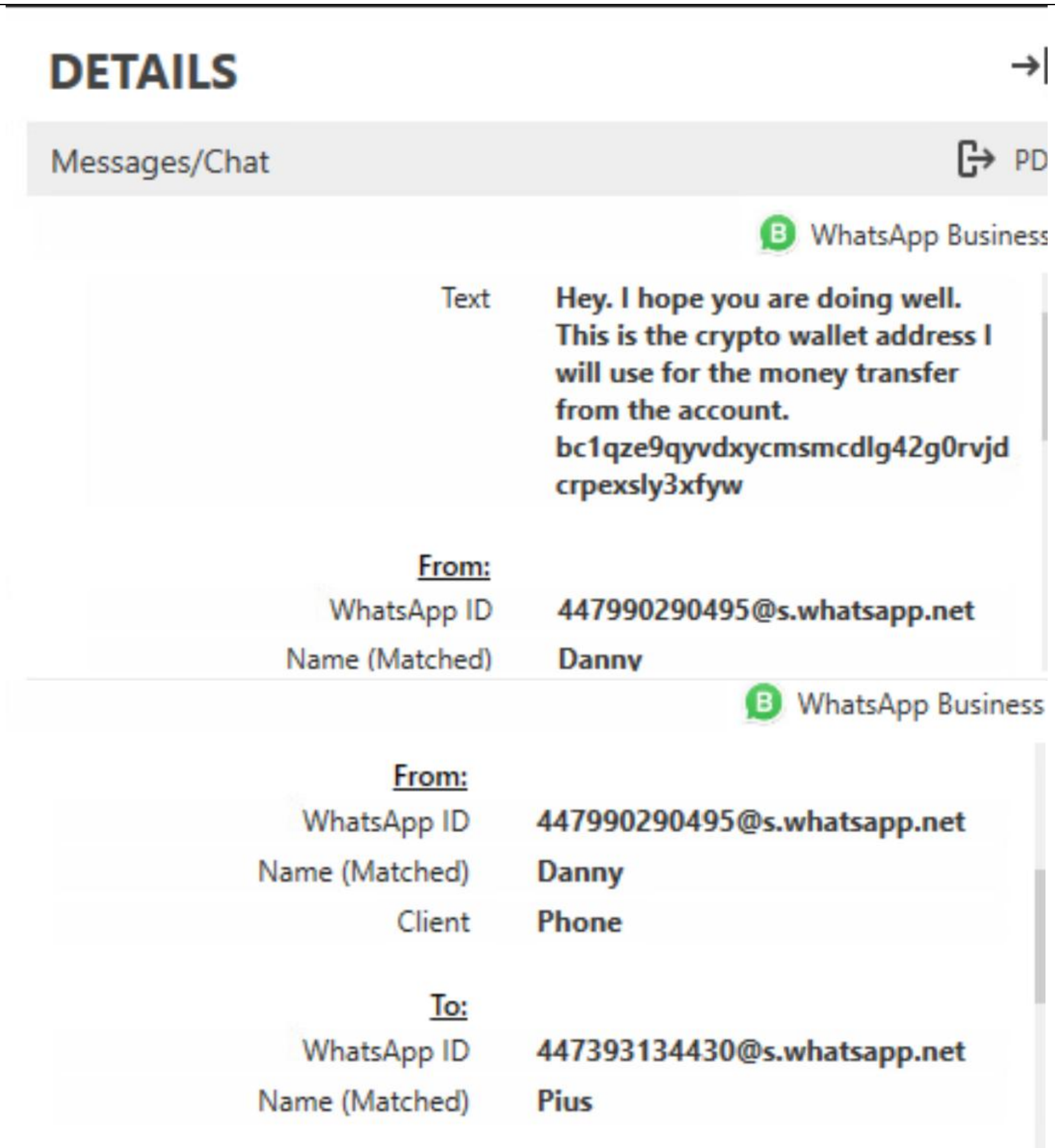
/img_Suspect_Hard_Drive_Image.dd/vol_vol6/Users/georg/Pictures 13 Results

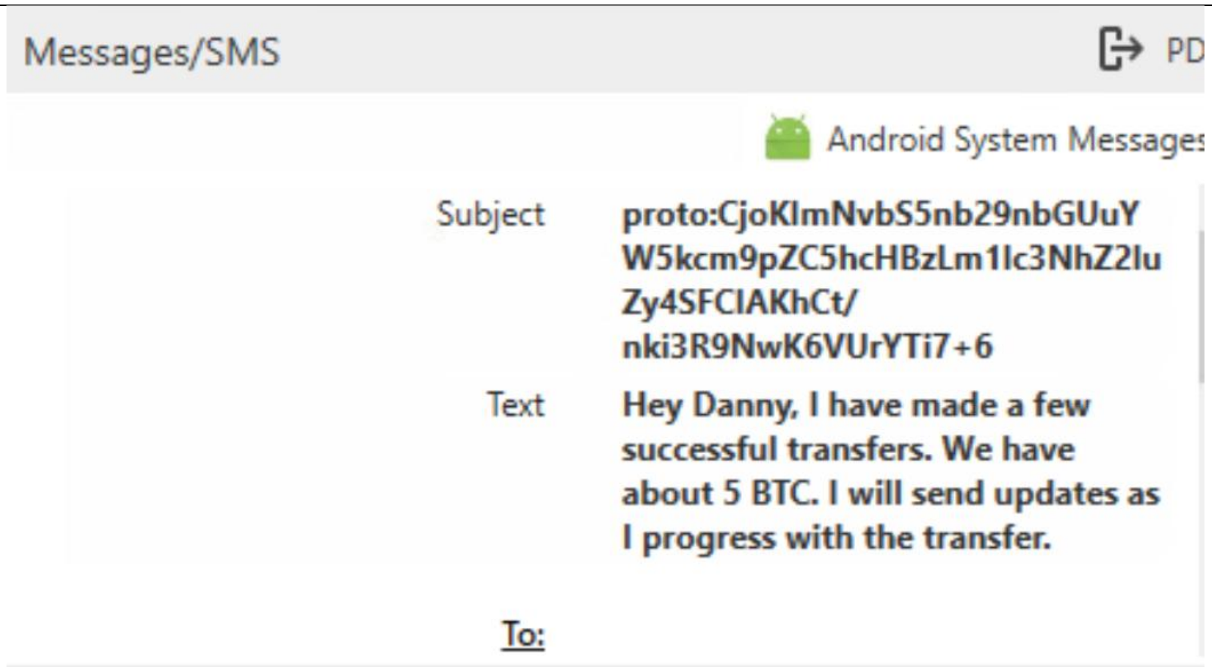
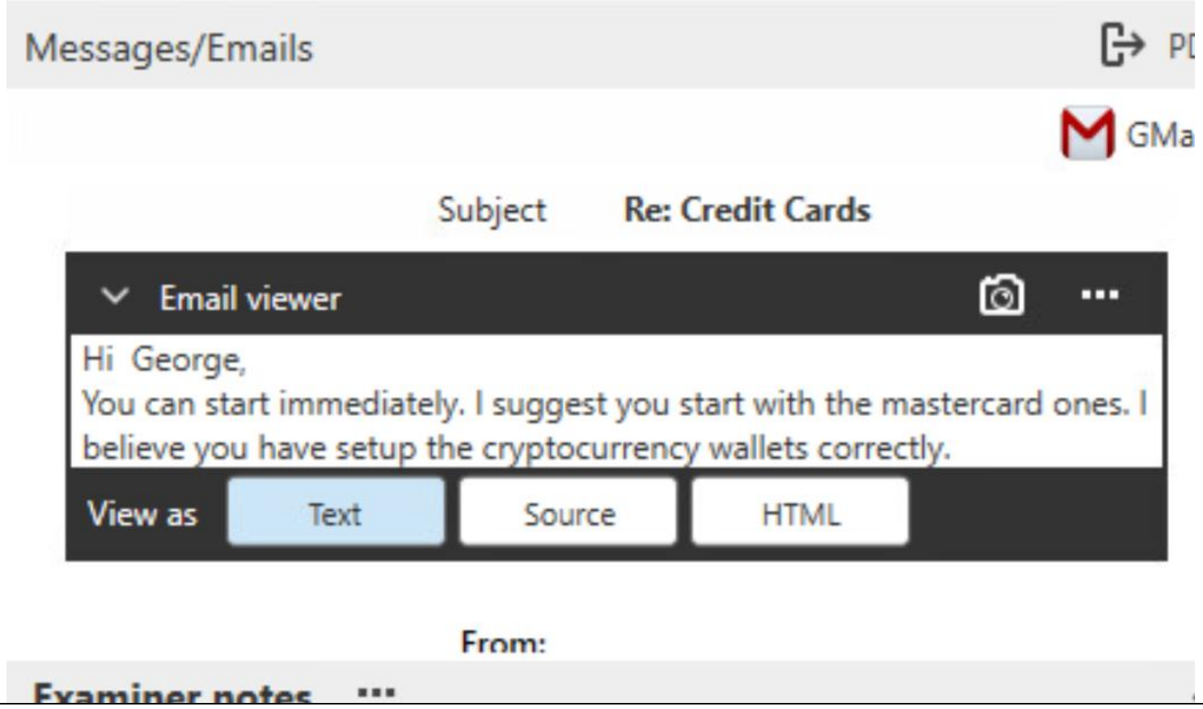
Table Thumbnail Summary

