ITN 276, Computer Forensics I

Course Project II: Analyzing A Case

May Pwint 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)

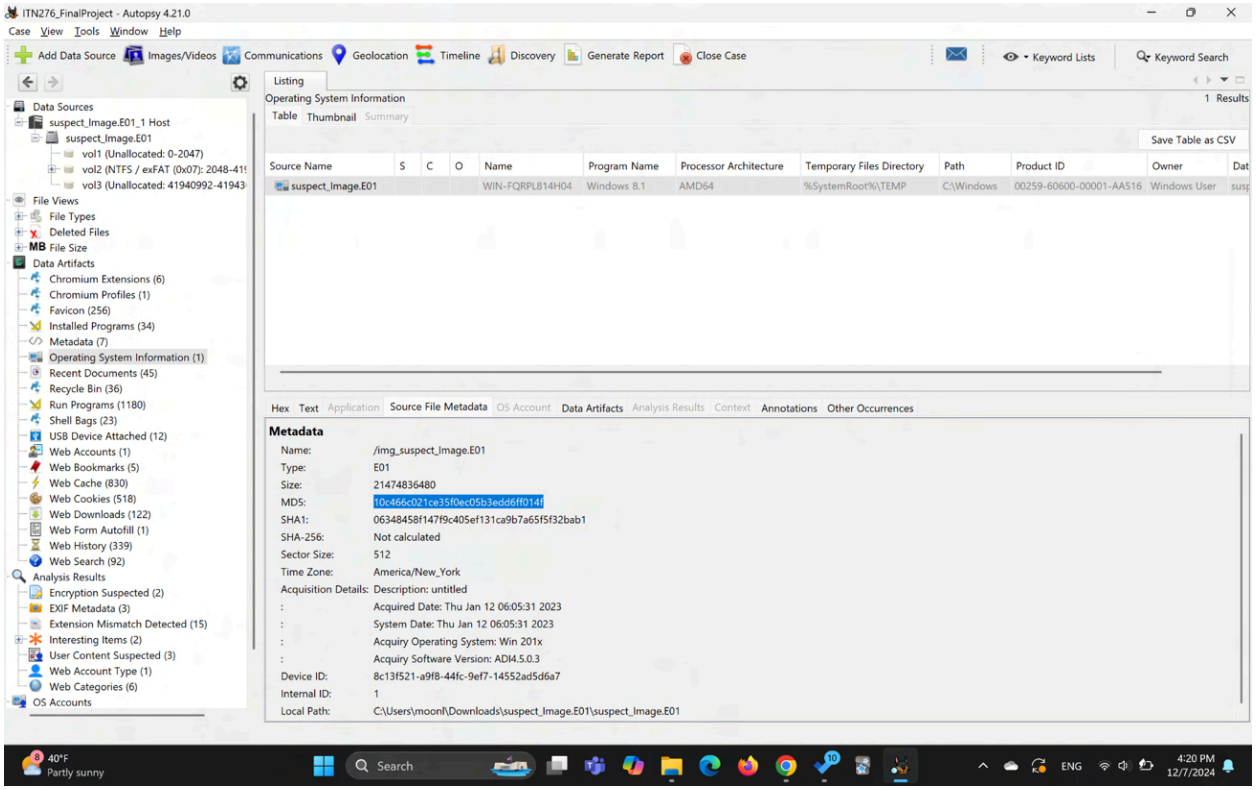

Figure 1: showing the MD5 hash result of the image file

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.

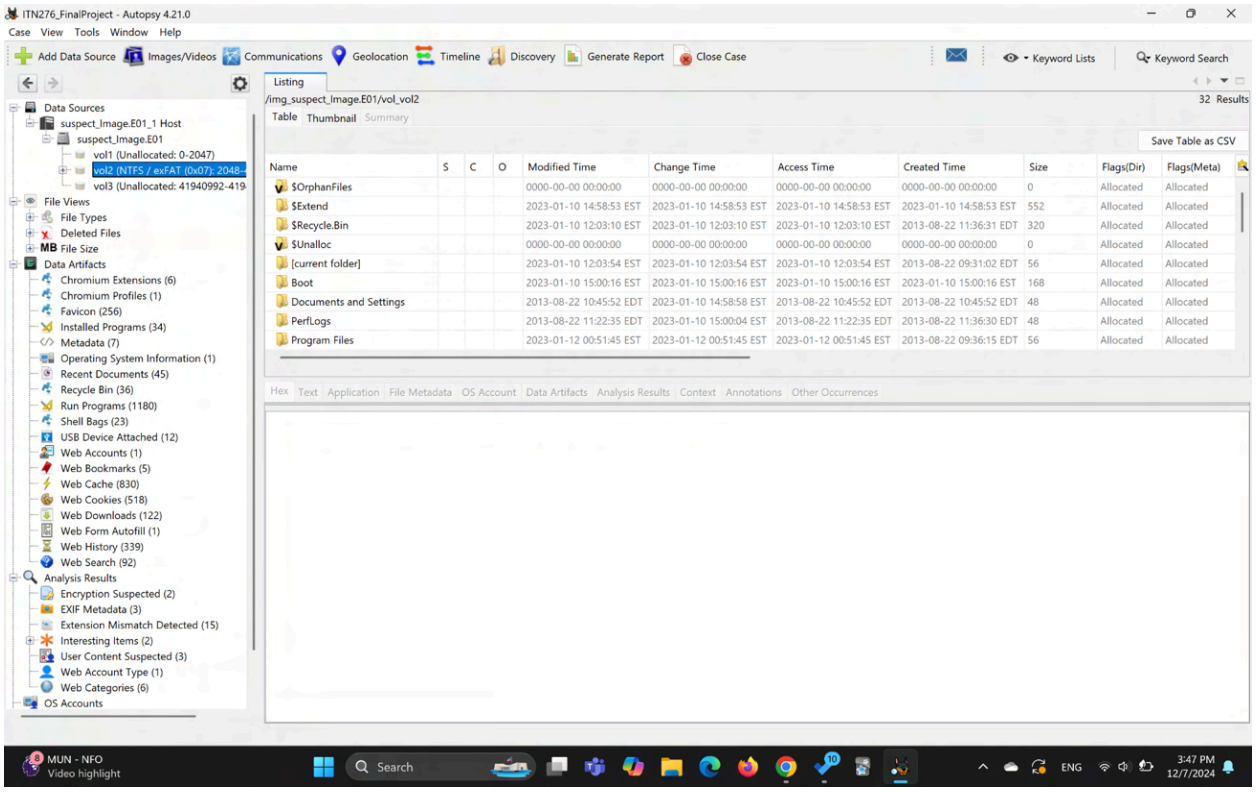

Figure 2: showing the 3 volumes and their file system installed on the hard drive

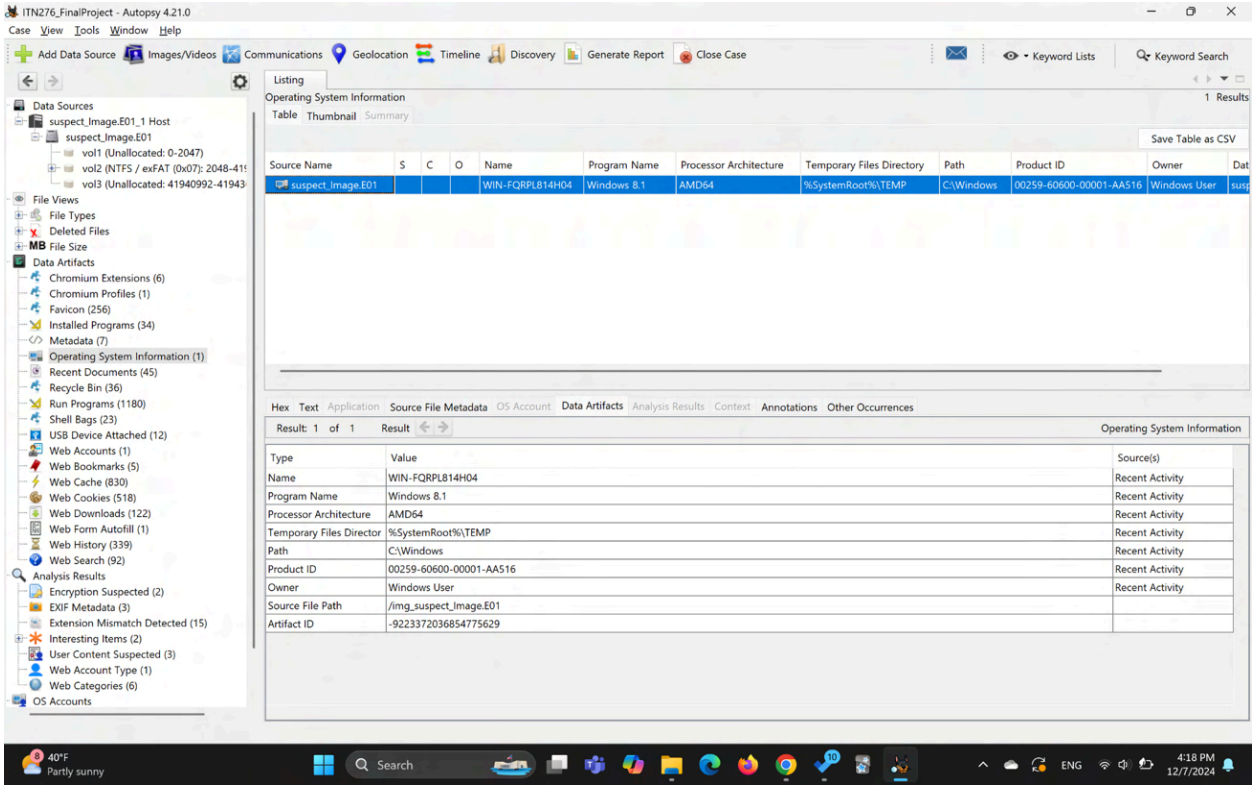

Figure 3: showing the operating system installed on the computer

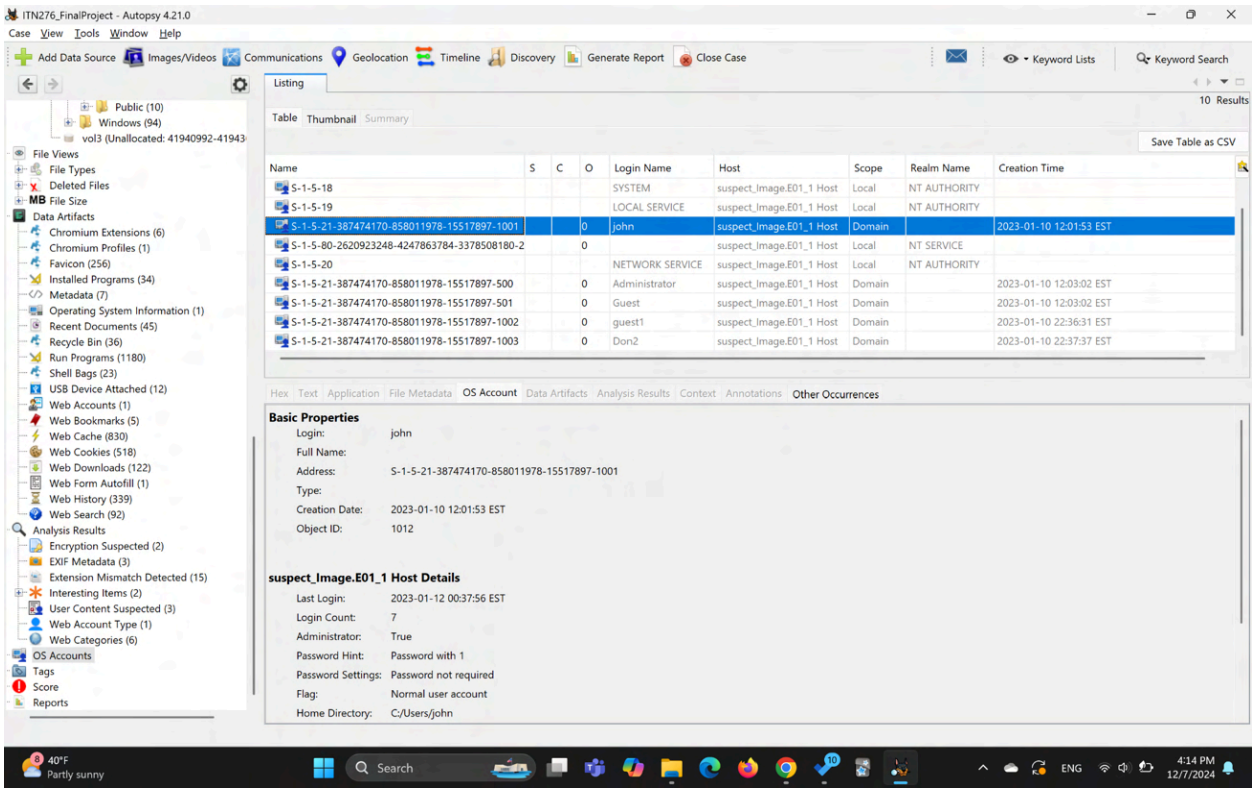

Figure 4: showing the user accounts existing on the computer

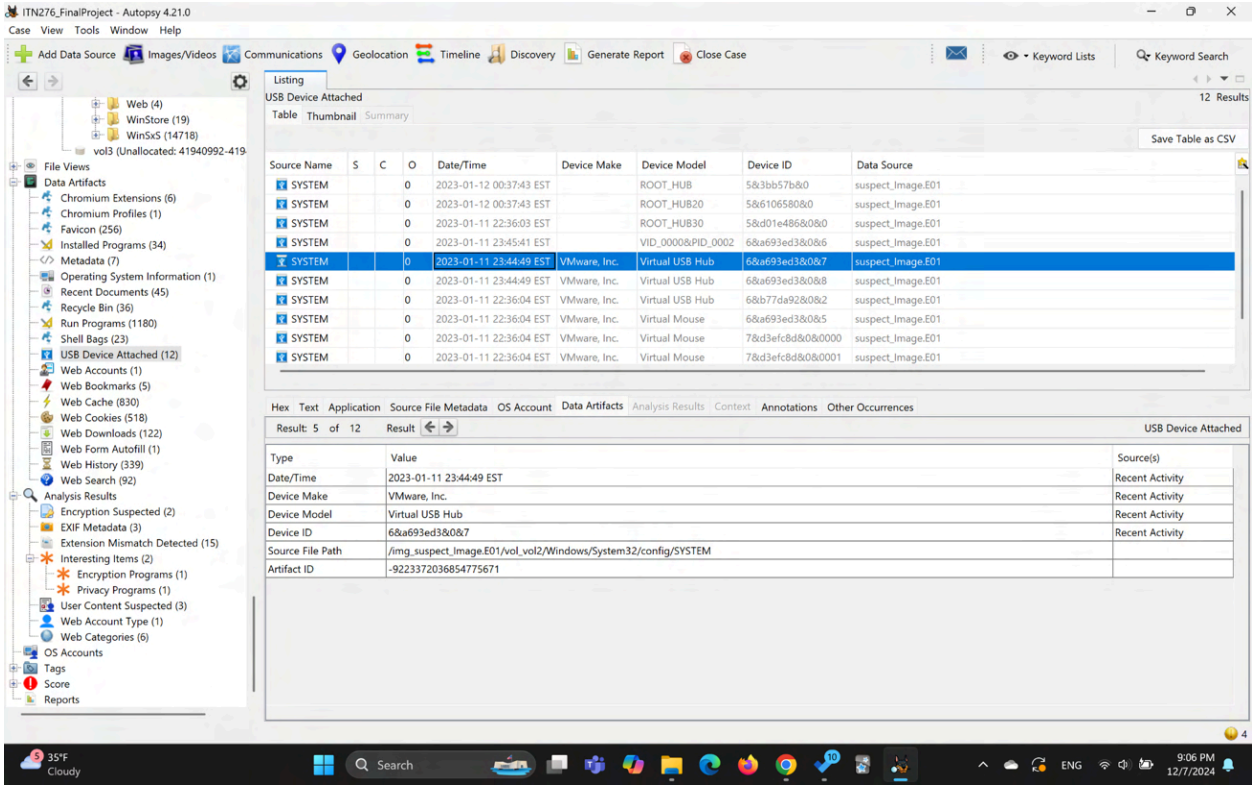

Figure 5: showing VMware running on the system (11 January, 2023 11:44:49 pm EST)

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)

