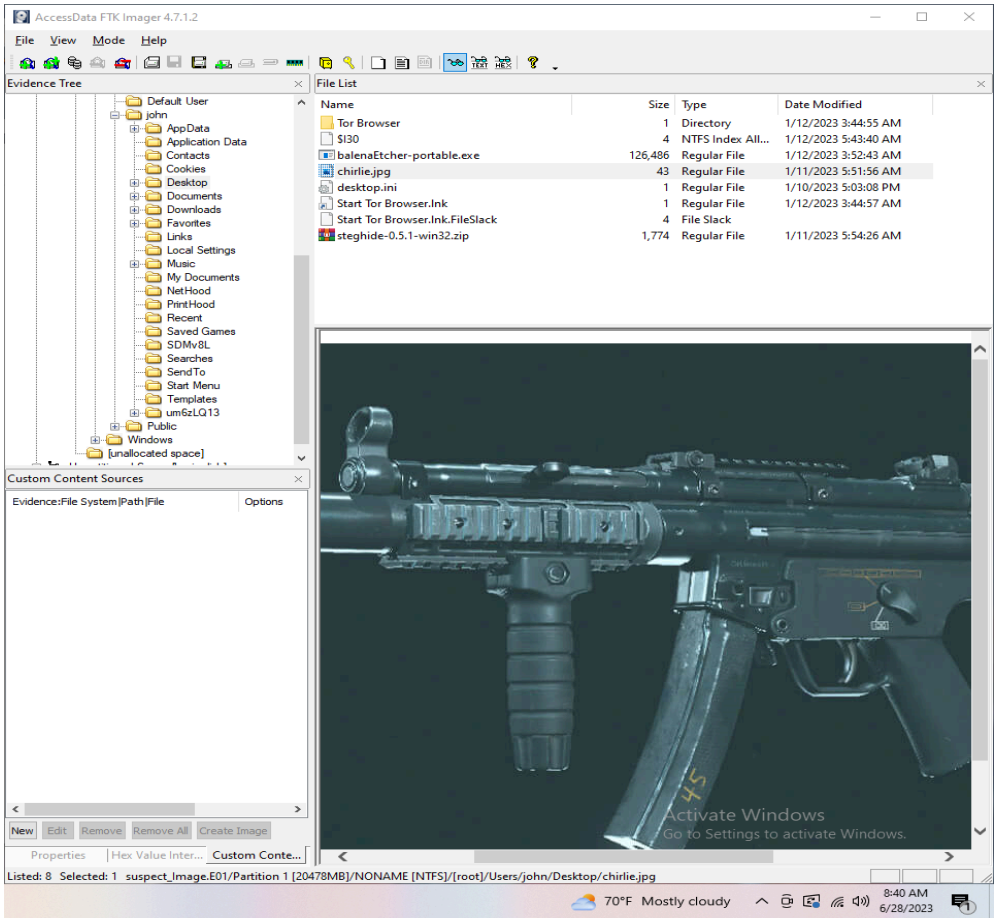
James Everett Tourtellotte IV
ITN 276 - Forensics Final Project Part II
7/1/2023
Deliverable of Suspect Image

On 28JUN2023 I booted up FTK Imager, and loaded the suspect_image file into the program. FTK Imager is a data preview and imaging tool used in digital forensics. It helps users create exact copies of a computer system, hard drive, or disk for investigation while preserving the original evidence, enabling analysis without compromising data integrity. The following forensic examination was done to the best of my ability in regards to the image at hand. The process of said forensic examination was lengthy, and quite difficult - however as we know, it is the duty of a forensic analyst to be thorough in their investigation. The best of my ability was given in this process.

We start out by finding that the file system on this drive is NTFS, which is used with the Windows Operating System. In terms of total users, we saw two technically. The default user and user named John. John, being specific in name, is the primary target of concern. Of course, some digging was done in the Default User user but John was the primary focus here. We have a specific name, who is likely our suspect so this forensic examination focuses primarily on him.

In an attempt to analyze the artifacts within this computer efficaciously, I tried to put myself in the shoes of the average individual. I attempted to approach this unbiasedly, as my first inclination was “put myself in the shoes of a criminal”. If I were to do that, it would be too broad and not honest in regards to my “intentions” - which are to present the facts and the facts alone. Now, putting myself in the shoes of someone who is “technologically illiterate” is not bias at all. This allowed me to assume he is like any careless user who just downloads files willy-nilly and stores them in places you would expect to find them. We start with this approach by analyzing the documents in the Desktop, Downloads, and Documents directories.

I opened the root folder, I went to Users, then went to John. On the Desktop directory I found a picture of an MP5 in a jpg titled “chirlie”. Below is figure A: which is a screen capture of the Desktop folder containing said MP5 image and a few more important findings. Among the picture of the gun, you find a zip file for a program called “steghide”. Steghide is a steganography program that hides sensitive information within digital files. It supports a variety of file formats like JPEG, BMP, WAV, and AU. It offers encryption, compression, and embedding of data, ensuring concealed data cannot be detected or extracted without the appropriate passphrase. This is an anti-forensics program, which might be used in an effort to hide incriminating information. Also pictured below are files related to the Tor Browser. The Tor Browser is a web browser focused on privacy and anonymity. It routes internet traffic through the Tor network, obscuring users' identities and activities from surveillance and traffic analysis. This browser also can be used for Anti-Forensics.



I kept searching to find more about this User John and his activities, again by putting myself into the shoes of a careless technology user. This led me to the Documents folder. The documents folder had a plethora of interesting pieces. We see at the top, a folder titled “May a licensee sell a firearm to a nonlicensee….” - the folder is titled as a question that is relevant to USA gun laws. This is a reference to a query about a gun loophole in regards to the law. While questions are not illegal, I decided to probe more. You can see that there is a PDF involving Manassas VA to DOA arms, Google Maps. The Map is directly after the screencaps of the Documents folder. This Maps route might imply intent to go to XYZ place and meet ABC person.