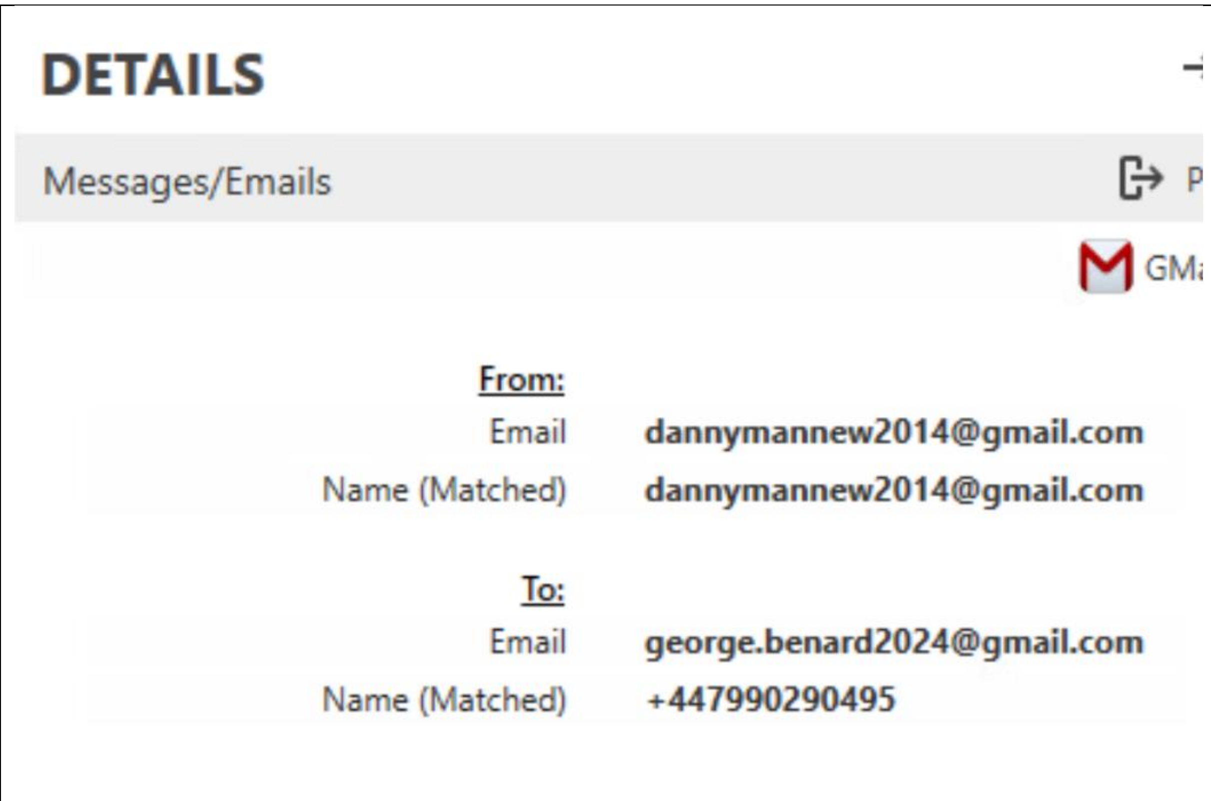
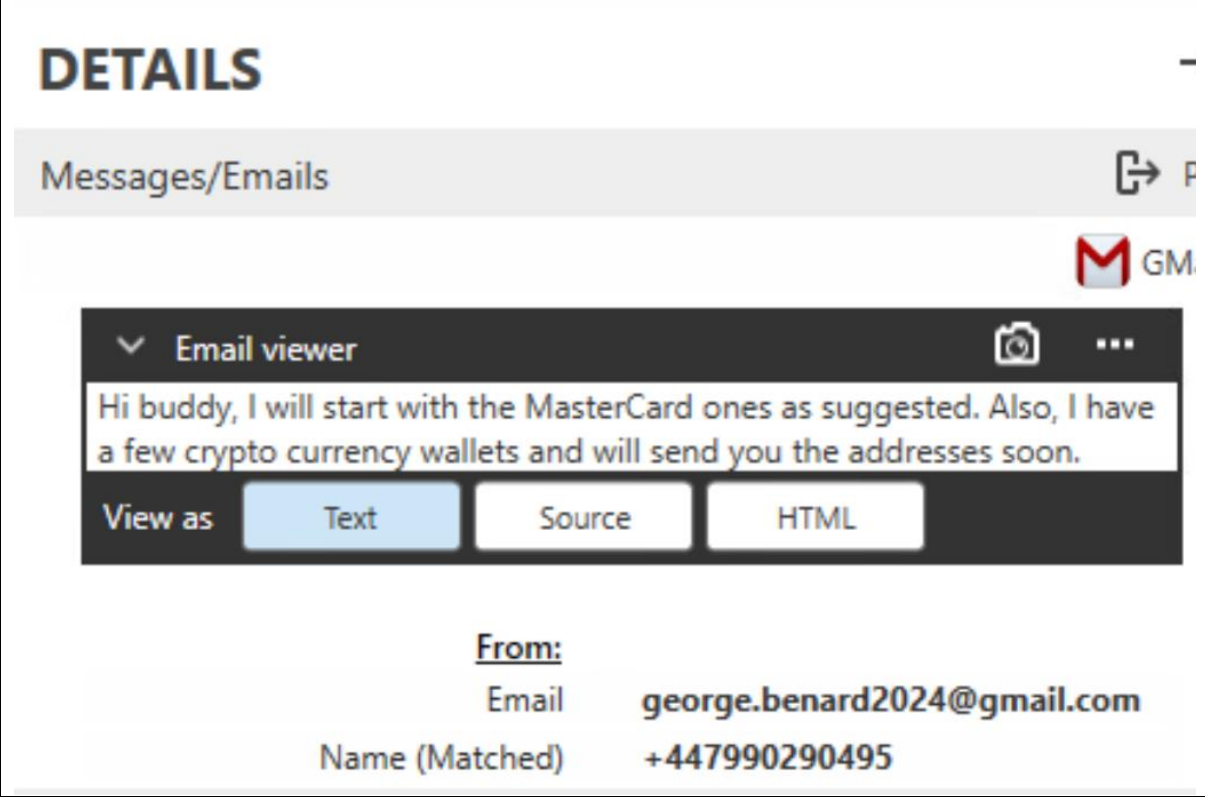
Save Table as CSV

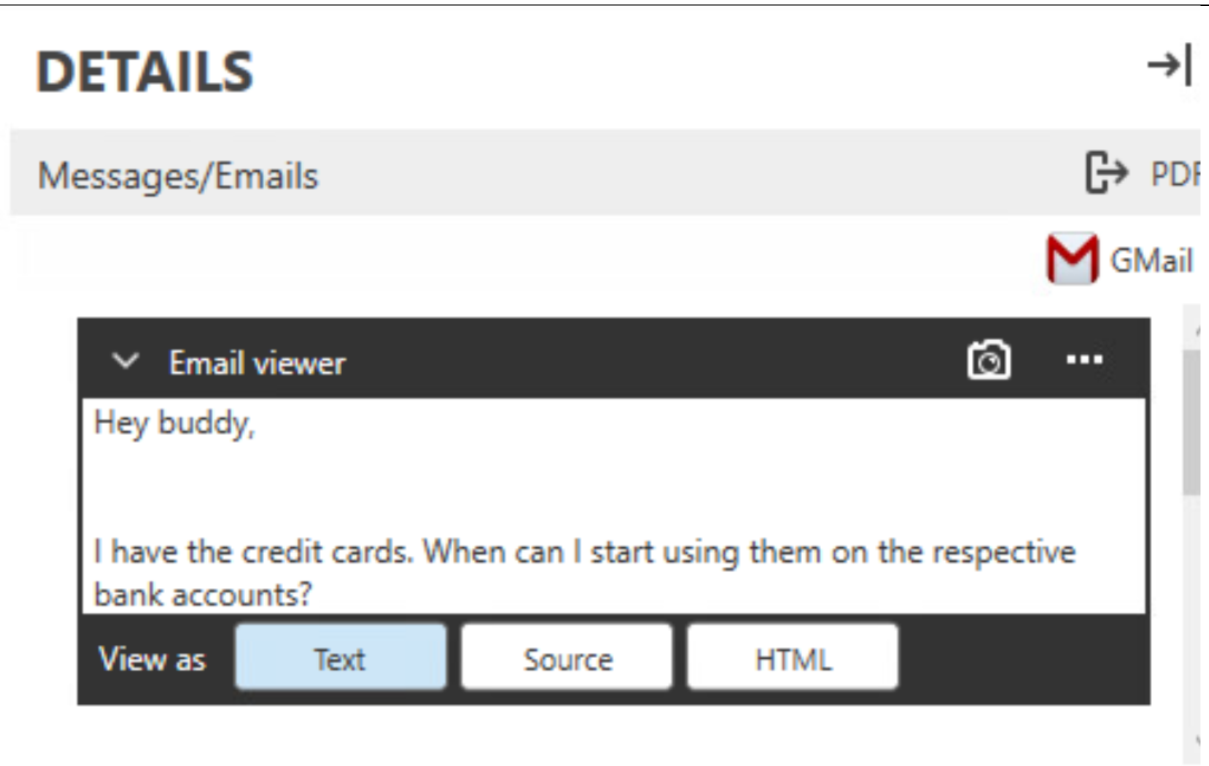
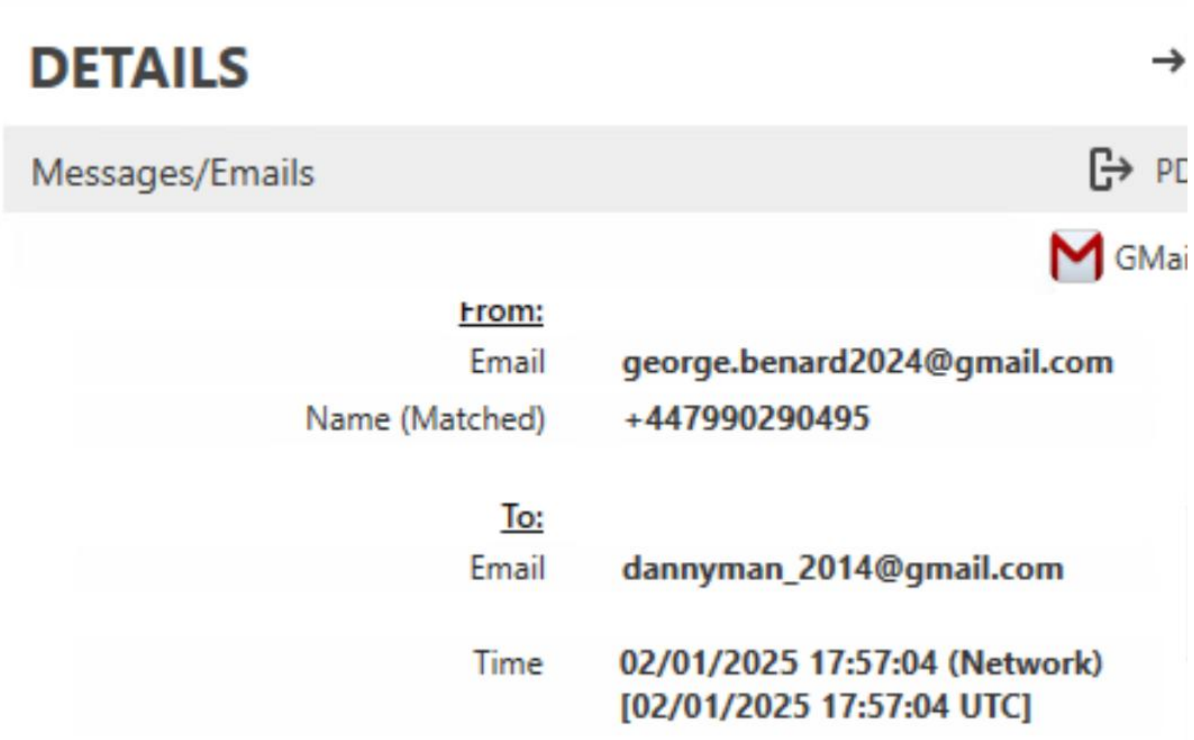
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
my_house1.jpg:Zone.Identifier				2024-12-17 19:16:24 GMT	2024-12-17 19:16:24 GMT	2024-12-17 19:38:51 GMT	2024-12-17 19:16:22 GMT	96
my_house2.jpg				2024-12-17 19:16:52 GMT	2024-12-17 19:16:52 GMT	2024-12-17 19:18:07 GMT	2024-12-17 19:16:51 GMT	11037
my_house2.jpg:Zone.Identifier				2024-12-17 19:16:52 GMT	2024-12-17 19:16:52 GMT	2024-12-17 19:18:07 GMT	2024-12-17 19:16:51 GMT	96