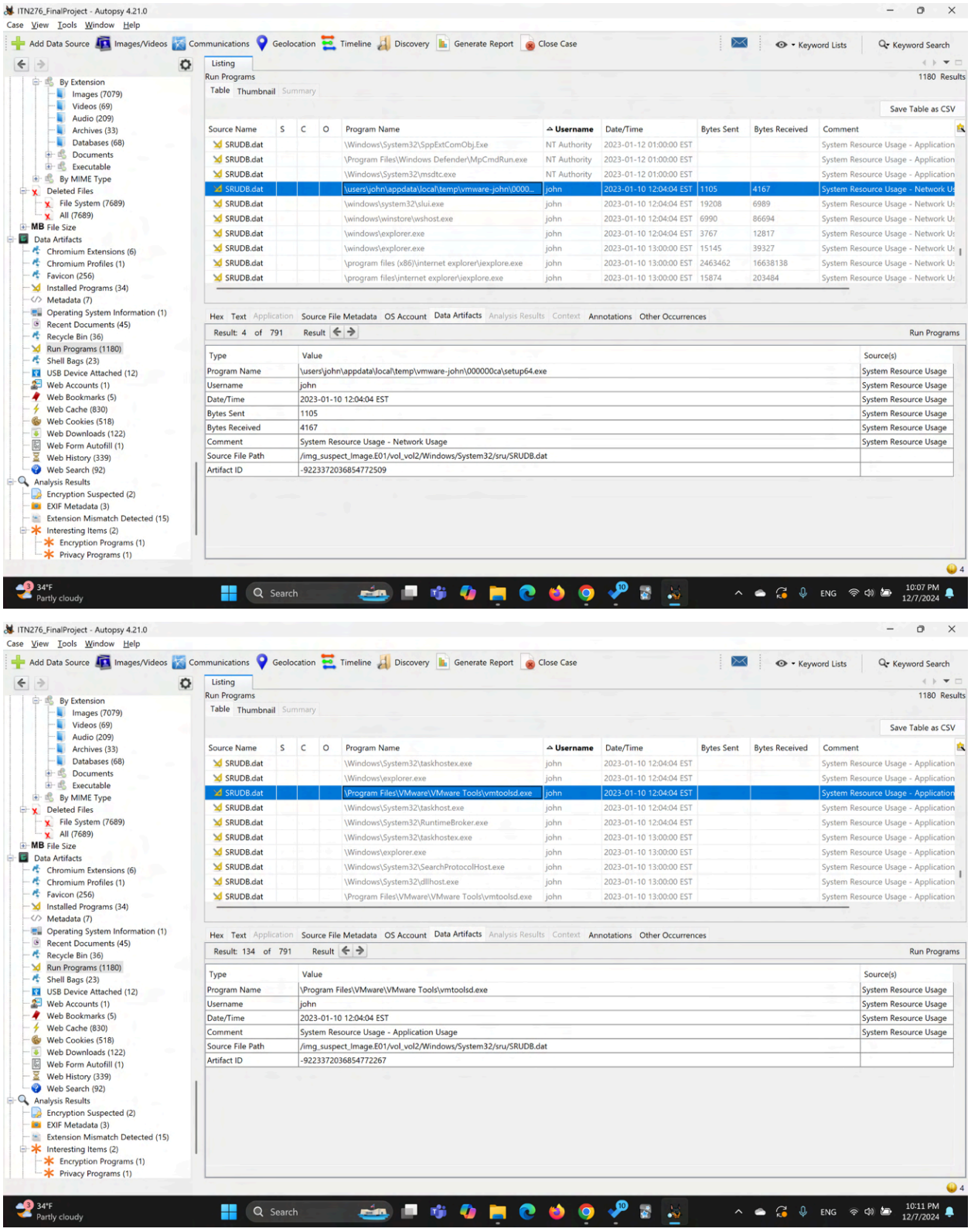

Figure 6.2: showing John installed VMware on the system on 10 Jan, 2021 (12:04:04 pm EST)

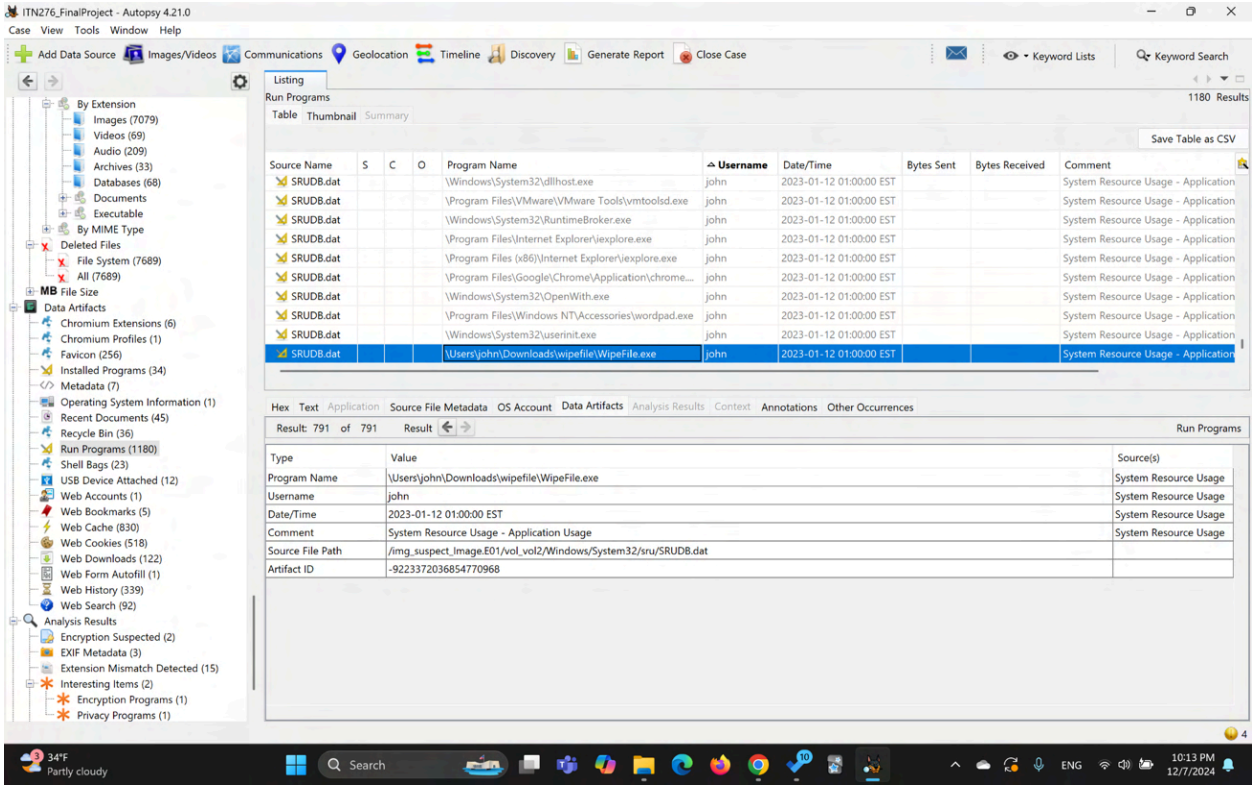

Figure 7: showing John has Wipefile.exe application downloaded

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

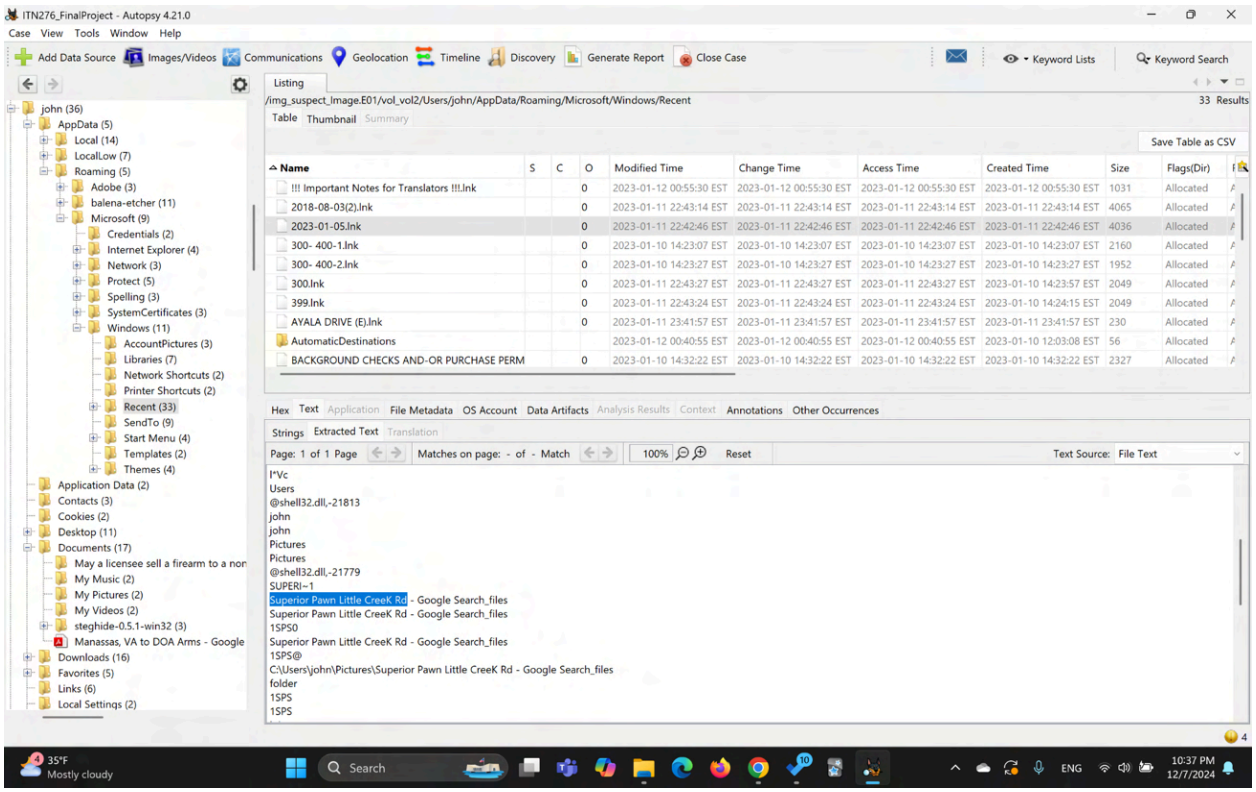

Figure 8.1: showing John searching “Superior Pawn Little CreeK Rd” in one of the results

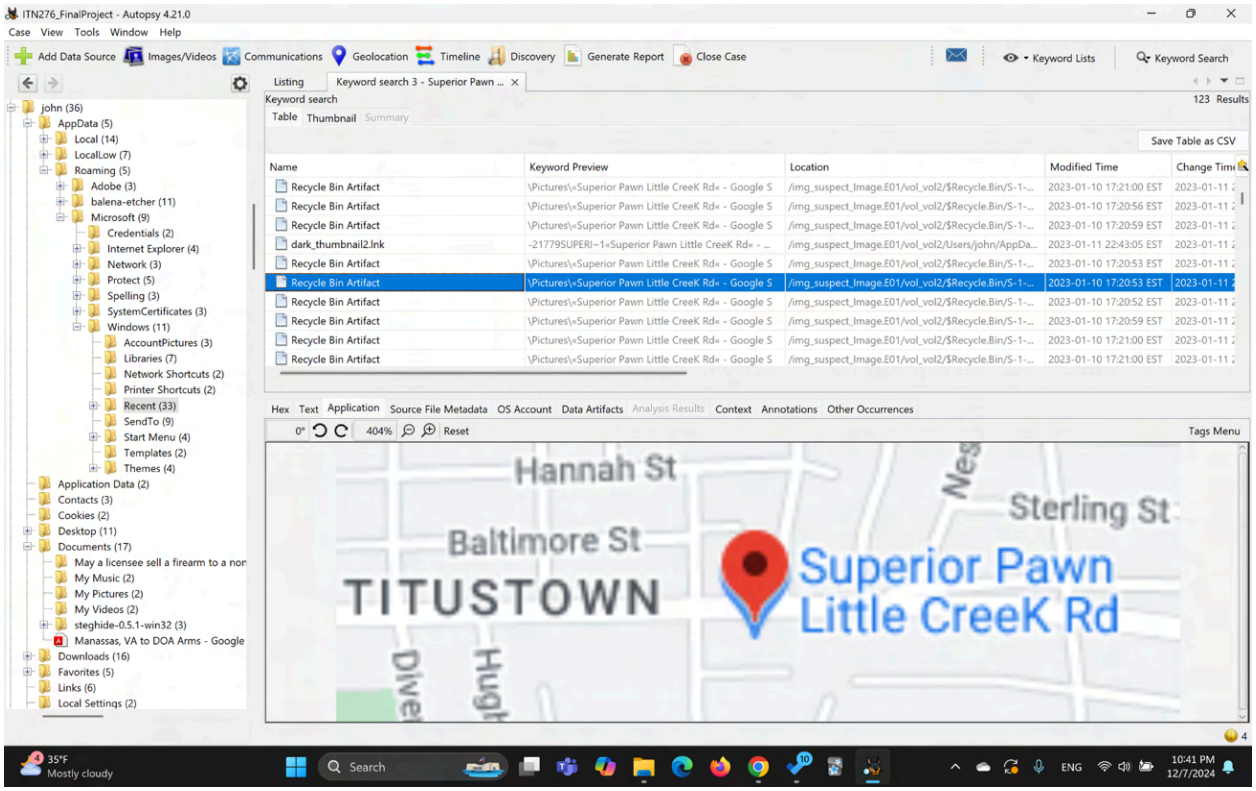

Figure 8.2: showing the location of the “Superior Pawn Little Creek Rd”

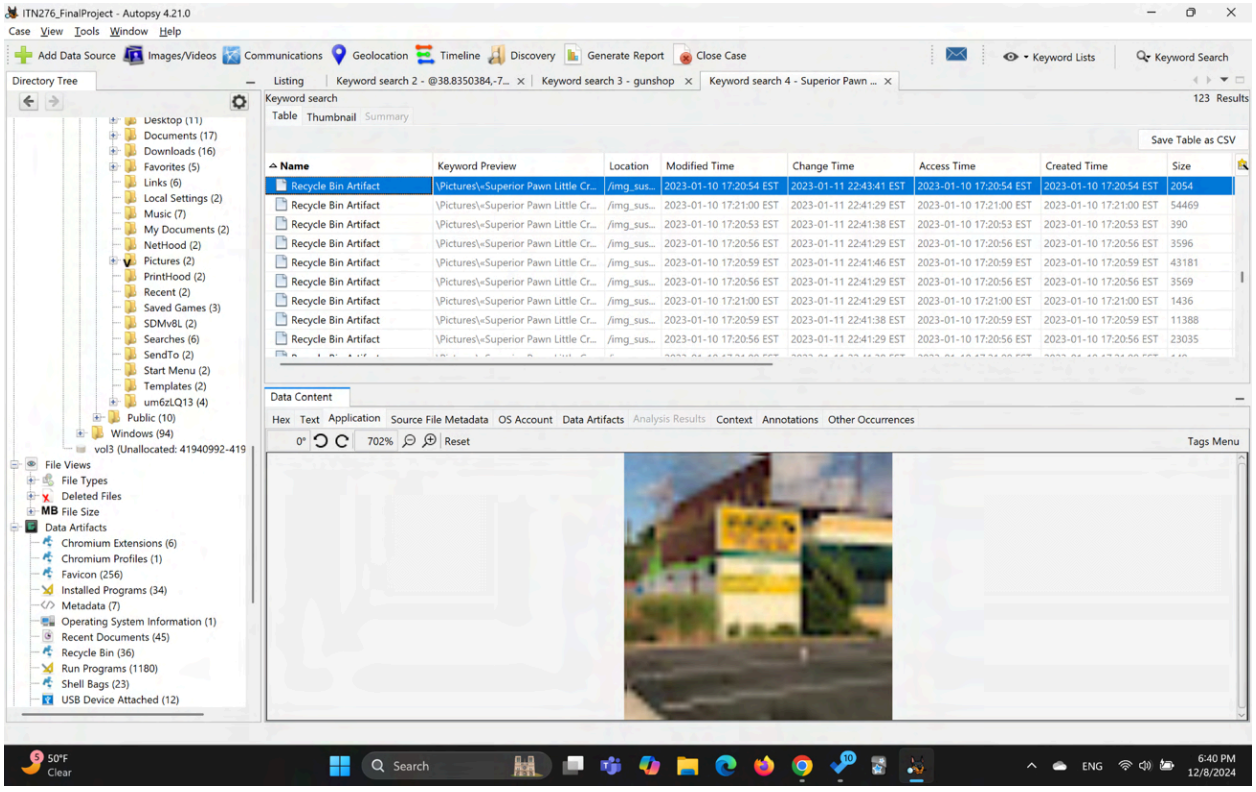

Figure 8.3: possible geolocation of “Superior Pawn Little Creek Rd”

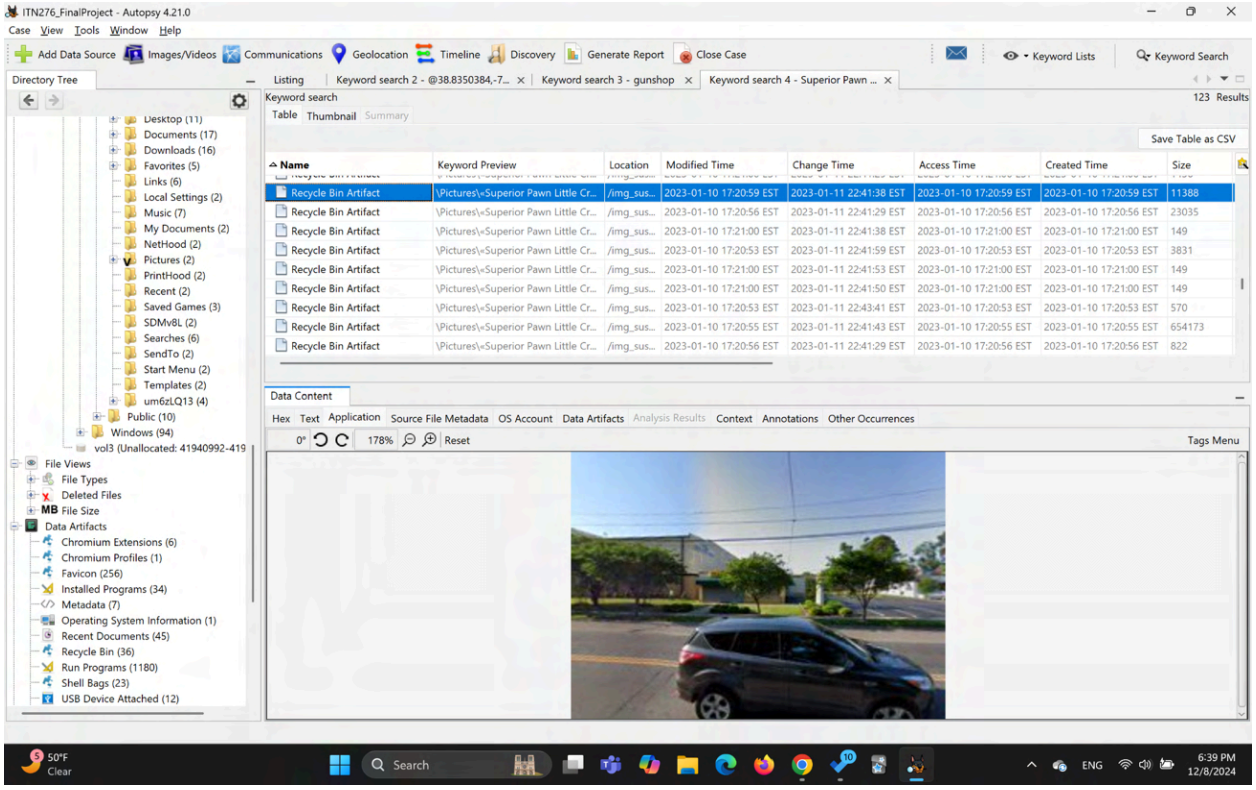

Figure 8.4: possible geolocation of “Superior Pawn Little Creek Rd”

