

ITN 276, Computer Forensics I

Course Project II: Analyzing A Case

May Twint Phyu

12/08/2024

Checking the integrity of the provided image file

The first step before examining an evident file is to check its integrity making sure nothing has changed since the image was captured.

Original checksum, MD5: 10c466c021ce35f0ec05b3edd6ff014f

Checksum of the downloaded image file, MD5: 10c466c021ce35f0ec05b3edd6ff014f (matched)

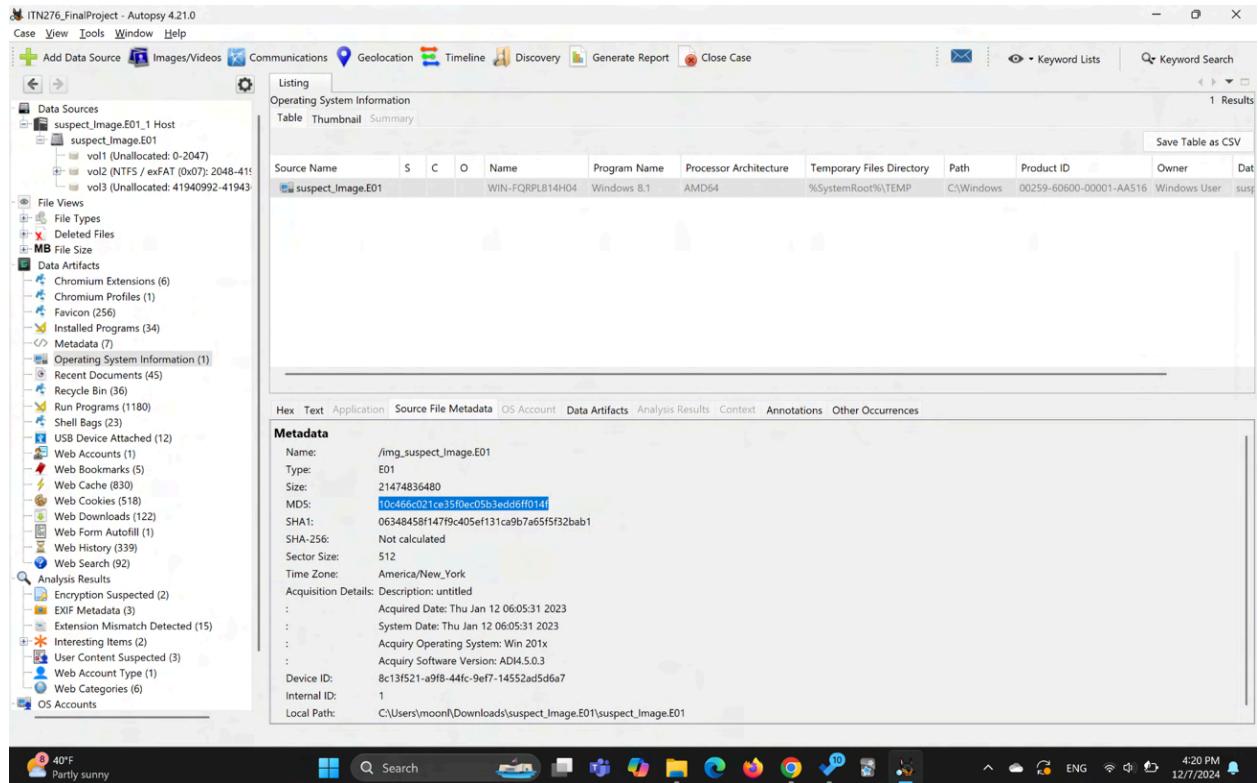


Figure 1: showing the MD5 hash result of the image file

General information of the image file

- *Figure 2:* File system - 3 volumes, where 2 are unallocated and 1 using NTFS file system
- *Figure 3:* Operating System - Windows 8.1
- *Figure 4:* User accounts - 9 (John and Don are one of the users)
- *Figure 5:* It is evident that the image is from a virtual machine (VMware). The virtual USB hub and the virtual mouse shows up in the “USB device attached” section suggesting the virtualization tools were actively running on the physical host system.

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows the project structure with 'suspect.Image.E01' selected. Under 'Data Sources', there are three volumes listed: 'vol1 (Unallocated: 0-2047)', 'vol2 (NTFS / exFAT 0x07: 2048)', and 'vol3 (Unallocated: 41940992-419)'. The main pane displays a table titled '/img_suspect_image.E01/vol_vol2' with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags(Meta). The table contains numerous entries, mostly system files and logs. At the bottom of the interface, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The bottom right corner of the screen shows the Windows taskbar with the date and time as 3:47 PM 12/7/2024.

Figure 2: showing the 3 volumes and their file system installed on the hard drive

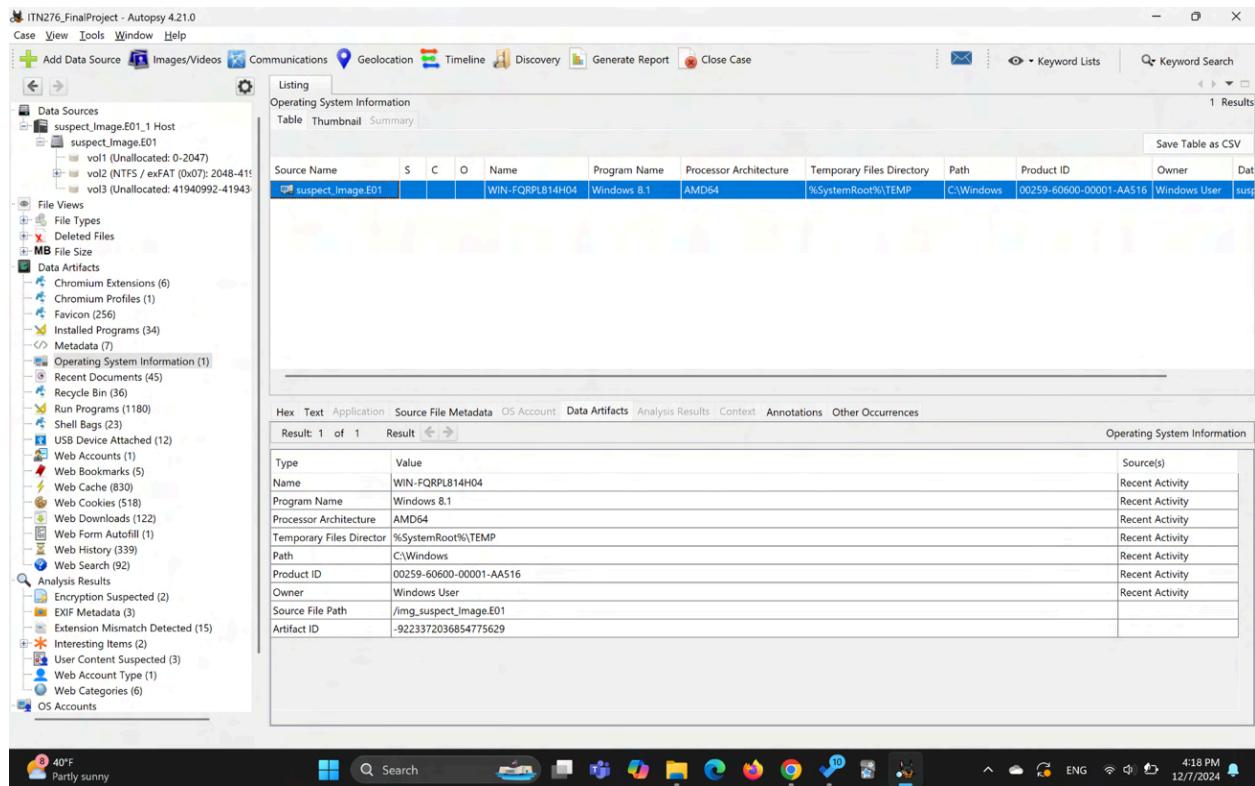


Figure 3: showing the operating system installed on the computer

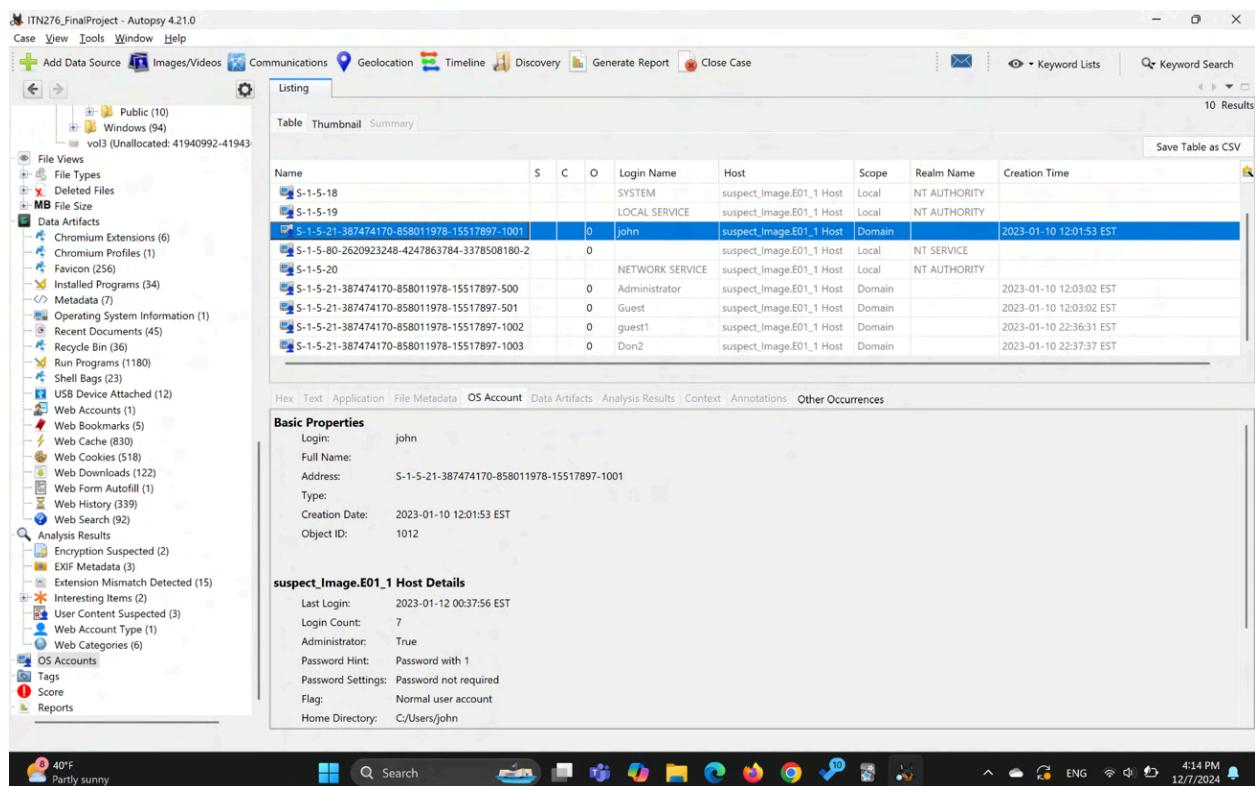


Figure 4: showing the user accounts existing on the computer

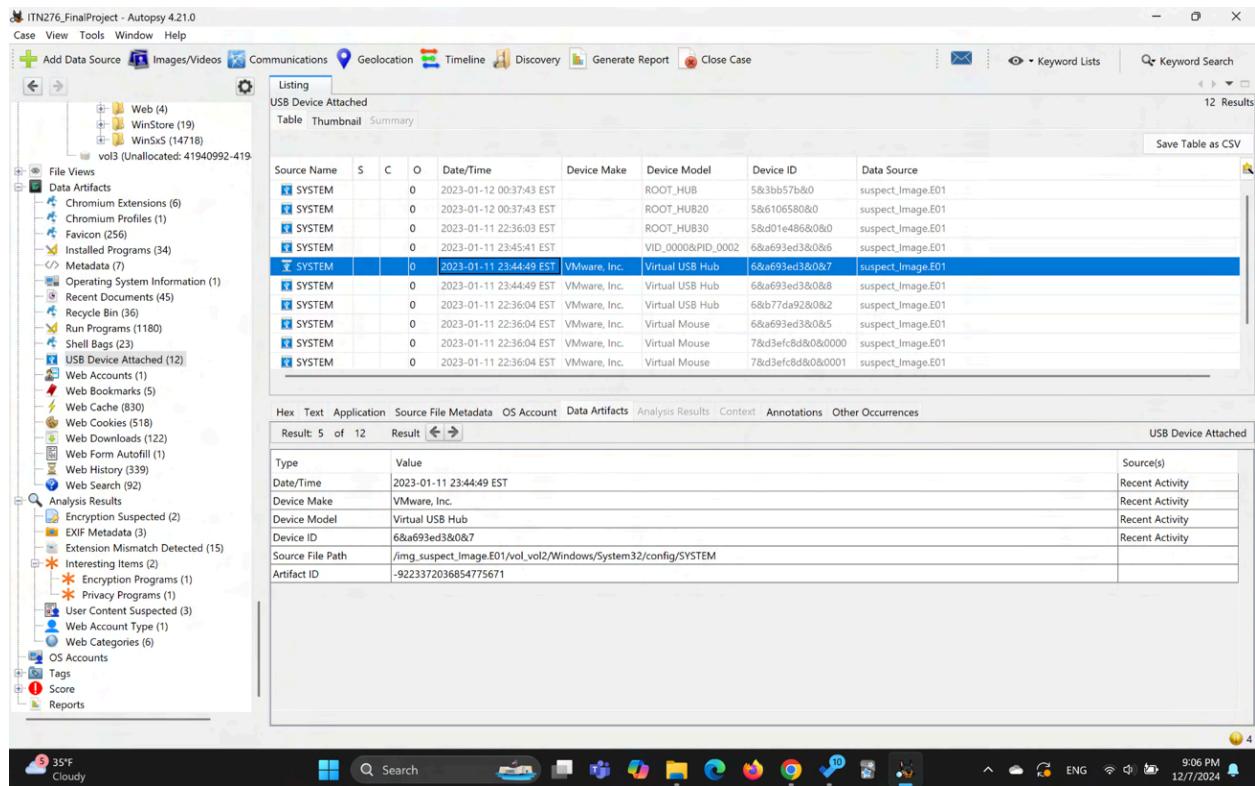
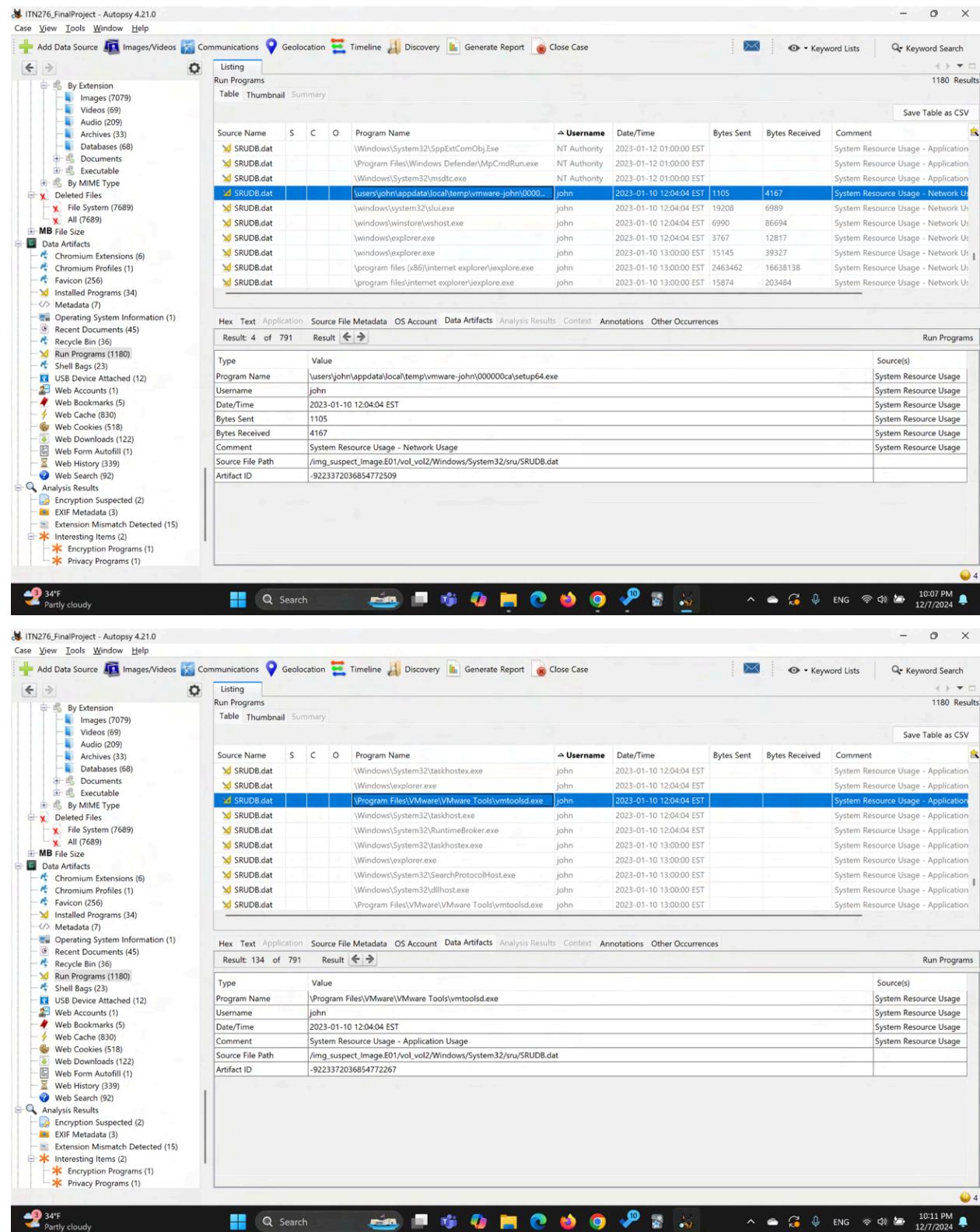


Figure 5: showing VMware running on the system (11 January, 2023 11:44:49 pm EST)

Finding Evidence in Data Artifacts

Run Programs - to figure out what suspect 'John' might have been doing on the system.
 (VMware, Tor browser, Wipefile.exe file are notable)



The screenshot displays two separate sessions of the Autopsy 4.21.0 forensic analysis tool. Both sessions show the 'Run Programs' analysis results table.