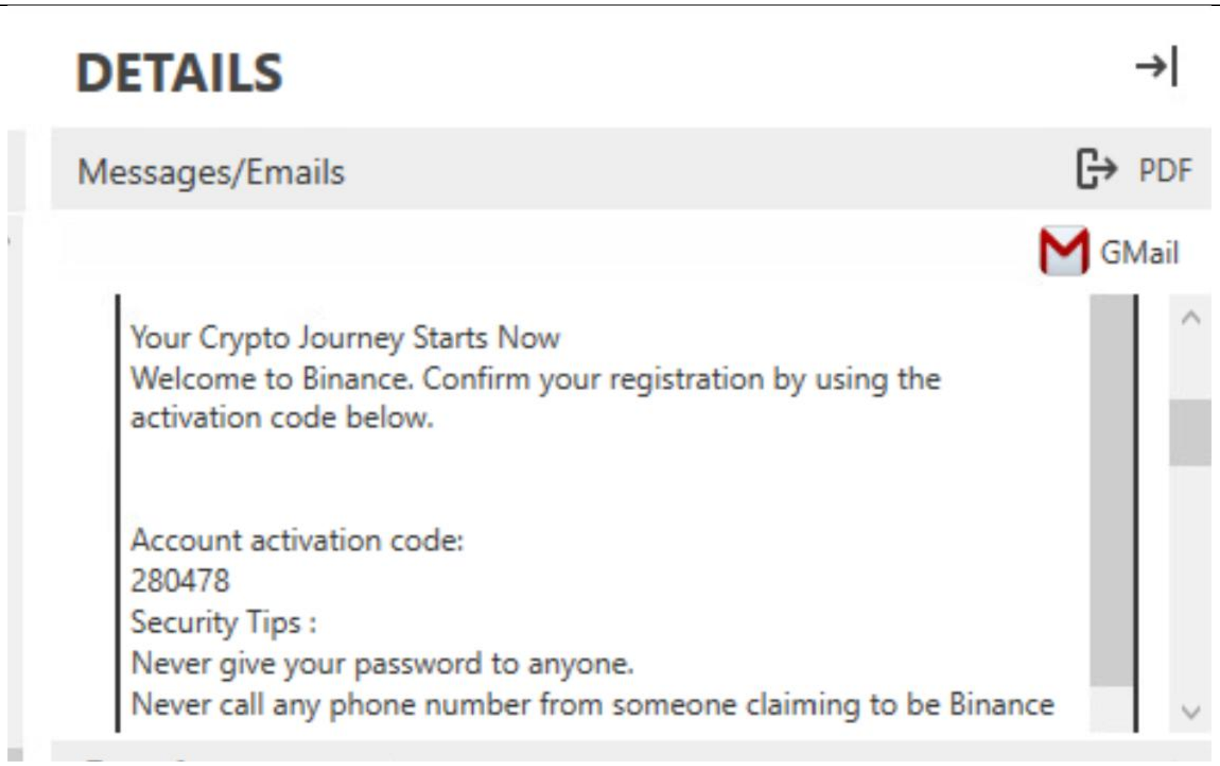
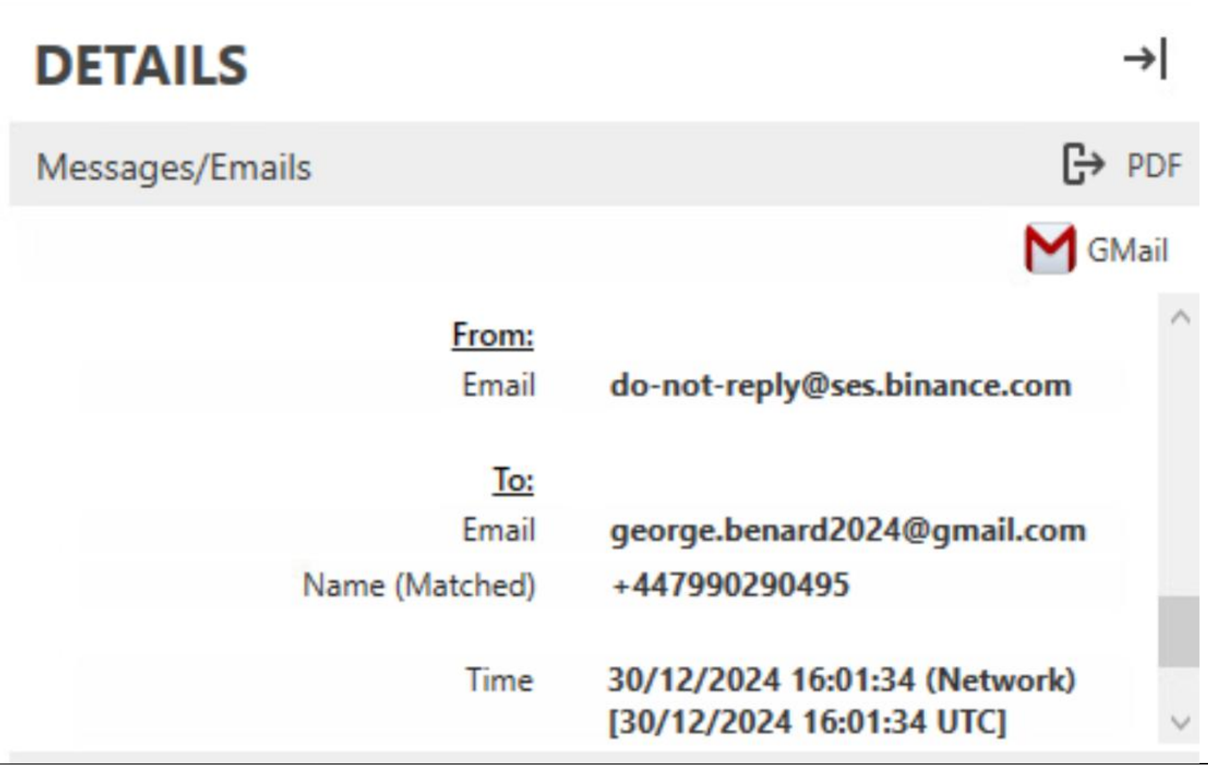
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0° 109% Reset
Tags Menu