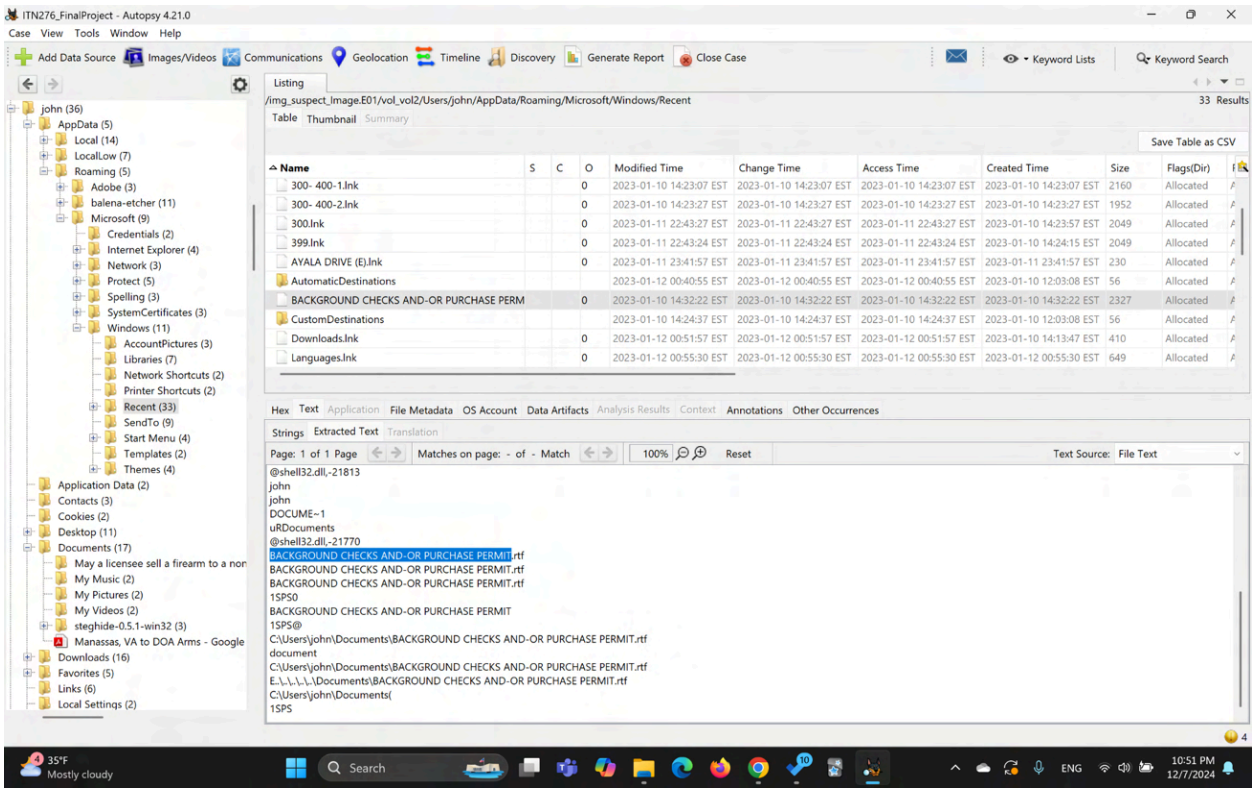

Figure 9.1: showing the document “BACKGROUND CHECKS AND-OR PURCHASE PERMIT” in recent accessed file

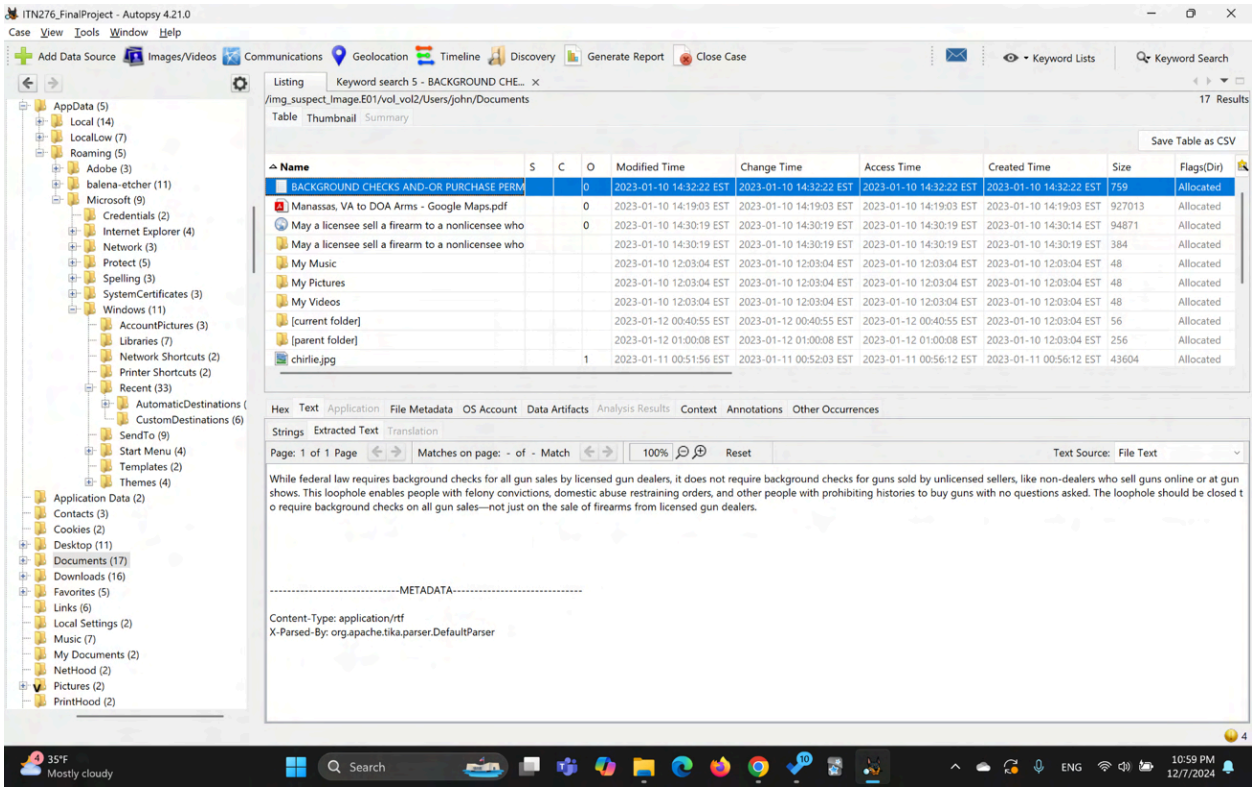

Figure 9.2: showing content of the "BACKGROUND CHECKS AND-OR PURCHASE PERMIT" file

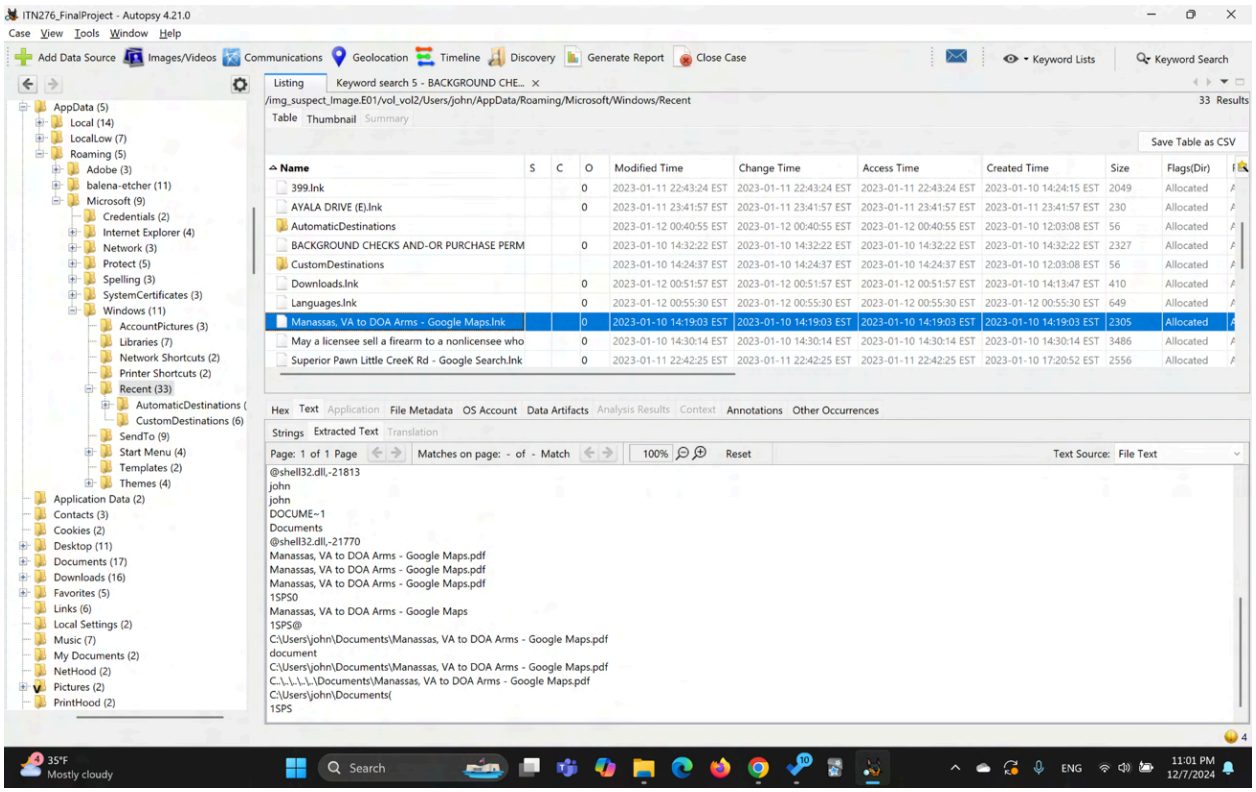

Figure 10.1: showing "Manassas, VA to DOA Arms - Google Maps" in recently opened folder and its actual file path

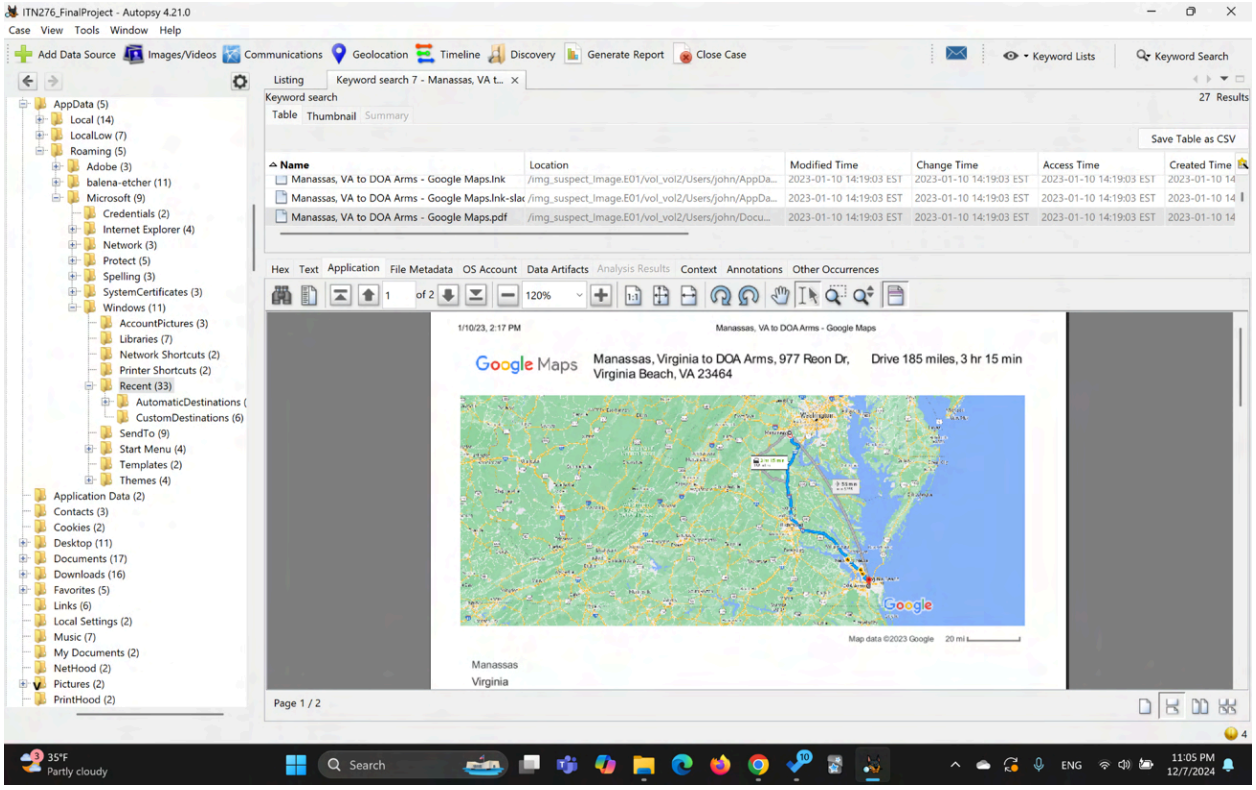

Figure 10.1: showing the content of “Manassas, VA to DOA Arms - Google Maps” pdf file

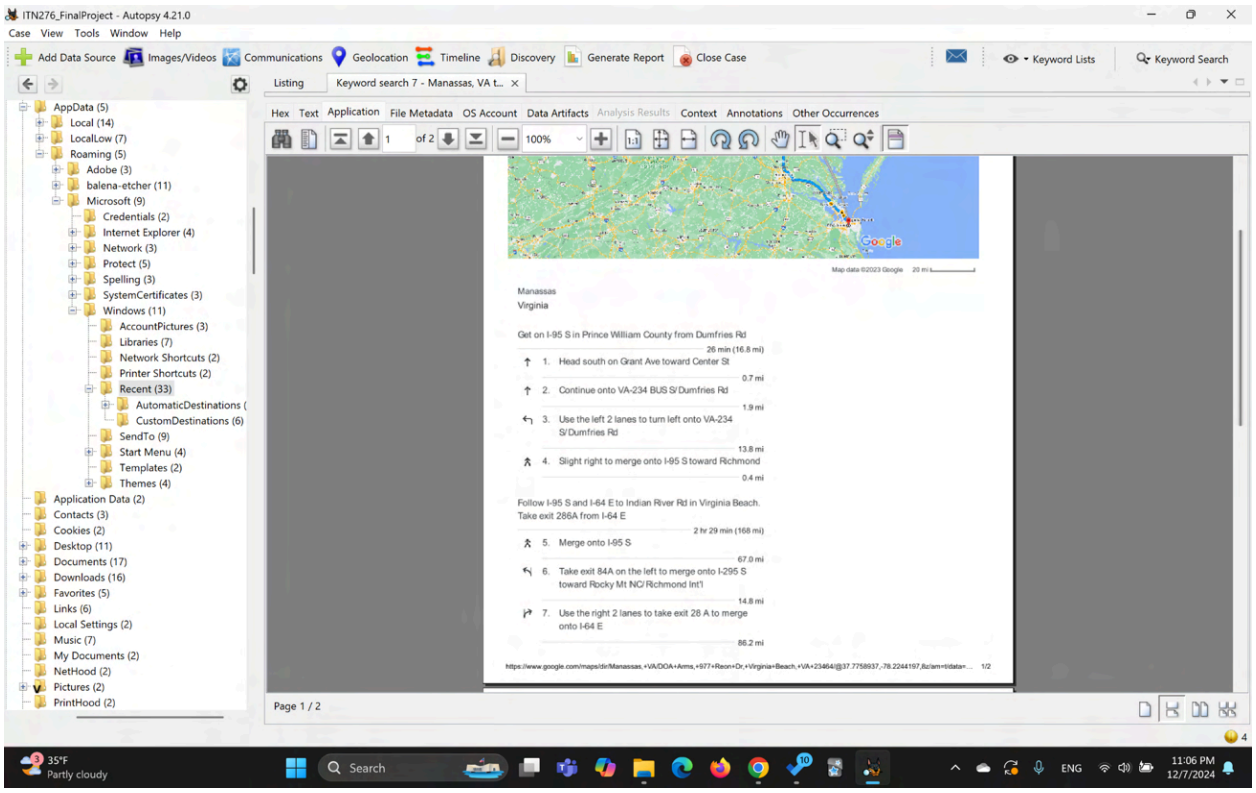

Figure 10.2: showing the content of “Manassas, VA to DOA Arms - Google Maps” pdf file