Figure B:

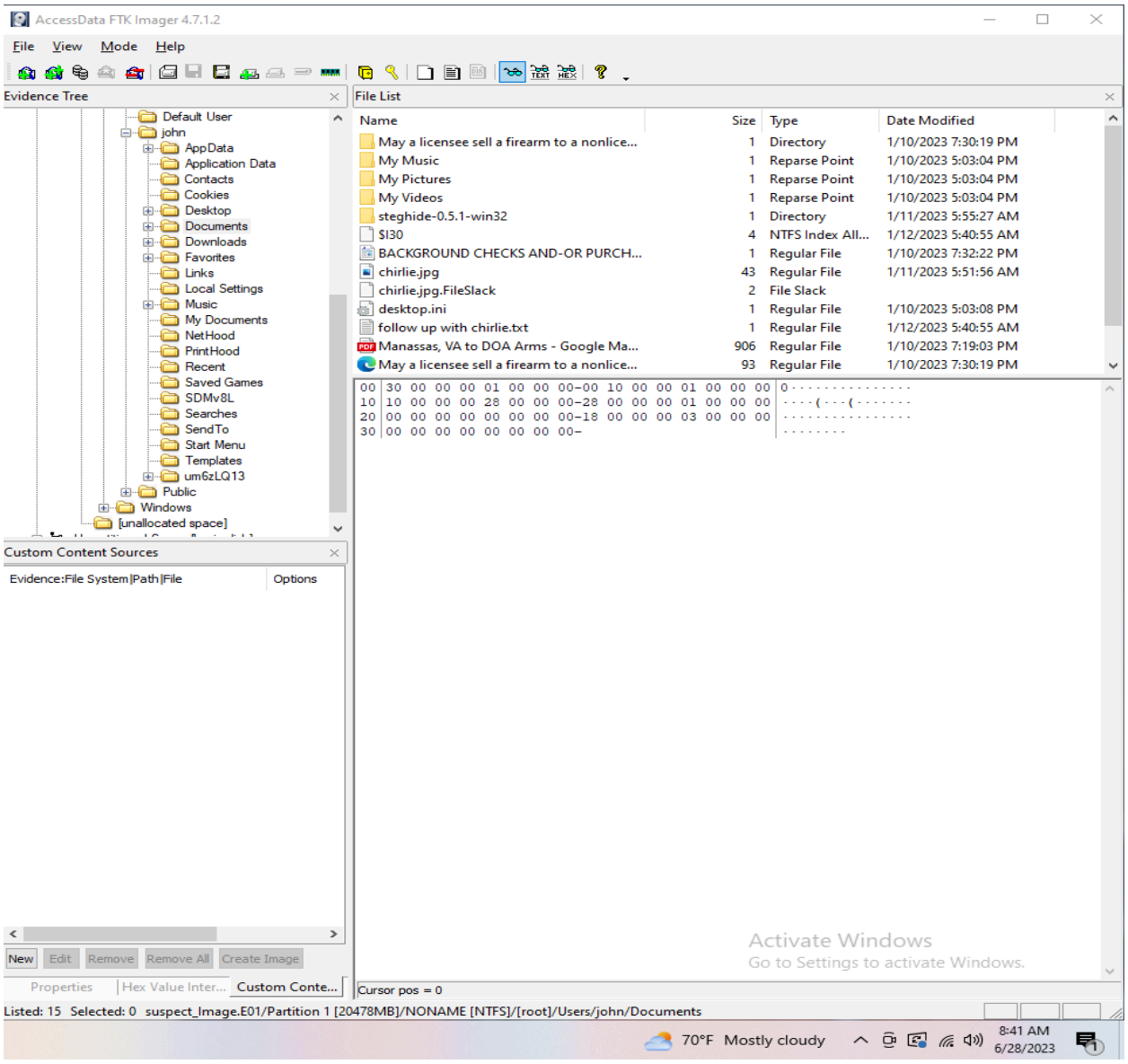
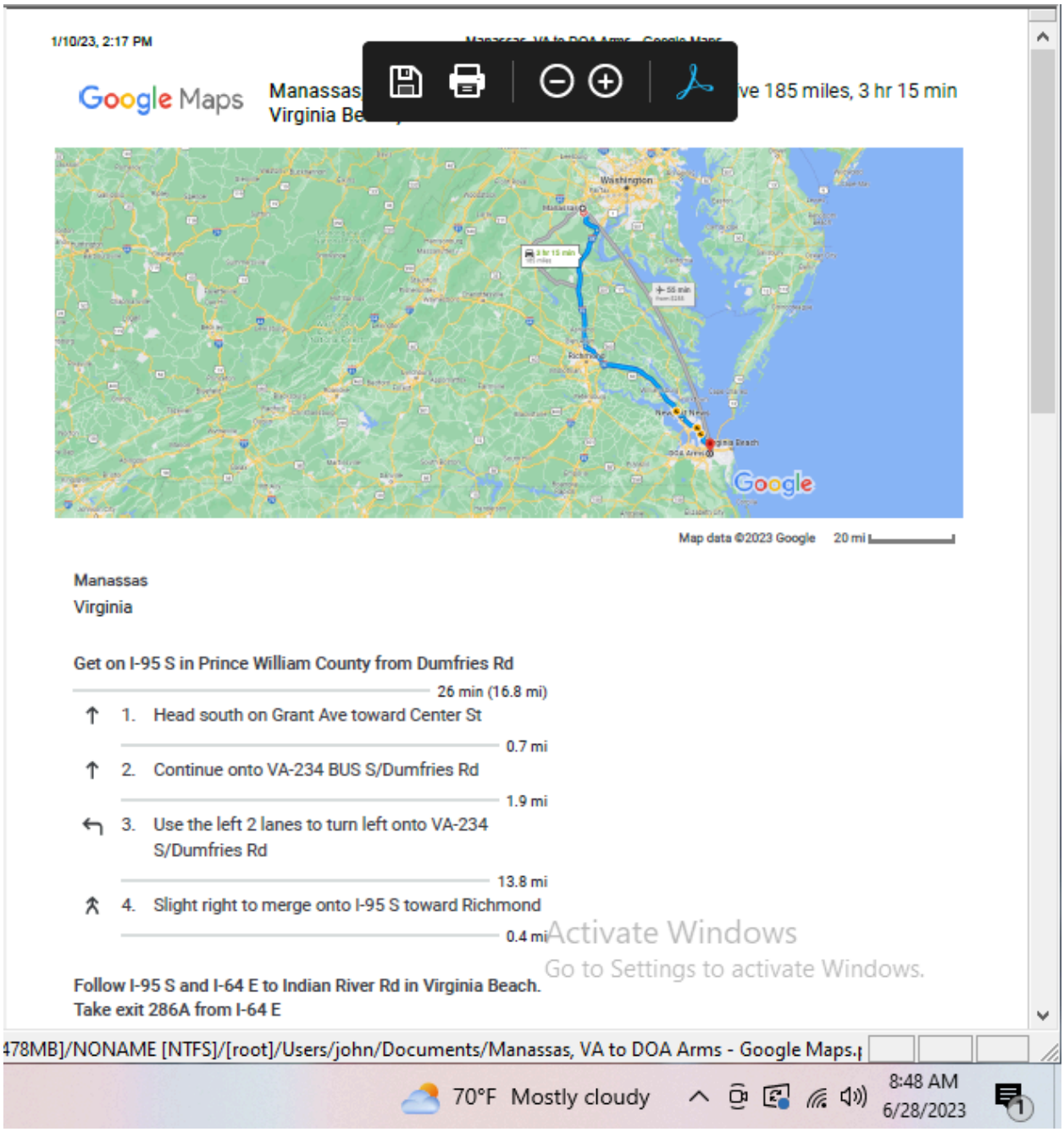
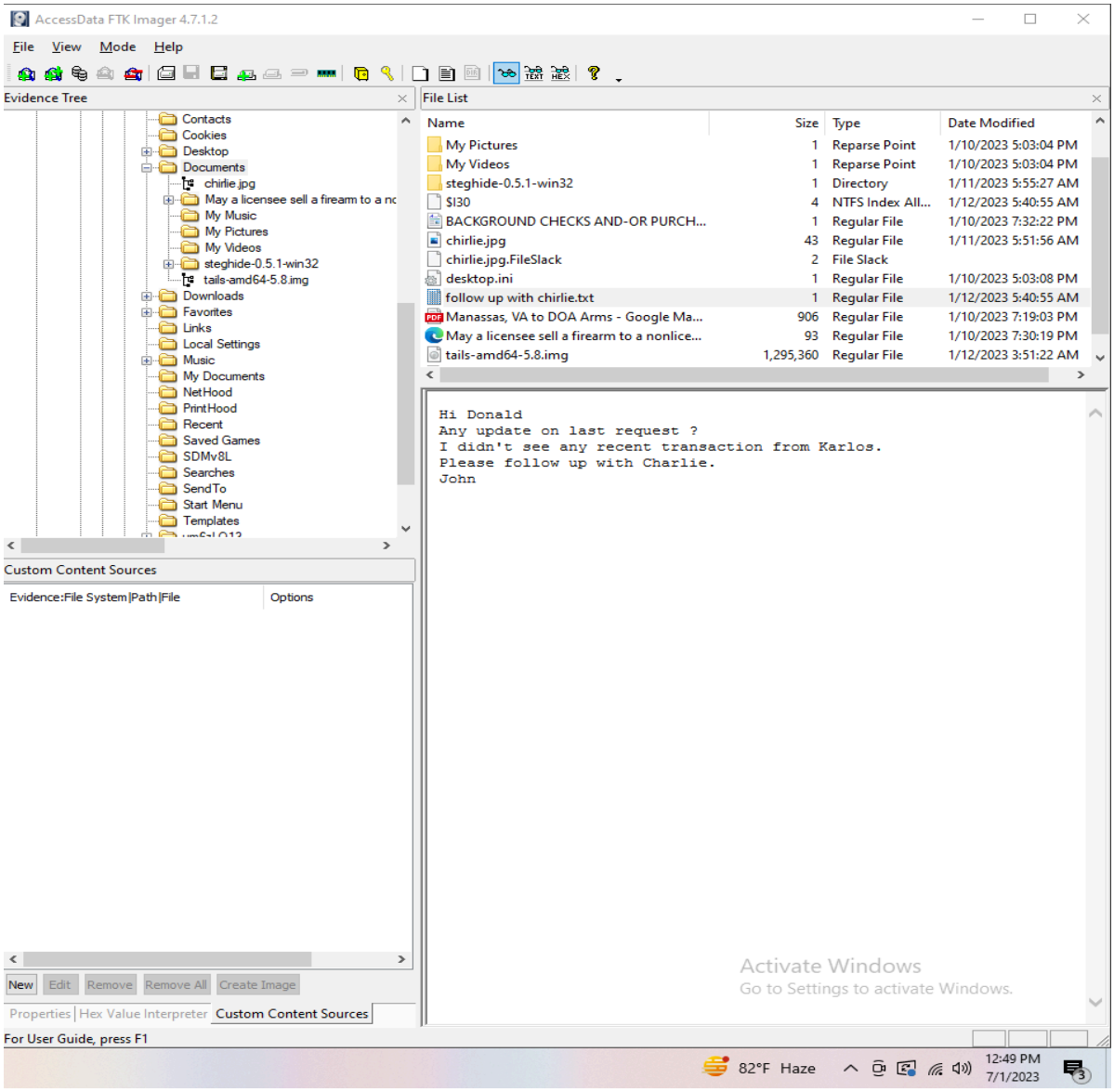