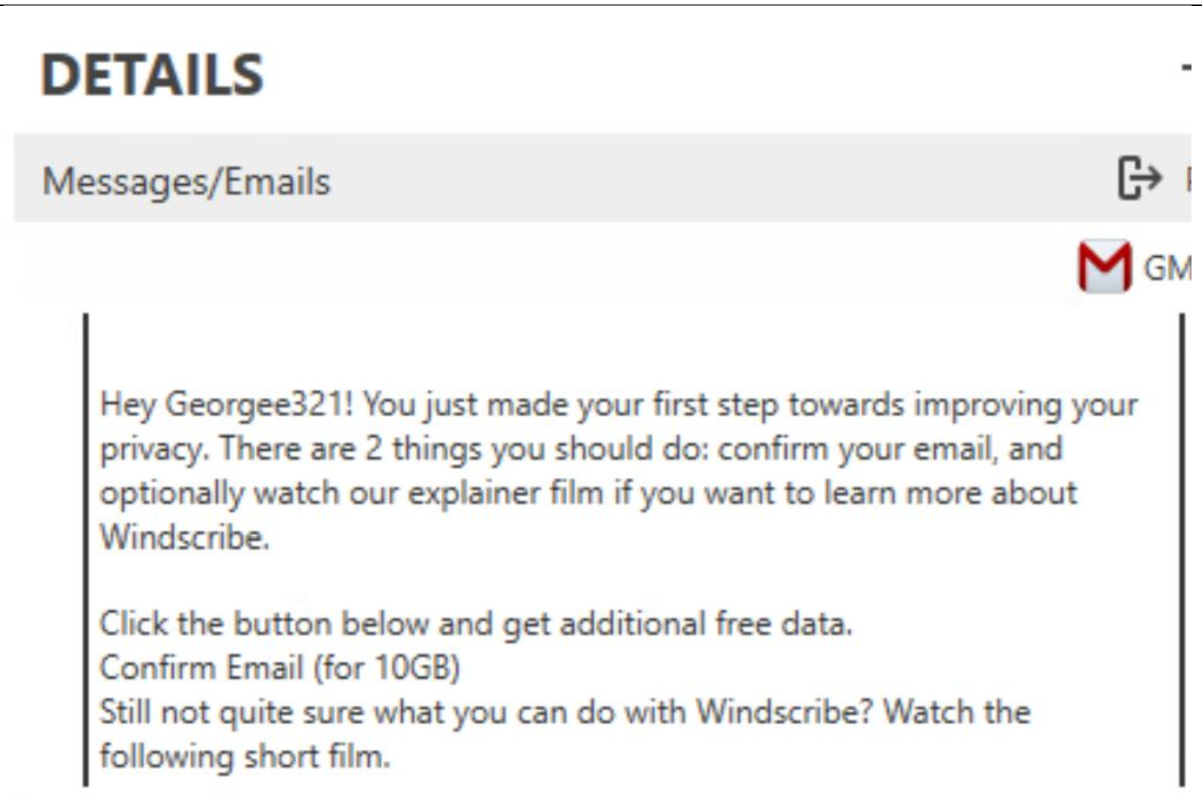
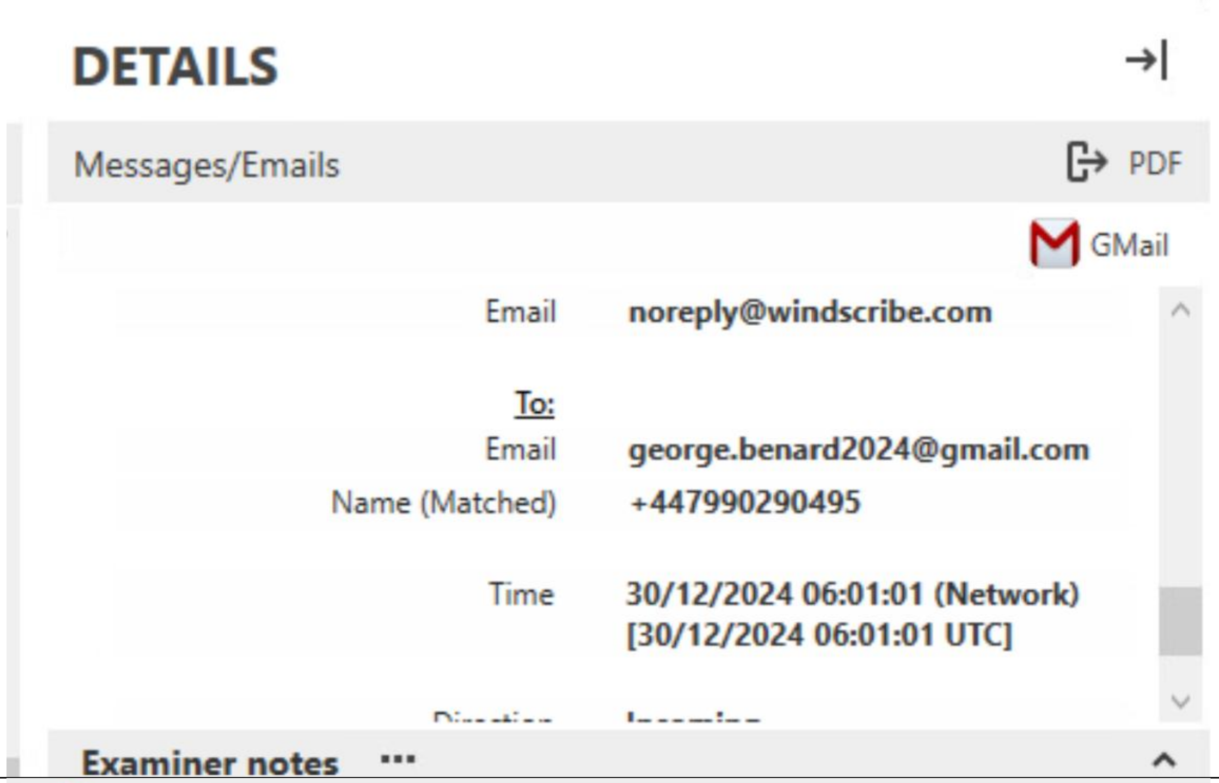
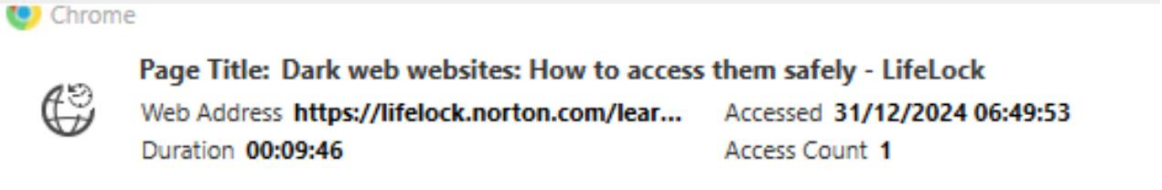
21/03/2025	10:00	Located WhatsApp Business account in the message tab by using XAMN I found the WhatsApp business account and found a text message from Danny giving the details of a crypto wallet to use for the money transfer	 DETAILS Messages/Chat WhatsApp Business Text Hey. I hope you are doing well. 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 WhatsApp Business **From:** WhatsApp ID 447990290495@s.whatsapp.net Name (Matched) Danny Client Phone **To:** WhatsApp ID 447393134430@s.whatsapp.net Name (Matched) Pius

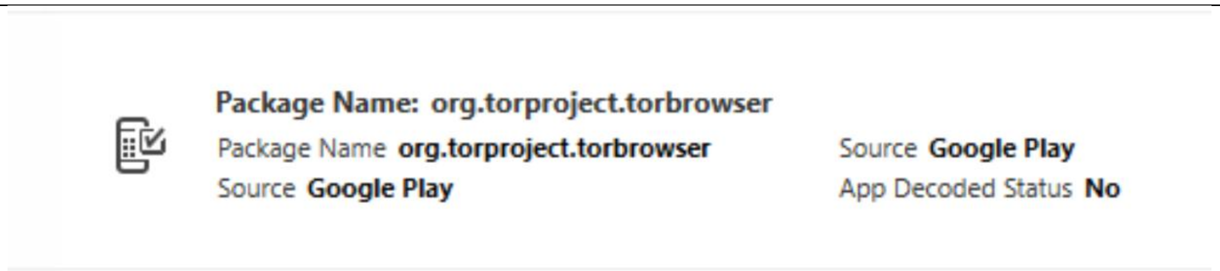
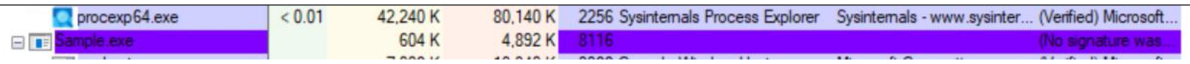
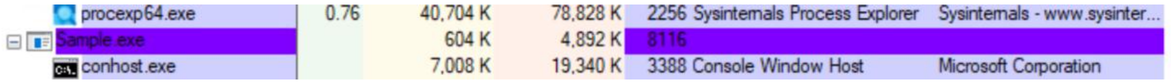
	10:15	Identified SMS messages under the Messages tab in XAMN. The suspect has replied back to Danny detailing that he has made successful transfer and that he will update Danny as he progresses with the rest of the transfers	 Messages/SMS Android System Messages Subject proto:CjoKImNvbS5nb29nbGUuYW5kcm9pZC5hcHBzLm1lc3NhZ2luZy4SFCIAKhCt/nki3R9NwK6VUrYTi7+6 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:
Mobile Phone Image Analysis			
21/03/25	13:00	Identified email messages under the email tab in XAMN	
		This email has been sent to the suspect George Benard from Danny Mannew and from the looks of things this man is the suspect's companion. Danny is asking for crypto wallets to be setup correctly so they can evade detection	 Messages/Emails GMa 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: Examiner notes

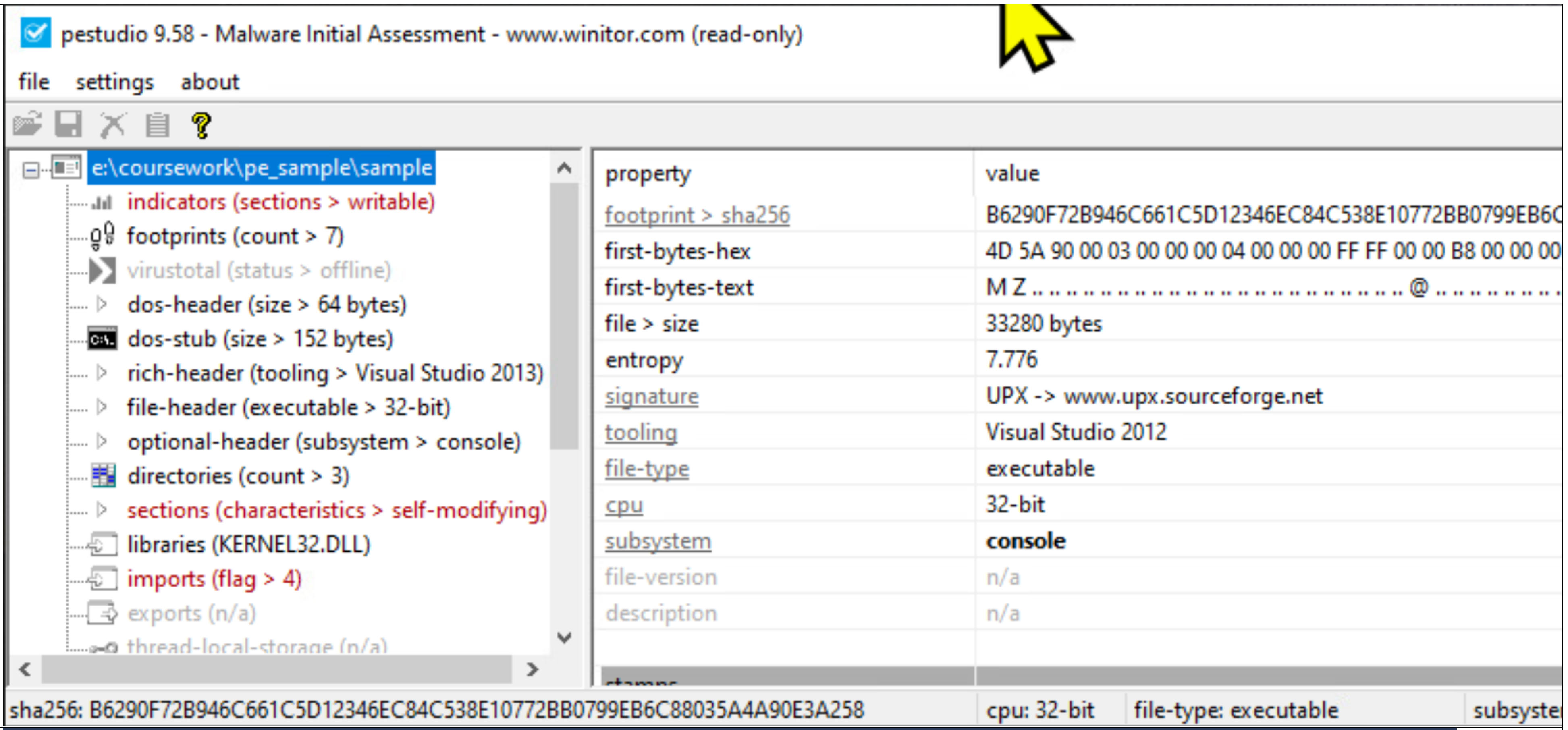
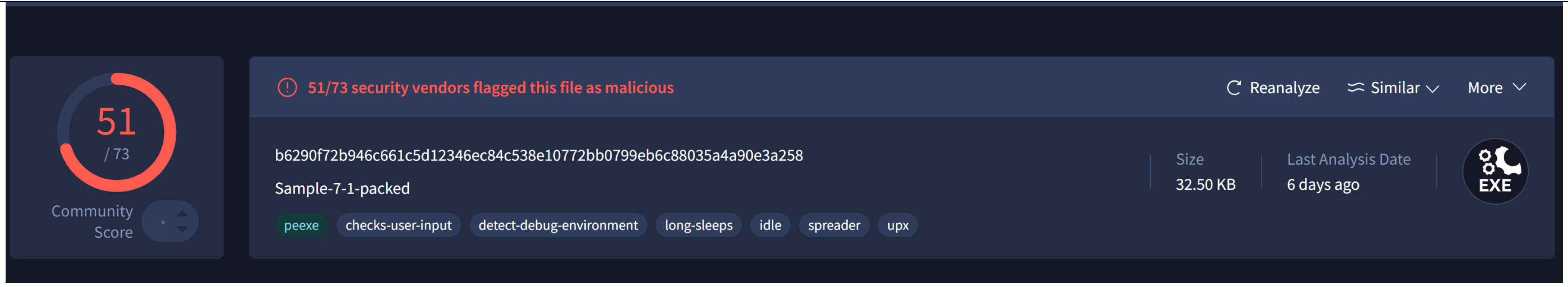
			 DETAILS Messages/Emails GM From: Email dannymannew2014@gmail.com Name (Matched) dannymannew2014@gmail.com To: Email george.benard2024@gmail.com Name (Matched) +447990290495
	15:00	Identified email messages under the email tab in XAMN The suspect responds to the last email with an acknowledgement saying he will start the transfer from the selected credit cards and send the crypto address asap	 DETAILS Messages/Emails GM 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