Session 1 (Top):

Source Name	S	C	O	Program Name	Username	Date/Time	Bytes Sent	Bytes Received	Comment
SRUDB.dat				\Windows\System32\SpkExtComObj.Exe	NT Authority	2023-01-12 01:00:00 EST			System Resource Usage - Application
SRUDB.dat				\Program Files\Windows Defender\MpCmdRun.exe	NT Authority	2023-01-12 01:00:00 EST			System Resource Usage - Application
SRUDB.dat				\Windows\System32\msdtc.exe	NT Authority	2023-01-12 01:00:00 EST			System Resource Usage - Application
SRUDB.dat				\users\john\appdata\local\temp\vmware-john\0000_00000ca\setup64.exe	John	2023-01-10 12:04:04 EST	1105	4167	System Resource Usage - Network U
SRUDB.dat				\windows\system32\slui.exe	John	2023-01-10 12:04:04 EST	19208	6989	System Resource Usage - Network U
SRUDB.dat				\windows\winstore\vhost.exe	John	2023-01-10 12:04:04 EST	6990	86694	System Resource Usage - Network U
SRUDB.dat				\windows\explorer.exe	john	2023-01-10 12:04:04 EST	3767	12817	System Resource Usage - Network U
SRUDB.dat				\windows\explorer.exe	john	2023-01-10 13:00:00 EST	15145	39327	System Resource Usage - Network U
SRUDB.dat				\program files (x86)\internet explorer\iexplore.exe	john	2023-01-10 13:00:00 EST	2463462	16638138	System Resource Usage - Network U
SRUDB.dat				\program files\internet explorer\iexplore.exe	john	2023-01-10 13:00:00 EST	15874	203484	System Resource Usage - Network U

Session 2 (Bottom):

Type	Value	Source(s)
Program Name	\users\john\appdata\local\temp\vmware-john\00000ca\setup64.exe	System Resource Usage
Username	john	System Resource Usage
Date/Time	2023-01-10 12:04:04 EST	System Resource Usage
Bytes Sent	1105	System Resource Usage
Bytes Received	4167	System Resource Usage
Comment	System Resource Usage - Network Usage	System Resource Usage
Source File Path	\img_suspect_ImageE01\vol_vol2\Windows\System32\sru\SRUDB.dat	System Resource Usage
Artifact ID	-9223372036854772509	

Figure 6.2: showing John installed VMware on the system on 10 Jan, 2021 (12:04:04 pm EST)

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar contains a tree view of file types and analysis results, including 'Recent Documents' which lists 'Superior Pawn Little Creek Rd' multiple times. The main pane displays a table of 'Run Programs' results. The table has columns for Source Name, S, C, O, Program Name, Username, Date/Time, Bytes Sent, Bytes Received, and Comment. Most entries are for 'SRUDB.dat' with various program names like 'dllhost.exe', 'vmtoolsd.exe', and 'explorer.exe'. One entry shows 'Wipefile.exe' with 'john' as the username and '2023-01-12 01:00:00 EST' as the date/time. The bottom pane shows detailed results for this entry, including the source file path as '/img_suspect_Image.E01/vol_vol2/Windows/System32/sru/SRUDB.dat'.

Figure 7: showing John has Wipefile.exe application downloaded

Recent Documents - to find out what suspect did recently

John was found to have searched “Superior Pawn Little Creek Rd” several times in his recent activities and thus it is used as the keyword to find what it is and any other connected files on the system. It was found that it was about the location on the map and was deleted

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows a tree view of recent documents, including 'Recent' which lists 'Superior Pawn Little Creek Rd' multiple times. The main pane displays a table of 'Recent Documents' results. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags(Dir). The table lists various files and folders, many of which are marked as deleted ('D'). The bottom pane shows the extracted text from one of the search results, which includes the search term 'Superior Pawn Little Creek Rd' and its file paths.

Figure 8.1: showing John searching “Superior Pawn Little Creek Rd” in one of the results

The screenshot shows the Autopsy 4.21.0 interface with a search results table. The table has columns: Name, Keyword Preview, Location, Modified Time, Change Time, and Size. There are 123 results. One result is highlighted: "Recycle Bin Artifact" located at "\Pictures\Superior Pawn Little Creek Rd - Google S" with a size of 2054 bytes. The "Location" column shows a thumbnail image of a map from Google Maps with a red pin pointing to "Superior Pawn Little Creek Rd". The desktop taskbar at the bottom shows various icons and the date/time as 12/7/2024.

Name	Keyword Preview	Location	Modified Time	Change Time	Size
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Rd - Google S	/img_suspect/Image.E01/vol.vol2/\$Recycle.Bin/S-1...	2023-01-10 17:21:00 EST	2023-01-11 22:43:41 EST	2054
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Rd - Google S	/img_suspect/Image.E01/vol.vol2/\$Recycle.Bin/S-1...	2023-01-10 17:20:56 EST	2023-01-11 22:41:29 EST	54469
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Rd - Google S	/img_suspect/Image.E01/vol.vol2/\$Recycle.Bin/S-1...	2023-01-10 17:20:53 EST	2023-01-11 22:41:38 EST	390
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Rd - Google S	/img_suspect/Image.E01/vol.vol2/\$Recycle.Bin/S-1...	2023-01-10 17:20:59 EST	2023-01-11 22:41:29 EST	3596
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Rd - Google S	/img_suspect/Image.E01/vol.vol2/\$Recycle.Bin/S-1...	2023-01-10 17:20:56 EST	2023-01-11 22:41:29 EST	43181
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Rd - Google S	/img_suspect/Image.E01/vol.vol2/\$Recycle.Bin/S-1...	2023-01-10 17:20:56 EST	2023-01-10 17:20:56 EST	3569
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Rd - Google S	/img_suspect/Image.E01/vol.vol2/\$Recycle.Bin/S-1...	2023-01-10 17:20:59 EST	2023-01-10 17:21:00 EST	1436
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Rd - Google S	/img_suspect/Image.E01/vol.vol2/\$Recycle.Bin/S-1...	2023-01-10 17:20:59 EST	2023-01-10 17:20:59 EST	11388
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Rd - Google S	/img_suspect/Image.E01/vol.vol2/\$Recycle.Bin/S-1...	2023-01-10 17:20:56 EST	2023-01-11 22:41:29 EST	23035

Figure 8.2: showing the location of the “Superior Pawn Little Creek Rd”

The screenshot shows the Autopsy 4.21.0 interface with a search results table. The table has columns: Name, Keyword Preview, Location, Modified Time, Change Time, Access Time, Created Time, and Size. There are 123 results. One result is highlighted: "Recycle Bin Artifact" located at "\Pictures\Superior Pawn Little Creek Cr..." with a size of 2054 bytes. The "Location" column shows a thumbnail image of a photograph from Google Photos showing a building with a sign that reads "Superior Pawn Little Creek Rd". The desktop taskbar at the bottom shows various icons and the date/time as 12/8/2024.

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Cr...	/img_sus...	2023-01-10 17:20:54 EST	2023-01-11 22:43:41 EST	2023-01-10 17:20:54 EST	2023-01-10 17:20:54 EST	2054
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Cr...	/img_sus...	2023-01-10 17:21:00 EST	2023-01-11 22:41:29 EST	2023-01-10 17:21:00 EST	2023-01-10 17:21:00 EST	54469
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Cr...	/img_sus...	2023-01-10 17:20:53 EST	2023-01-11 22:41:38 EST	2023-01-10 17:20:53 EST	2023-01-10 17:20:53 EST	390
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Cr...	/img_sus...	2023-01-10 17:20:59 EST	2023-01-11 22:41:29 EST	2023-01-10 17:20:59 EST	2023-01-10 17:20:59 EST	3596
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Cr...	/img_sus...	2023-01-10 17:20:56 EST	2023-01-11 22:41:29 EST	2023-01-10 17:20:56 EST	2023-01-10 17:20:56 EST	43181
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Cr...	/img_sus...	2023-01-10 17:20:56 EST	2023-01-11 22:41:29 EST	2023-01-10 17:20:56 EST	2023-01-10 17:20:56 EST	3569
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Cr...	/img_sus...	2023-01-10 17:21:00 EST	2023-01-11 22:41:29 EST	2023-01-10 17:21:00 EST	2023-01-10 17:21:00 EST	1436
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Cr...	/img_sus...	2023-01-10 17:20:59 EST	2023-01-11 22:41:38 EST	2023-01-10 17:20:59 EST	2023-01-10 17:20:59 EST	11388
Recycle Bin Artifact	\Pictures\Superior Pawn Little Creek Cr...	/img_sus...	2023-01-10 17:20:56 EST	2023-01-11 22:41:29 EST	2023-01-10 17:20:56 EST	2023-01-10 17:20:56 EST	23035

Figure 8.3: possible geolocation of “Superior Pawn Little Creek Rd”

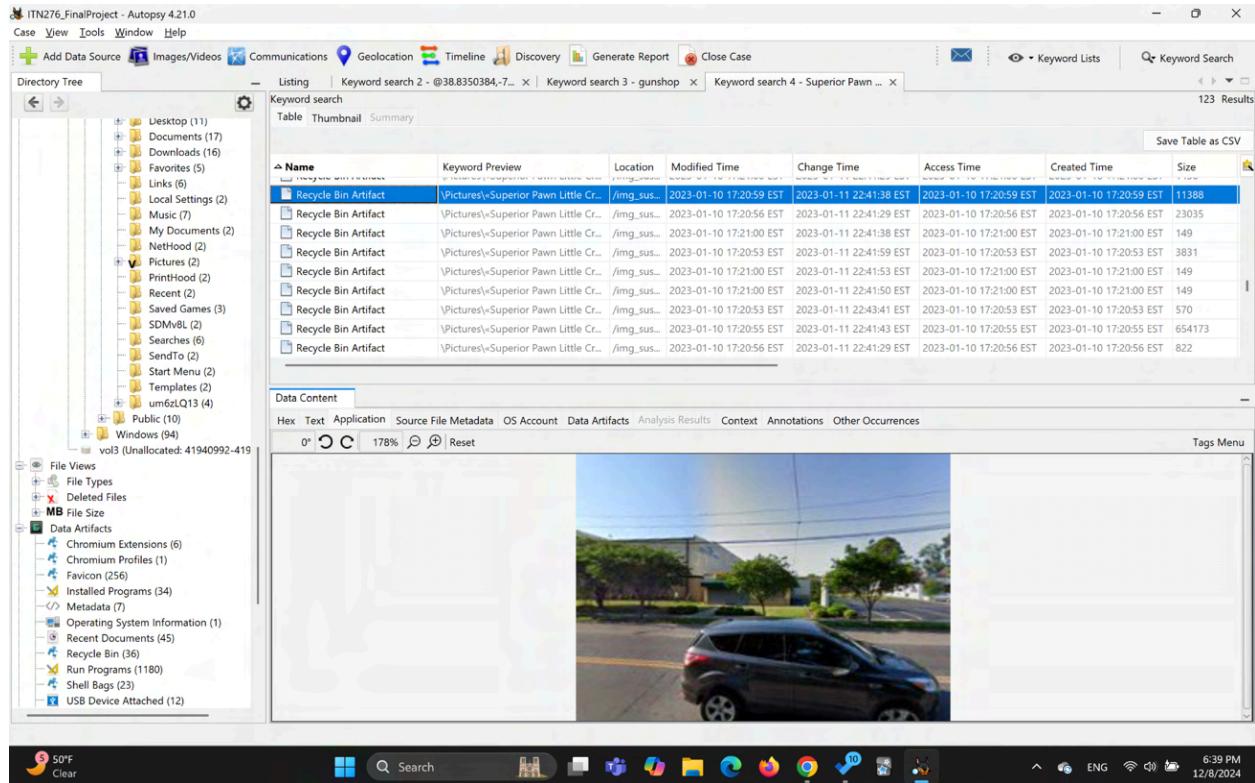


Figure 8.4: possible geolocation of “Superior Pawn Little Creek Rd”

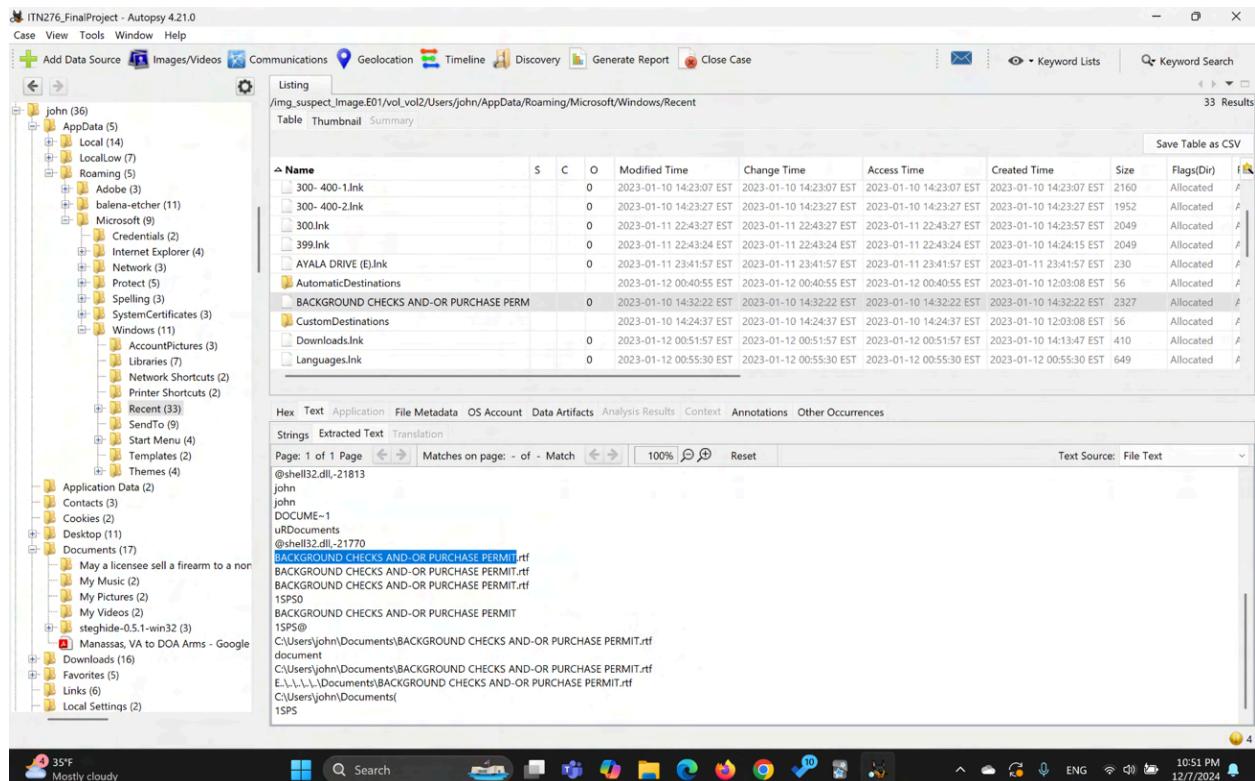


Figure 9.1: showing the document “BACKGROUND CHECKS AND-OR PURCHASE PERMIT” in recent accessed file