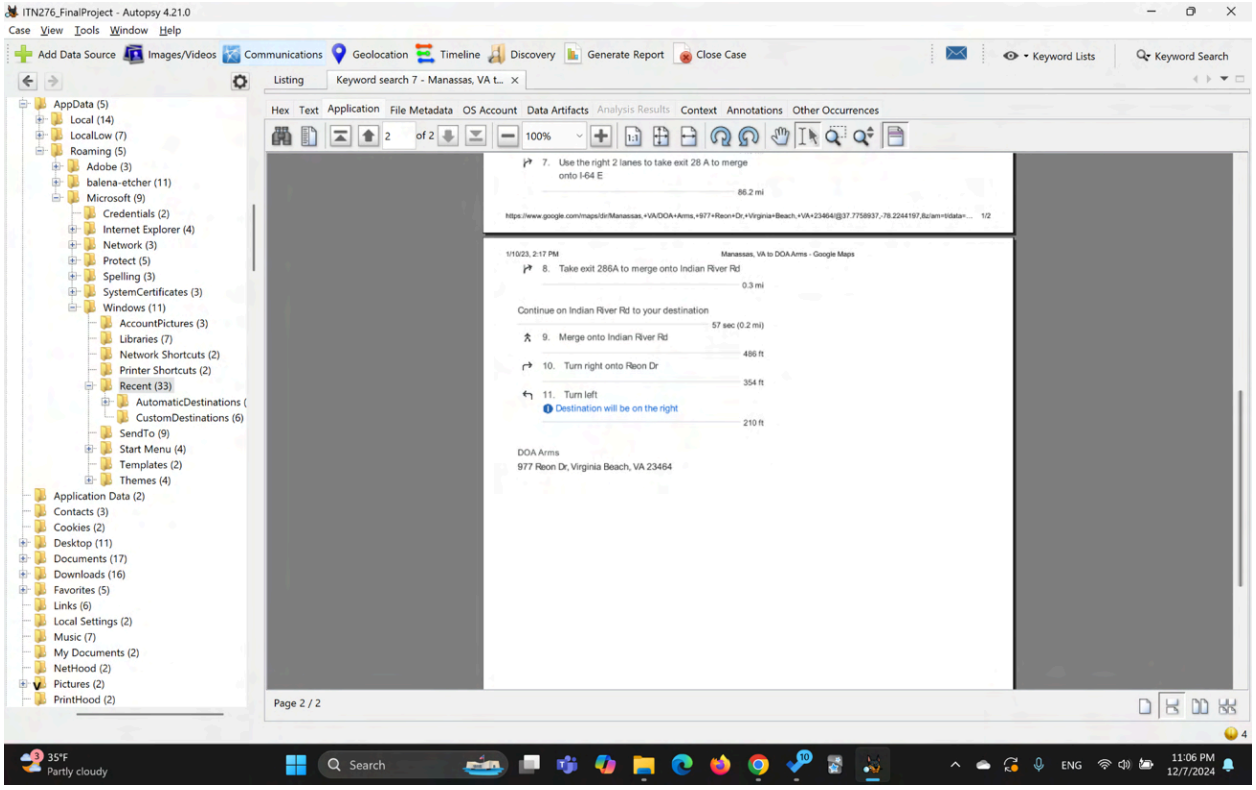

Figure 10.3: showing the content of “Manassas, VA to DOA Arms - Google Maps” pdf file

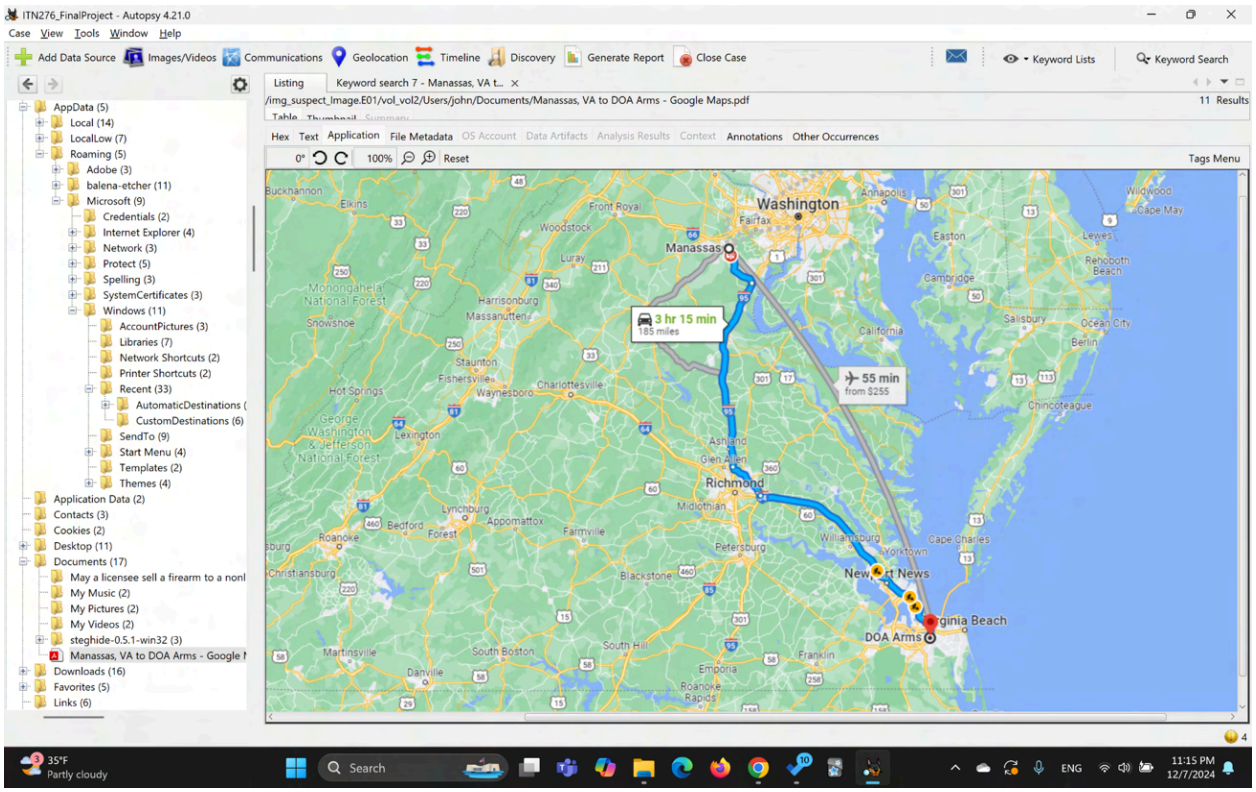

Figure 10.4: showing the map in clearer resolution

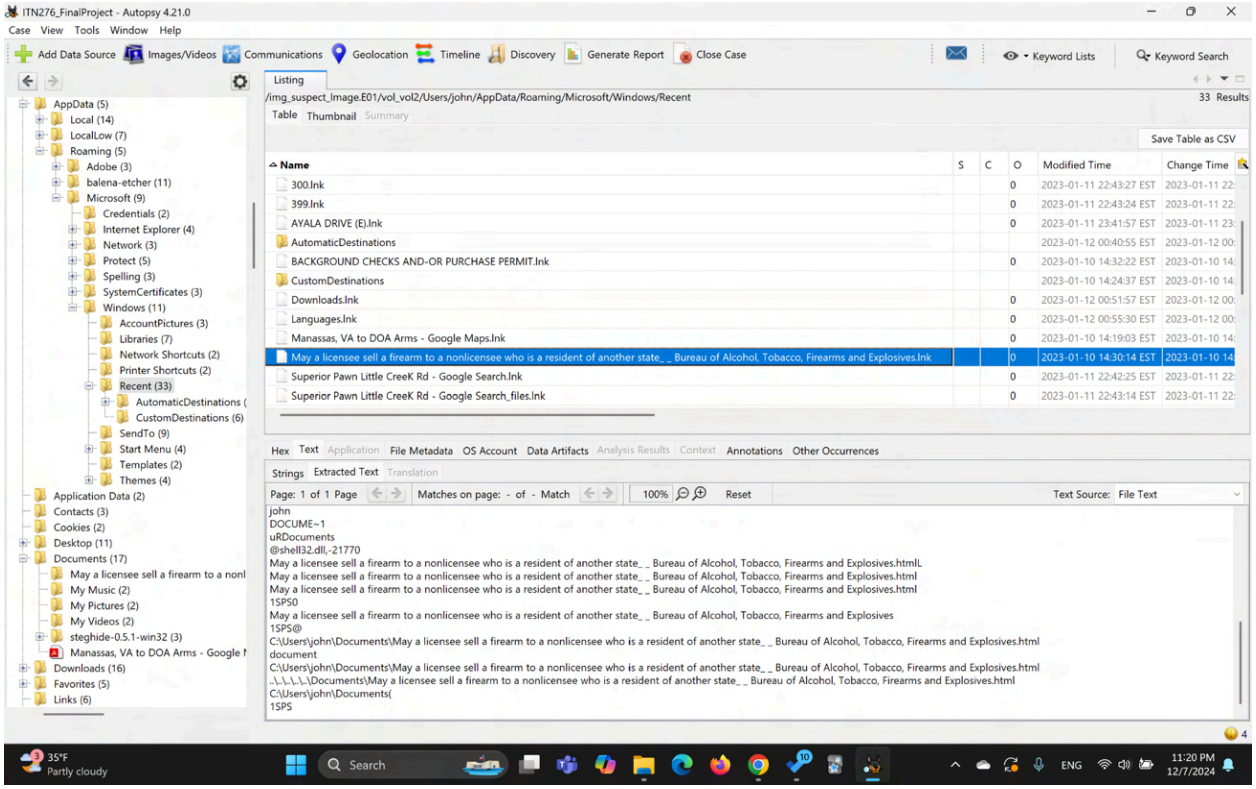

Figure 11.1: showing John searched “May a licensee sell a firearm to a nonlicensee who is a resident of another state_ _ Bureau of Alcohol, Tobacco, Firearms and Explosives” on the web

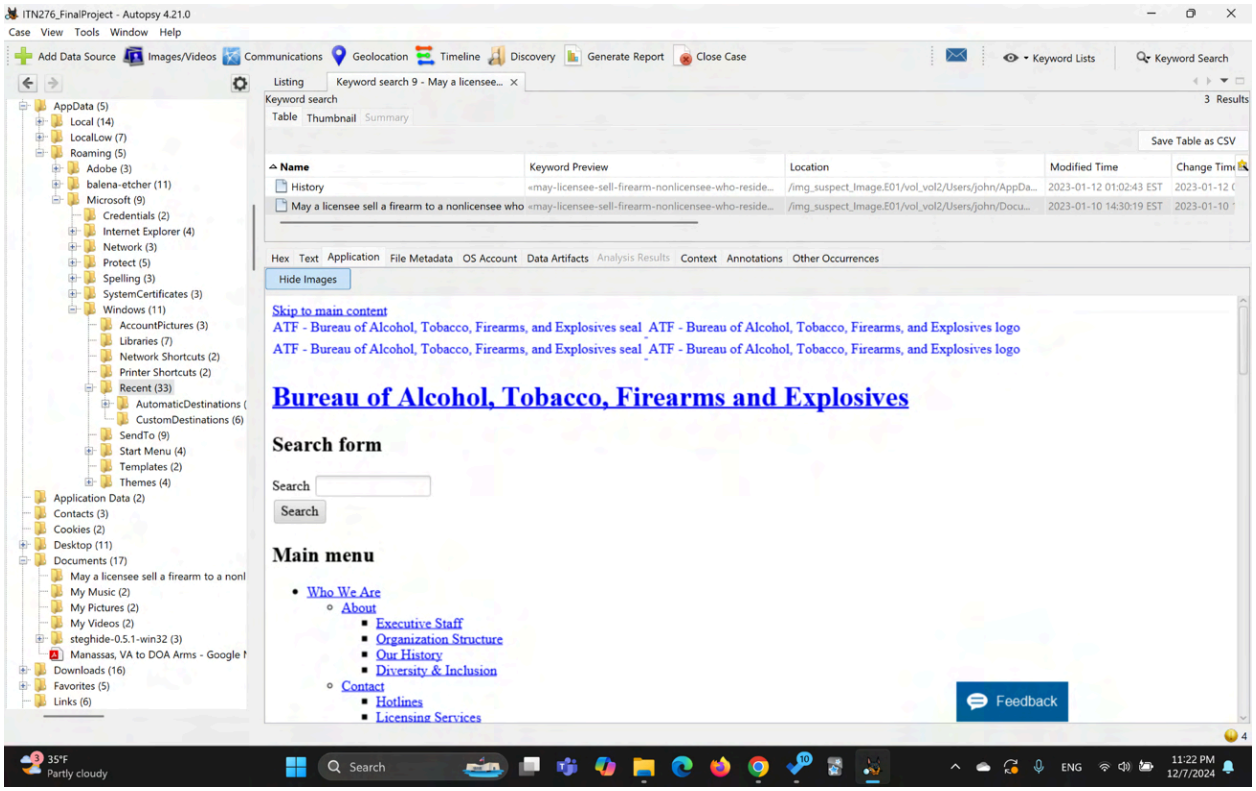

Figure 11.2: showing the content of the search result “May a licensee sell a firearm to a nonlicensee who is a resident of another state_ _ Bureau of Alcohol, Tobacco, Firearms and Explosives” that John accessed

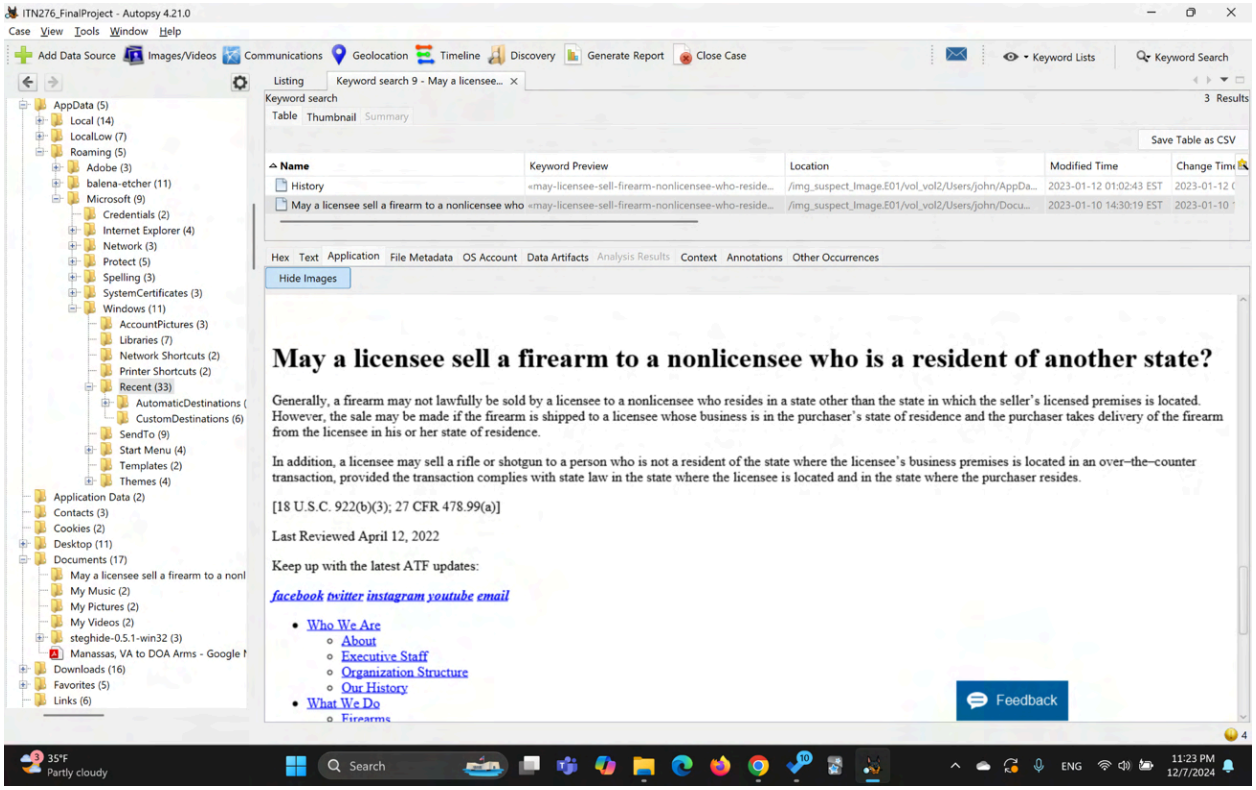

Figure 11.3: showing the content of the search result "May a licensee sell a firearm to a nonlicensee who is a resident of another state_ _ Bureau of Alcohol, Tobacco, Firearms and Explosives" indicating that John has intention to do something with selling firearm to clients