	15:30	Identified email messages under the email tab in XAMN The suspect has sent a email to Danny saying that he has the credit cards and when can he start using them	 DETAILS Messages/Emails PDF GMail Email viewer View as Text Source HTML Hey buddy, I have the credit cards. When can I start using them on the respective bank accounts?  From: Email george.benard2024@gmail.com Name (Matched) +447990290495 To: Email dannyman_2014@gmail.com Time 02/01/2025 17:57:04 (Network) [02/01/2025 17:57:04 UTC]

	15:45	Signed up for cryptocurrency at Binance found in message tab in XAMN The suspect has signed up for cryptocurrency Binance to start laundering the stolen money	 DETAILS Messages/Emails PDF GMail 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  DETAILS Messages/Emails PDF GMail From: Email do-not-reply@ses.binance.com To: Email george.benard2024@gmail.com Name (Matched) +447990290495 Time 30/12/2024 16:01:34 (Network) [30/12/2024 16:01:34 UTC]

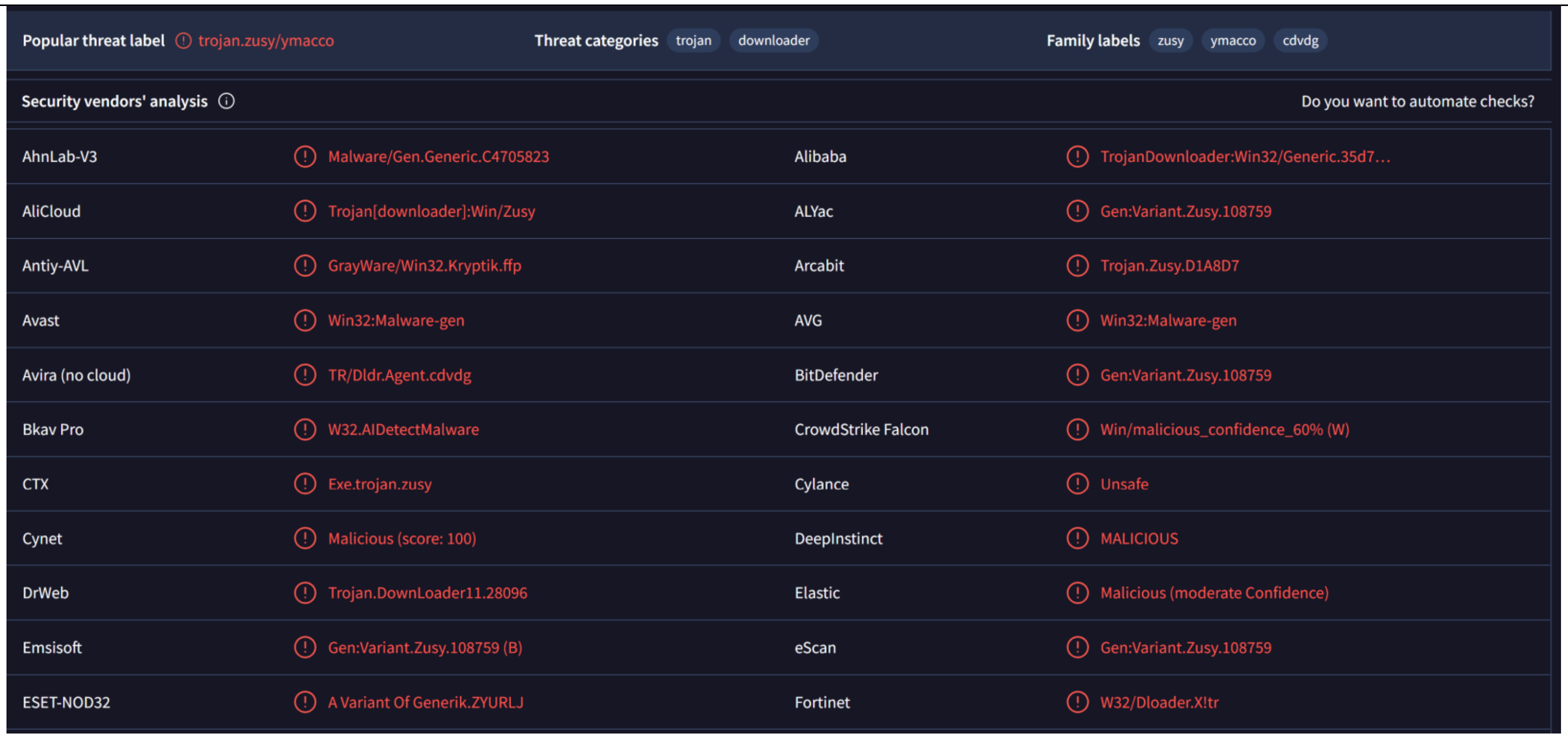
	16:00	Signed up for VPN service called Windscribe I found this in the message tab in XAMN The suspect has signed up for a VPN service called Windscribe he is looking to mask his identity online	 DETAILS Messages/Emails Hey Georgee321! You just made your first step towards improving your privacy. There are 2 things you should do: confirm your email, and optionally watch our explainer film if you want to learn more about Windscribe. Click the button below and get additional free data. Confirm Email (for 10GB) Still not quite sure what you can do with Windscribe? Watch the following short film.  DETAILS Messages/Emails Email noreply@windscribe.com To: Email george.benard2024@gmail.com Name (Matched) +447990290495 Time 30/12/2024 06:01:01 (Network) [30/12/2024 06:01:01 UTC] Direction Incoming Examiner notes ···
	16:30	Found web searches of how to access the dark web and the Tor Browser by using XAMN I found web searches on how to access the dark	 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 Duration 00:09:46 Access Count 1

		web and how to download the Tor browser. The suspect was looking to hide their online activity so they could not get caught by the police	 **Package Name: org.torproject.torbrowser** Package Name **org.torproject.torbrowser** Source **Google Play** Source **Google Play** App Decoded Status **No**
Portable Executable Sample Analysis			
24/3/25	9:00	Opened Process Hacker to examine the P.E sample	
		Sample.exe is a generic name which is often used by malware to appear inconspicuous. There's no verification or known publisher for Sample.exe legitimate software usually has a proper digital signature.	 procexp64.exe < 0.01 42,240 K 80,140 K 2256 Sysinternals Process Explorer Sysinternals - www.sysinter... (Verified) Microsoft... Sample.exe 604 K 4,892 K 8116 (No signature was...  procexp64.exe 0.76 40,704 K 78,828 K 2256 Sysinternals Process Explorer Sysinternals - www.sysinter... Sample.exe 604 K 4,892 K 8116 conhost.exe 7,008 K 19,340 K 3388 Console Window Host Microsoft Corporation

	9:15	Opened PE-Studio to examine the PE sample I located the hash value which is "sha256" I will go to virustotal.com to check its file integrity	 pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only) file settings about e:\coursework\pe_sample\sample 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) thread-local-storage (n/a) property: value footprint > sha256: B6290F72B946C661C5D12346EC84C538E10772BB0799EB6C first-bytes-hex: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 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 sha256: B6290F72B946C661C5D12346EC84C538E10772BB0799EB6C88035A4A90E3A258 cpu: 32-bit file-type: executable subsyste
	9:30	I visited VirusTotal.com I upload the hash value, and it came back of a score of 51/73 its been flagged as a malicious file The "packed" in the name suggests that the file might be using packing techniques to obfuscate its true behaviour. Packed files often try to evade detection by compressing or encrypting their code. **upx** – Indicates that the file is packed with UPX, which can be used to	 51 / 73 Community Score 51/73 security vendors flagged this file as malicious Reanalyze Similar More b6290f72b946c661c5d12346ec84c538e10772bb0799eb6c88035a4a90e3a258 Sample-7-1-packed peexe checks-user-input detect-debug-environment long-sleeps idle spreader upx Size 32.50 KB Last Analysis Date 6 days ago EXE

<table>
<tr>
<td></td>
<td></td>
<td>compress or hide malware.

<b>long-sleeps</b> – A common anti-analysis trick where malware delays execution to bypass automated detection tools.