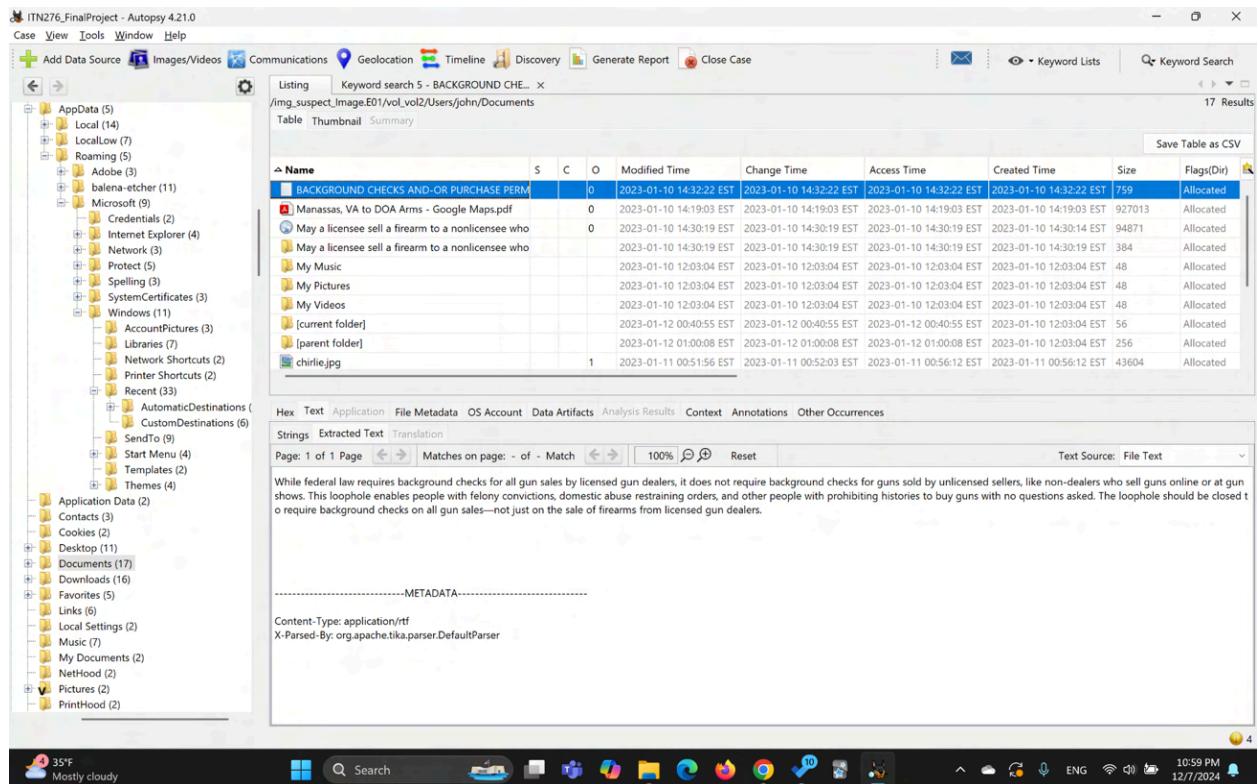


Figure 9.2: showing content of the “BACKGROUND CHECKS AND-OR PURCHASE PERMIT” file

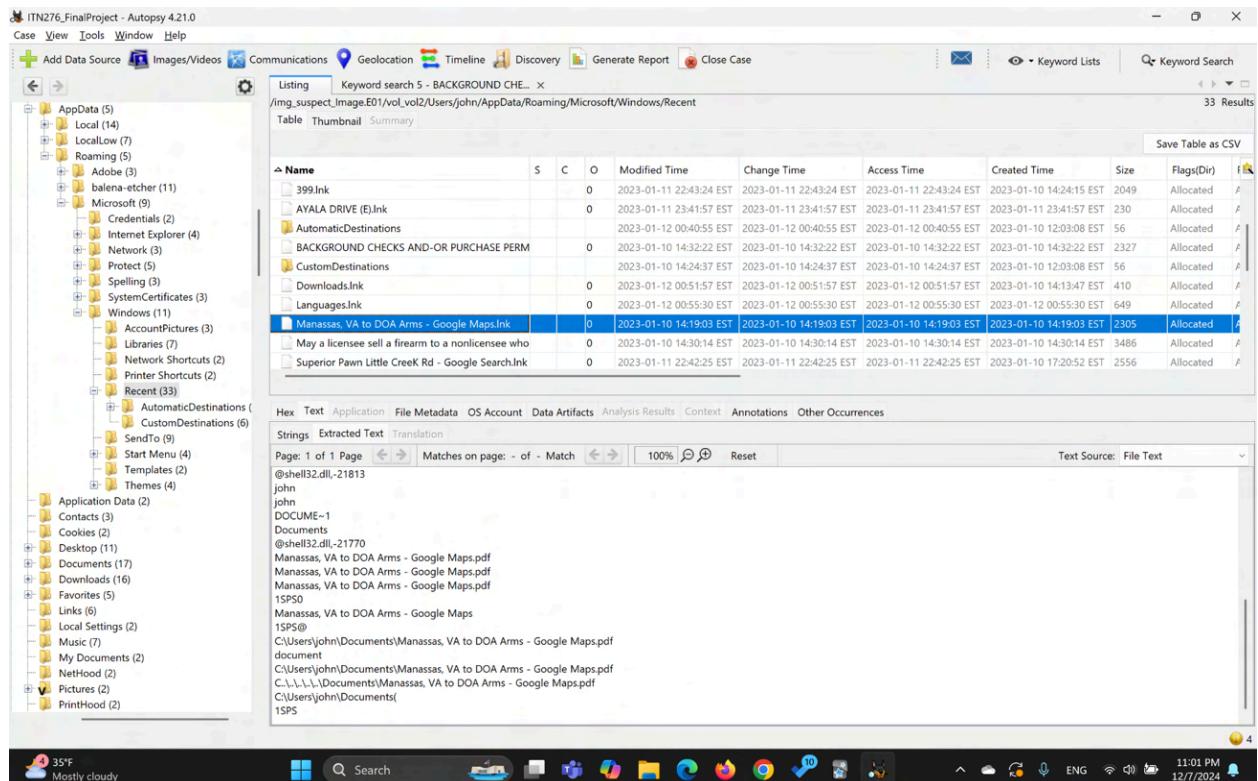


Figure 10.1: showing “Manassas, VA to DOA Arms - Google Maps” in recently opened folder and its actual file path

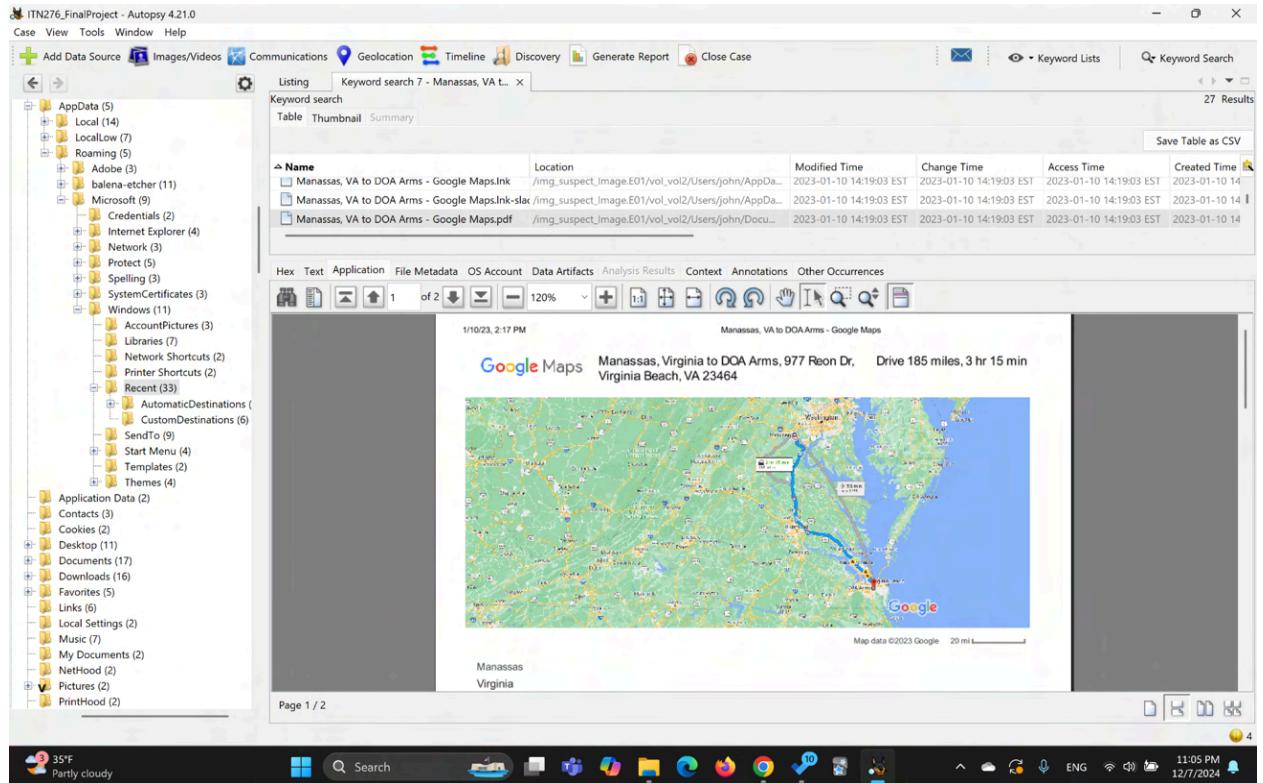


Figure 10.1: showing the content of “Manassas, VA to DOA Arms - Google Maps” pdf file

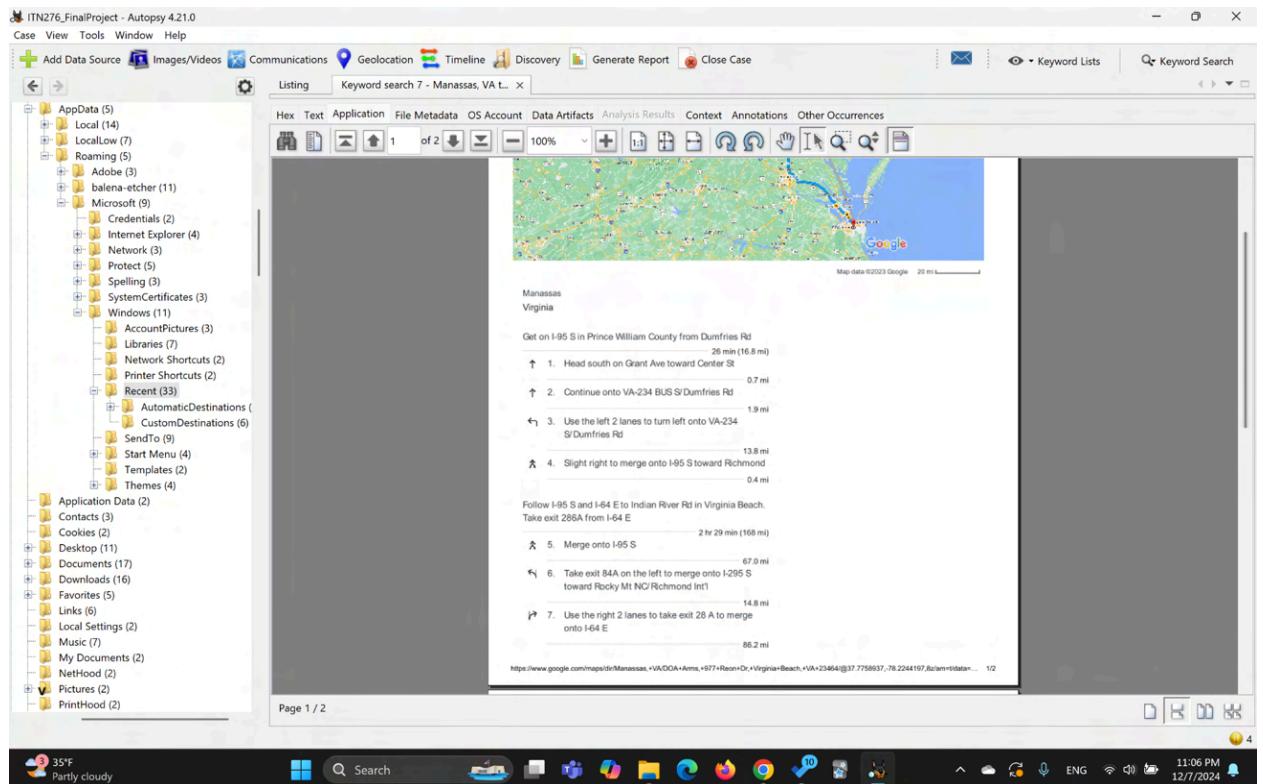


Figure 10.2: showing the content of “Manassas, VA to DOA Arms - Google Maps” pdf file

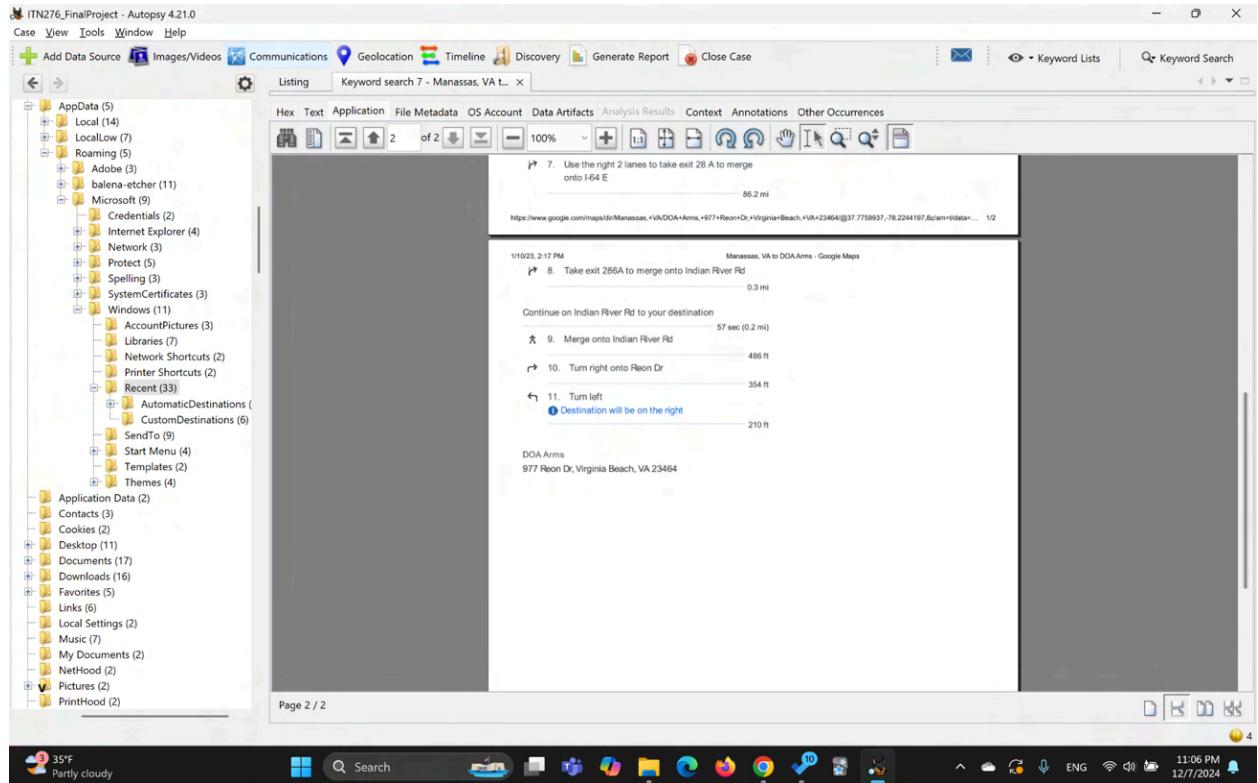


Figure 10.3: showing the content of “Manassas, VA to DOA Arms - Google Maps” pdf file