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
Default User
john
AppData
Application Data
Contacts
Cookies
Desktop
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood
PrintHood
Recent
Saved Games
SDMv8L
Searches
SendTo
Start Menu
Templates
um6zLQ13
Public
Windows
[unallocated space]
File List
Name Size Type Date Modified
May a licensee sell a firearm to a nonlice... 1 Directory 1/10/2023 7:30:19 PM
My Music 1 Reparse Point 1/10/2023 5:03:04 PM
My Pictures 1 Reparse Point 1/10/2023 5:03:04 PM
My Videos 1 Reparse Point 1/10/2023 5:03:04 PM
steghide-0.5.1-win32 1 Directory 1/11/2023 5:55:27 AM
$I30 4 NTFS Index All... 1/12/2023 5:40:55 AM
BACKGROUND CHECKS AND-OR PURCH... 1 Regular File 1/10/2023 7:32:22 PM
chirlie.jpg 43 Regular File 1/11/2023 5:51:56 AM
chirlie.jpg.FileSlack 2 File Slack
desktop.ini 1 Regular File 1/10/2023 5:03:08 PM
follow up with chirlie.txt 1 Regular File 1/12/2023 5:40:55 AM
Manassas, VA to DOA Arms - Google Ma... 906 Regular File 1/10/2023 7:19:03 PM
May a licensee sell a firearm to a nonlice... 93 Regular File 1/10/2023 7:30:19 PM
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00
30 00 00 00 00 00 00 00 00-
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Activate Windows
Go to Settings to activate Windows.
Cursor pos = 0
Listed: 15 Selected: 0 suspect_Image.E01/Partition 1 [20478MB]/NONAME [NTFS]/[root]/Users/john/Documents
70°F Mostly cloudy
8:41 AM
6/28/2023

Figure C:



Once we got an understanding of what might be going on here, it was clear that a more thorough investigation and assessment needed to be done. For example, we could think that there might be some form of meeting going on between a few individuals. This is found in the same documents folder, by a “follow up with chirlie.txt” file - which contains communications between john and Donald - referencing a “charlie”. This can be seen in the image below, Figure D, where there is a message between said people. It is important to note before we move on, another Anti Forensics tool, tails, is found as an img file in this folder. Tails is self-destructing.