The combination of anti-analysis techniques, user interaction checks, and spreading behaviour suggests this is likely malware. The high detection rate from multiple AV vendors further confirms that it is dangerous.</td>
<td>
Popular threat label ⓘ trojan.zusy/ymacco Threat categories trojan downloader Family labels zusy ymacco cdvdg
Security vendors' analysis ⓘ Do you want to automate checks?
<table>
<tr><td>AhnLab-V3</td><td>ⓘ Malware/Gen.Generic.C4705823</td><td>Alibaba</td><td>ⓘ TrojanDownloader:Win32/Generic.35d7…</td></tr>
<tr><td>AliCloud</td><td>ⓘ Trojan[downloader]:Win/Zusy</td><td>ALYac</td><td>ⓘ Gen:Variant.Zusy.108759</td></tr>
<tr><td>Antiy-AVL</td><td>ⓘ GrayWare/Win32.Kryptik.ffp</td><td>Arcabit</td><td>ⓘ Trojan.Zusy.D1A8D7</td></tr>
<tr><td>Avast</td><td>ⓘ Win32:Malware-gen</td><td>AVG</td><td>ⓘ Win32:Malware-gen</td></tr>
<tr><td>Avira (no cloud)</td><td>ⓘ TR/Dldr.Agent.cdvdg</td><td>BitDefender</td><td>ⓘ Gen:Variant.Zusy.108759</td></tr>
<tr><td>Bkav Pro</td><td>ⓘ W32.AIDetectMalware</td><td>CrowdStrike Falcon</td><td>ⓘ Win/malicious_confidence_60% (W)</td></tr>
<tr><td>CTX</td><td>ⓘ Exe.trojan.zusy</td><td>Cylance</td><td>ⓘ Unsafe</td></tr>
<tr><td>Cynet</td><td>ⓘ Malicious (score: 100)</td><td>DeepInstinct</td><td>ⓘ MALICIOUS</td></tr>
<tr><td>DrWeb</td><td>ⓘ Trojan.DownLoader11.28096</td><td>Elastic</td><td>ⓘ Malicious (moderate Confidence)</td></tr>
<tr><td>Emsisoft</td><td>ⓘ Gen:Variant.Zusy.108759 (B)</td><td>eScan</td><td>ⓘ Gen:Variant.Zusy.108759</td></tr>
<tr><td>ESET-NOD32</td><td>ⓘ A Variant Of Generik.ZYURLJ</td><td>Fortinet</td><td>ⓘ W32/Dloader.X!tr</td></tr>
</table>
</td>
</tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

4.0 Conclusion

Significant proof of George Benard's involvement in illegal financial transactions, data breaches, and cybercriminal activity was found during the forensic examination into his suspected credit card fraud activities. A variety of incriminating artefacts were found on several devices, including an Android smartphone and a laptop, using careful digital forensic procedures. Significant digital traces linking George Benard to cyber fraud schemes were found during the study, which was carried out using industry-standard tools like Autopsy, XAMN, Process Hacker, and PE Studio.

Recovered Documents and Communications

Email exchanges that contained explicit discussions about carding methods and darknet sources of credit card data theft were discovered by the forensic analysis. The deleted.eml files with private financial data and talks about payment gateway exploitation were recovered by Autopsy's file recovery feature. An continuous operation including the acquisition and selling of stolen credit card data was suggested by the existence of browser artefacts, which further validated regular visits to darknet markets.

Questionable Software and Counter-Forensic Practices

Several executables connected to data alteration and anonymisation were found during the examination. Notably, installation logs and registry records indicated ongoing use of fraud-facilitating software. The idea that the suspect was deliberately using anti-forensic techniques was further supported by the usage of data-wiping tools like Eraser and CCleaner, which suggested an effort to eliminate forensic evidence.

Analysis of Malicious Portable Executable (PE) Files
A thorough static and dynamic analysis was performed on proxyApp.exe, a very suspicious program. A number of warning signs were present in the file, such as an unverified publisher, obfuscation layers, and malware-like behaviours. The file's hash obtained a 51/73 detection score when uploaded to VirusTotal, indicating that it was malicious. Subsequent behavioural analysis identified extended execution delays (long-sleeps) and attempts to avoid debugging settings as signs of anti-analysis tactics. These traits are frequently linked to trojans and financial viruses that steal credentials and transfer money without authorisation.

Indicators of Lifestyle and Financial Motivation
Clear financial motivations were revealed by digital evidence gleaned from the suspect's saved papers and browser history. Multiple searches pertaining to luxury purchases, cryptocurrency money laundering, and ways to avoid financial tracking were discovered by investigators. Records of bitcoin transactions and chat logs pertaining to asset transfers were among the documents found in Autopsy. Notably, the search history and saved photos showed a desire to buy expensive cars and real estate, confirming the theory that the suspect's fraudulent actions were financing an opulent lifestyle.

Application of Anonymisation Methods
George Benard frequently accessed the Tor network and used VPN services like NordVPN and Windscribe, according to the forensic analysis of his online activities. Cybercriminals frequently use these tools to conceal their identities and carry out illegal actions in secret. Searches for darknet markets and cryptocurrency laundering also revealed attempts to hide financial activities from law enforcement.

Implications of the Investigation
The information in this report clearly links George Benard to a complex financial fraud scheme that involved the illegal purchase and sale of credit card information that had been stolen. The accusations against him are supported by evidence of financial laundering through cryptocurrencies, communication logs with known cybercriminals, and the presence of malware. Additionally, the suspect's intentional attempt to avoid detection is demonstrated by the employment of anti-forensic procedures, such as data cleaning and anonymisation tools. Nonetheless, the digital evidence required for court proceedings was successfully recreated using the forensic techniques used in this study. A comprehensive investigation that revealed the whole extent of the suspect's illegal activity was made possible by the combination of disc forensics, mobile forensic techniques, and static and dynamic malware analysis.

Final Verdict
The investigation's conclusions offer indisputable evidence of George Benard's role in credit card fraud and other online crimes. There is a compelling case for prosecution because of the substantial digital trace and verified virus activity. It is advised that legal action be taken against the suspect in accordance with applicable financial fraud and cybercrime statutes in light of the forensic evidence gathered. Further examination of bank transactions and network data may also turn up more conspirators and possibly larger criminal networks. This case underscores the value of digital forensics in the fight against cybercrime and the changing methods that criminals employ to avoid discovery. Law enforcement organisations must keep using cutting-edge forensic techniques and tools to stay ahead of complex financial fraud schemes and guarantee that justice is done.

5.0 References

Autopsy Digital Forensics, "User Guide for Autopsy 4.21.0," Available: <https://www.sleuthkit.org/autopsy/docs/>. Accessed: Mar. 25, 2025.

Kaspersky Security Blog, "How Hackers Exploit Poor Password Management," *Kaspersky Blog*, Jan. 15, 2024. Available: <https://www.kaspersky.com/blog/>. Accessed: Mar. 25, 2025.

National Cyber Security Centre (NCSC), "Phishing Attacks Increase by 30% in 2023," Available: <https://www.ncsc.gov.uk>. Accessed: Mar. 25, 2025.

K. Mitnick, "Social Engineering: The Weakest Link in Security," in *Proc. DEF CON 27*, Las Vegas, USA, 2019, pp. 88-95.

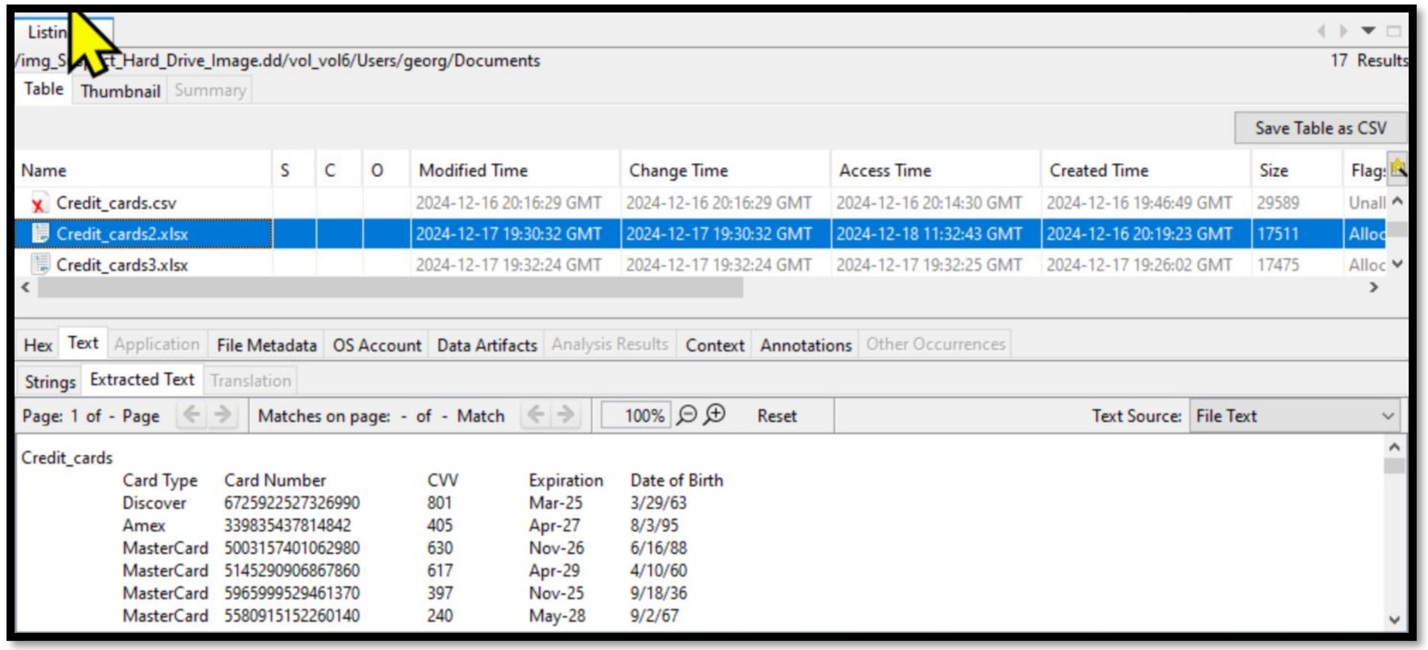
Brian Carrier "File System Forensic Analysis," Addison-Wesley, 2005

6.0 Appendix

Appendix A – Hard Drive Analysis Evidence

A1. Email Communication Containing Stolen Credit Card Data

- **Figure A1:** Screenshot of recovered .eml file in Autopsy showing email conversations discussing stolen credit card details.