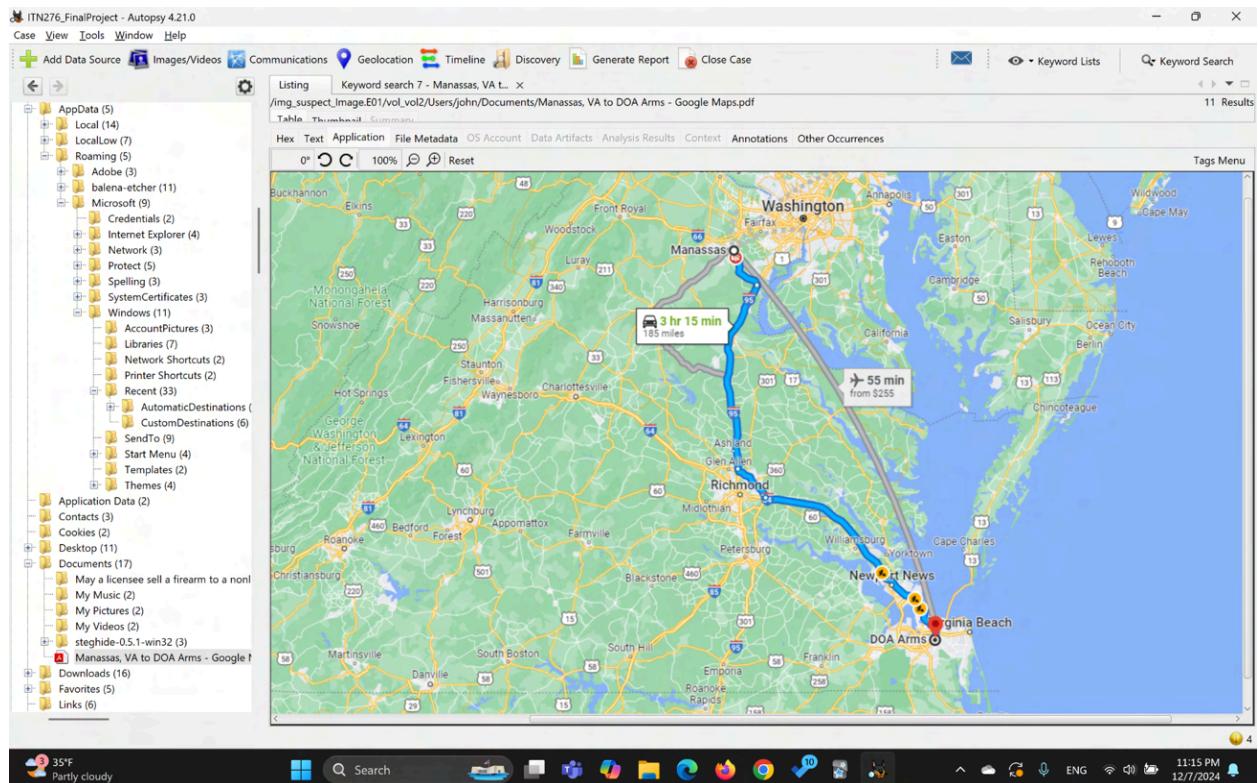


Figure 10.4: showing the map in clearer resolution

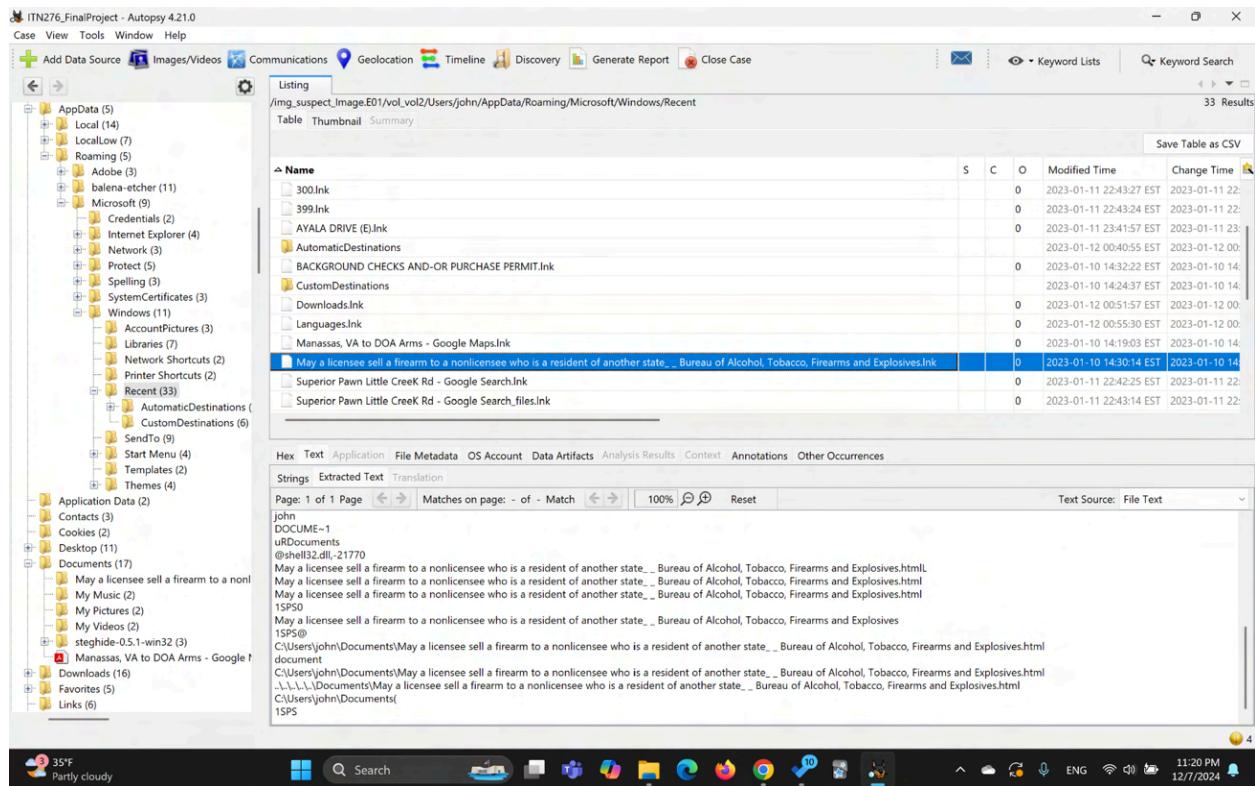


Figure 11.1: showing John searched “May a licensee sell a firearm to a nonlicensee who is a resident of another state_ _ Bureau of Alcohol, Tobacco, Firearms and Explosives” on the web

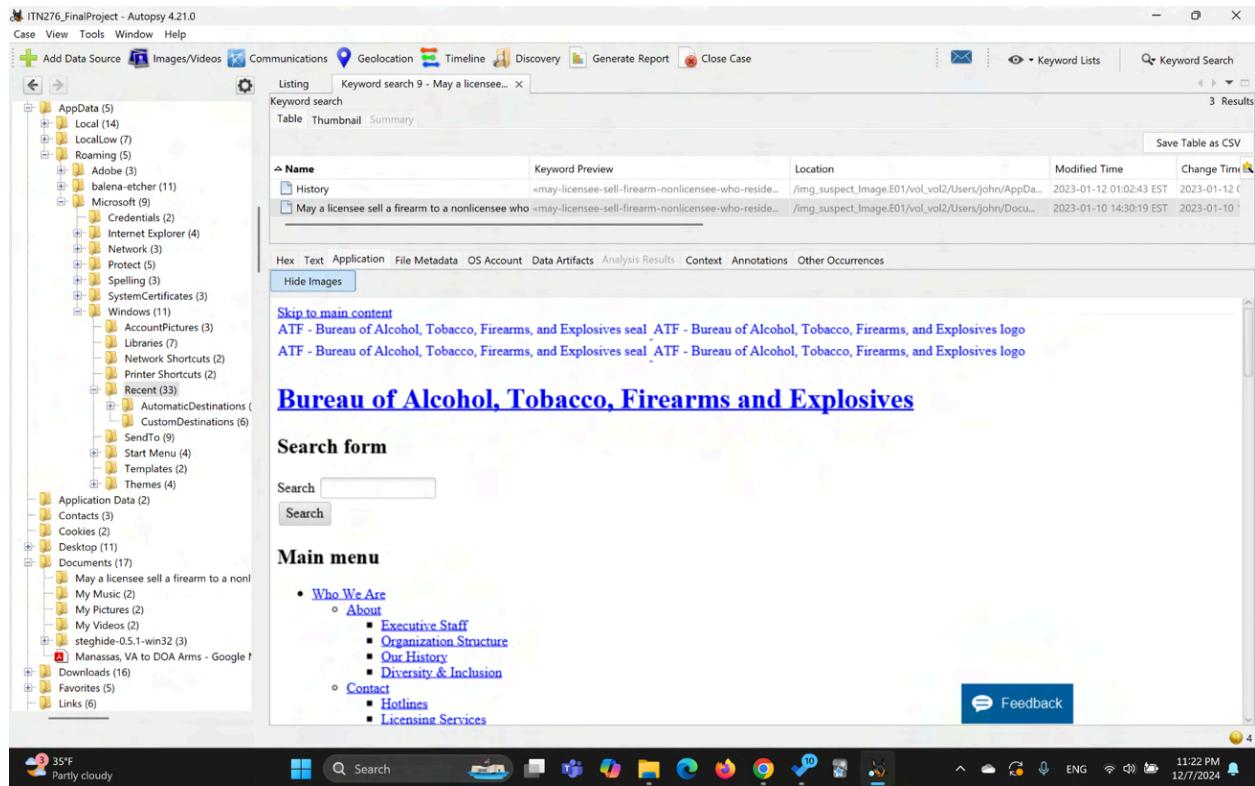


Figure 11.2: showing the content of the search result “May a licensee sell a firearm to a nonlicensee who is a resident of another state_ _ Bureau of Alcohol, Tobacco, Firearms and Explosives” that John accessed

The screenshot shows the Autopsy 4.21.0 interface with a search result for "May a licensee sell a firearm to a nonlicensee who is a resident of another state". The search results table has three columns: Name, Keyword Preview, and Location. There are two entries:

Name	Keyword Preview	Location
History	<may-licensee-sell-firearm-nonlicensee-who-reside...	2023-01-12 01:02:43 EST
May a licensee sell a firearm to a nonlicensee who is a resident of another state	<may-licensee-sell-firearm-nonlicensee-who-reside...	2023-01-10 14:30:19 EST

Below the table, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. A "Hide Images" button is also present. The main content area displays the search query and its context from a document.

May a licensee sell a firearm to a nonlicensee who is a resident of another state?

Generally, a firearm may not lawfully be sold by a licensee to a nonlicensee who resides in a state other than the state in which the seller's licensed premises is located. However, the sale may be made if the firearm is shipped to a licensee whose business is in the purchaser's state of residence and the purchaser takes delivery of the firearm from the licensee in his or her state of residence.

In addition, a licensee may sell a rifle or shotgun to a person who is not a resident of the state where the licensee's business premises is located in an over-the-counter transaction, provided the transaction complies with state law in the state where the licensee is located and in the state where the purchaser resides.

[18 U.S.C. 922(b)(3); 27 CFR 478.99(a)]

Last Reviewed April 12, 2022

Keep up with the latest ATF updates:

[facebook](#) [twitter](#) [instagram](#) [youtube](#) [email](#)

[Who We Are](#) [About](#) [Executive Staff](#) [Organization Structure](#) [Our History](#) [What We Do](#) [Firearms](#)

Feedback

Figure 11.3: showing the content of the search result “May a licensee sell a firearm to a nonlicensee who is a resident of another state__ Bureau of Alcohol, Tobacco, Firearms and Explosives” indicating that John has intention to do something with selling firearm to clients

The screenshot shows the Autopsy 4.21.0 interface with a search result for "chirlie.link". The search results table has four columns: S, C, O, and Modified Time. There are five entries:

S	C	O	Modified Time
0	0	0	2023-01-12 00:55:30 EST
0	0	0	2023-01-10 12:03:08 EST
0	0	0	2023-01-11 00:52:03 EST
0	0	0	2023-01-11 22:42:34 EST
0	0	0	2023-01-11 22:43:05 EST
0	0	0	2023-01-10 12:03:08 EST
0	0	0	2023-01-10 12:03:08 EST
0	0	0	2023-01-12 00:43:46 EST
0	0	0	2023-01-12 00:44:01 EST
0	0	0	2023-01-10 14:15:20 EST
0	0	0	2023-01-10 14:13:47 EST
0	0	0	2023-01-10 14:14:02 EST
0	0	0	2023-01-10 14:14:29 EST

Below the table, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. A "Strings", "Extracted Text", and "Translation" button is also present. The main content area displays the search query and its context from a document.

Figure 12.1: showing potential client or dealer “Chirlie”

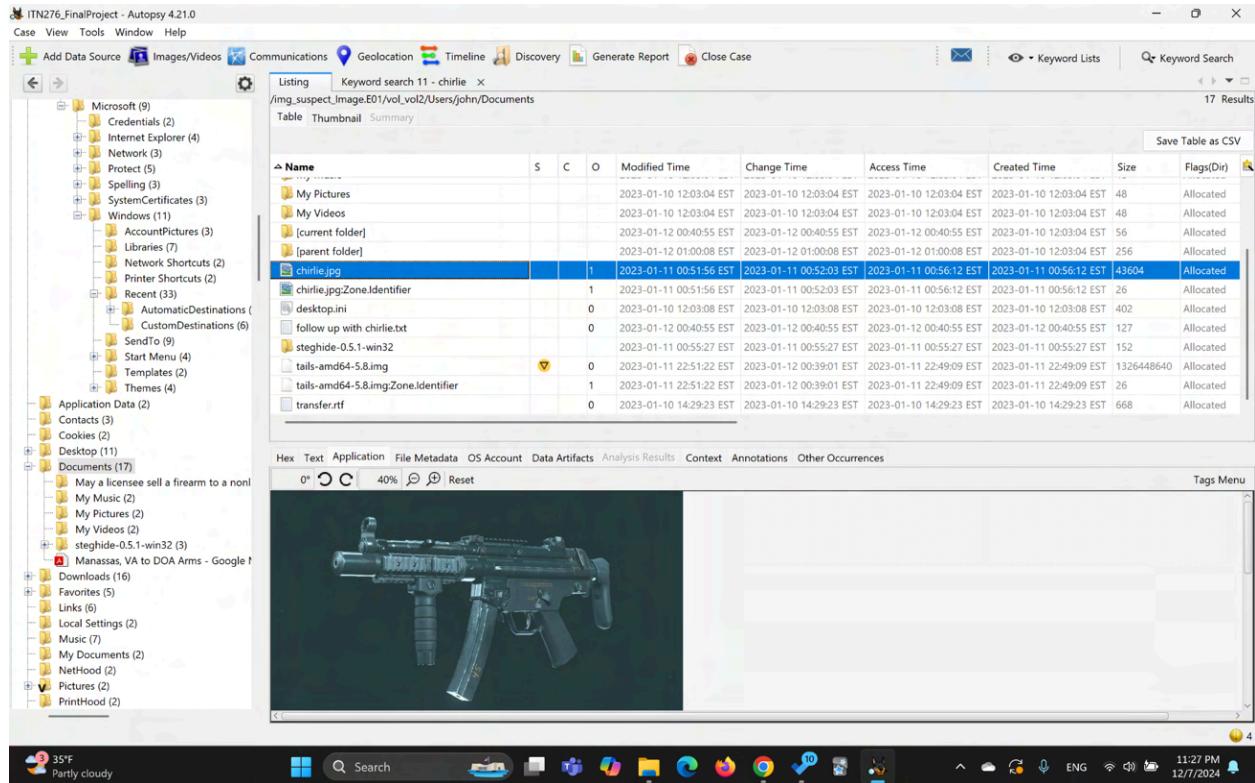


Figure 12.2: showing photo of Chirlie.jpg proving that John has something to do with firearm case

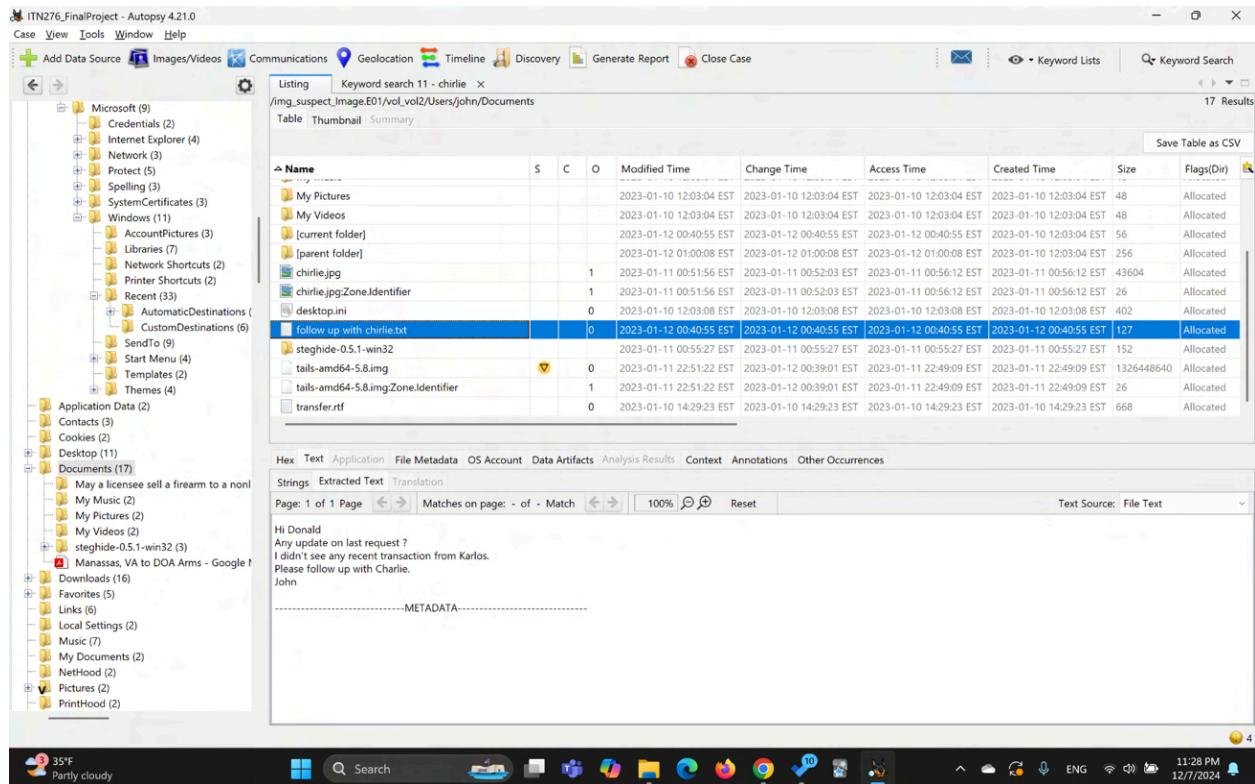


Figure 12.3: “follow up with chirlie.txt” revealing other people (Donald, Karlos, Charlie) who could also be involving in the case

The screenshot shows the Autopsy 4.21.0 interface with a keyword search for "donald". The results table lists several files, with one entry for "male_names.txt" highlighted. The file path is shown as "/img_suspect_Image.E01/vol.vol2/Users/john/AppData/Local/Google/Chrome/User Data/ZxcvbnData/1/male_names.txt". The file contains the names "christopherdanielpaulmark-donald-georgekenneth".