Figure D:



As we move on, this time to the downloads folder, we find some relatively underwhelming anti-forensics tools. In Figure E, pictured below, we see wipefile.7z and the tor browser installer. WipeFile is a secure file deletion tool that permanently erases data from storage devices. It overwrites files with binary patterns multiple times, making the information irretrievable. This ensures that sensitive data isn't recoverable with forensic methods, providing an added layer of security for data privacy. This is another anti-forensics tool that could be used to cause trouble or cover ones tracks. Below Figure E we have Figure F, Figure F is a screen capture of “document.pdf” which has a file from “www.helplinecenter.org”. It has the title “creating an email account without a Phone Number”. Below, you can read the contents. This appears to be a decision made with anti-forensics in mind. Most emails require a phone number for a plethora of reasons. When one is trying to bypass that, it might infer malintent or abuse.
Figure E:

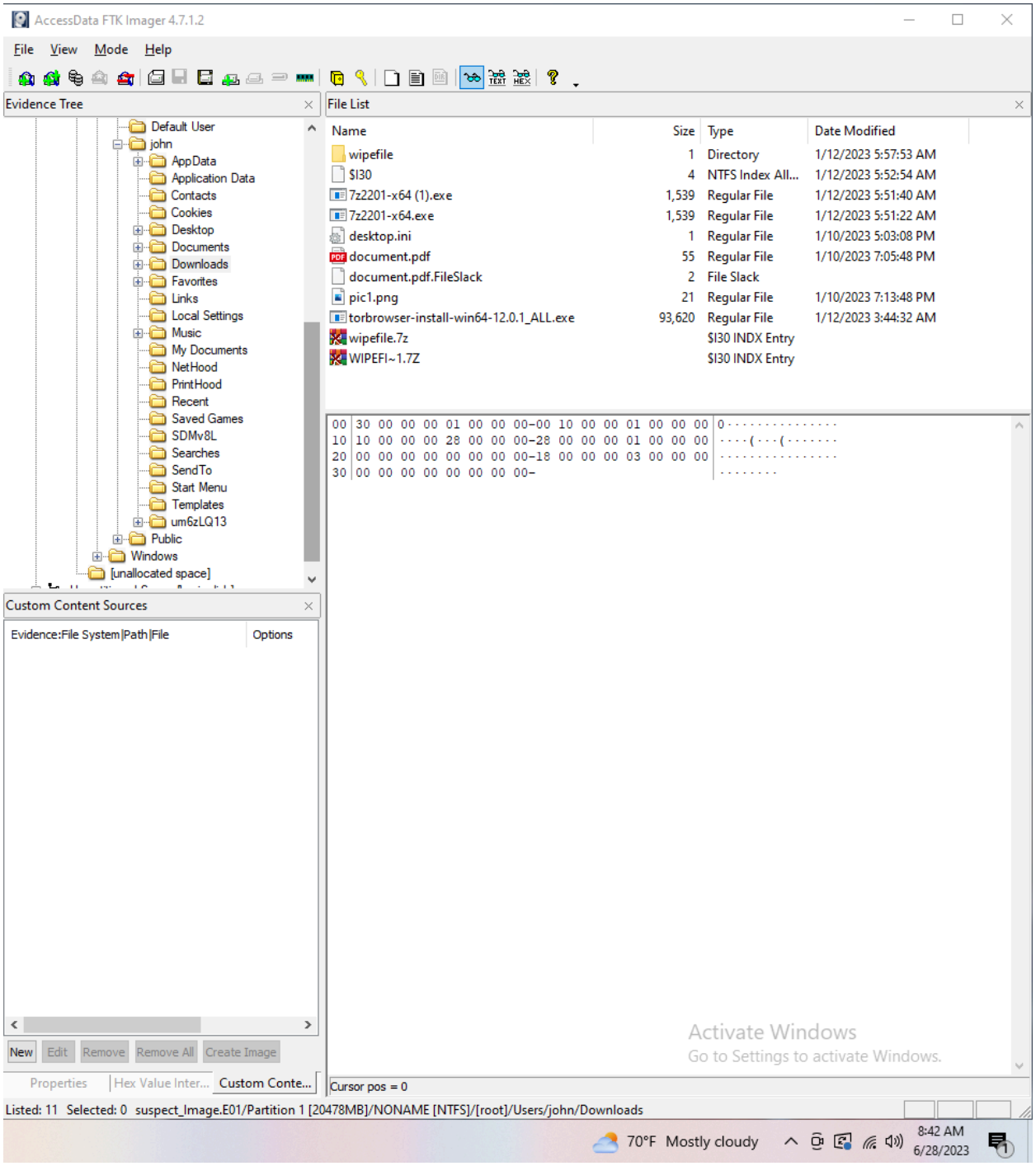
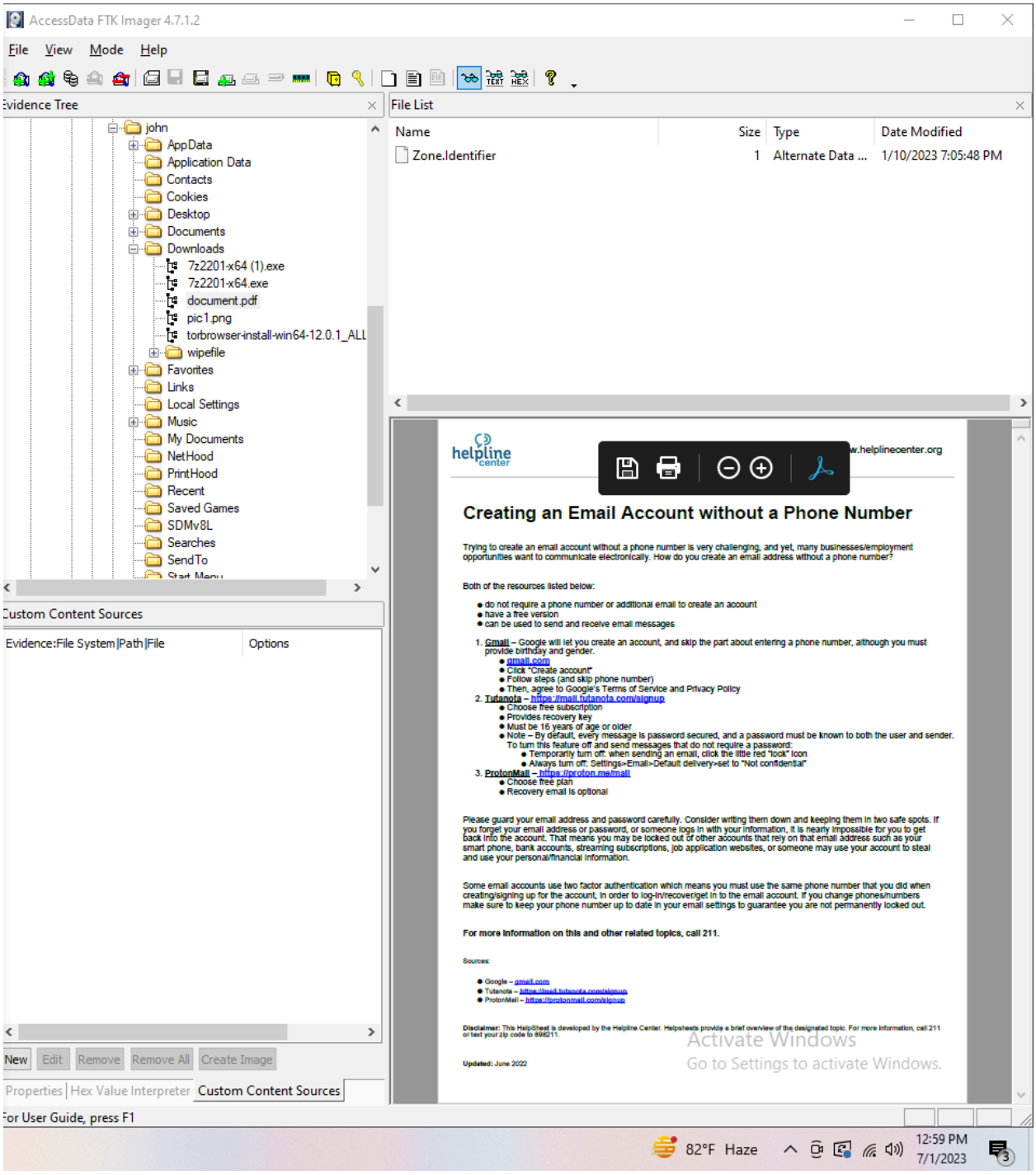

AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
Default User
john
AppData
Application Data
Contacts
Cookies
Desktop
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood
PrintHood
Recent
Saved Games
SDMv8L
Searches
SendTo
Start Menu
Templates
um6zLQ13
Public
Windows
[unallocated space]
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
File List
Name
Size
Type
Date Modified
wipefile 1 Directory 1/12/2023 5:57:53 AM
$I30 4 NTFS Index All... 1/12/2023 5:52:54 AM
7z2201-x64 (1).exe 1,539 Regular File 1/12/2023 5:51:40 AM
7z2201-x64.exe 1,539 Regular File 1/12/2023 5:51:22 AM
desktop.ini 1 Regular File 1/10/2023 5:03:08 PM
document.pdf 55 Regular File 1/10/2023 7:05:48 PM
document.pdf.FileSlack 2 File Slack
pic1.png 21 Regular File 1/10/2023 7:13:48 PM
torbrowser-install-win64-12.0.1_ALL.exe 93,620 Regular File 1/12/2023 3:44:32 AM
wipefile.7z $I30 INDX Entry
WIPEFI~1.7Z $I30 INDX Entry
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00
30 00 00 00 00 00 00 00 00-
Activate Windows
Go to Settings to activate Windows.
Cursor pos = 0
Listed: 11 Selected: 0 suspect_Image.E01/Partition 1 [20478MB]/NONAME [NTFS]/[root]/Users/john/Downloads
70°F Mostly cloudy
8:42 AM
6/28/2023

Figure F:


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
File List
john
AppData
Application Data
Contacts
Cookies
Desktop
Documents
Downloads
7z2201-x64 (1).exe
7z2201-x64.exe
document.pdf
pic1.png
torbrowser-install-win64-12.0.1_ALL
wipefile
Favorites
Links
Local Settings
Music
My Documents
NetHood
PrintHood
Recent
Saved Games
SDMv8L
Searches
SendTo
Name
Size
Type
Date Modified
Zone.Identifier
1
Alternate Data ...
1/10/2023 7:05:48 PM
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Interpreter
Custom Content Sources
For User Guide, press F1
helpline center
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:
do not require a phone number or additional email to create an account
have a free version
can be used to send and receive email messages
1. Gmail – Google will let you create an account, and skip the part about entering a phone number, although you must provide birthday and gender.
gmail.com
Click "Create account"
Follow steps (and skip phone number)
Then, agree to Google's Terms of Service and Privacy Policy
2. Tutanota – https://mail.tutanota.com/signup
Choose free subscription
Provides recovery key
Must be 16 years of age or older
Note – By default, every message is password secured, and a password must be known to both the user and sender. To turn this feature off and send messages that do not require a password:
Temporarily turn off: when sending an email, click the little red "lock" icon
Always turn off: Settings>Email>Default delivery>set to "Not confidential"
3. ProtonMail – https://proton.me/mail
Choose free plan
Recovery email is optional
Please guard your email address and password carefully. Consider writing them down and keeping them in two safe spots. If you forget your email address or password, or someone logs in with your information, it is nearly impossible for you to get back into the account. That means you may be locked out of other accounts that rely on that email address such as your smart phone, bank accounts, streaming subscriptions, job application websites, or someone may use your account to steal and use your personal/financial information.
Some email accounts use two factor authentication which means you must use the same phone number that you did when creating/signing up for the account, in order to log-in/recover/get in to the email account. If you change phones/numbers make sure to keep your phone number up to date in your email settings to guarantee you are not permanently locked out.
For more information on this and other related topics, call 211.
Sources:
Google – gmail.com
Tutanota – https://mail.tutanota.com/signup
ProtonMail – https://protonmail.com/signup
Disclaimer: This HelpSheet is developed by the Helpline Center. Helpsheets provide a brief overview of the designated topic. For more information, call 211 or text your zip code to 898211.
Updated: June 2022
Activate Windows
Go to Settings to activate Windows.
82°F Haze
12:59 PM
7/1/2023