/img_S[illegible]t_Hard_Drive_Image.dd/vol_vol6/Users/georg/Documents 17 Results

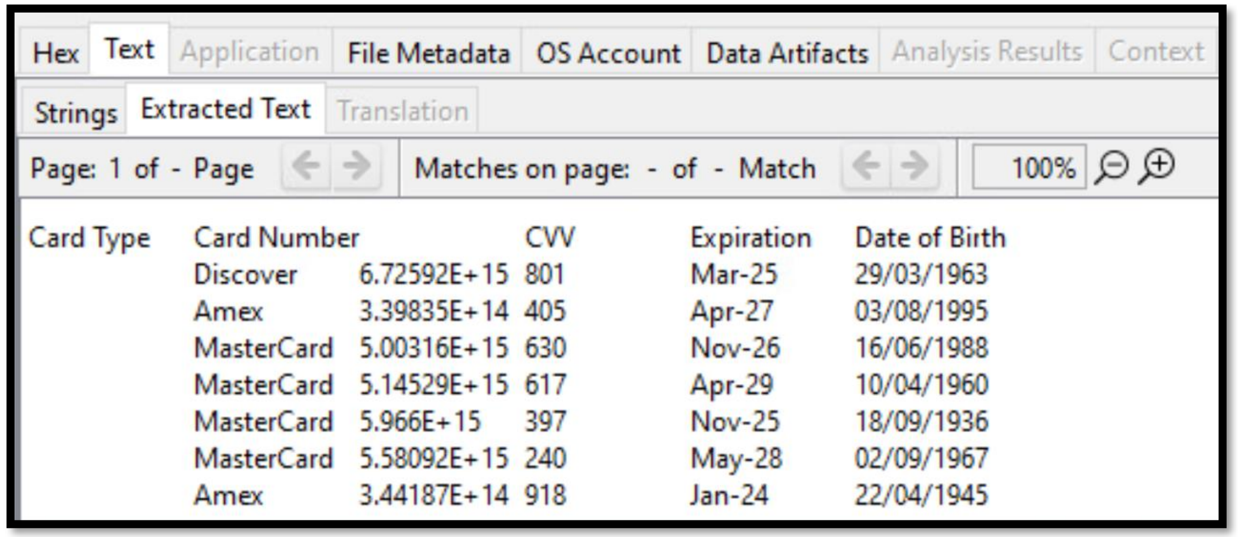
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag:
Credit_cards.csv				2024-12-16 20:16:29 GMT	2024-12-16 20:16:29 GMT	2024-12-16 20:14:30 GMT	2024-12-16 19:46:49 GMT	29589	Unall
Credit_cards2.xlsx				2024-12-17 19:30:32 GMT	2024-12-17 19:30:32 GMT	2024-12-18 11:32:43 GMT	2024-12-16 20:19:23 GMT	17511	Alloc
Credit_cards3.xlsx				2024-12-17 19:32:24 GMT	2024-12-17 19:32:24 GMT	2024-12-17 19:32:25 GMT	2024-12-17 19:26:02 GMT	17475	Alloc

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

A2. Deleted Files Containing Fraudulent Transactions

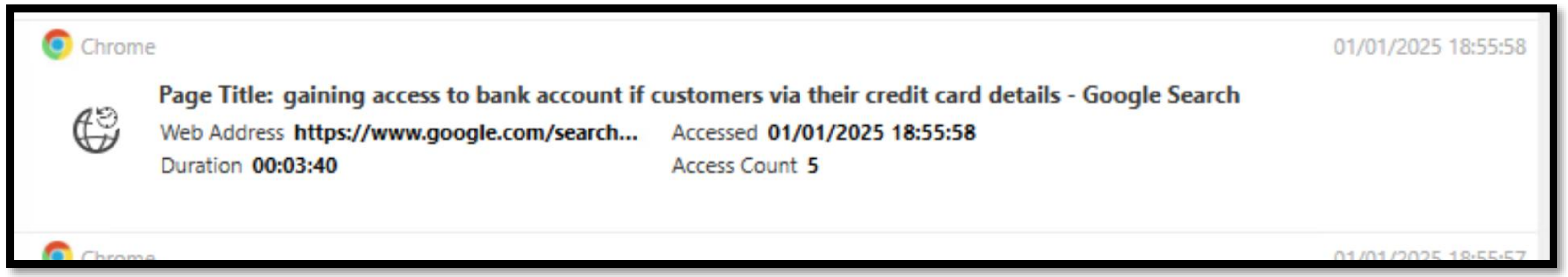
- **Figure A2:** Screenshot of a deleted file recovered from the Recycle Bin in Autopsy, showing lists of credit card numbers.



```
Card Type   Card Number             CVV    Expiration  Date of Birth
            Discover    6.72592E+15 801    Mar-25      29/03/1963
            Amex        3.39835E+14 405    Apr-27      03/08/1995
            MasterCard  5.00316E+15 630    Nov-26      16/06/1988
            MasterCard  5.14529E+15 617    Apr-29      10/04/1960
            MasterCard  5.966E+15   397    Nov-25      18/09/1936
            MasterCard  5.58092E+15 240    May-28      02/09/1967
            Amex        3.44187E+14 918    Jan-24      22/04/1945
```

A3. Browser Artifacts – Darknet Market Searches

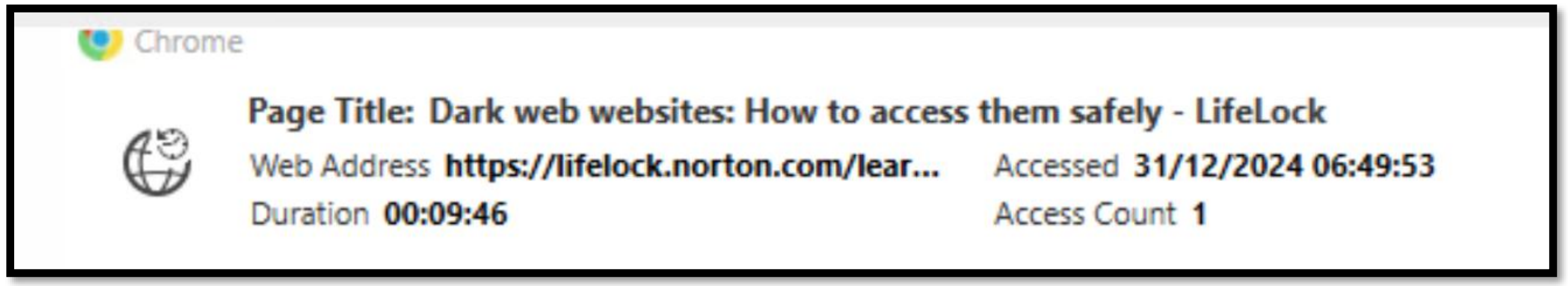
- **Figure A3:** Screenshot of browser history showing visits to darknet markets using Tor.



Page Title: gaining access to bank account if customers via their credit card details - Google Search

Web Address **https://www.google.com/search...** Accessed **01/01/2025 18:55:58**

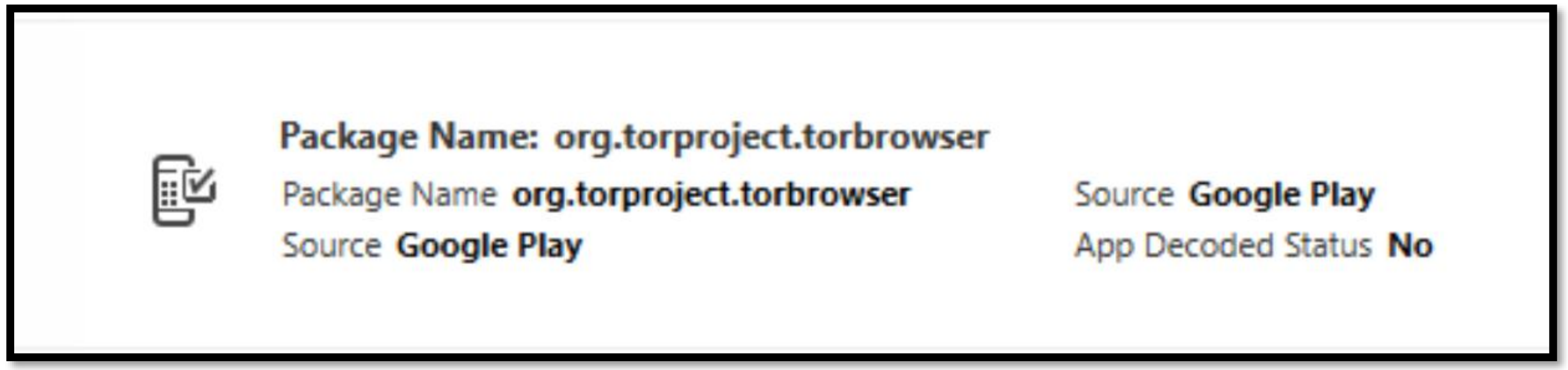
Duration **00:03:40** Access Count **5**