Name	Keyword Preview	Location	Modified Time	Change Time
\$MFT	with chirlie.txt Hi «Donald» Any update on last quest /img_suspect_Image.E01/vol.vol2/\$MFT	2023-01-10 14:58:53 EST	2023-01-10 14:58:53 EST	
ChsPinyin.lex	thurbethcabeehiato-donald-rategregoryveravelli	/img_suspect_Image.E01/vol.vol2/Windows/InputMe... 2014-11-21 04:53:54 EST	2014-11-21 04:53:54 EST	
IMPNW.DIC	_>_Leonardo>_=Aguinaldo>_=>Donald	/img_suspect_Image.E01/vol.vol2/Windows/IME/IME... 2013-07-24 14:48:06 EDT	2023-01-10 14:58:53 EST	
cr_en-us.2022-12-28.499614841_500000_index.bir	meaningdefinitionmeaning=>Donald->hawkickX cards...	/img_suspect_Image.E01/vol.vol2/Users/john/AppDa... 2023-01-09 20:20:12 EST	2023-01-10 14:58:53 EST	
en-US.dic	Dona/MDonahue/MDona/Donald-/MDonaldson...	/img_suspect_Image.E01/vol.vol2/Users/john/Desktop... 2022-12-14 13:34:00 EST	0000-00-00 Sync	
follow up with chirlie.txt	up with chirlie.txt Hi «Donald» Any update on last re...	/img_suspect_Image.E01/vol.vol2/Users/john/Docu... 2023-01-12 00:04:55 EST	2023-01-12 00:04:55 EST	
global-entities_metadata	Nasopharyngeal carcinomallyU=Donald« TrumpSkille...	/img_suspect_Image.E01/vol.vol2/Users/john/AppDa... 2022-12-05 01:35:32 EST	2023-01-10 14:58:53 EST	
male_names.txt	christopherdanielpaulmark-donald-georgekenneth...	/img_suspect_Image.E01/vol.vol2/Users/john/AppDa... 2020-07-28 08:42:18 EDT	2023-01-10 14:58:53 EST	

Figure 13.1: result of keyword “Donald”, suspicious file naming “male_names.txt”, the file path “/img_suspect_Image.E01/vol.vol2/Users/john/AppData/Local/Google/Chrome/User Data/ZxcvbnData/1/male_names.txt”

The screenshot shows the content of the file "male_names.txt" from Figure 13.1. The file contains the following names:

- christopherdanielpaulmark-donald-georgekenneth
- james
- john
- robert
- michael
- william
- david
- richard
- charles
- joseph
- thomas
- christopher
- daniel
- paul
- michael
- george
- kenneth
- steven
- charles
- brian
- ronald
- anthony
- kevin
- jason
- matthew
- gary
- timothy
- jose
- larry
- jeffrey
- frank
- scott
- eric
- stephen
- andrew

Figure 13.2: showing content of the file “male_names.txt”

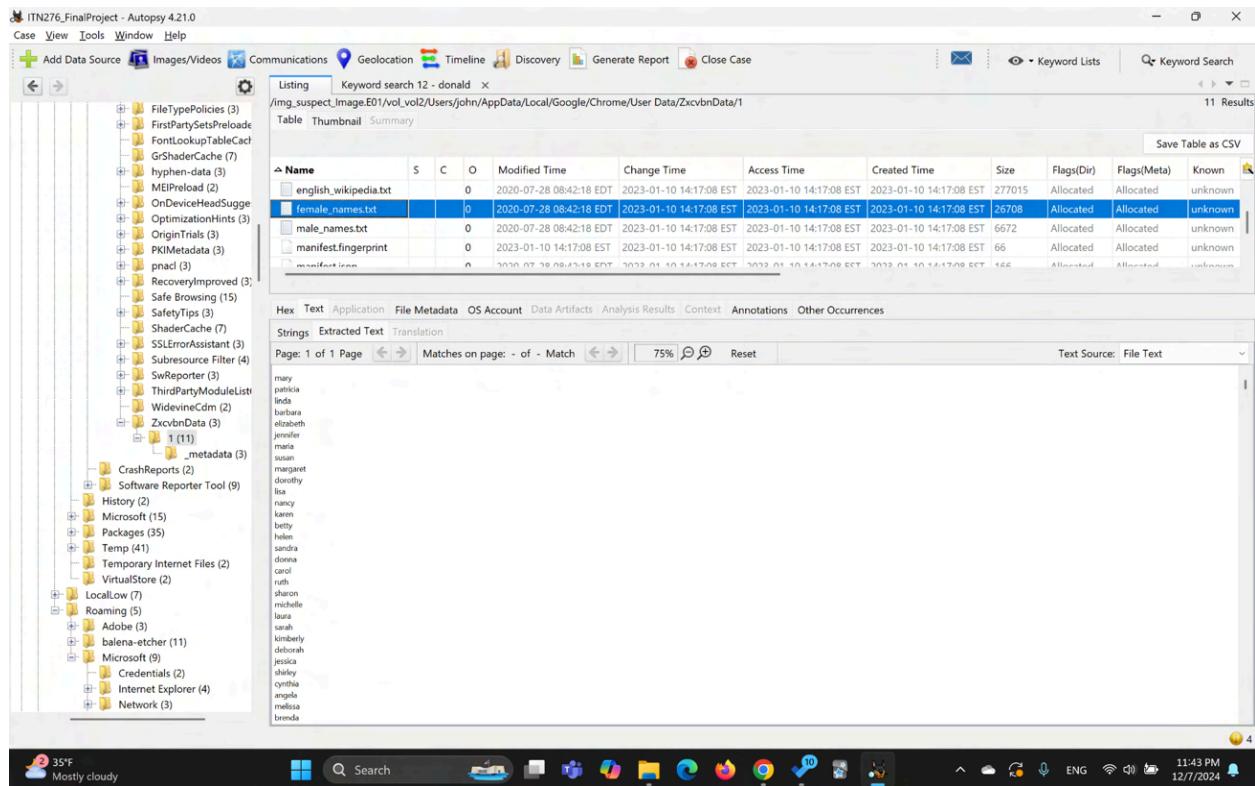


Figure 13.3: showing the content of the file “female_names.txt”

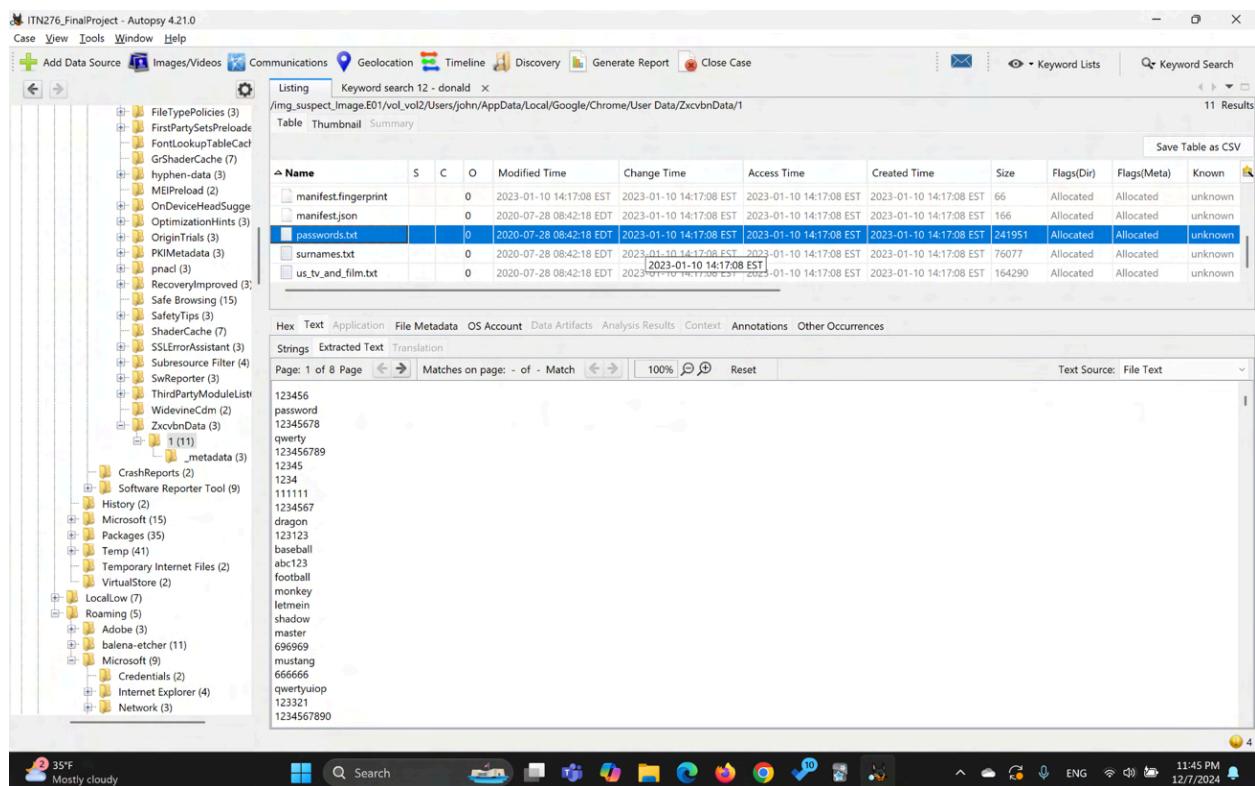


Figure 13.4: showing the content of the “passwords.txt” file

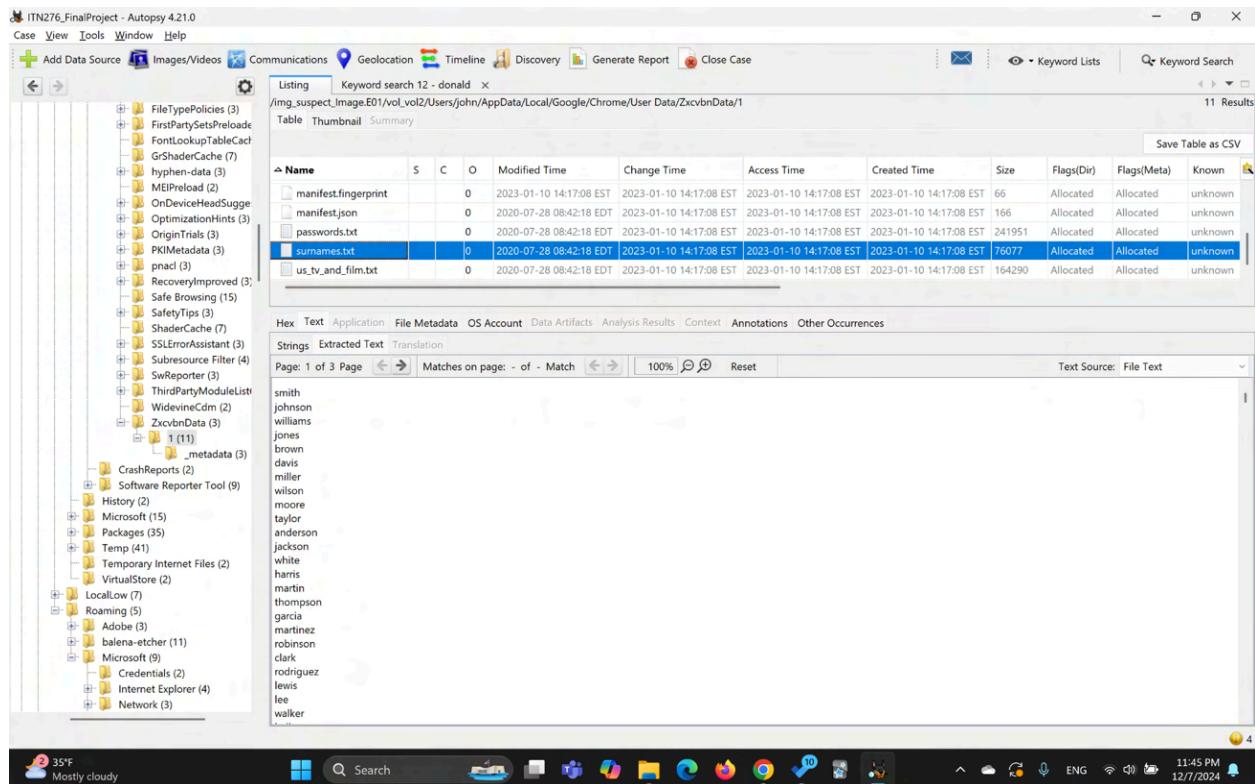


Figure 13.5: showing the content of the “surname.txt” file

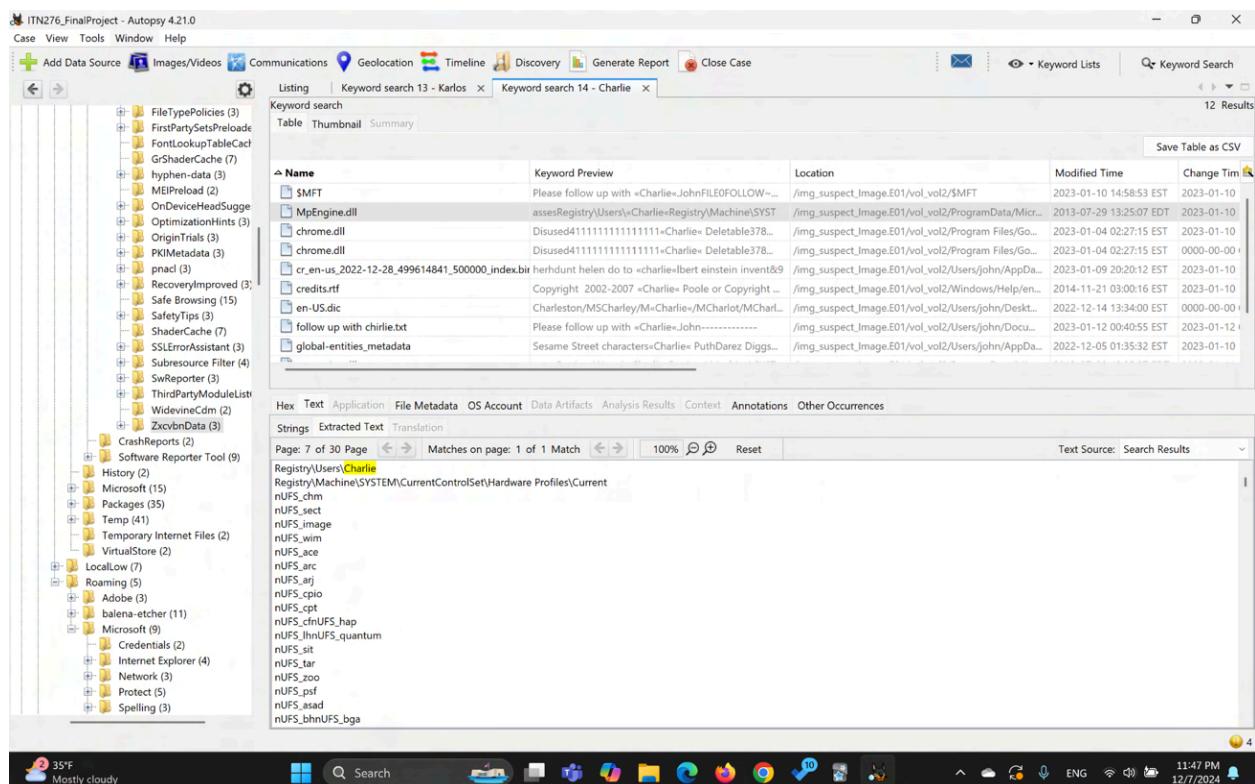


Figure 13.6: showing the search result of the “Charlie” keyword and found that there is Charlie is one of the users in the registry

Recycle Bin - to find out new important evidence from the files that John had deleted

The screenshot shows the Autopsy 4.21.0 interface with the 'Recycle Bin' selected in the Directory Tree. The main pane displays a table of deleted files, and the preview pane shows a thumbnail of the image file \$R1O1F30.

Source Name	S	C	O	Path	Time Deleted	Username	Data Source
\$RIG20M6.html				C:\Users\john\Pictures\Superior Pawn Little Creek R...	2023-01-11 22:41:43 EST	suspect_Image.E01	
\$RZP9NH1				C:\Users\john\Pictures\Superior Pawn Little Creek R...	2023-01-11 22:41:29 EST	suspect_Image.E01	
\$R04ZOMV				C:\Users\john\Pictures\Superior Pawn Little Creek R...	2023-01-11 22:41:29 EST	suspect_Image.E01	
\$R1O1F30				C:\Users\john\Pictures\high Velocity	2023-01-11 22:42:20 EST	suspect_Image.E01	
\$R1THFFI				C:\Users\john\Pictures\Superior Pawn Little Creek R...	2023-01-11 22:41:38 EST	suspect_Image.E01	
\$R2ONUQQ				C:\Users\john\Pictures\Superior Pawn Little Creek R...	2023-01-11 22:41:56 EST	suspect_Image.E01	
\$R3N99GQ.loaded_0				C:\Users\john\Pictures\Superior Pawn Little Creek R...	2023-01-11 22:42:06 EST	suspect_Image.E01	
\$R4BR2WW				C:\Users\john\Pictures\Superior Pawn Little Creek R...	2023-01-11 22:41:29 EST	suspect_Image.E01	
\$R51UO88				C:\Users\john\Pictures\Superior Pawn Little Creek R...	2023-01-11 22:41:29 EST	suspect_Image.E01	

Figure 14: image \$R1O1F30

Metadata

The screenshot shows the Autopsy 4.21.0 interface with the 'Metadata' selected in the Directory Tree. The main pane displays a table of metadata files, and the preview pane shows the content of the file 'Creating an Email Account without a Phone Number'.

Source Name	S	C	O	Version	Date Created	Data Source	Date Modified
manual.pdf				1.2	2003-10-13 09:15:23 EDT	suspect_Image.E01	
Manassas, VA to DOA Arms - Google Maps.pdf				1.4	2023-01-10 19:17:46 EST	suspect_Image.E01	2023-01-10 19:17:46 EST
manual.pdf				1.2	2003-10-13 09:15:23 EDT	suspect_Image.E01	
manual_es.pdf				1.2	2003-10-13 09:18:20 EDT	suspect_Image.E01	
document.pdf				1.7	2023-01-10 19:04:53 EST	suspect_Image.E01	2023-01-10 19:04:53 EST
credits.rtf					2013-07-02 20:18:00 EDT	suspect_Image.E01	

Creating an Email Account without a Phone Number

Trying to create an email account without a phone number is very challenging, and yet, many businesses/employment opportunities want to communicate electronically. How do you create an email address without a phone number?

Both of the resources listed below:

- I do not require a phone number or additional email to create an account
- I have a free version
- I can be used to send and receive email messages

1. Gmail <https://accounts.google.com/signup>

Gmail will let you create an account, and skip the part about entering a phone number, although you must provide birthday and gender.

2. Tutanota <https://www.tutanota.com/signup>

Tutanota will let you create an account without a phone number. It's a secure, encrypted email service.

3. ProtonMail <https://protonmail.com/mail>

ProtonMail is another secure, encrypted email service.

Figure 15: showing John was finding information to create an email account without a phone number

Web Accounts

The screenshot shows the Autopsy 4.21.0 interface with the 'Web Accounts' analysis module selected. The left sidebar displays a tree view of artifacts, including Data Sources, File Views, File Types, Deleted Files, MB File Size, Data Artifacts (such as Chromium Extensions, Favicons, Installed Programs, Metadata, Operating System Information, Recent Documents, Recycle Bin, Run Programs, Shell Bags, USB Device Attached, Web Accounts, Web Bookmarks, Web Cache, Web Cookies, Web Downloads, Web Form Autofill, Web History, and Web Search), Analysis Results (Encryption Suspected, EXIF Metadata, Extension Mismatch Detected, Interesting Items, Keyword Hits, User Content Suspected, Web Account Type, Web Categories, OS Accounts, Tags, Score, and Reports), and a Weather alert indicating 'In effect'. The main pane shows a table of 'Web Accounts' results with one entry:

Source Name	S	C	O	URL	Date Created	Decoded URL	Username	Realm	Domain	Program Name	Data Source
Login Data				https://account.proton.me/	2023-01-10 22:38:42 EST	proton.me	Default	https://account.proton.me/	proton.me	Google Chrome	suspect_image.E01

Below the table is a 'Data Content' section with tabs for Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Result' tab is selected, showing detailed information for the single entry:

Type	Value	Source(s)
URL	https://account.proton.me/	Recent Activity
Date Created	2023-01-10 22:38:42 EST	Recent Activity
Decoded URL	proton.me	Recent Activity
Username	Default	Recent Activity
Realm	https://account.proton.me/	Recent Activity
Domain	proton.me	Recent Activity
Program Name	Google Chrome	Recent Activity
Source File Path	/img_suspect_image.E01/vol_vol2/Users/john/AppData/Local/Google/Chrome/User Data/Default/Login Data	Recent Activity
Artifact ID	-9223372036854774950	

The bottom of the window shows the Windows taskbar with various icons and the system tray.

Figure 16: showing John using proton mail (which was one of the secure email and able to use without phone number), high possibility to contact his partners via proton mail

Web Bookmarks

The screenshot shows the Autopsy 4.21.0 interface with the 'Web Bookmarks' analysis module selected. The left sidebar displays a tree view of artifacts, including Data Sources, File Views, File Types, Deleted Files, MB File Size, Data Artifacts (such as Chromium Extensions, Favicons, Installed Programs, Metadata, Operating System Information, Recent Documents, Recycle Bin, Run Programs, Shell Bags, USB Device Attached, Web Accounts, Web Bookmarks, Web Cache, Web Cookies, Web Downloads, Web Form Autofill, Web History, and Web Search), Analysis Results (Encryption Suspected, EXIF Metadata, Extension Mismatch Detected, Interesting Items, Keyword Hits, User Content Suspected, Web Account Type, Web Categories, OS Accounts, Tags, Score, and Reports), and a Weather alert indicating 'Rain Wednesday'. The main pane shows a table of 'Web Bookmarks' results with five entries:

Source Name	S	C	O	URL	Title	Date Created	Program Name	Dom
Bookmarks	1			https://www.google.com/search?q=virginia+beach+g...	virginia beach gun shop - Google Search	2023-01-10 17:21:16 EST	Google Chrome	goog
Bookmarks	1			https://www.findlaw.com/consumer/consumer-trans...	Private Gun Sale Laws by State - FindLaw	2023-01-10 17:22:21 EST	Google Chrome	findla
Bookmarks	1			https://codes.findlaw.com/va/title-18-2-crimes-and-...	Virginia Code Title 18.2. Crimes and Offenses Gener...	2023-01-10 17:22:32 EST	Google Chrome	findla
Bookmarks	1			https://www.google.com/travel/hotels/Guatemala%2...	Hilton Guatemala City - Google hotels	2023-01-11 22:39:41 EST	Google Chrome	goog
Bing.url	1			http://go.microsoft.com/fwlink/?Linkid=255142	Bing.url	2023-01-10 12:03:08 EST	Internet Explorer Analyzer	micro

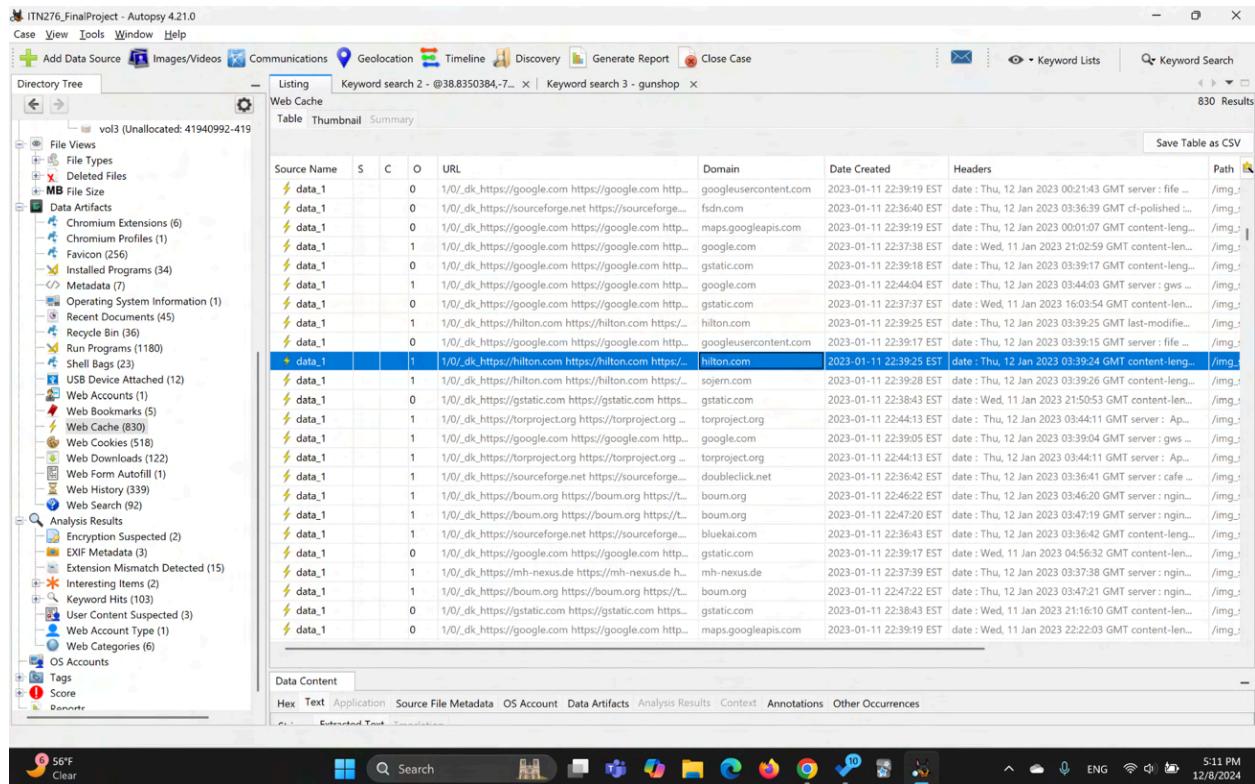
Below the table is a 'Data Content' section with tabs for Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Result' tab is selected, showing detailed information for the first bookmark entry:

Title	virginia beach gun shop - Google Search
Date Created:	2023-01-10 17:21:16 EST
Domain:	google.com
URL:	https://www.google.com/search?q=virginia+beach+gun+shop&rll=1C1ONGR_enUS1040US1040&ei=ouS9Y-7EK3k5NoP8rin-Ak&ved=0ahUKEwjuxLPhL78AhUtMlkFHxLcZBQd4UDCBA&u...
Program Name:	Google Chrome

The bottom of the window shows the Windows taskbar with various icons and the system tray.

Figure 17: showing John bookmarked some of the search result for easy access (virginia beach gun shop, about private gun sale laws by state, Virginia Code Title 18.2 Crimes and Offenses, Hilton Guatemala city hotels)

Web Cache



The screenshot shows the Autopsy 4.21.0 interface with the 'Web Cache' tab selected. The left sidebar contains a tree view of artifacts, including 'File Views', 'Data Artifacts' (with sub-categories like 'Chromium Extensions', 'Favicons', 'Installations', etc.), 'Analysis Results' (with sub-categories like 'Encryption Suspected', 'Extension Mismatch Detected', 'Interesting Items', 'Keyword Hits', 'User Content Suspected', etc.), and 'OS Accounts'. The main pane displays a table of cache entries. The columns are: Source Name, S, C, O, URL, Domain, Date Created, Headers, and Path. A specific row for 'hilton.com' is highlighted in blue. The table shows numerous entries from various domains, mostly from Google and its services, with dates ranging from January 11 to January 12, 2023.

Source Name	S	C	O	URL	Domain	Date Created	Headers	Path
data_1	0	1/0	dk	https://google.com https://google.com http...	googleusercontent.com	2023-01-11 22:39:19 EST	date : Thu, 12 Jan 2023 00:21:43 GMT server : file ... /img...	/img...
data_1	0	1/0	dk	https://sourceforge.net https://sourceforge...	fsdn.com	2023-01-11 22:36:40 EST	date : Thu, 12 Jan 2023 03:36:39 GMT cf-polished ... /img...	/img...
data_1	0	1/0	dk	https://google.com https://google.com http...	maps.googleapis.com	2023-01-11 22:39:19 EST	date : Thu, 12 Jan 2023 00:01:07 GMT content-leng... /img...	/img...
data_1	1	1/0	dk	https://google.com https://google.com http...	google.com	2023-01-11 22:37:38 EST	date : Wed, 11 Jan 2023 21:02:59 GMT content-leng... /img...	/img...
data_1	0	1/0	dk	https://google.com https://google.com http...	gstatic.com	2023-01-11 22:39:18 EST	date : Thu, 12 Jan 2023 03:39:17 GMT content-leng... /img...	/img...
data_1	1	1/0	dk	https://google.com https://google.com http...	google.com	2023-01-11 22:44:04 EST	date : Thu, 12 Jan 2023 03:44:03 GMT server : gws ... /img...	/img...
data_1	0	1/0	dk	https://google.com https://google.com http...	gstatic.com	2023-01-11 22:37:37 EST	date : Wed, 11 Jan 2023 16:03:54 GMT content-leng... /img...	/img...
data_1	1	1/0	dk	https://hilton.com https://hilton.com https...	hilton.com	2023-01-11 22:39:25 EST	date : Thu, 12 Jan 2023 03:39:25 GMT last-modifie... /img...	/img...
data_1	0	1/0	dk	https://google.com https://google.com http...	googleusercontent.com	2023-01-11 22:39:17 EST	date : Thu, 12 Jan 2023 03:39:15 GMT server : file ... /img...	/img...
data_1	1	1/0	dk	https://hilton.com https://hilton.com https...	hilton.com	2023-01-11 22:39:25 EST	date : Thu, 12 Jan 2023 03:39:24 GMT content-leng... /img...	/img...
data_1	1	1/0	dk	https://hilton.com https://hilton.com https...	sojern.com	2023-01-11 22:39:28 EST	date : Thu, 12 Jan 2023 03:39:28 GMT content-leng... /img...	/img...
data_1	0	1/0	dk	https://gstatic.com https://gstatic.com https...	gstatic.com	2023-01-11 22:38:43 EST	date : Wed, 11 Jan 2023 21:50:53 GMT content-leng... /img...	/img...
data_1	1	1/0	dk	https://torproject.org https://torproject.org ...	torproject.org	2023-01-11 22:44:13 EST	date : Thu, 12 Jan 2023 03:44:11 GMT server : Ap... /img...	/img...
data_1	1	1/0	dk	https://google.com https://google.com http...	google.com	2023-01-11 22:39:05 EST	date : Thu, 12 Jan 2023 03:39:05 GMT server : gws ... /img...	/img...
data_1	1	1/0	dk	https://torproject.org https://torproject.org ...	torproject.org	2023-01-11 22:44:13 EST	date : Thu, 12 Jan 2023 03:44:11 GMT server : Ap... /img...	/img...
data_1	1	1/0	dk	https://sourceforge.net https://sourceforge...	doubleclick.net	2023-01-11 22:36:42 EST	date : Thu, 12 Jan 2023 03:36:41 GMT server : cafe ... /img...	/img...
data_1	1	1/0	dk	https://boum.org https://boum.org https://bou...	boum.org	2023-01-11 22:46:22 EST	date : Thu, 12 Jan 2023 03:46:20 GMT server : ngn... /img...	/img...
data_1	1	1/0	dk	https://boum.org https://boum.org https://bou...	boum.org	2023-01-11 22:47:20 EST	date : Thu, 12 Jan 2023 03:47:19 GMT server : ngn... /img...	/img...
data_1	1	1/0	dk	https://sourceforge.net https://sourceforge...	bluekai.com	2023-01-11 22:36:43 EST	date : Thu, 12 Jan 2023 03:36:42 GMT content-leng... /img...	/img...
data_1	0	1/0	dk	https://google.com https://google.com http...	gstatic.com	2023-01-11 22:39:17 EST	date : Wed, 11 Jan 2023 04:56:32 GMT content-leng... /img...	/img...
data_1	1	1/0	dk	https://mh-nexus.de https://mh-nexus.de h...	mh-nexus.de	2023-01-11 22:37:39 EST	date : Thu, 12 Jan 2023 03:37:38 GMT server : ngn... /img...	/img...
data_1	1	1/0	dk	https://boum.org https://boum.org https://bou...	boum.org	2023-01-11 22:47:22 EST	date : Thu, 12 Jan 2023 03:47:21 GMT server : ngn... /img...	/img...
data_1	0	1/0	dk	https://gstatic.com https://gstatic.com https...	gstatic.com	2023-01-11 22:38:43 EST	date : Wed, 11 Jan 2023 21:16:10 GMT content-leng... /img...	/img...
data_1	0	1/0	dk	https://google.com https://google.com http...	maps.googleapis.com	2023-01-11 22:39:19 EST	date : Wed, 11 Jan 2023 22:22:03 GMT content-leng... /img...	/img...