To further wrap up the findings within that folder, we found “pic1.png” was a file that contained an image of a CZ pistol - chambered in 9mm. This could potentially be used as a graphic for better understanding of potential products delivered, but again I am here to analyze the facts. The CZ is pictured below, Figure G. After Figure G, comes Figure H - We are running out of letters here! Figure H is a screencapture of a “wipefile log” this is a log that comes with using wipefile, that luckily for us - is evident and existent on the Windows system. At minimum, it is available to the forensic expert to analyze. What we see there is the action of wiping files in the Pictures directory. An image will be displayed, however here is the text from the log:

—----------

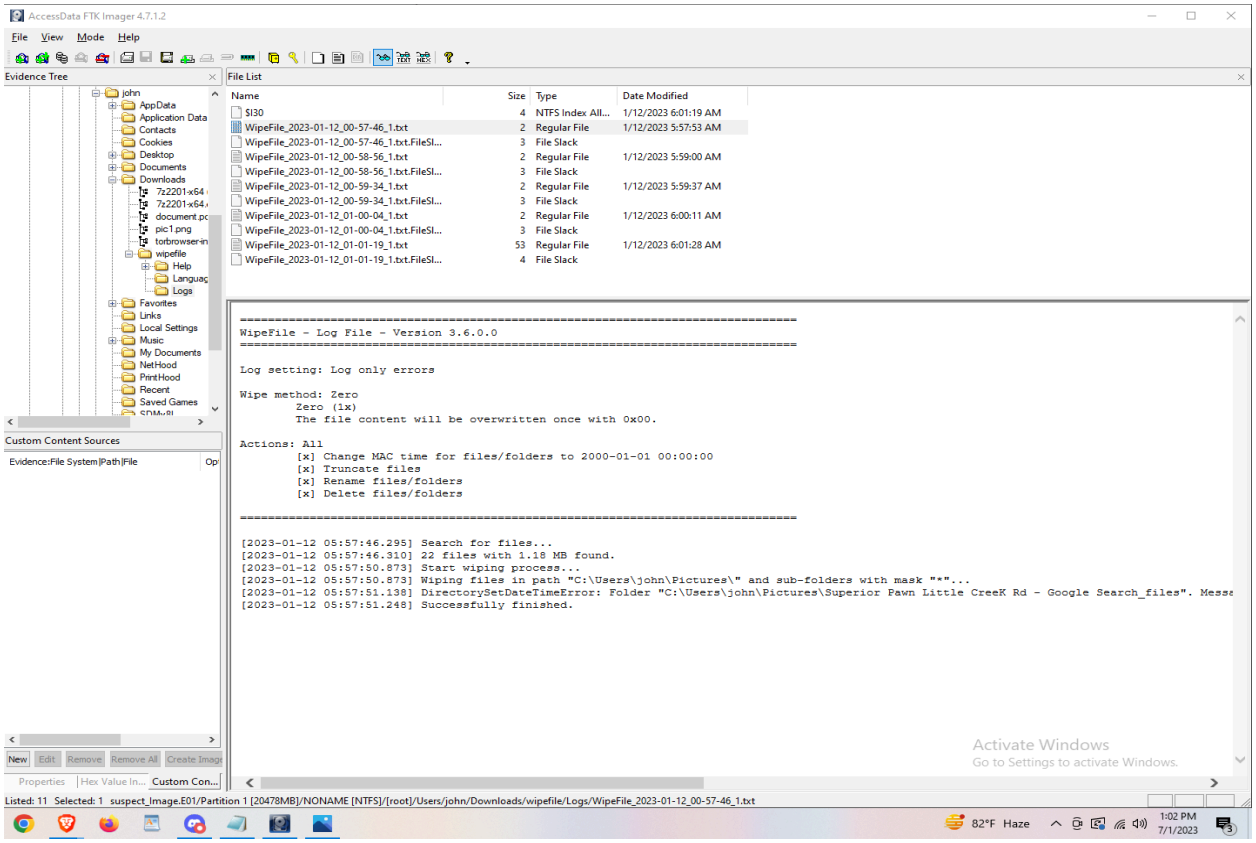
[2023-01-12 05:57:46.295] Search for files...
[2023-01-12 05:57:46.310] 22 files with 1.18 MB found.
[2023-01-12 05:57:50.873] Start wiping process...
[2023-01-12 05:57:50.873] Wiping files in path "C:\Users\john\Pictures\" and sub-folders with mask "*"...
[2023-01-12 05:57:51.138] DirectorySetDateTimeError: Folder "C:\Users\john\Pictures\Superior Pawn Little CreeK Rd - Google Search_files". Message: The process cannot access the file 'C:\Users\john\Pictures\gyaXTvfRWzxYfLyC7K16r7ibV4VIjY6ENQDIiaPcvXozRiDBiTo' because it is being used by another process.
[2023-01-12 05:57:51.248] Successfully finished.

—----------

The above output was crucial, or would have been crucial (I did not find this until 1JULY2023, initial analysis was June 28) for moving forward. When I initially put myself in the shoes of someone careless, I found myself at a loss after the obvious Desktop, Documents, and Downloads folder analysis. However, I found more, which will be shown - but it was the diligence in looking into the wipefiles log that would have led me to where I went unintentionally. We see above that john attempted to delete what could be a file that is related to “Superior Pawn Little Creek Road”. Given the analysis, this could be a visual cue or aid for the gun transaction that is appearing to be of interest here. Below are the Figures of relevance, a segue into further analysis will come thereafter.