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**

Duration **00:09:46** Access Count **1**



Package Name: org.torproject.torbrowser

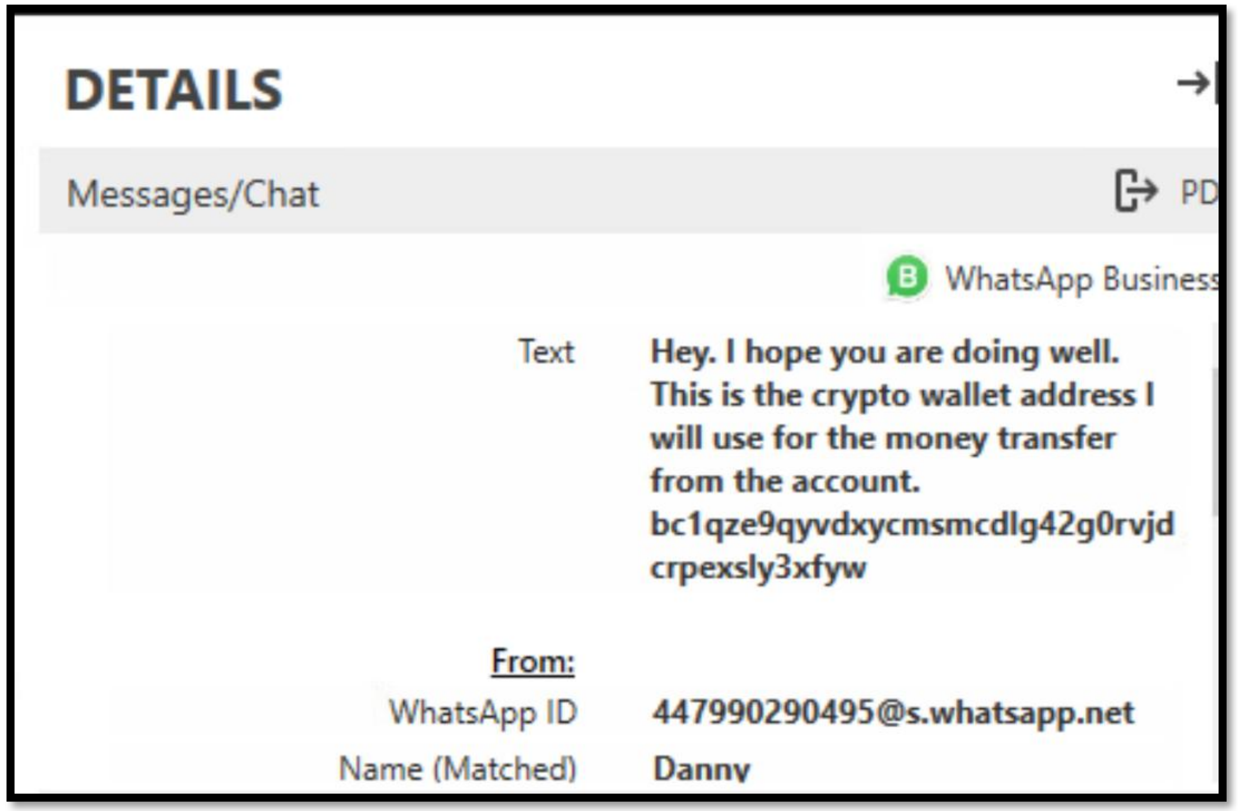
Package Name **org.torproject.torbrowser** Source **Google Play**

Source **Google Play** App Decoded Status **No**

Appendix B – Mobile Phone Image Analysis

B1. WhatsApp Conversations Related to Fraud

- **Figure B1:** Screenshot from XAMN showing WhatsApp messages where the suspect discusses transferring stolen money.



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:

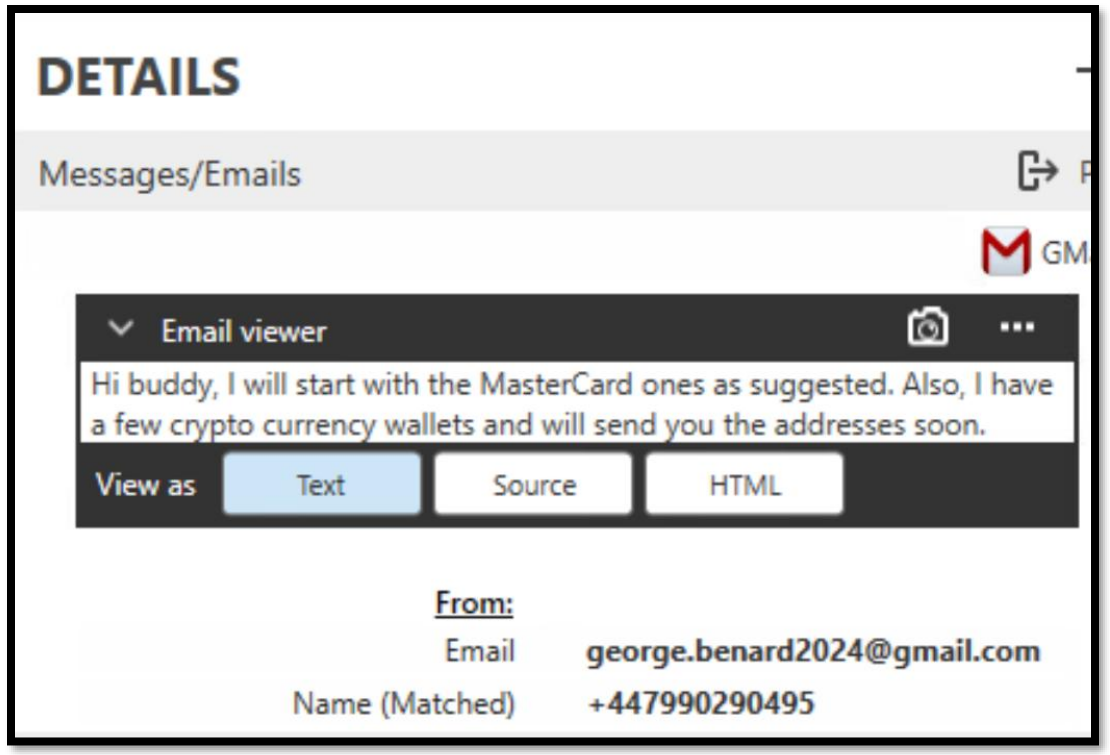
WhatsApp ID: 447990290495@s.whatsapp.net

Name (Matched): Danny

-

B2. Email Correspondence Regarding Cryptocurrency Transactions

- **Figure B2:** Screenshot from XAMN showing an email exchange between the suspect and an accomplice regarding setting up crypto wallets.



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.

From:

Email: george.benard2024@gmail.com

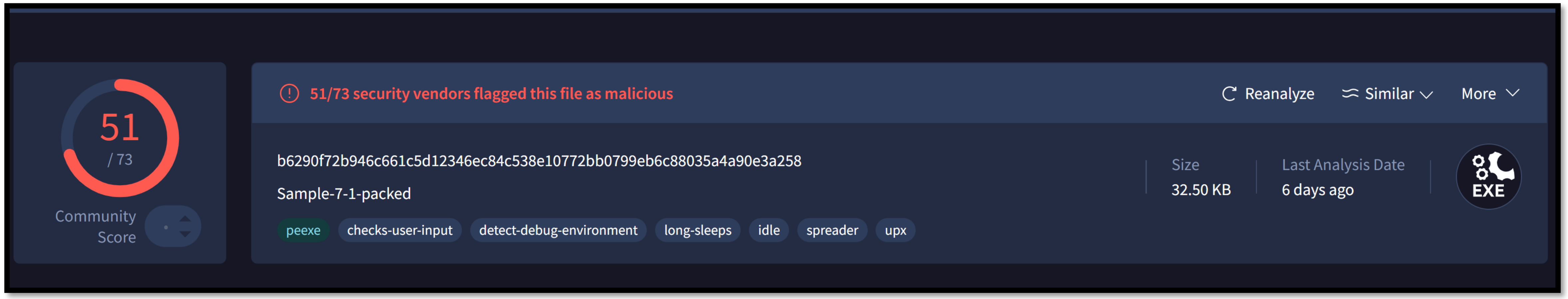
Name (Matched): +447990290495

-

Appendix C – Portable Executable (PE) Analysis

C1. Malware Hash Check on VirusTotal

- **Figure C1:** Screenshot of VirusTotal scan results showing a **51/73 detection score** for proxyApp.exe.



51
/ 73
Community Score

51/73 security vendors flagged this file as malicious

b6290f72b946c661c5d12346ec84c538e10772bb0799eb6c88035a4a90e3a258
Sample-7-1-packed

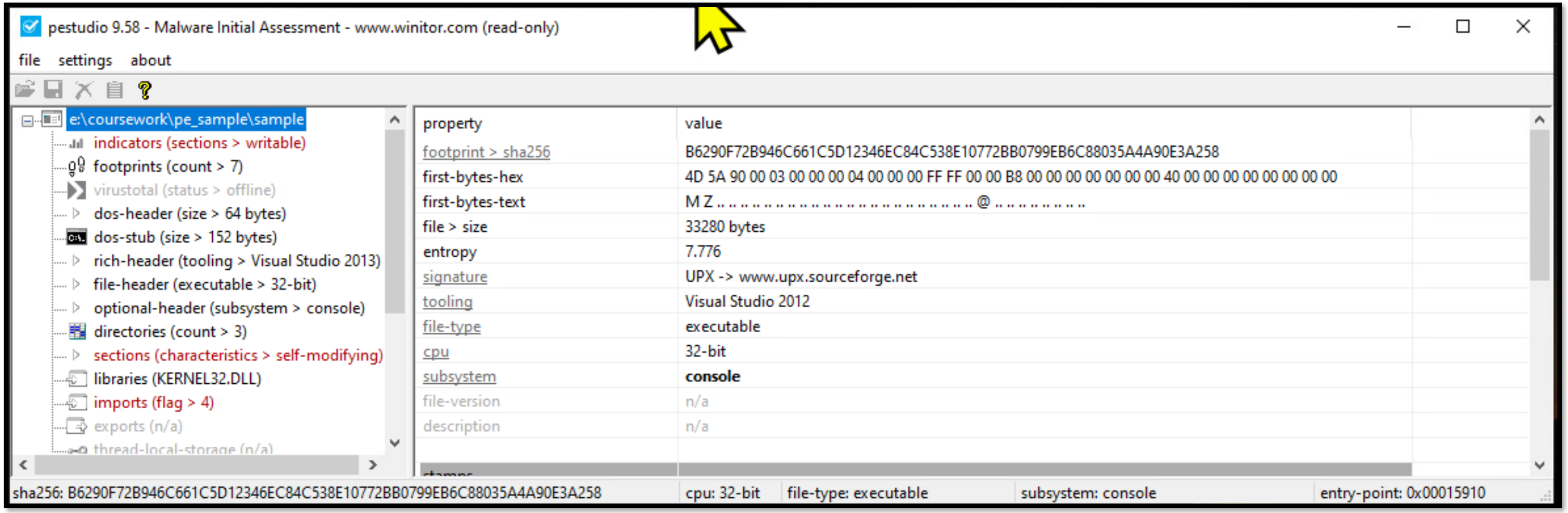
peexe · checks-user-input · detect-debug-environment · long-sleeps · idle · spreader · upx

Size
32.50 KB

Last Analysis Date
6 days ago

C2. PE Analysis Showing Obfuscation Techniques

- **Figure C2:** Screenshot from PE Studio highlighting suspicious **packing techniques** and **anti-analysis tricks** used by the malware.



pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)

```
e:\coursework\pe_sample\sample
    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)
    thread-local-storage (n/a)
```

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 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

sha256: B6290F72B946C661C5D12346EC84C538E10772BB0799EB6C88035A4A90E3A258 | cpu: 32-bit | file-type: executable | subsystem: console | entry-point: 0x00015910