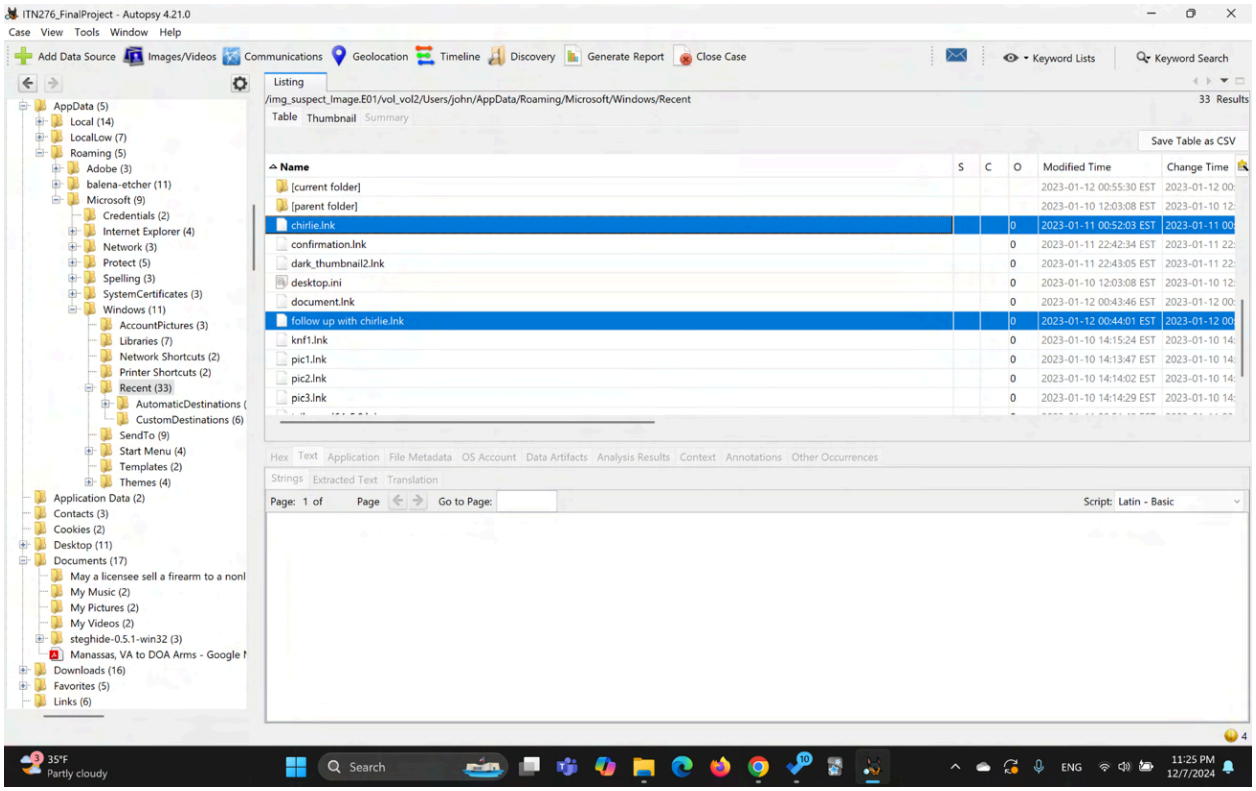

Figure 12.1: showing potential client or dealer "Chirlie"

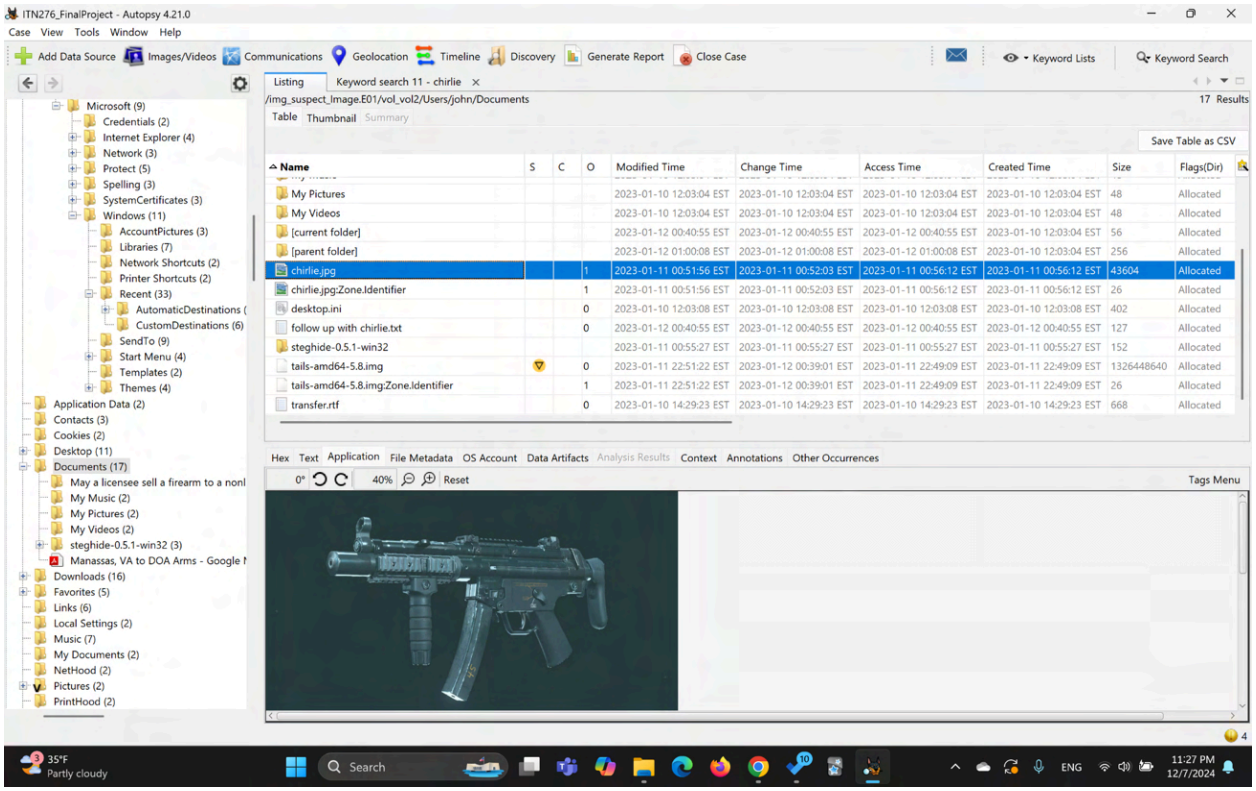

Figure 12.2: showing photo of Chirlie.jpg proving that John has something to do with firearm case

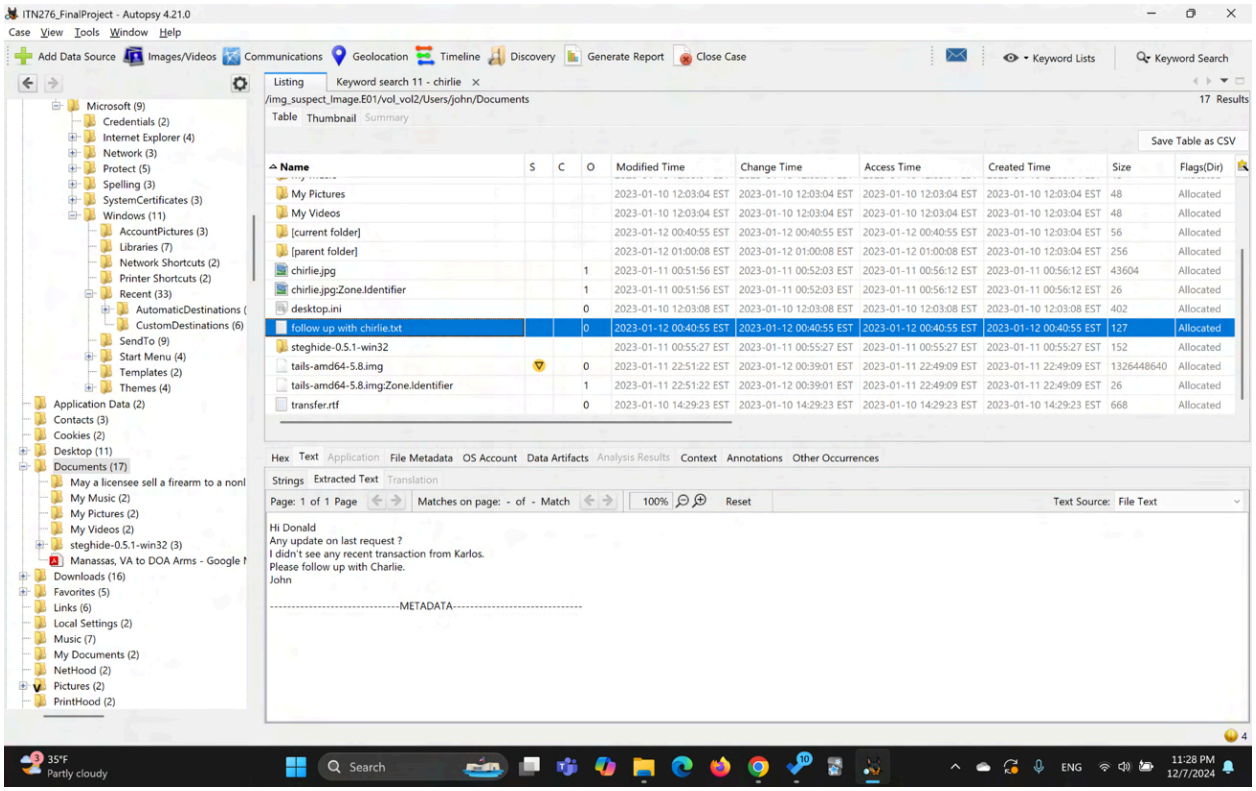

Figure 12.3: "follow up with chirlie.txt" revealing other people (Donald, Karlos, Charlie) who could also be involving in the case

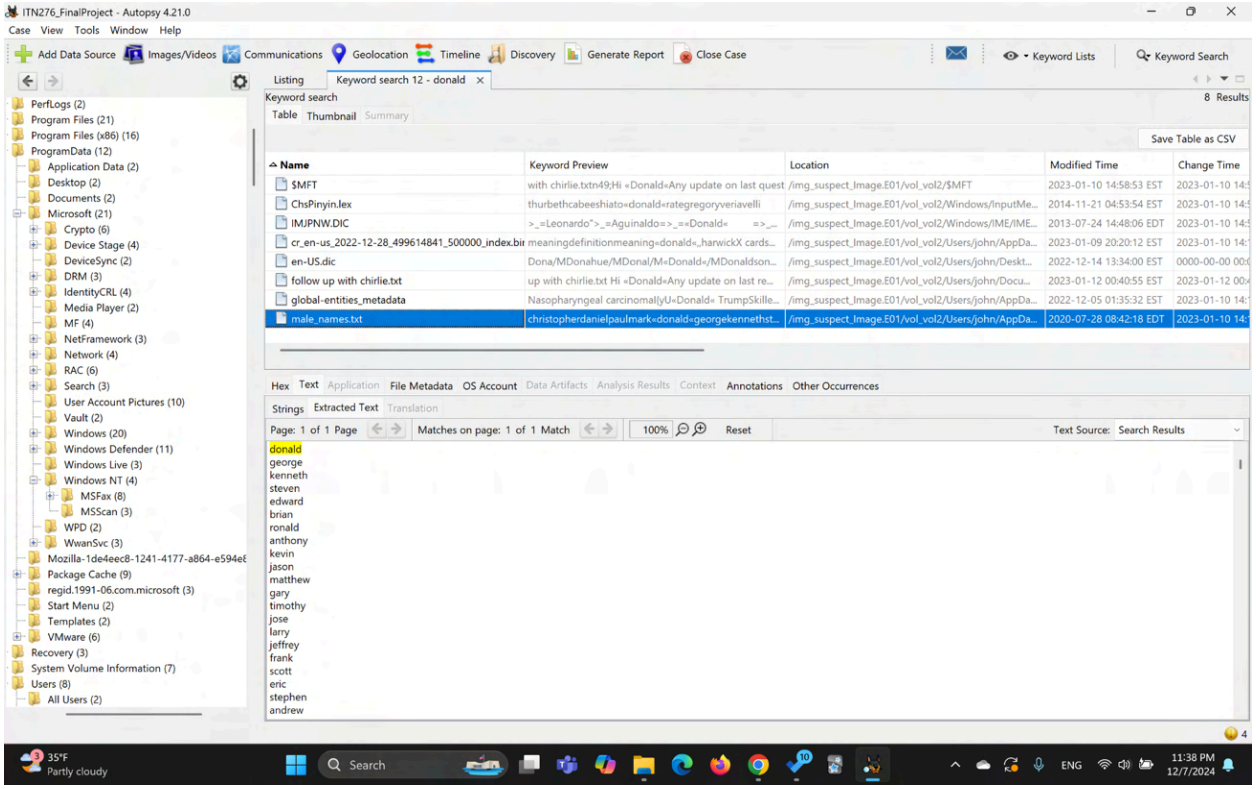

Figure 13.1: result of keyword “Donald”, suspicious file naming “male_names.txt”, the file path “ /img_suspect_Image.E01/vol_vol2/Users/john/AppData/Local/Google/Chrome/User Data/ZxcvbnData/1/male_names.txt”

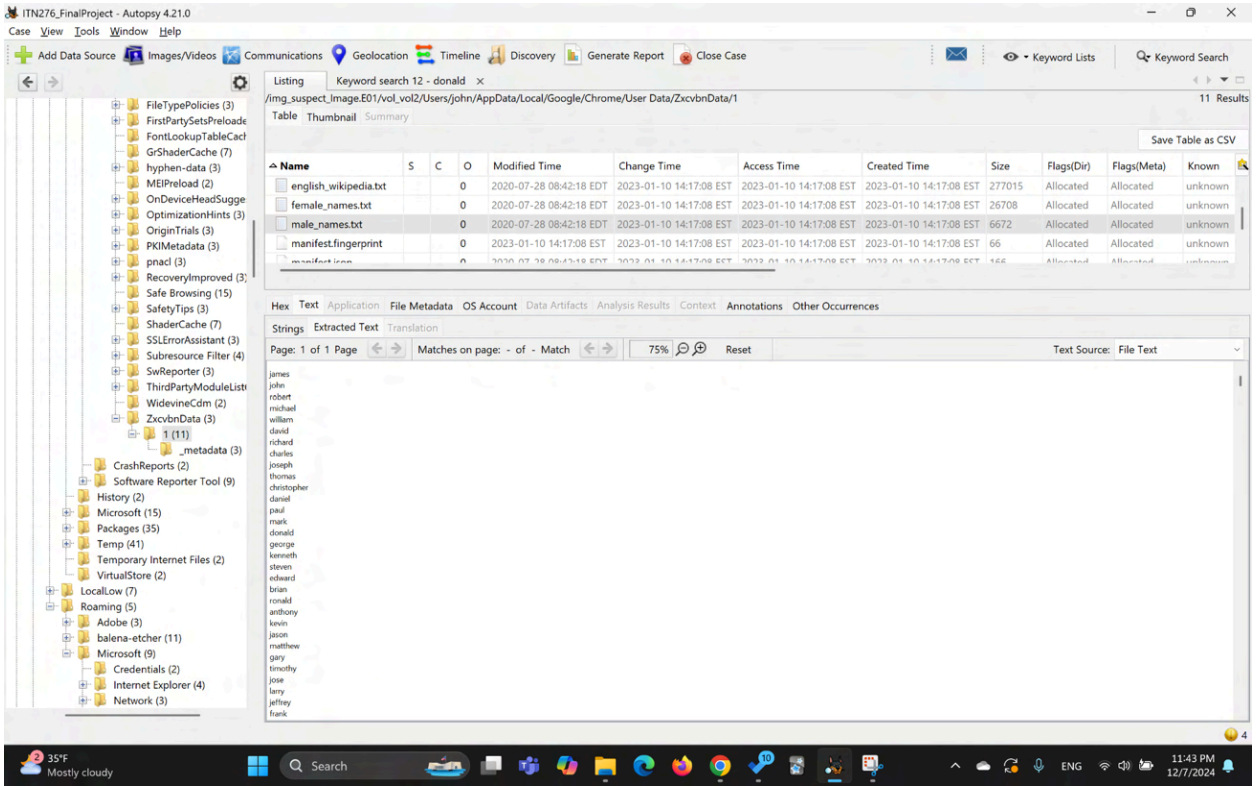

Figure 13.2: showing content of the file “male_names.txt”

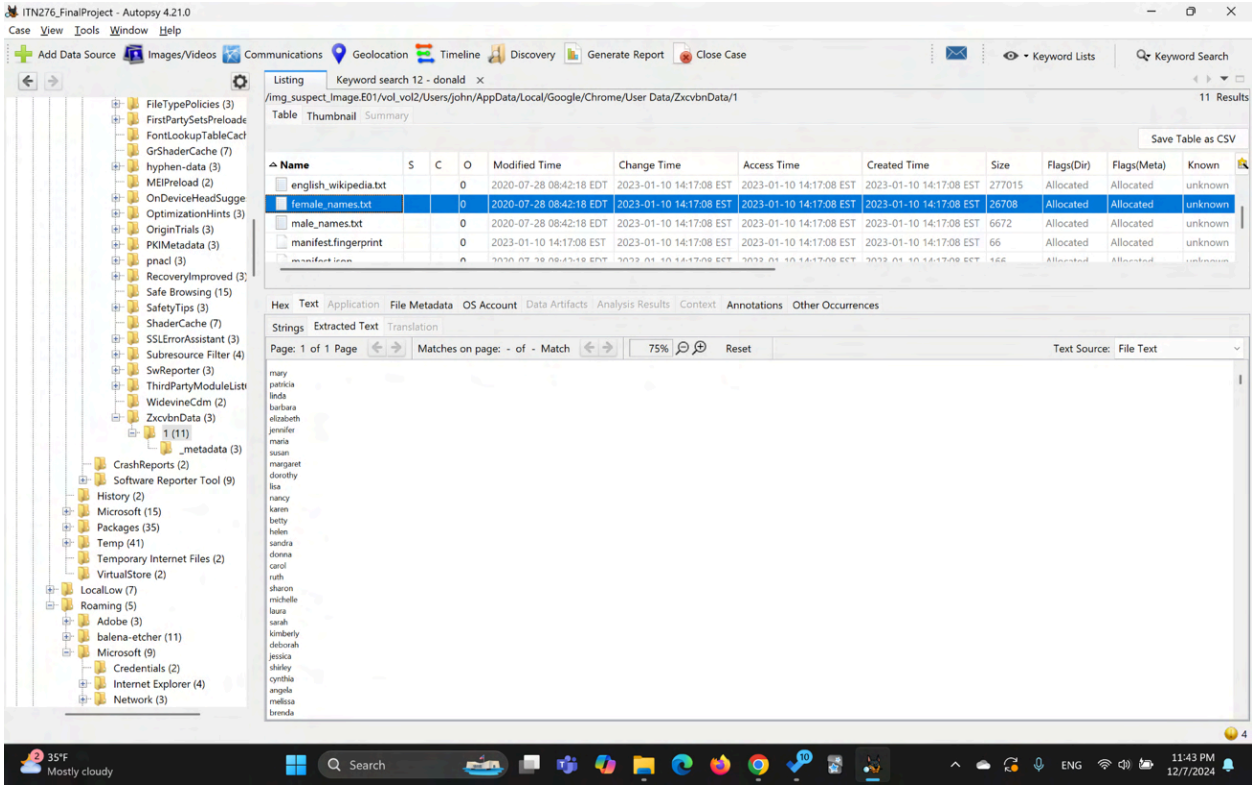

Figure 13.3: showing the content of the file “female_names.txt”

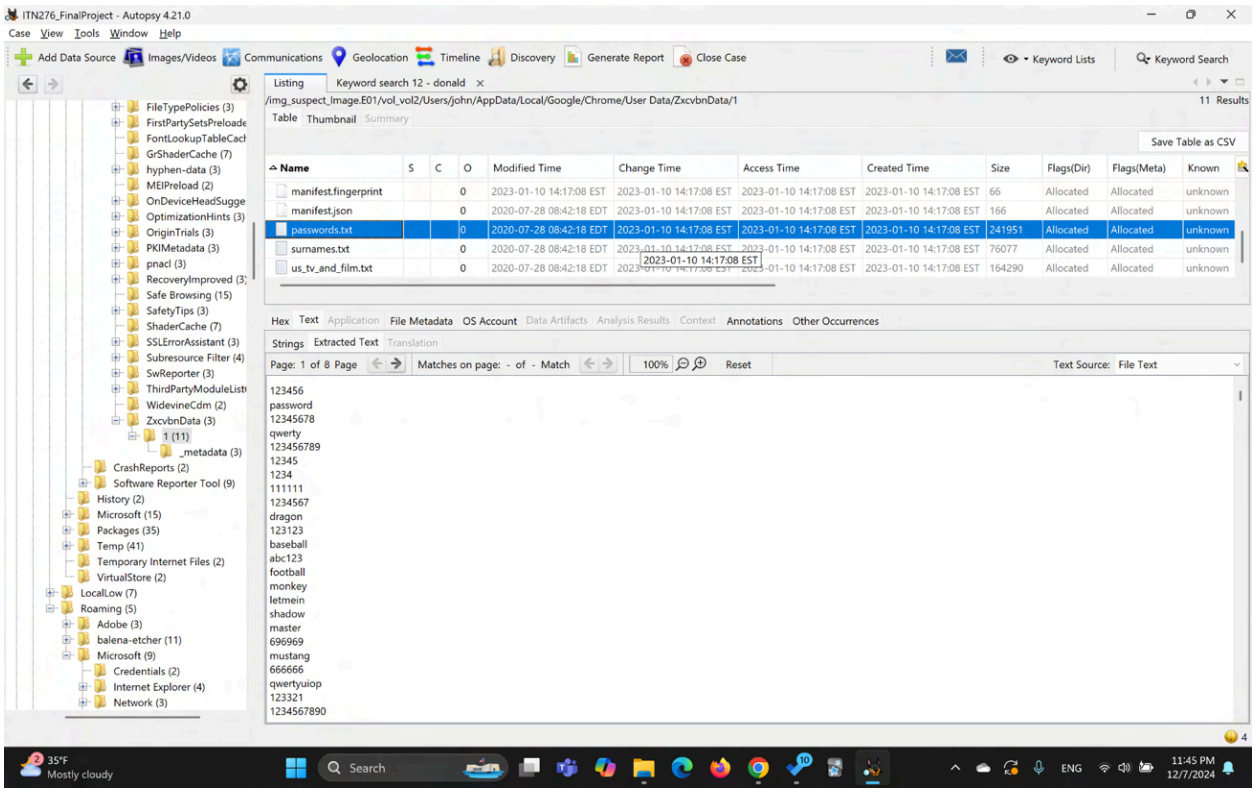

Figure 13.4: showing the content of the “password.txt” file

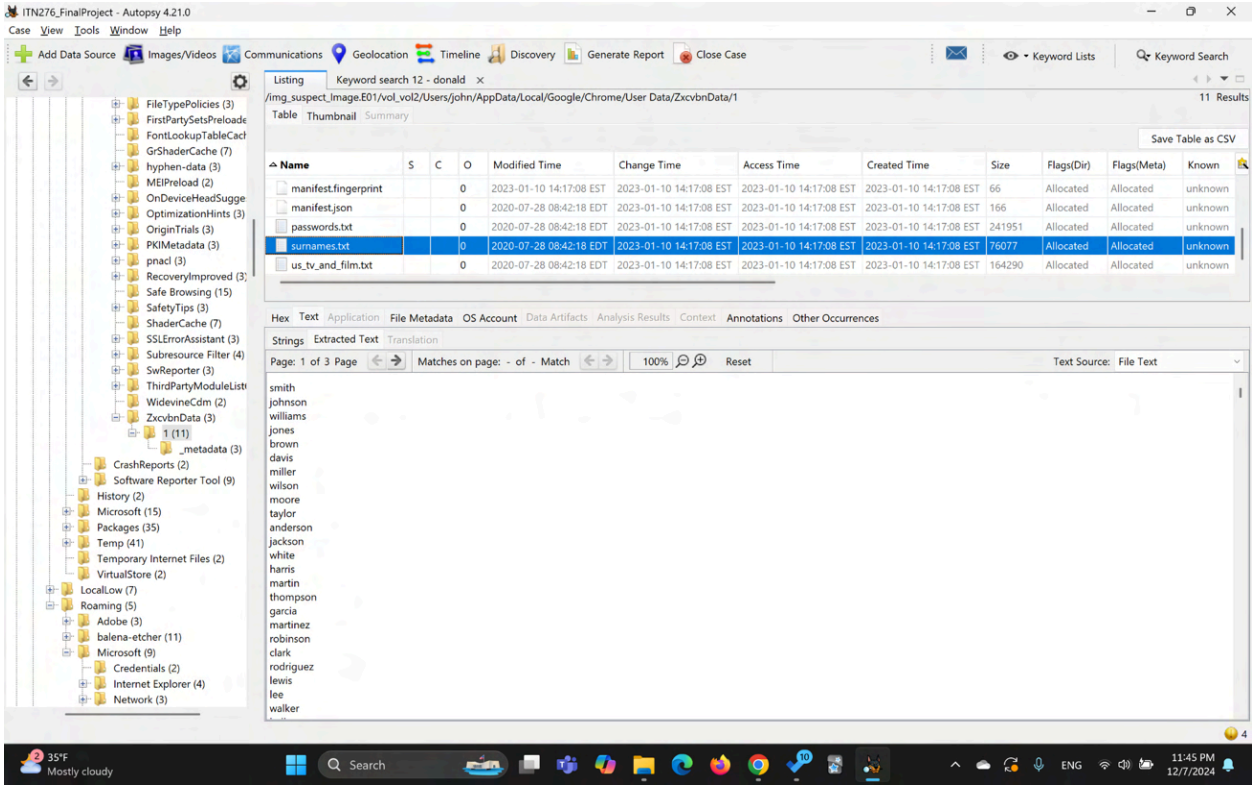

Figure 13.5: showing the content of the “surname.txt” file

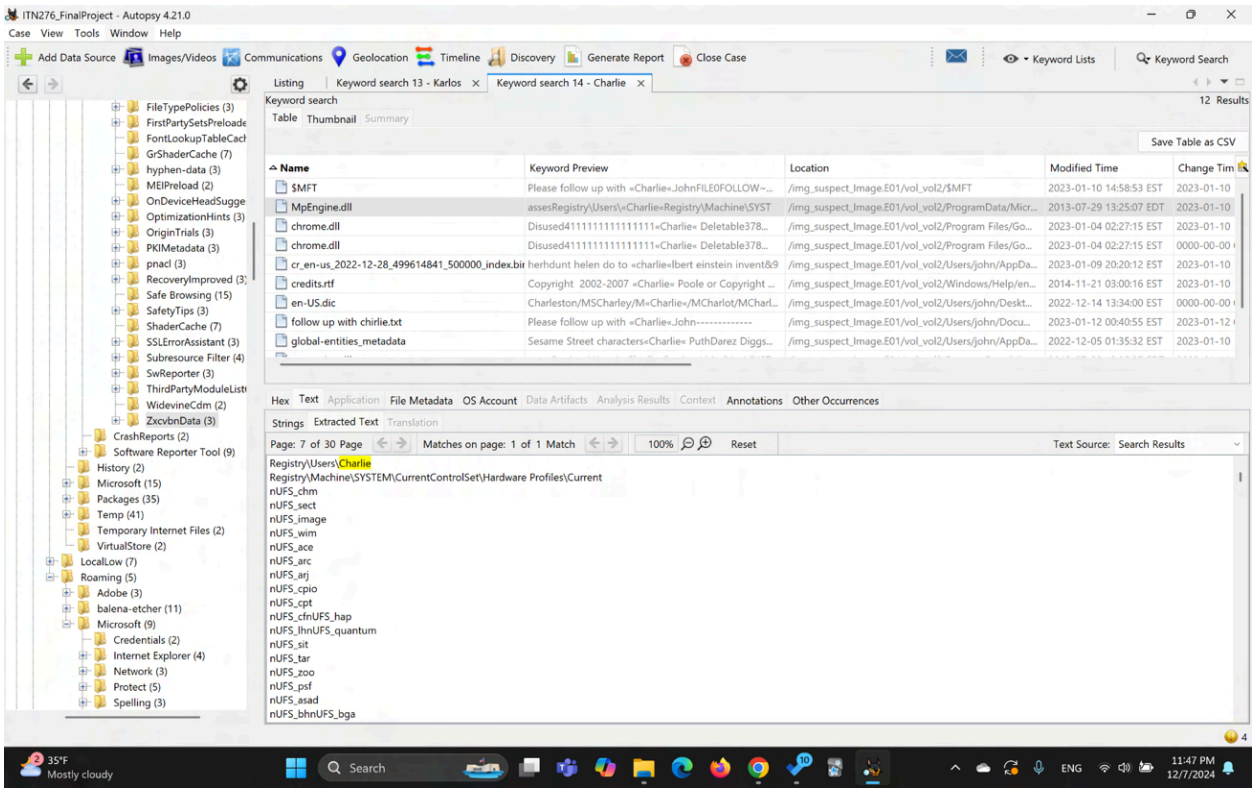

Figure 13.6: showing the search result of the “Charlie” keyword and found that there is Charlie is one of the users in the registry

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

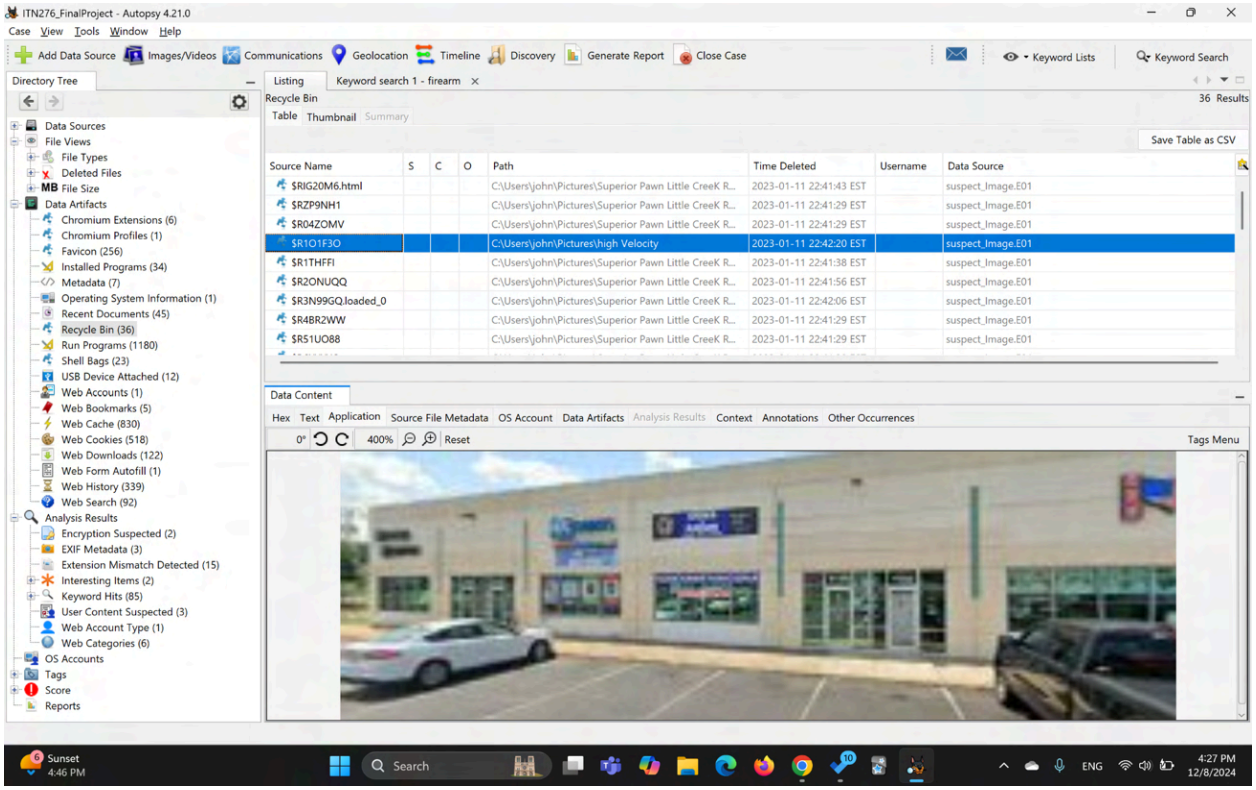

Figure 14: image $R1O1F3O

Metadata

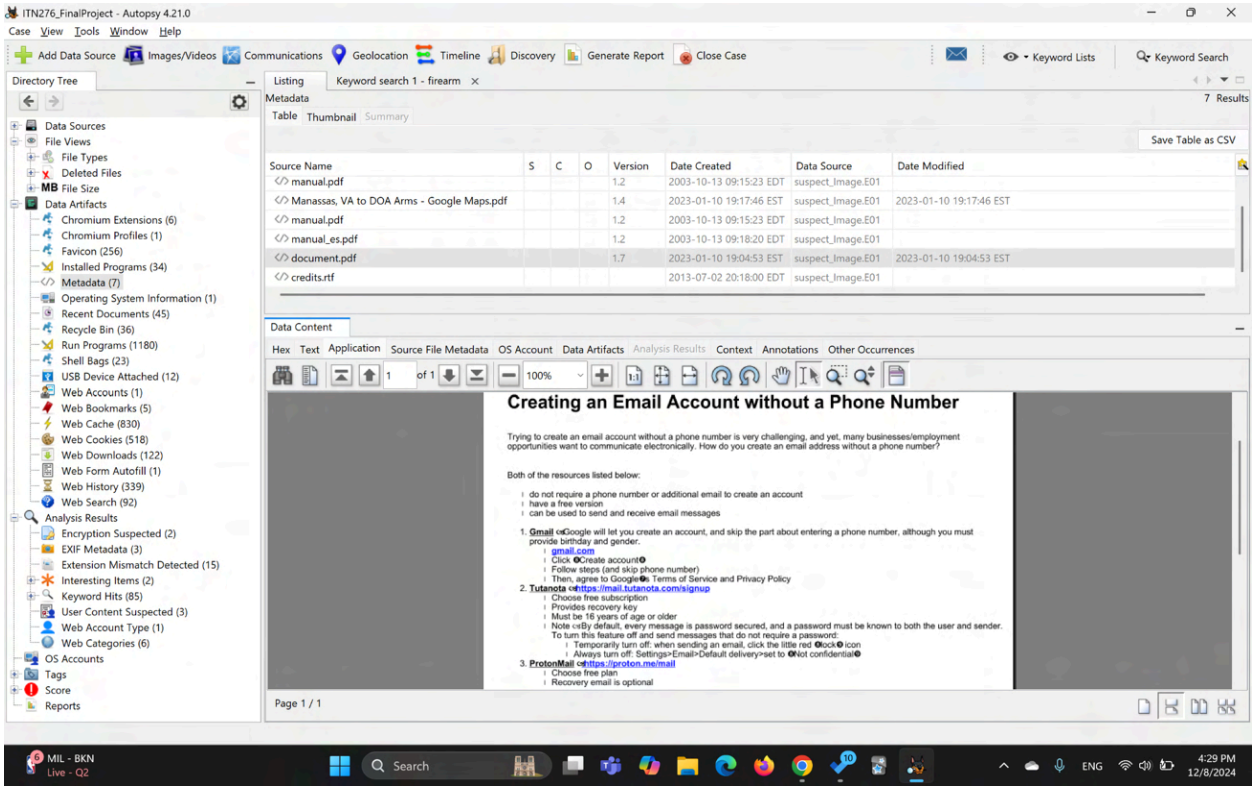

Figure 15: showing John was finding information to create an email account without a phone number

Web Accounts

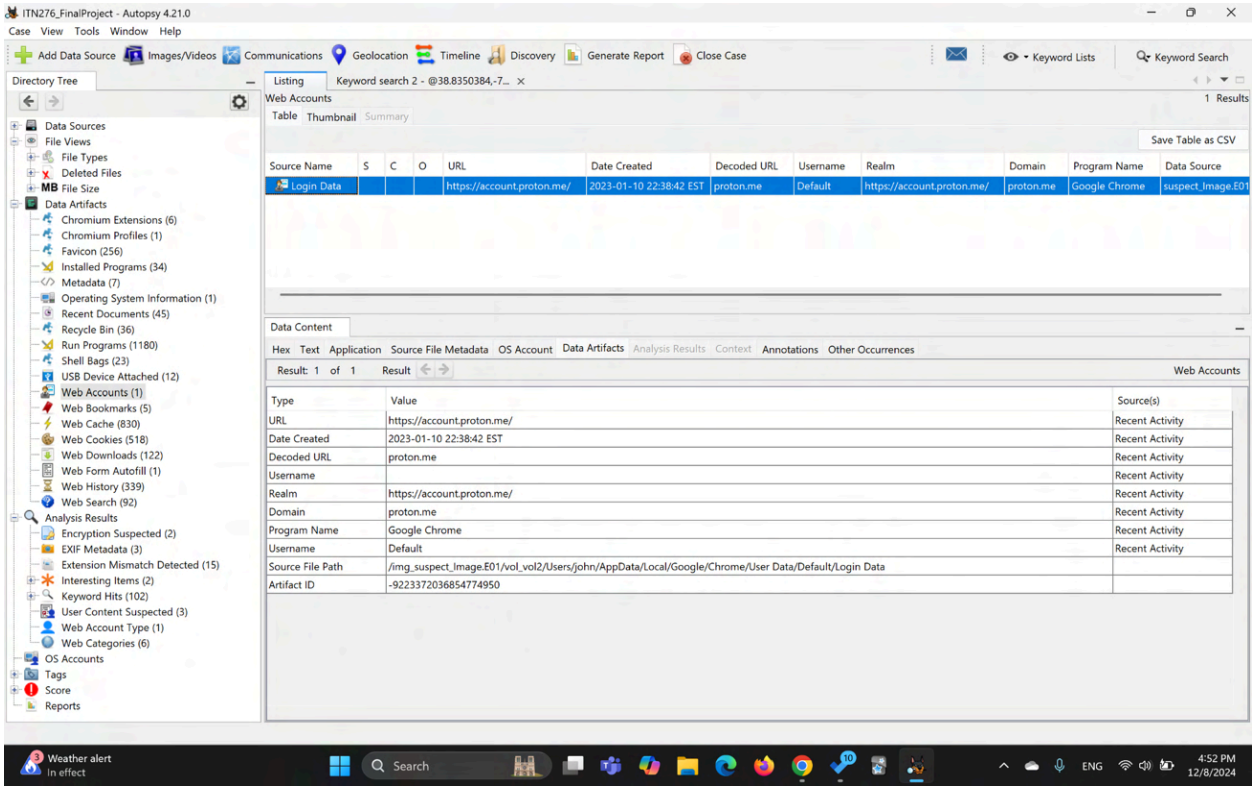

Figure 16: showing John using proton mail (which was one of the secure email and able to use without phone number), high possibility to contact his partners via proton mail

Web Bookmarks

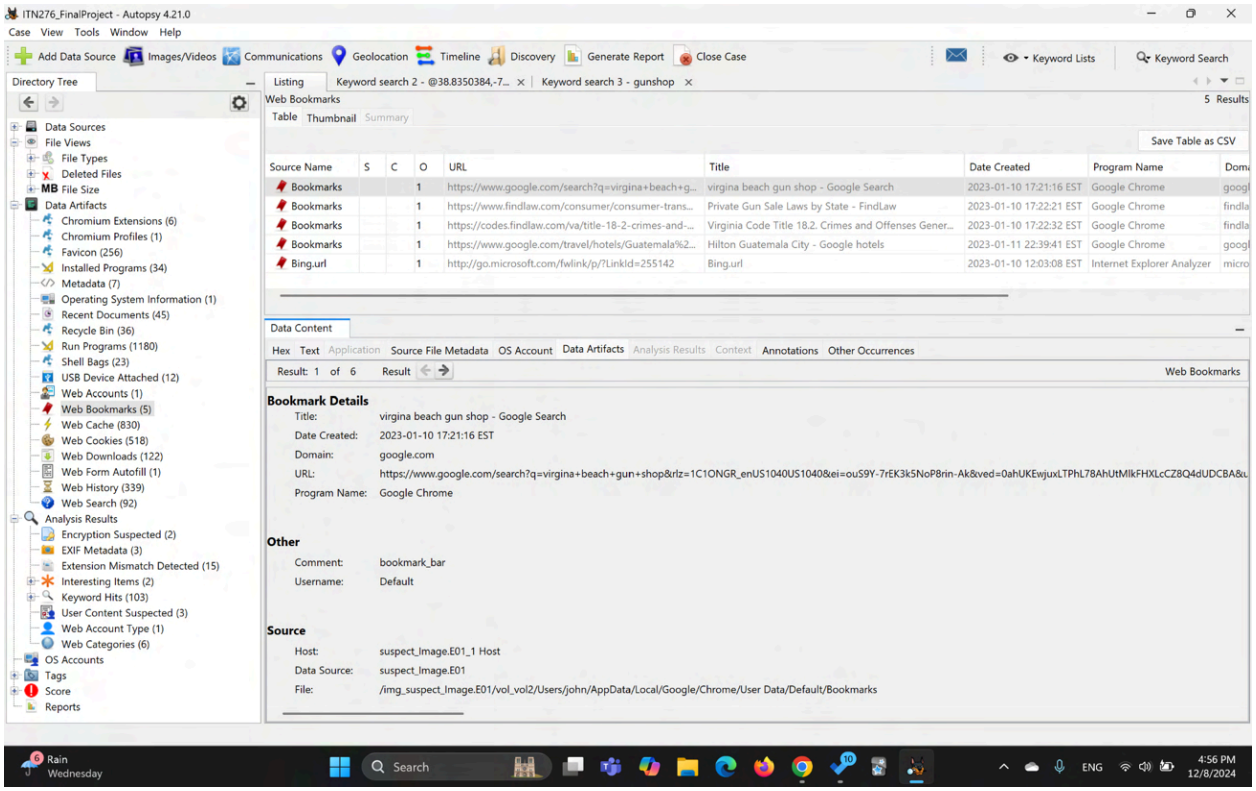

Figure 17: showing John bookmarked some of the search result for easy access (virginia beach gun shop, about private gun sale laws by state, Virginia Code Title 18.2 Crimes and Offenses, Hilton Guatemala city hotels)

Web Cache

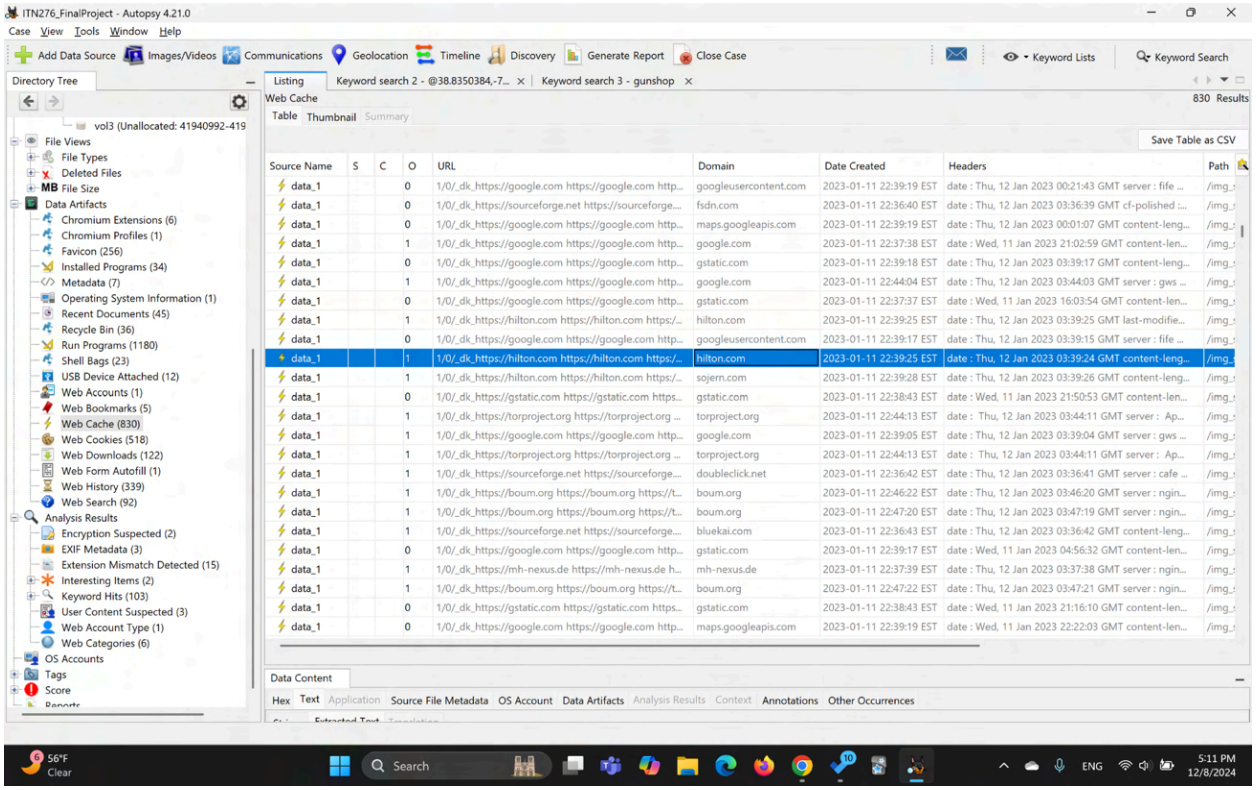

Figure 18: showing the result of the cache, hilton hotel could probably be one of the place they are staying and need to investigate the room physically

Web Cookies

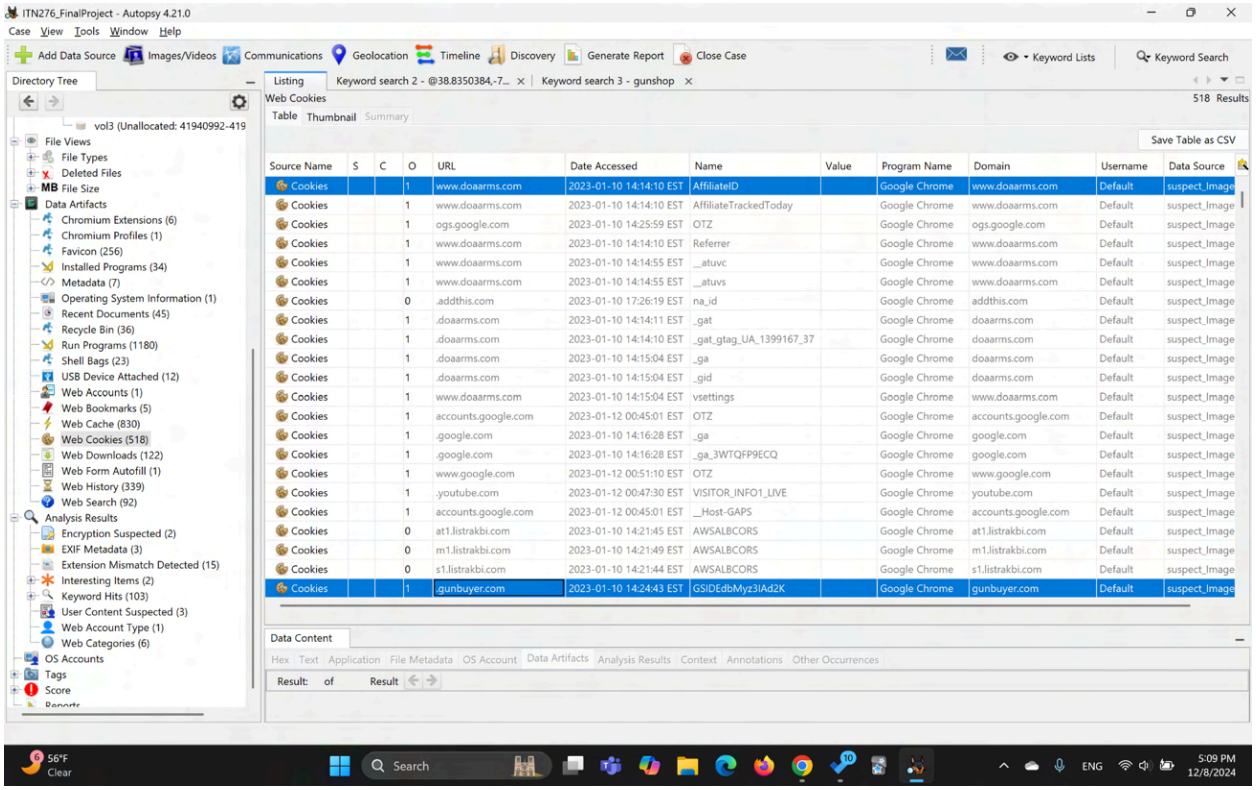

Figure 19: showing web domains related to firearm case

Web Downloads

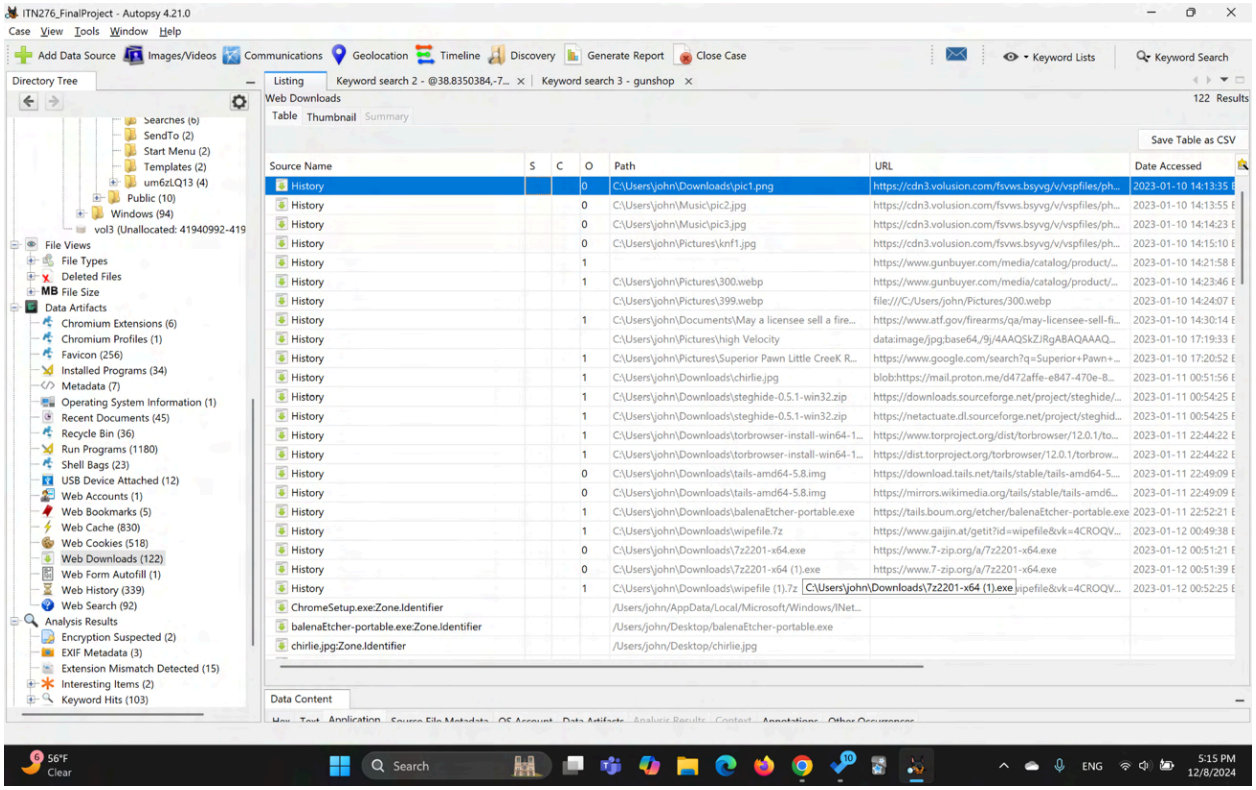

Figure 20: showing the files that John had downloaded, noted that there are image files in the Music folder which needs to be checked

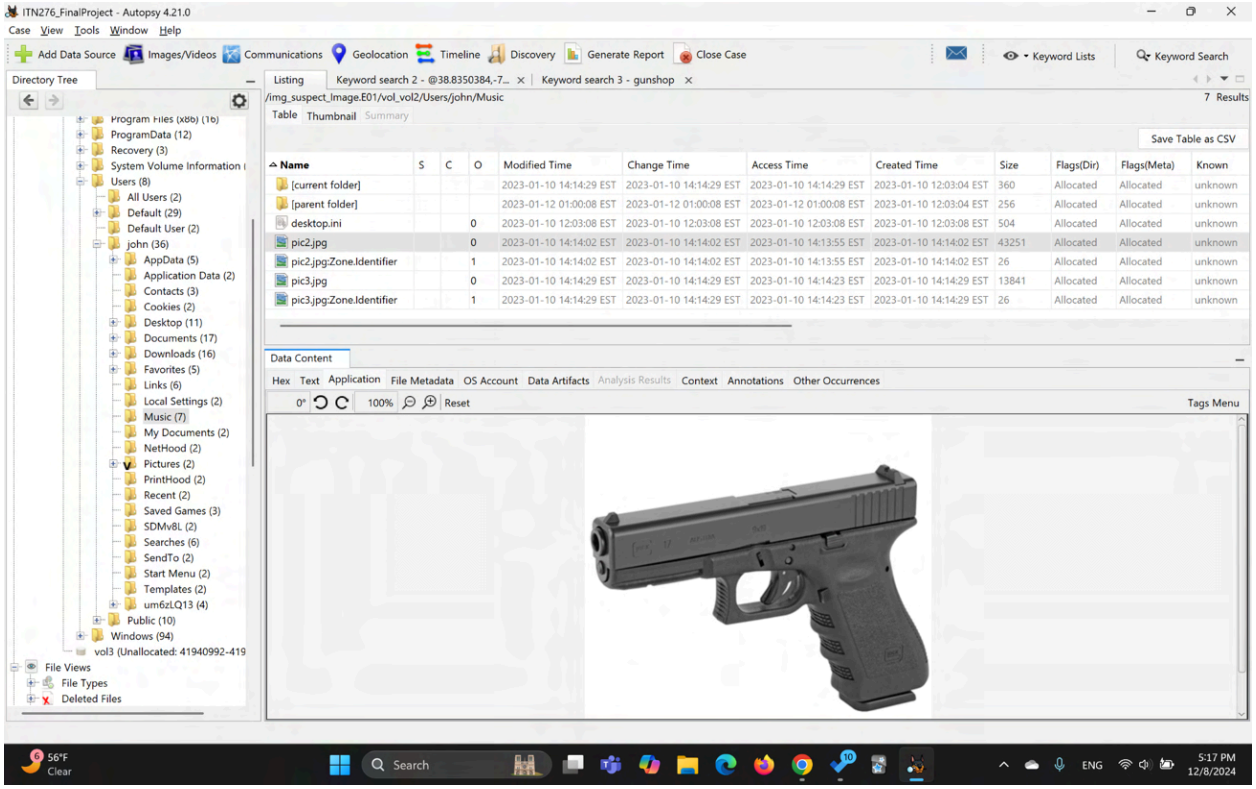

Figure 20.1: showing the pic2.jpg under Music folder of user John

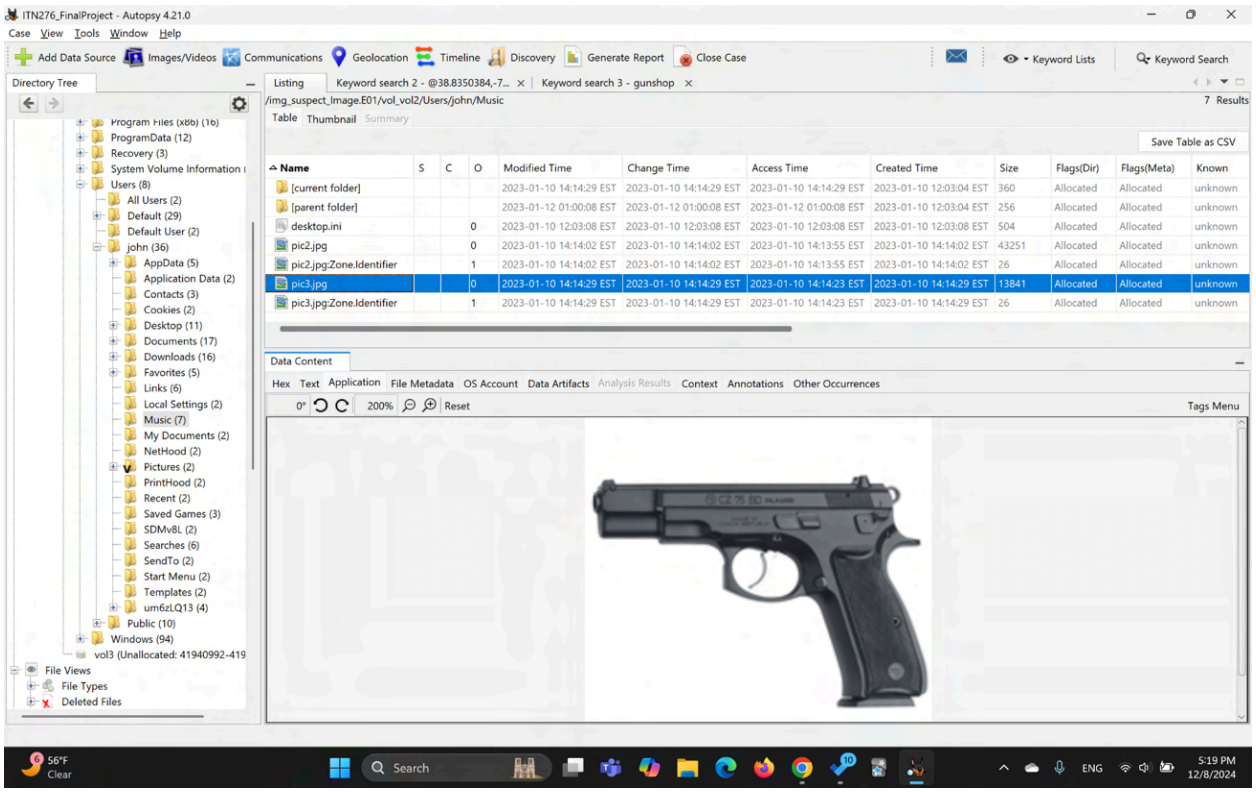

Figure 20.2: showing the pic3.jpg under Music folder of user John

Web History

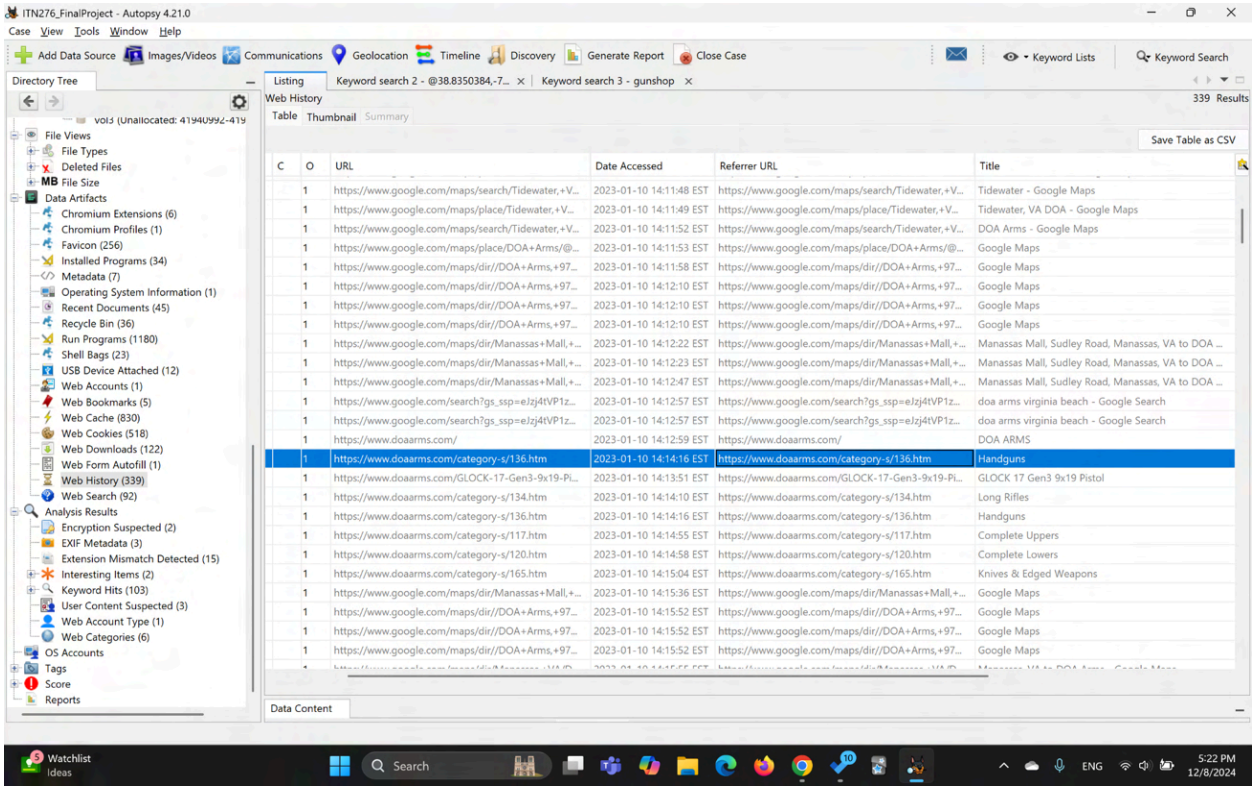

Figure 21: showing what John was finding on the web, proving that he was browsing weapons and gun on the goaarms.com and how to get there by using google maps

Web Search

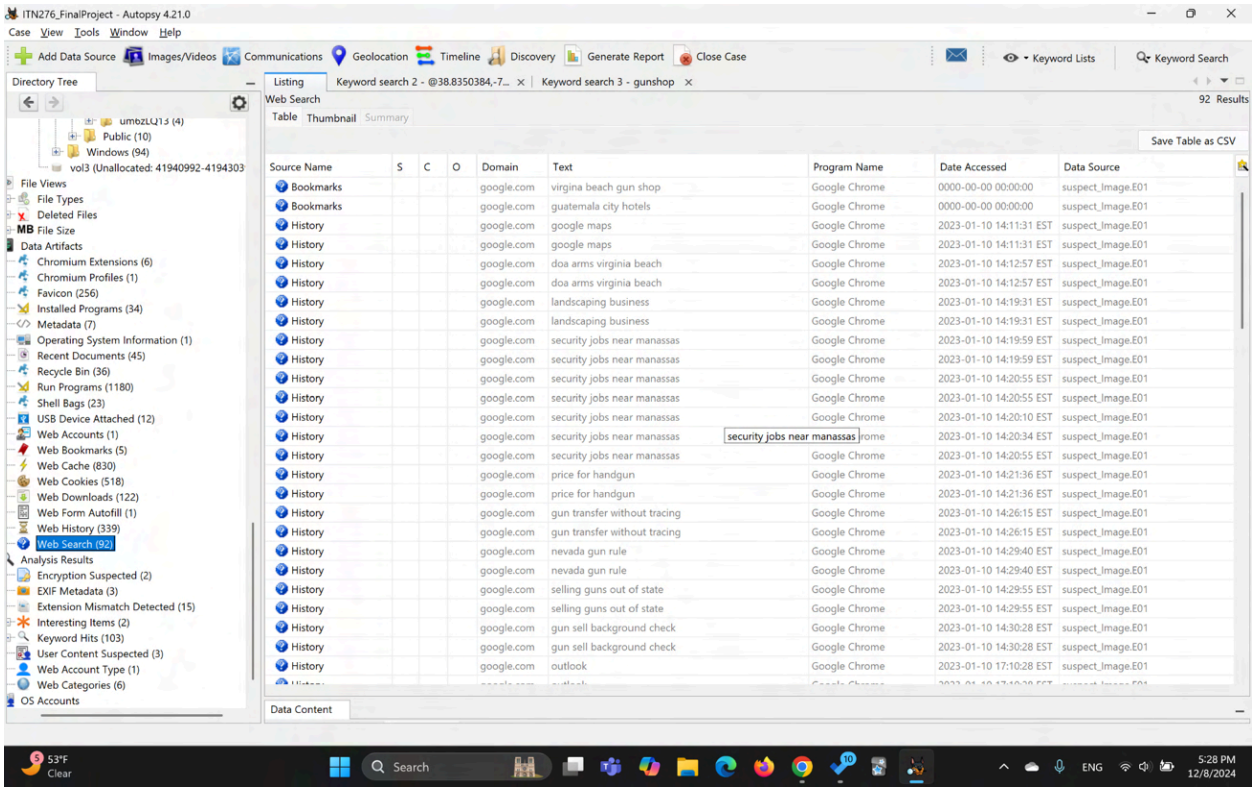

Figure 22.1: showing the result of web search (virginia beach gun shop, guatemala city hotels, doa gun shop, security jobs near manassas which indicate John might have been living in Manassas, price for handgun, gun transfer without tracing, nevada gun rule, selling gun outside the US, background check)

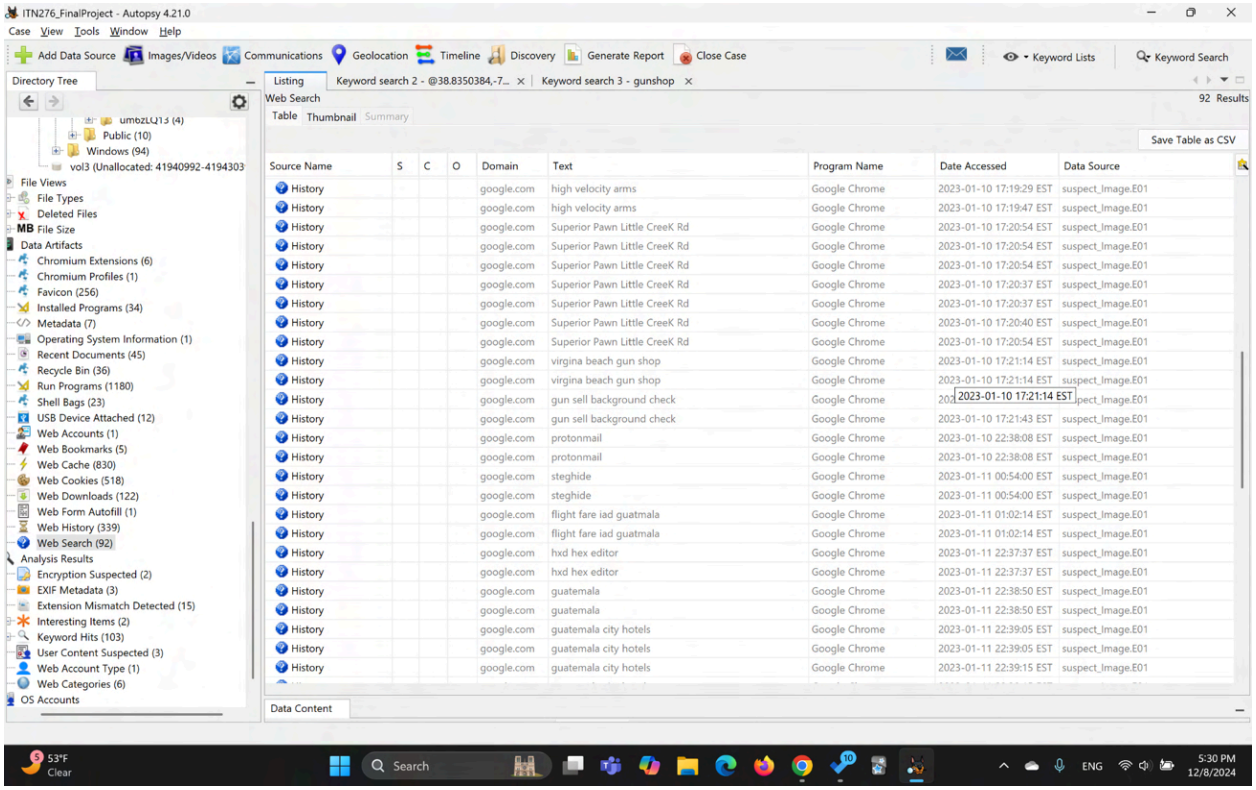

Figure 22.2: showing the result of web search (high velocity arms, superior pawn little creek road, protonmail, steghide, flight fare to IAD guatemala, hex editor)

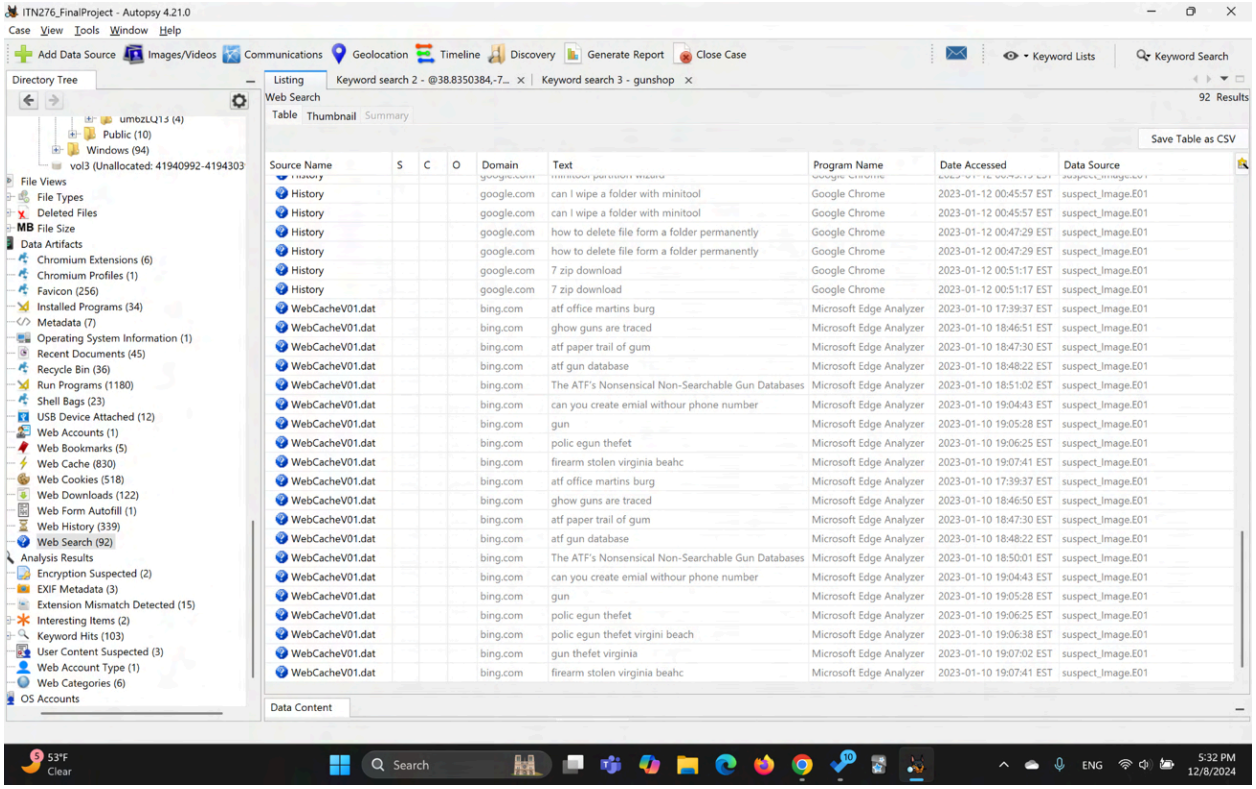

Figure 22.3: showing the result of web search (wiping a folder, deleting file permanently, arf office martins burg, guns, gun database, theft at virginia beach)

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)