Figure 18: showing the result of the cache, hilton hotel could probably be one of the place they are staying and need to investigate the room physically

Web Cookies

Source Name	S	C	O	URL	Date Accessed	Name	Value	Program Name	Domain	Username	Data Source
Cookies	1			www.doarms.com	2023-01-10 14:14:10 EST	AffiliateTrackedToday		Google Chrome	www.doarms.com	Default	suspect_Image
Cookies	1			ogs.google.com	2023-01-10 14:25:59 EST	OTZ		Google Chrome	ogs.google.com	Default	suspect_Image
Cookies	1			www.doarms.com	2023-01-10 14:14:10 EST	Referrer		Google Chrome	www.doarms.com	Default	suspect_Image
Cookies	1			www.doarms.com	2023-01-10 14:14:55 EST	_alutvc		Google Chrome	www.doarms.com	Default	suspect_Image
Cookies	1			www.doarms.com	2023-01-10 14:14:55 EST	_alutvs		Google Chrome	www.doarms.com	Default	suspect_Image
Cookies	0			addthis.com	2023-01-10 17:26:19 EST	na_id		Google Chrome	addthis.com	Default	suspect_Image
Cookies	1			.doarms.com	2023-01-10 14:14:11 EST	_gat		Google Chrome	doarms.com	Default	suspect_Image
Cookies	1			.doarms.com	2023-01-10 14:14:10 EST	_gat_gtag_UA_1399167_37		Google Chrome	doarms.com	Default	suspect_Image
Cookies	1			.doarms.com	2023-01-10 14:15:04 EST	_gid		Google Chrome	doarms.com	Default	suspect_Image
Cookies	1			www.doarms.com	2023-01-10 14:15:04 EST	vsettings		Google Chrome	www.doarms.com	Default	suspect_Image
Cookies	1			accounts.google.com	2023-01-12 00:45:01 EST	OTZ		Google Chrome	accounts.google.com	Default	suspect_Image
Cookies	1			google.com	2023-01-10 14:16:28 EST	_ga		Google Chrome	google.com	Default	suspect_Image
Cookies	1			google.com	2023-01-10 14:16:28 EST	_ga_3WTQFP9ECQ		Google Chrome	google.com	Default	suspect_Image
Cookies	1			www.google.com	2023-01-10 14:21:09 EST	OTZ		Google Chrome	www.google.com	Default	suspect_Image
Cookies	1			youtube.com	2023-01-12 00:47:30 EST	VISITOR_INFO1_LIVE		Google Chrome	youtube.com	Default	suspect_Image
Cookies	1			accounts.google.com	2023-01-12 00:45:01 EST	_Host-GAPS		Google Chrome	accounts.google.com	Default	suspect_Image
Cookies	0			at1.listrakbi.com	2023-01-10 14:21:45 EST	AWALSALBCORS		Google Chrome	at1.listrakbi.com	Default	suspect_Image
Cookies	0			m1.listrakbi.com	2023-01-10 14:21:49 EST	AWALSALBCORS		Google Chrome	m1.listrakbi.com	Default	suspect_Image
Cookies	0			s1.listrakbi.com	2023-01-10 14:21:44 EST	AWALSALBCORS		Google Chrome	s1.listrakbi.com	Default	suspect_Image
Cookies	1			gunbuyer.com	2023-01-10 14:24:43 EST	GSIIDebMyz3Ad2K		Google Chrome	gunbuyer.com	Default	suspect_Image

Figure 19: showing web domains related to firearm case

Web Downloads

Source Name	S	C	O	Path	URL	Date Accessed
History	0			C:\Users\john\Downloads\pic1.png	https://cdn3.volusion.com/fsvws.bsyvg/v/vspfiles/ph...	2023-01-10 14:13:35 E
History	0			C:\Users\john\Music\pic2.jpg	https://cdn3.volusion.com/fsvws.bsyvg/v/vspfiles/ph...	2023-01-10 14:13:55 E
History	0			C:\Users\john\Pictures\pic3.jpg	https://cdn3.volusion.com/fsvws.bsyvg/v/vspfiles/ph...	2023-01-10 14:14:23 E
History	0			C:\Users\john\Pictures\knf1.jpg	https://cdn3.volusion.com/fsvws.bsyvg/v/vspfiles/ph...	2023-01-10 14:15:01 E
History	1			C:\Users\john\Pictures\300.webp	https://www.gunbuyer.com/media/catalog/product/...	2023-01-10 14:21:58 E
History	1			C:\Users\john\Pictures\399.webp	file:///C:/Users/john/Pictures/300.webp	2023-01-10 14:24:07 E
History	1			C:\Users\john\Documents\May a licensee sell a fire...	https://www.ataf.gov/firearms/qz/may-licensee-sell-fi...	2023-01-10 14:30:14 E
History	1			C:\Users\john\Pictures\high Velocity	data:image/jpg;base64,9j/4AAQSkZJRgABAQAAAQ...	2023-01-10 17:19:33 E
History	1			C:\Users\john\Pictures\Superior Pawn Little Creek R...	https://www.google.com/search?q=Superior+Pawn+...	2023-01-10 17:20:52 E
History	1			C:\Users\john\Downloads\chirlie.jpg	blob:https://mail.proton.net/d472affe-e847-470e-...	2023-01-11 00:51:56 E
History	1			C:\Users\john\Downloads\steeghide-0.5.1-win32.zip	https://downloads.sourceforge.net/project/steeghid...	2023-01-11 00:54:25 E
History	1			C:\Users\john\Downloads\steeghide-0.5.1-win32.zip	https://netactuate.sourceforge.net/project/steeghid...	2023-01-11 00:54:25 E
History	1			C:\Users\john\Downloads\torbrowser-install-win64-1...	https://www.torproject.org/dist/torbrowser/12.0.1/...	2023-01-11 22:42:22 E
History	1			C:\Users\john\Downloads\torbrowser-install-win64-1...	https://dist.torproject.org/torbrowser/12.0.1/torbro...	2023-01-11 22:42:22 E
History	0			C:\Users\john\Downloads\tails-amd64-5.8.img	https://download.tails.tails/stable/tails-amd64-5...	2023-01-11 22:49:09 E
History	0			C:\Users\john\Downloads\tails-amd64-5.8.img	https://mirrors.wikimedia.org/tails/stable/tails-amd...	2023-01-11 22:49:09 E
History	1			C:\Users\john\Downloads\balenaEtcher-portable.exe	https://tails.boum.org/etcher/balenaEtcher-portable.exe	2023-01-11 22:52:21 E
History	1			C:\Users\john\Downloads\wipefile7z	https://www.gajin.at/get?id=wipefile&vk=4CROQV...	2023-01-12 00:49:38 E
History	0			C:\Users\john\Downloads\7z2201-x64.exe	https://www.7-zip.org/a/7z2201-x64.exe	2023-01-12 00:51:21 E
History	0			C:\Users\john\Downloads\7z2201-x64.exe	https://www.7-zip.org/a/7z2201-x64.exe	2023-01-12 00:51:39 E
History	1			C:\Users\john\Downloads\wipefile17z	/C:\Users\john\Downloads\7z2201-x64.exe wipefile&vk=4CROQV...	2023-01-12 00:52:25 E
ChromeSetup.exe.Zone.Identifier				/Users/john/AppData/Local/Microsoft/Windows/Net...		
balenaEtcher-portable.exe.Zone.Identifier				/Users/john/Desktop/balenaEtcher-portable.exe		
chirlie.jpg.Zone.Identifier				/Users/john/Desktop/chirlie.jpg		

Figure 20: showing the files that John had downloaded, noted that there are image files in the Music folder which needs to be checked

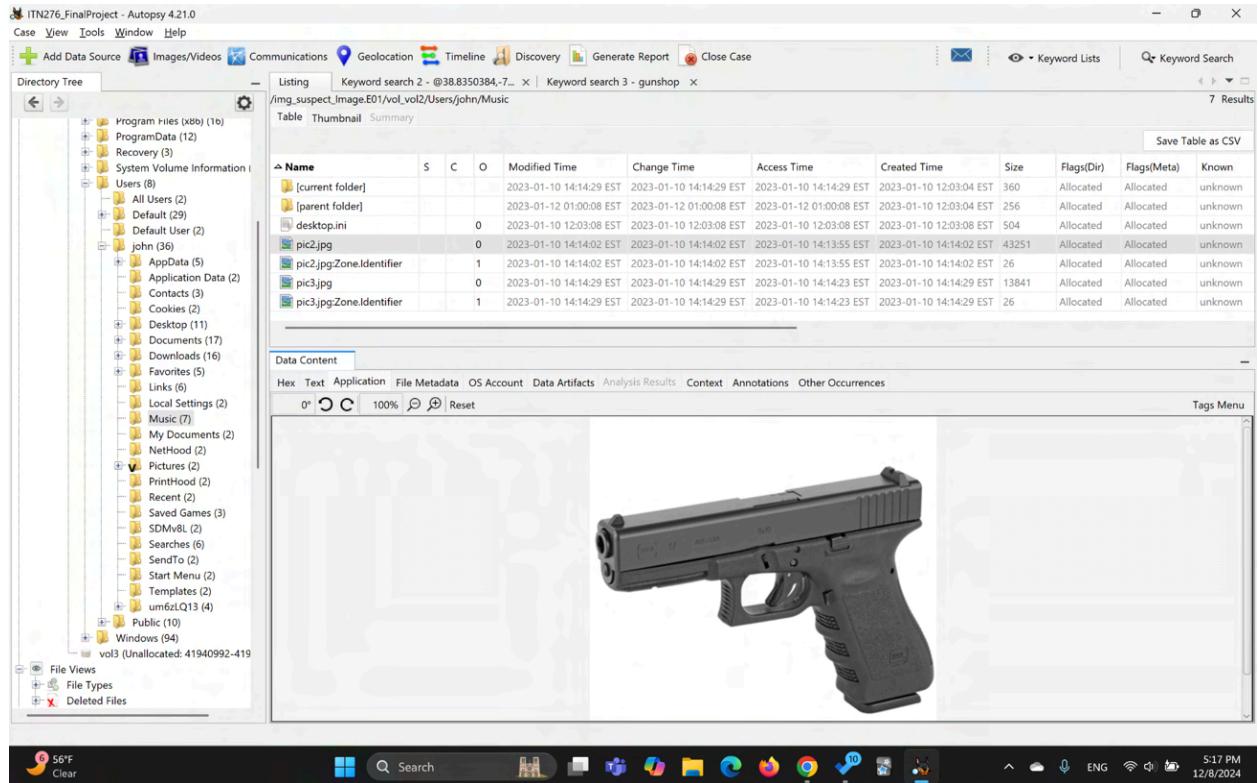


Figure 20.1: showing the pic2.jpg under Music folder of user John

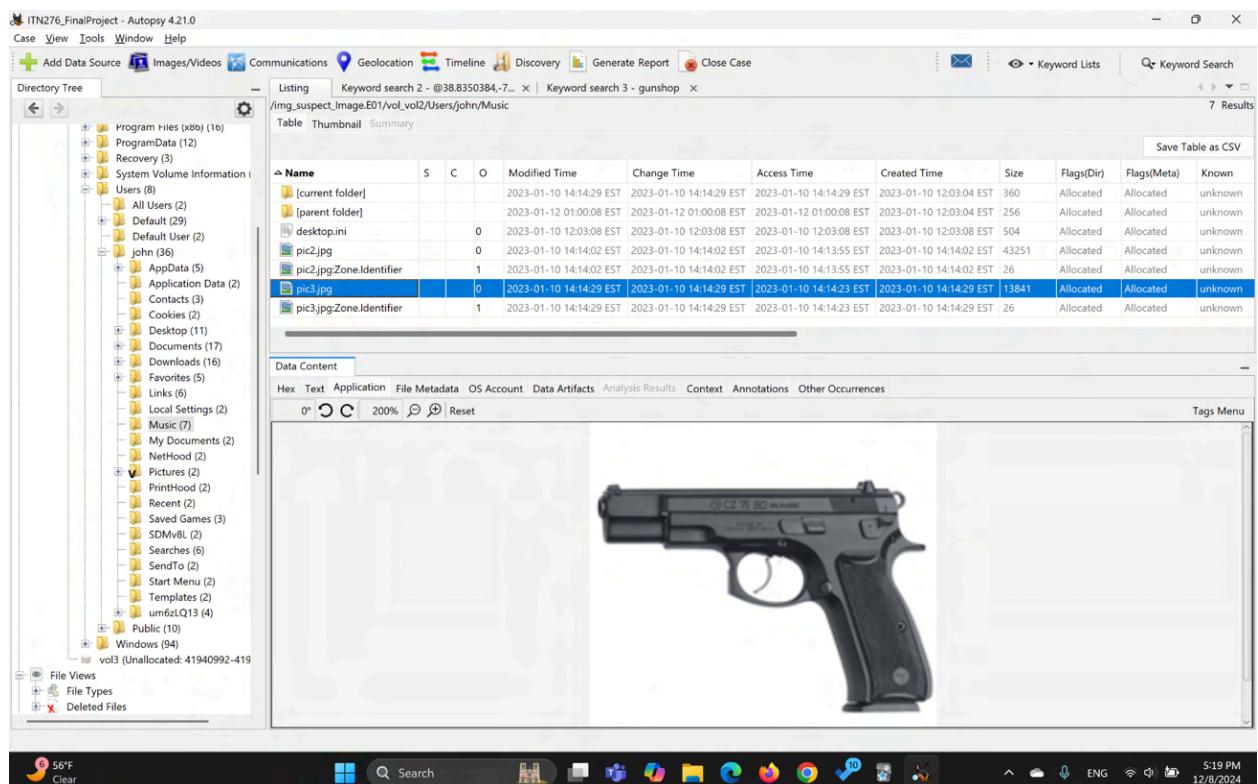


Figure 20.2: showing the pic3.jpg under Music folder of user John

Web History

The screenshot shows the Autopsy 4.21 interface with the 'Web History' tab selected. The left sidebar displays a directory tree of the evidence volume, including sections like 'File Views', 'Data Artifacts', 'Analysis Results', and 'Web Search'. The main pane shows a table of search results with columns for URL, Date Accessed, Referrer URL, and Title. Many of the titles and URLs contain keywords related to firearms and gun stores.

C	O	URL	Date Accessed	Referrer URL	Title
1		https://www.google.com/maps/search/Tidewater,+V...	2023-01-10 14:11:48 EST	https://www.google.com/maps/search/Tidewater,+V...	Tidewater - Google Maps
1		https://www.google.com/maps/place/Tidewater,+V...	2023-01-10 14:11:49 EST	https://www.google.com/maps/place/Tidewater,+V...	Tidewater, VA DOA - Google Maps
1		https://www.google.com/maps/search/Tidewater,+V...	2023-01-10 14:11:52 EST	https://www.google.com/maps/search/Tidewater,+V...	DOA Arms - Google Maps
1		https://www.google.com/maps/place/DOA+Arms/@...	2023-01-10 14:11:53 EST	https://www.google.com/maps/place/DOA+Arms/@...	Google Maps
1		https://www.google.com/maps/dir/DOA+Arms,+97...	2023-01-10 14:11:58 EST	https://www.google.com/maps/dir/DOA+Arms,+97...	Google Maps
1		https://www.google.com/maps/dir/DOA+Arms,+97...	2023-01-10 14:12:01 EST	https://www.google.com/maps/dir/DOA+Arms,+97...	Google Maps
1		https://www.google.com/maps/dir/DOA+Arms,+97...	2023-01-10 14:12:10 EST	https://www.google.com/maps/dir/DOA+Arms,+97...	Google Maps
1		https://www.google.com/maps/dir/DOA+Arms,+97...	2023-01-10 14:12:22 EST	https://www.google.com/maps/dir/DOA+Arms,+97...	Manassas Mall, Sudley Road, Manassas, VA to DOA ...
1		https://www.google.com/maps/dir/DOA+Arms,+97...	2023-01-10 14:12:23 EST	https://www.google.com/maps/dir/DOA+Arms,+97...	Manassas Mall, Sudley Road, Manassas, VA to DOA ...
1		https://www.google.com/maps/dir/DOA+Arms,+97...	2023-01-10 14:12:47 EST	https://www.google.com/maps/dir/DOA+Arms,+97...	Manassas Mall, Sudley Road, Manassas, VA to DOA ...
1		https://www.google.com/search?qs=eljz4VP1z...	2023-01-10 14:12:57 EST	https://www.google.com/search?qs=eljz4VP1z...	doa arms virginia beach - Google Search
1		https://www.google.com/search?qs=eljz4VP1z...	2023-01-10 14:12:57 EST	https://www.google.com/search?qs=eljz4VP1z...	doa arms virginia beach - Google Search
1		https://www.doaarms.com/	2023-01-10 14:12:59 EST	https://www.doaarms.com/	DOA ARMS
1		https://www.doaarms.com/category-s/136.htm	2023-01-10 14:14:16 EST	https://www.doaarms.com/category-s/136.htm	Handgun
1		https://www.doaarms.com/GLOCK-17-Gen3-9x19-P...	2023-01-10 14:13:51 EST	https://www.doaarms.com/GLOCK-17-Gen3-9x19-P...	GLOCK 17 Gen3 9x19 Pistol
1		https://www.doaarms.com/category-s/134.htm	2023-01-10 14:14:10 EST	https://www.doaarms.com/category-s/134.htm	Long Rifles
1		https://www.doaarms.com/category-s/136.htm	2023-01-10 14:14:16 EST	https://www.doaarms.com/category-s/136.htm	Handguns
1		https://www.doaarms.com/category-s/117.htm	2023-01-10 14:14:55 EST	https://www.doaarms.com/category-s/117.htm	Complete Uppers
1		https://www.doaarms.com/category-s/120.htm	2023-01-10 14:14:58 EST	https://www.doaarms.com/category-s/120.htm	Complete Lower
1		https://www.doaarms.com/category-s/165.htm	2023-01-10 14:15:04 EST	https://www.doaarms.com/category-s/165.htm	Knives & Edged Weapons
1		https://www.google.com/maps/dir/DOA+Arms,+97...	2023-01-10 14:15:36 EST	https://www.google.com/maps/dir/DOA+Arms,+97...	Google Maps
1		https://www.google.com/maps/dir/DOA+Arms,+97...	2023-01-10 14:15:52 EST	https://www.google.com/maps/dir/DOA+Arms,+97...	Google Maps
1		https://www.google.com/maps/dir/DOA+Arms,+97...	2023-01-10 14:15:52 EST	https://www.google.com/maps/dir/DOA+Arms,+97...	Google Maps

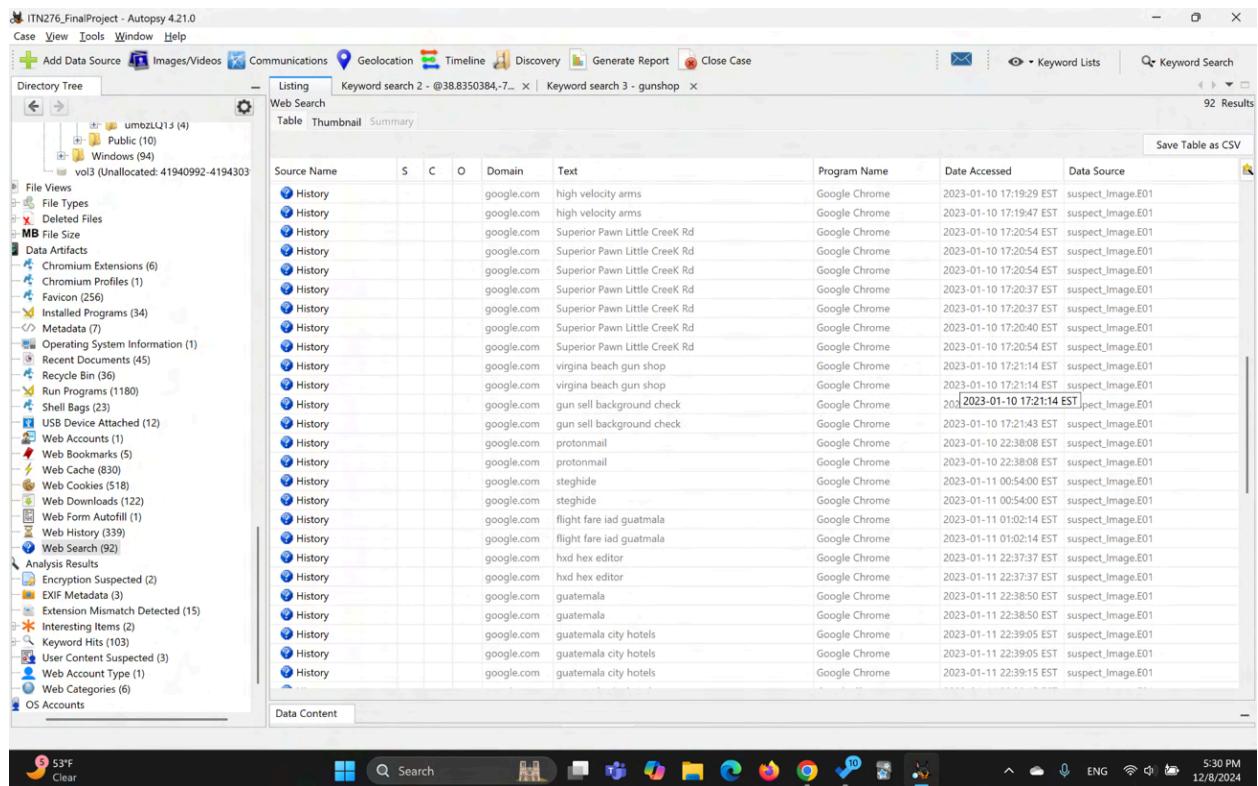
Figure 21: showing what John was finding on the web, proving that he was browsing weapons and gun on the goaarms.com and how to get there by using google maps

Web Search

The screenshot shows the Autopsy 4.21 interface with the 'Web Search' tab selected. The left sidebar displays a directory tree of the evidence volume, including sections like 'File Views', 'Data Artifacts', 'Analysis Results', and 'Web Search'. The main pane shows a table of search results with columns for Source Name, S, C, O, Domain, Text, Program Name, Date Accessed, and Data Source. Many of the search terms relate to job listings and specific firearms.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
Bookmarks				google.com	virginia beach gun shop	Google Chrome	0000-00-00 00:00:00	suspect_Image.E01
Bookmarks				google.com	guatemala city hotels	Google Chrome	0000-00-00 00:00:00	suspect_Image.E01
History				google.com	google maps	Google Chrome	2023-01-10 14:11:31 EST	suspect_Image.E01
History				google.com	doa arms virginia beach	Google Chrome	2023-01-10 14:12:57 EST	suspect_Image.E01
History				google.com	doa arms virginia beach	Google Chrome	2023-01-10 14:12:57 EST	suspect_Image.E01
History				google.com	landscaping business	Google Chrome	2023-01-10 14:19:31 EST	suspect_Image.E01
History				google.com	landscaping business	Google Chrome	2023-01-10 14:19:31 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:19:59 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:19:59 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:20:55 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:20:55 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:20:55 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:20:55 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:20:55 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:20:55 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:20:55 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:20:55 EST	suspect_Image.E01
History				google.com	security jobs near manassas	Google Chrome	2023-01-10 14:20:55 EST	suspect_Image.E01
History				google.com	nevada gun rule	Google Chrome	2023-01-10 14:29:40 EST	suspect_Image.E01
History				google.com	nevada gun rule	Google Chrome	2023-01-10 14:29:40 EST	suspect_Image.E01
History				google.com	selling guns out of state	Google Chrome	2023-01-10 14:29:55 EST	suspect_Image.E01
History				google.com	gun sell background check	Google Chrome	2023-01-10 14:30:28 EST	suspect_Image.E01
History				google.com	outlook	Google Chrome	2023-01-10 17:10:28 EST	suspect_Image.E01

Figure 22.1: showing the result of web search (virginia beach gun shop, guatemala city hotels, doa gun shop, security jobs near manassas which indicate John might have been living in Manassas, price for handgun, gun transfer without tracing, nevada gun rule, selling gun outside the US, background check)



The screenshot shows the Autopsy 4.21.0 interface with a search results table titled "Web Search". The table has columns: Source Name, S, C, O, Domain, Text, Program Name, Date Accessed, and Data Source. The "Text" column contains search terms like "high velocity arms", "superior pawn little creek rd", "gun sell background check", "protonmail", "steghide", "flight fare iad guatemala", and "hex editor". The "Program Name" column shows Google Chrome was used for all searches. The "Date Accessed" column shows dates from January 10, 2023, to January 11, 2023. The "Data Source" column shows "suspect_Image.E01" for most entries, with one entry from "2023-01-10 17:21:14 EST suspect_Image.E01". The left sidebar shows a file tree with various data artifacts like History, Cookies, and Web Cache.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	high velocity arms	Google Chrome	2023-01-10 17:19:29 EST	suspect_Image.E01
History				google.com	high velocity arms	Google Chrome	2023-01-10 17:19:47 EST	suspect_Image.E01
History				google.com	Superior Pawn Little Creek Rd	Google Chrome	2023-01-10 17:20:54 EST	suspect_Image.E01
History				google.com	Superior Pawn Little Creek Rd	Google Chrome	2023-01-10 17:20:54 EST	suspect_Image.E01
History				google.com	Superior Pawn Little Creek Rd	Google Chrome	2023-01-10 17:20:57 EST	suspect_Image.E01
History				google.com	Superior Pawn Little Creek Rd	Google Chrome	2023-01-10 17:20:57 EST	suspect_Image.E01
History				google.com	Superior Pawn Little Creek Rd	Google Chrome	2023-01-10 17:20:40 EST	suspect_Image.E01
History				google.com	Superior Pawn Little Creek Rd	Google Chrome	2023-01-10 17:20:54 EST	suspect_Image.E01
History				google.com	virginia beach gun shop	Google Chrome	2023-01-10 17:21:14 EST	suspect_Image.E01
History				google.com	virginia beach gun shop	Google Chrome	2023-01-10 17:21:14 EST	suspect_Image.E01
History				google.com	gun sell background check	Google Chrome	2023-01-10 17:21:14 EST	suspect_Image.E01
History				google.com	gun sell background check	Google Chrome	2023-01-10 17:21:43 EST	suspect_Image.E01
History				google.com	protonmail	Google Chrome	2023-01-10 22:38:08 EST	suspect_Image.E01
History				google.com	protonmail	Google Chrome	2023-01-10 22:38:08 EST	suspect_Image.E01
History				google.com	steghide	Google Chrome	2023-01-11 00:54:00 EST	suspect_Image.E01
History				google.com	steghide	Google Chrome	2023-01-11 00:54:00 EST	suspect_Image.E01
History				google.com	flight fare iad guatemala	Google Chrome	2023-01-11 01:02:14 EST	suspect_Image.E01
History				google.com	flight fare iad guatemala	Google Chrome	2023-01-11 01:02:14 EST	suspect_Image.E01
History				google.com	hxd hex editor	Google Chrome	2023-01-11 22:37:37 EST	suspect_Image.E01
History				google.com	hxd hex editor	Google Chrome	2023-01-11 22:37:37 EST	suspect_Image.E01
History				google.com	guatemala	Google Chrome	2023-01-11 22:38:50 EST	suspect_Image.E01
History				google.com	guatemala	Google Chrome	2023-01-11 22:38:50 EST	suspect_Image.E01
History				google.com	guatemala city hotels	Google Chrome	2023-01-11 22:39:05 EST	suspect_Image.E01
History				google.com	guatemala city hotels	Google Chrome	2023-01-11 22:39:05 EST	suspect_Image.E01
History				google.com	guatemala city hotels	Google Chrome	2023-01-11 22:39:15 EST	suspect_Image.E01

Figure 22.2: showing the result of web search (high velocity arms, superior pawn little creek road, protonmail, steghide, flight fare to IAD guatemala, hex editor)

ITN276_FinalProject - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword search 2 - @38.8350384,-7... | Keyword search 3 - gunshop

92 Results

Save Table as CSV

Directory Tree Listing Web Search Table Thumbnail Summary

Source Name S C O Domain Text Program Name Date Accessed Data Source

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	can i wipe a folder with mintool	Google Chrome	2023-01-12 00:45:57 EST	suspect_Image.E01
History				google.com	can i wipe a folder with mintool	Google Chrome	2023-01-12 00:45:57 EST	suspect_Image.E01
History				google.com	how to delete file form a folder permanently	Google Chrome	2023-01-12 00:47:29 EST	suspect_Image.E01
History				google.com	7 zip download	Google Chrome	2023-01-12 00:51:17 EST	suspect_Image.E01
History				google.com	7 zip download	Google Chrome	2023-01-12 00:51:17 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	atf office martins burg	Microsoft Edge Analyzer	2023-01-10 17:39:37 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	ghow guns are traced	Microsoft Edge Analyzer	2023-01-10 18:46:51 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	atf paper trail of gum	Microsoft Edge Analyzer	2023-01-10 18:47:30 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	atf gun database	Microsoft Edge Analyzer	2023-01-10 18:48:22 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	The ATF's Nonsensical Non-Searchable Gun Databases	Microsoft Edge Analyzer	2023-01-10 18:51:02 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	can you create emial without phone number	Microsoft Edge Analyzer	2023-01-10 19:04:43 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	gun	Microsoft Edge Analyzer	2023-01-10 19:05:28 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	polic egun thefet	Microsoft Edge Analyzer	2023-01-10 19:06:25 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	firearm stolen virginia beach	Microsoft Edge Analyzer	2023-01-10 19:07:41 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	atf office martins burg	Microsoft Edge Analyzer	2023-01-10 17:39:37 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	ghow guns are traced	Microsoft Edge Analyzer	2023-01-10 18:46:50 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	atf paper trail of gum	Microsoft Edge Analyzer	2023-01-10 18:47:30 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	atf gun database	Microsoft Edge Analyzer	2023-01-10 18:48:22 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	The ATF's Nonsensical Non-Searchable Gun Databases	Microsoft Edge Analyzer	2023-01-10 18:50:01 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	can you create emial without phone number	Microsoft Edge Analyzer	2023-01-10 19:04:43 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	gun	Microsoft Edge Analyzer	2023-01-10 19:05:28 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	polic egun thefet	Microsoft Edge Analyzer	2023-01-10 19:06:25 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	polic egun thefet virginia beach	Microsoft Edge Analyzer	2023-01-10 19:06:38 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	gun thefet virginia	Microsoft Edge Analyzer	2023-01-10 19:07:02 EST	suspect_Image.E01
WebCacheV01.dat				bing.com	firearm stolen virginia beach	Microsoft Edge Analyzer	2023-01-10 19:07:41 EST	suspect_Image.E01

Data Content

53° Clear Search

12/8/2024

Figure 22.3: showing the result of web search (wiping a folder, deleting file permanently, arf office martins burg, guns, gun database, theft at virginia beach)

Analyzing Evidence

The investigation reveal that John is aware of the activities that are highly suggestive of the involvement in the case, such as using secure browsing (tor), secure email (proton mail), steghide to hide information in carrier file, finding information on how to delete files permanently, doing research about the target destination shop and reconnaissance (DOA Arms), how are the state laws regarding firearms, how to sell them back within law, etc.

According to the circumstantial evidence and the subsequent definitive evidence, it is highly likely that John is involved in the theft.

- proof of John searching items on the DOA Arms website (*Figure 21*)
- proof of John searching to go to Virginia Beach DOA Arms from Manassas (*Figure 10.1-4*)
- proof of John searching about Virginia Beach firearm theft (*Figure 22.3*), by nature, the perpetrator usually used to comes back to the crime scene or looks for news about what is happening concerning what he has done. All of the findings and circumstantial evidence point that he is certainly involved in the firearm theft case.

Moreover, he probably has sold the stolen firearms back to another buyer, according to the following evidence.

- proof of John selling guns to Charlie, and transaction of Karlos (*Figure 12.1-3*)

High potential associates: Donald (accomplice), Charlie and Karlos (customers who probably bought the stolen guns), gunbuyer.com (possible platform to buy the stolen firearms, *Figure 19*)

Locations connecting the case:

- Manassas, VA (high probability of the suspect's base of operation)
- DOA Arms, Virginia Beach VA (location of the theft)
- Superior Pawn Little Creek Rd, Norfolk VA (potential place to have the guns exchanged or drop-off point to sold to his customer)
- Coordinates 38.8350384, -77.4523482 (near Chantilly VA, highly suggestive of IAD airport, Dulles, Virginia VA)
- Hilton, guatemala city hotel (which could be where the suspect is now, *Figure 22.2 - flight fare to IAD guatemala*)

Timeline estimation of the event:

- Jan 10, 2023 (2:17 pm) - planning to go to DOA Arms, Virginia Beach, from Manassas (*Figure 10.1-4*)
- Jan 10, 2023 (5:20 pm) - setting location to exchange the stolen items at "Superior Pawn Little Creek Rd" (*Figure 8.2-4*)
- Jan 11, 2023 (12:56 am) - proof that John has sold the stolen guns to Charlie and Karlos (*Figure 12.1-3*)

Possible time of theft - between Jan 10, 2023 after (2pm) to Jan 11, 2023 (12am)