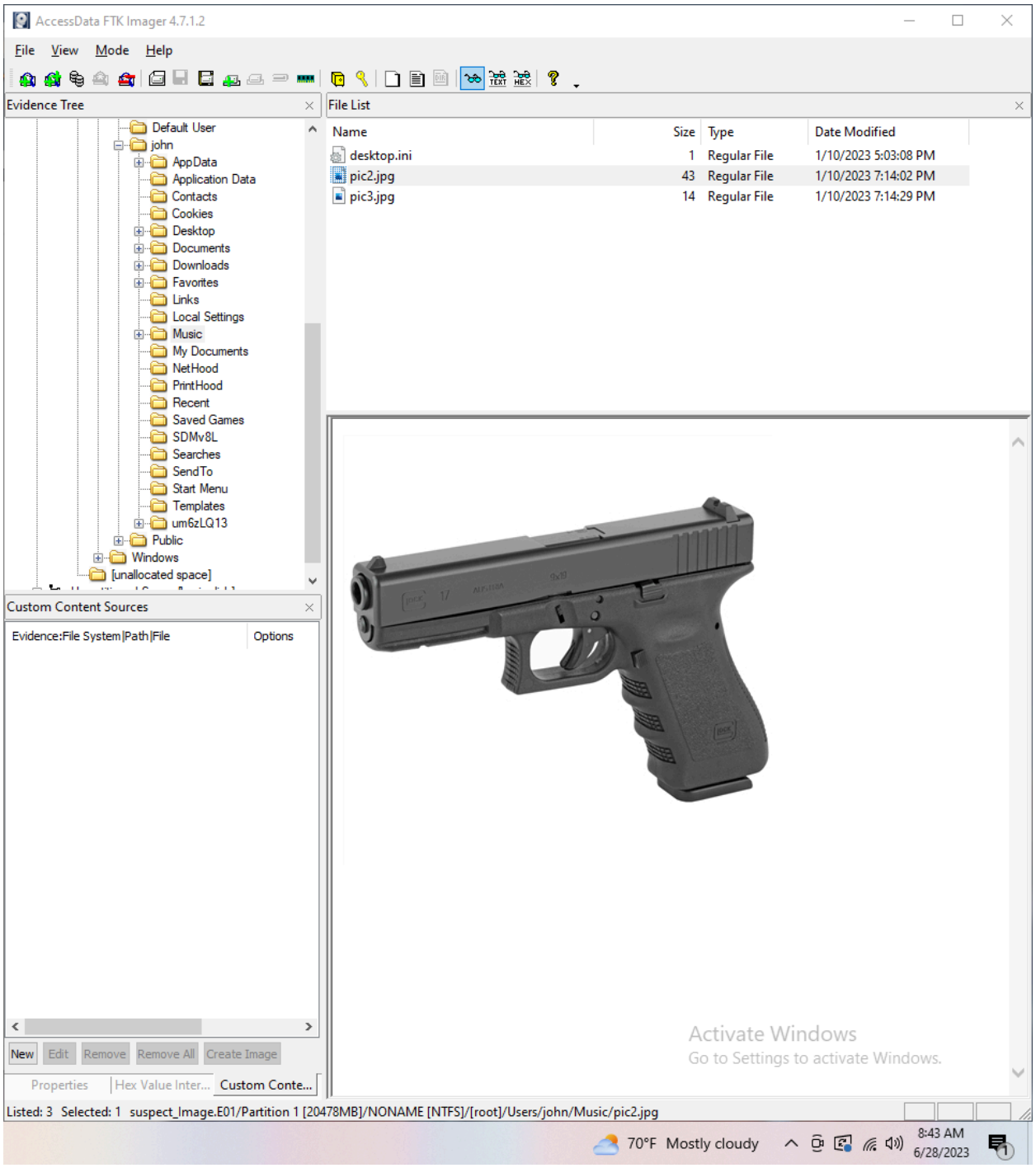
Figure G:

Figure H:



Where did I go when the trail went cold. I started out by checking the Music Folder. This of course, would be an unlikely folder for anything, but as we can see in Figure I - there was a picture of a Glock 19.

Figure I:



After I finished up in the music folder, I decided to look inside of the “[unallocated space]” folder. This folder, had a bunch of interesting files, specifically two I found very odd. The first one, Figure J was titled “0920427” - This figure had an unknown output of what might be anti-forensics. It starts querying with “were_old_google_logins_removed”. This makes me believe that search logs on google were wiped, or attempted to have been wiped. Within that same folder, in Figure K, I found a picture to the aforementioned gun store. The file “0207928” was a picture of the storefront of said pawn shop, which is mentioned in surfaced files.

Figure J:

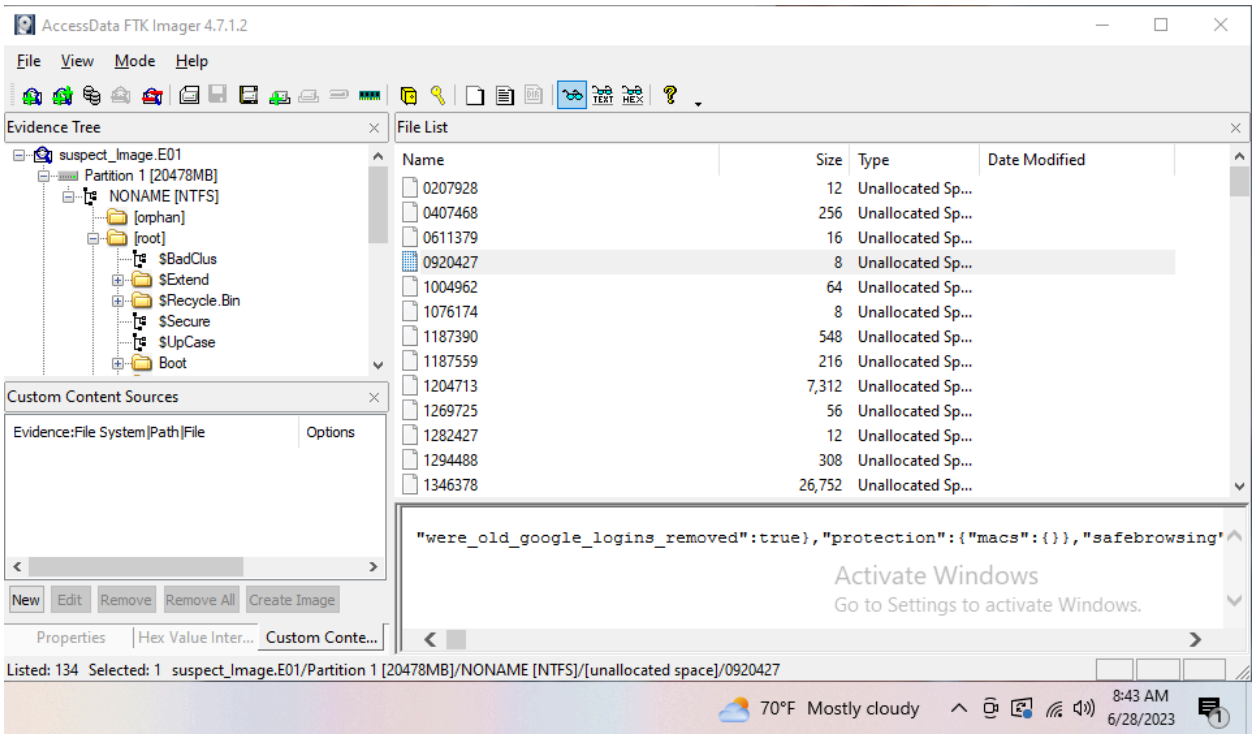
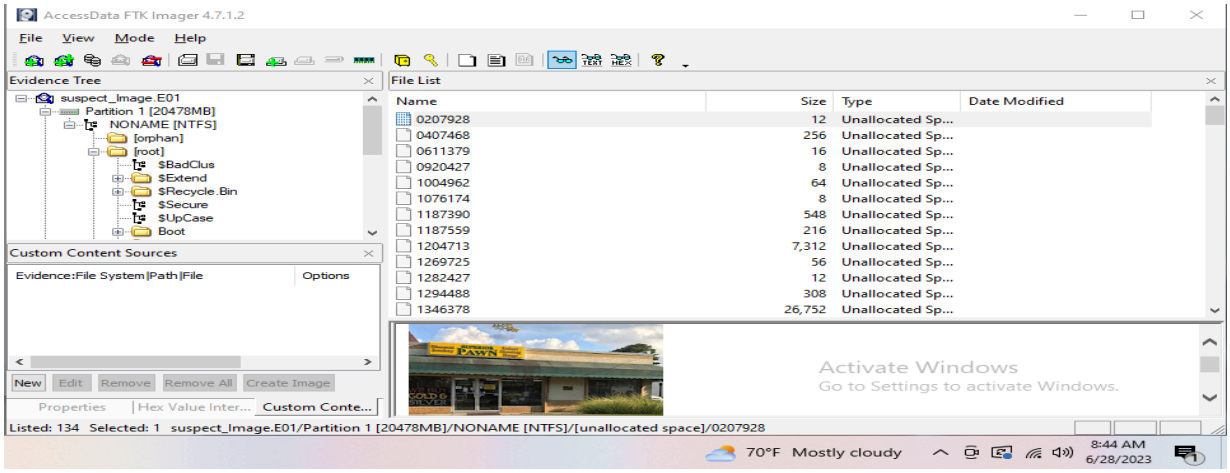


Figure K:



It was after that, I went to the last spot in my forensics analysis - not by choice however. The recycle bin contained a few images of interest. One titled “$R1O1FO” and one titled “$R2ONUQQ”. The first image, Figure L, shows an image of a storefront that is unidentifiable in the photo. The second image, Figure M, shows an image of a screencap of the Pawn Shop with a location pin over it. The reason this was my last spot was because the trail went cold after these two images, I tried my best - but to no avail could I find any other artifacts that stood out to me. A forensics analysis is as best as the analyst is thorough, and sadly - this was all I could muster. Below are the aforementioned artifacts:

Figure L:

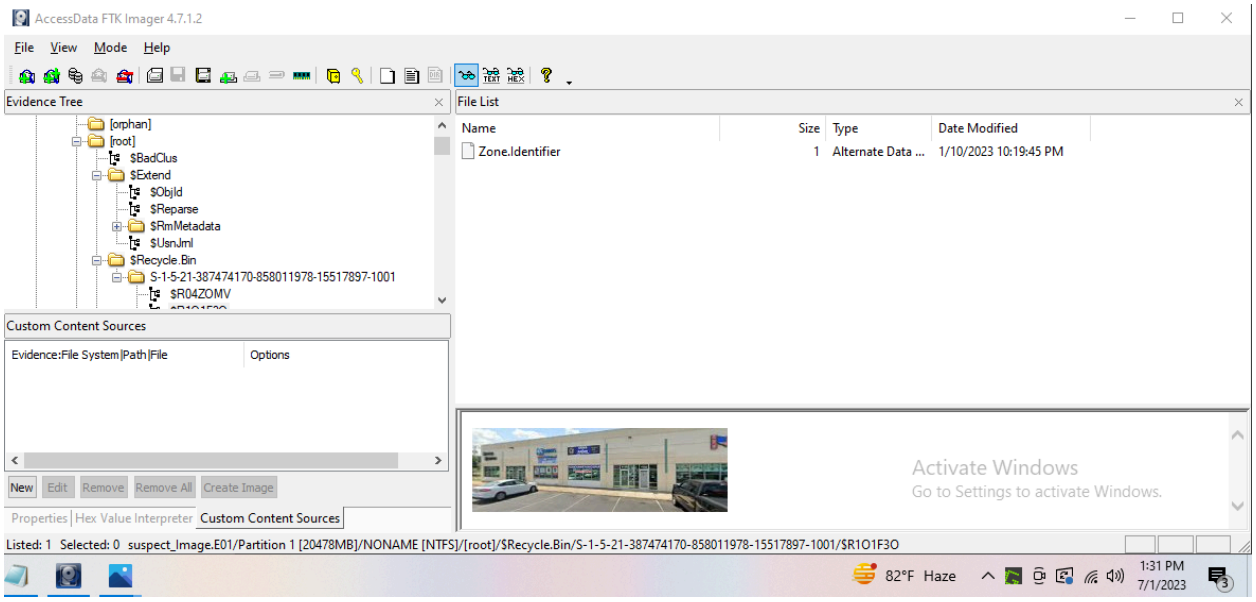


Figure M: