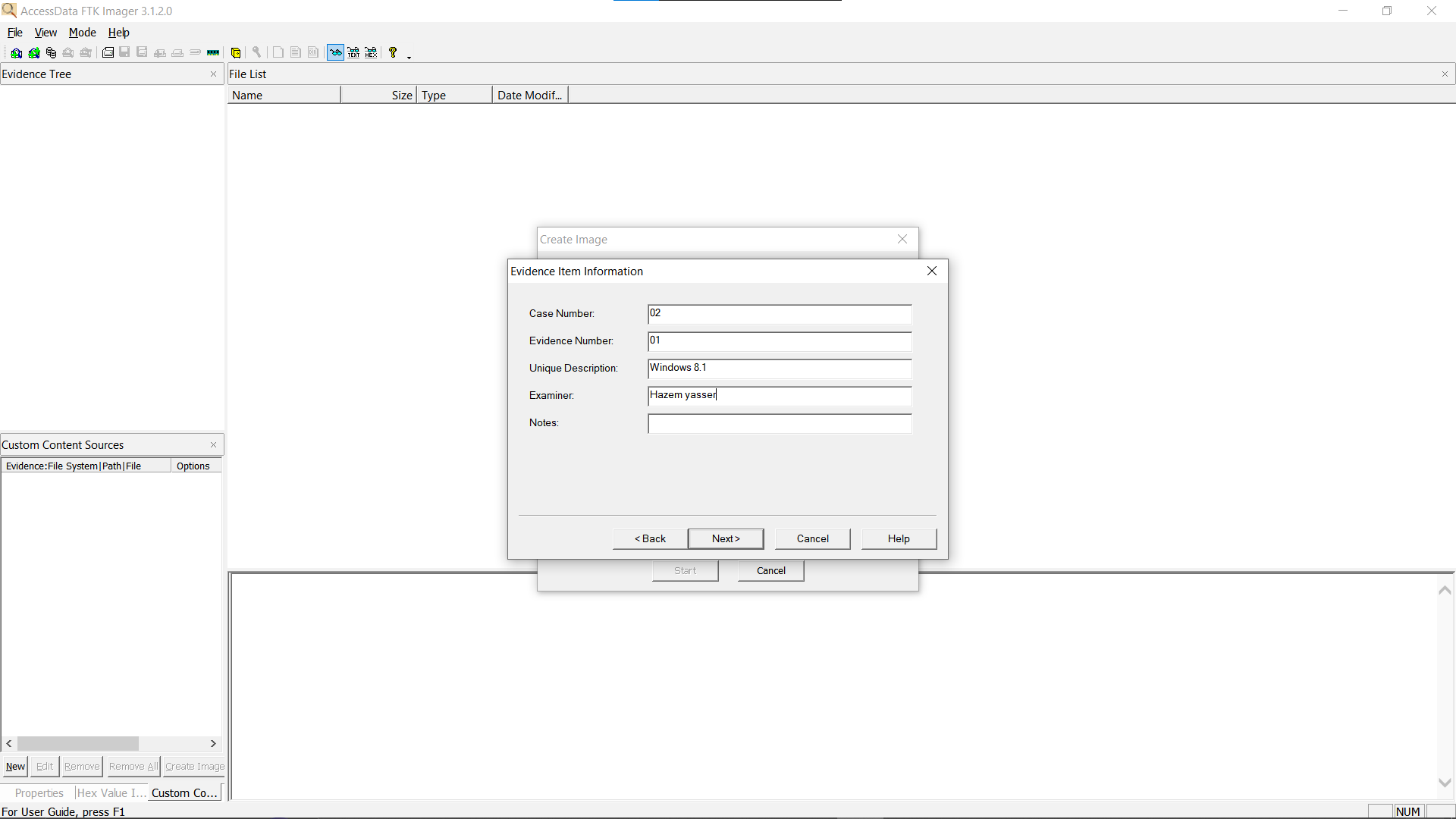
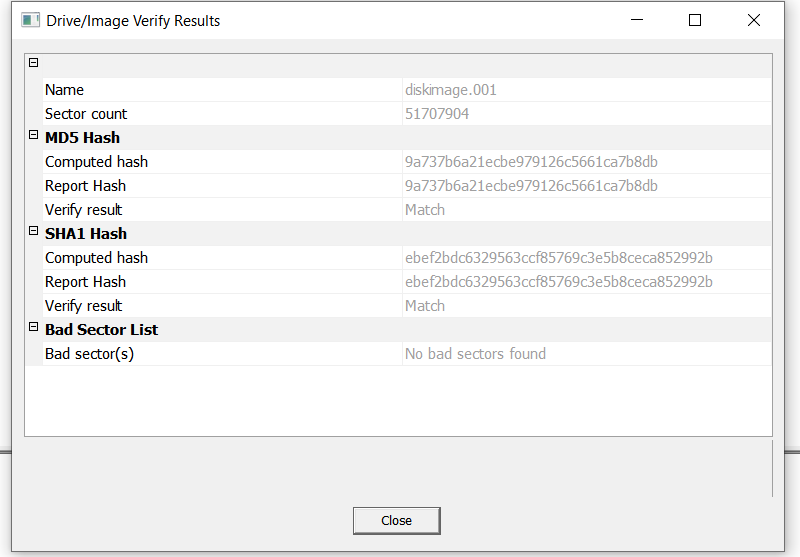
extracting the disk image



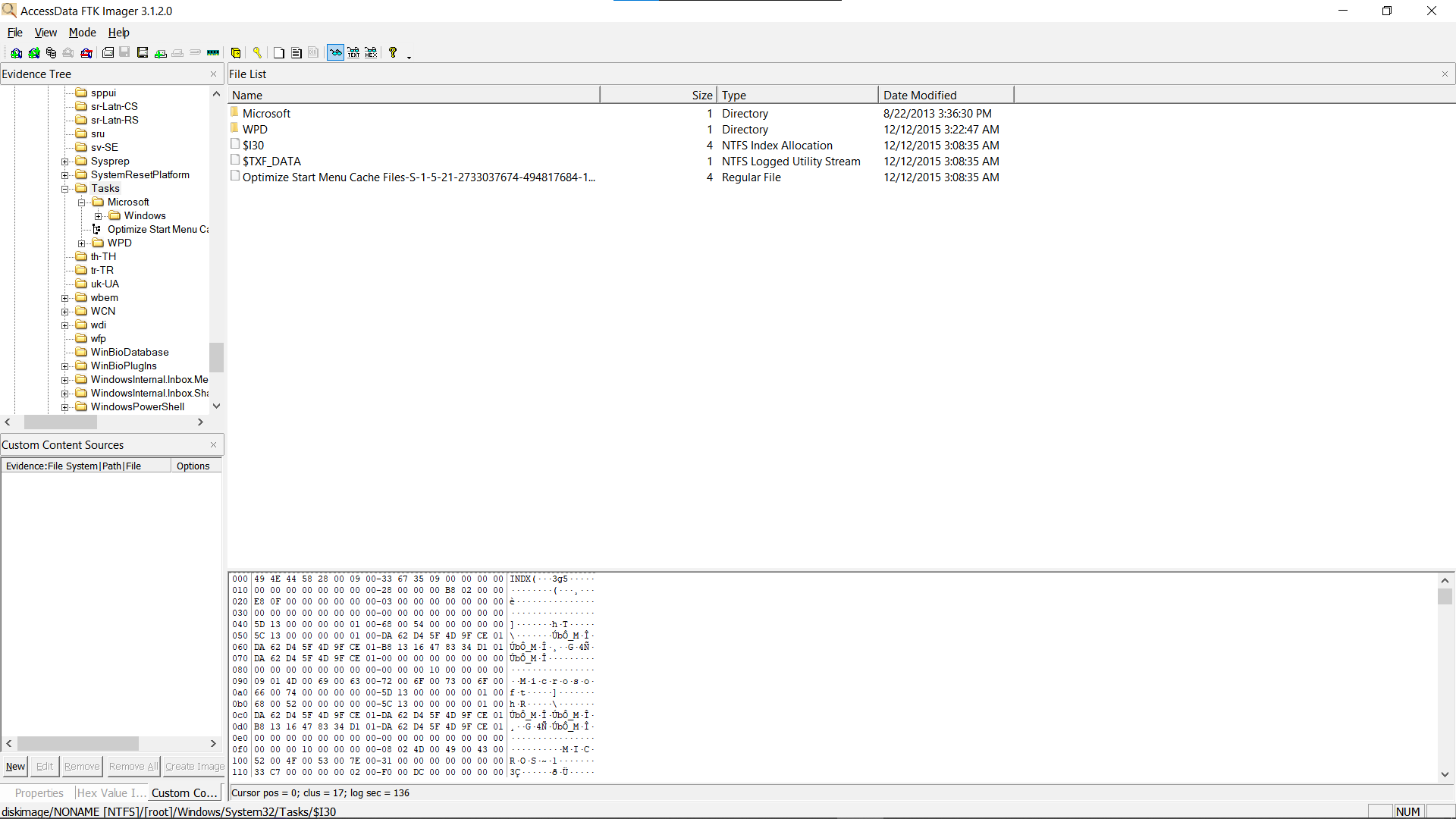
4:05 PM 11/27/2025 now we make another copy of the disk image using ftk image





4:31 PM 11/27/2025 now we start analyzing the new image

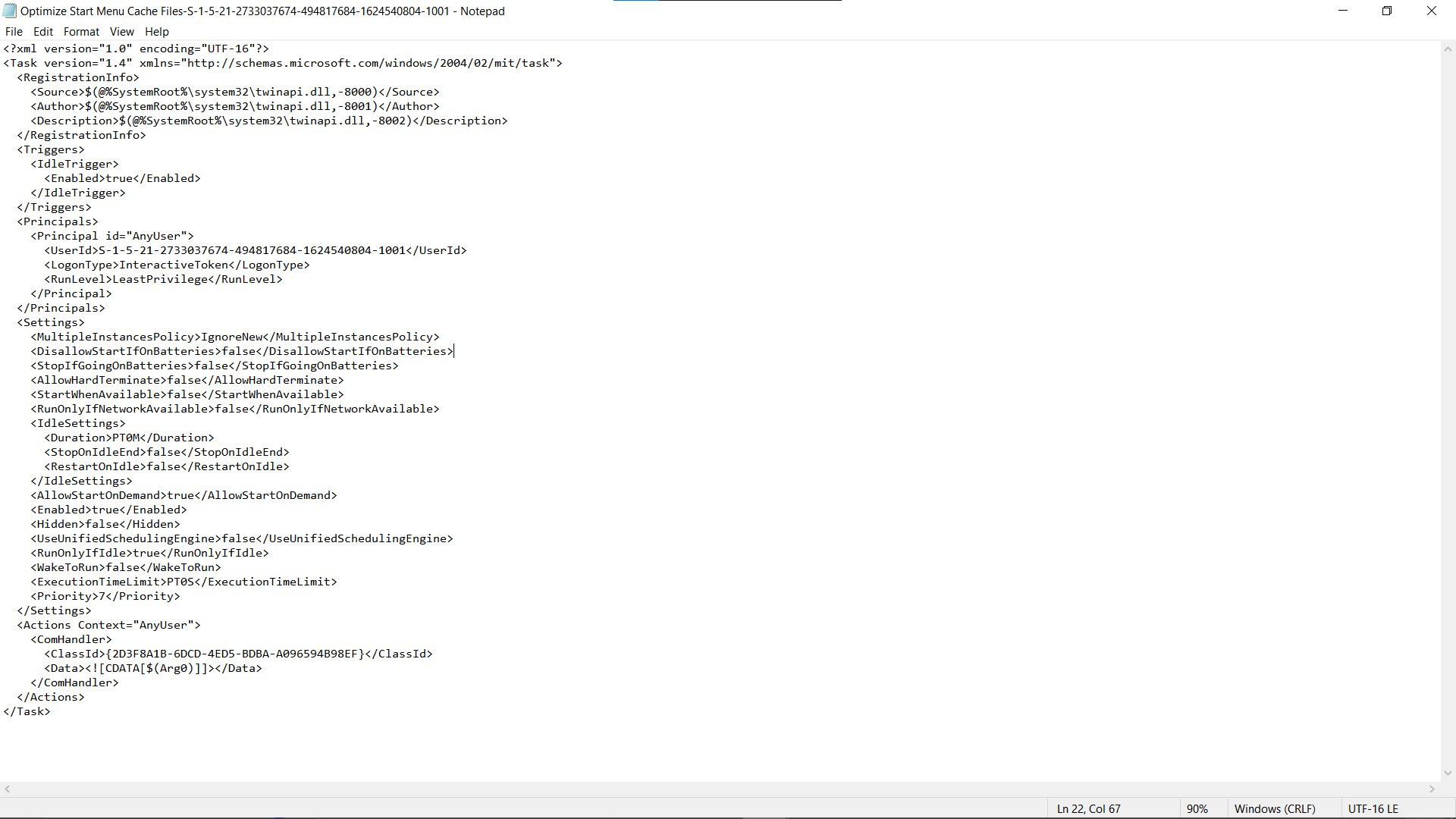
4:40 PM 11/27/2025 now we would check scheduled files



checking the scheduled tasks on ftk imager we found at System32/Tasks a couple of files that was modified at the same day

one file is an XML file that is called Optimize Start Menu Cache Files-S-1-5-21-2733037674-494817684-1624540804-1001

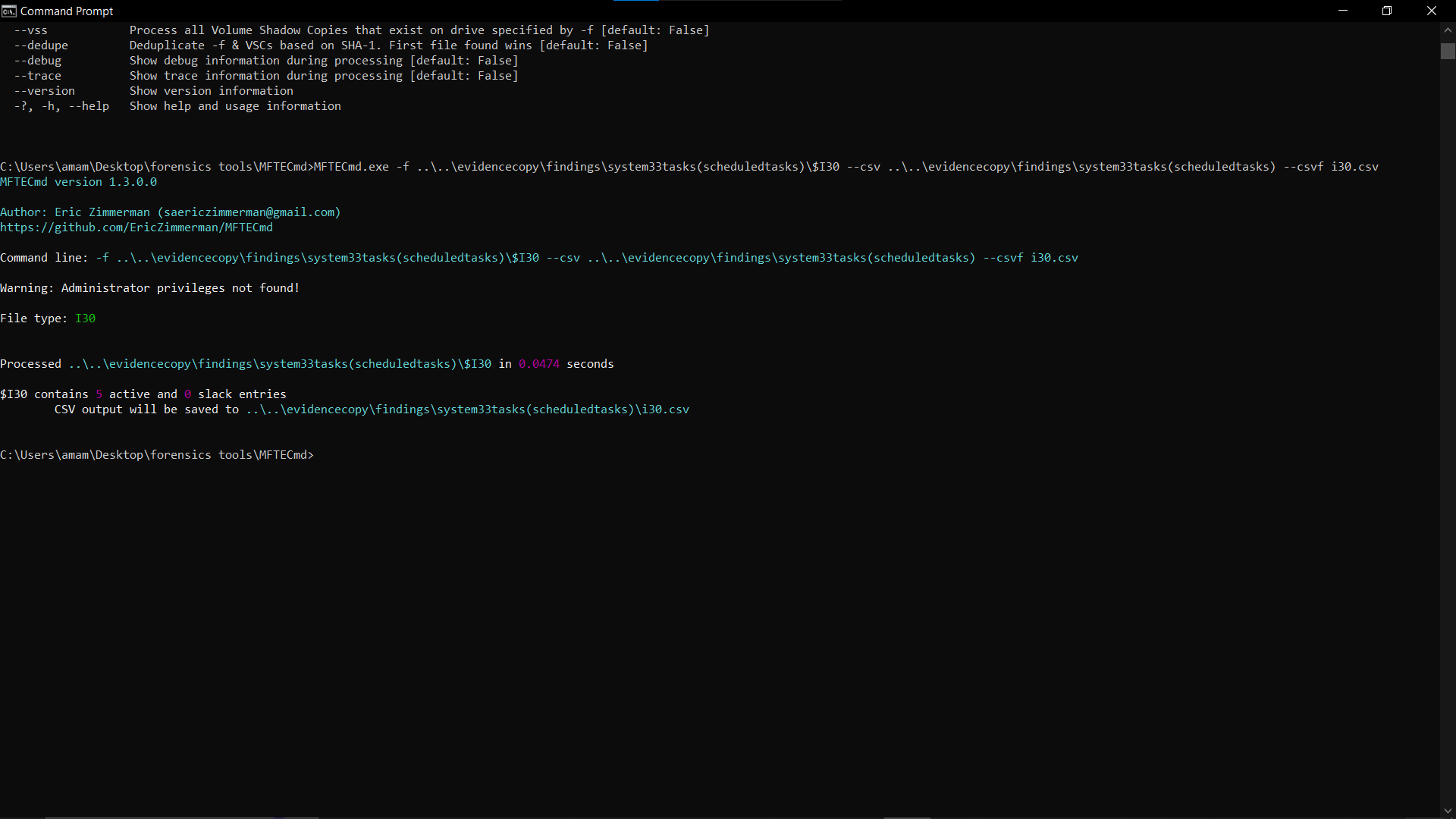
lets analyze it



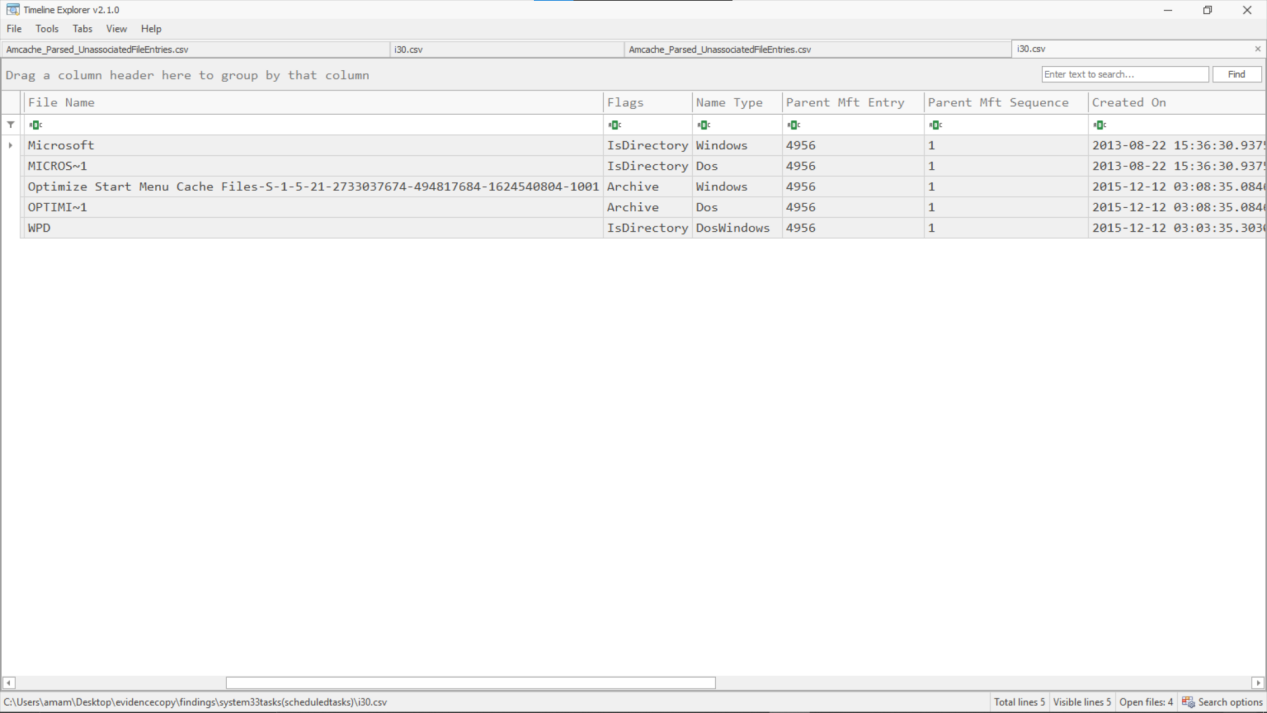
opend it using notepad every thing looks legitimate in it runs twinapi.dll = Microsoft Windows Modern UI Framework

Used for Windows Store apps, UWP components, and UI tasks.

we also got $I30 file lets first process it using MFTECmd to get csv



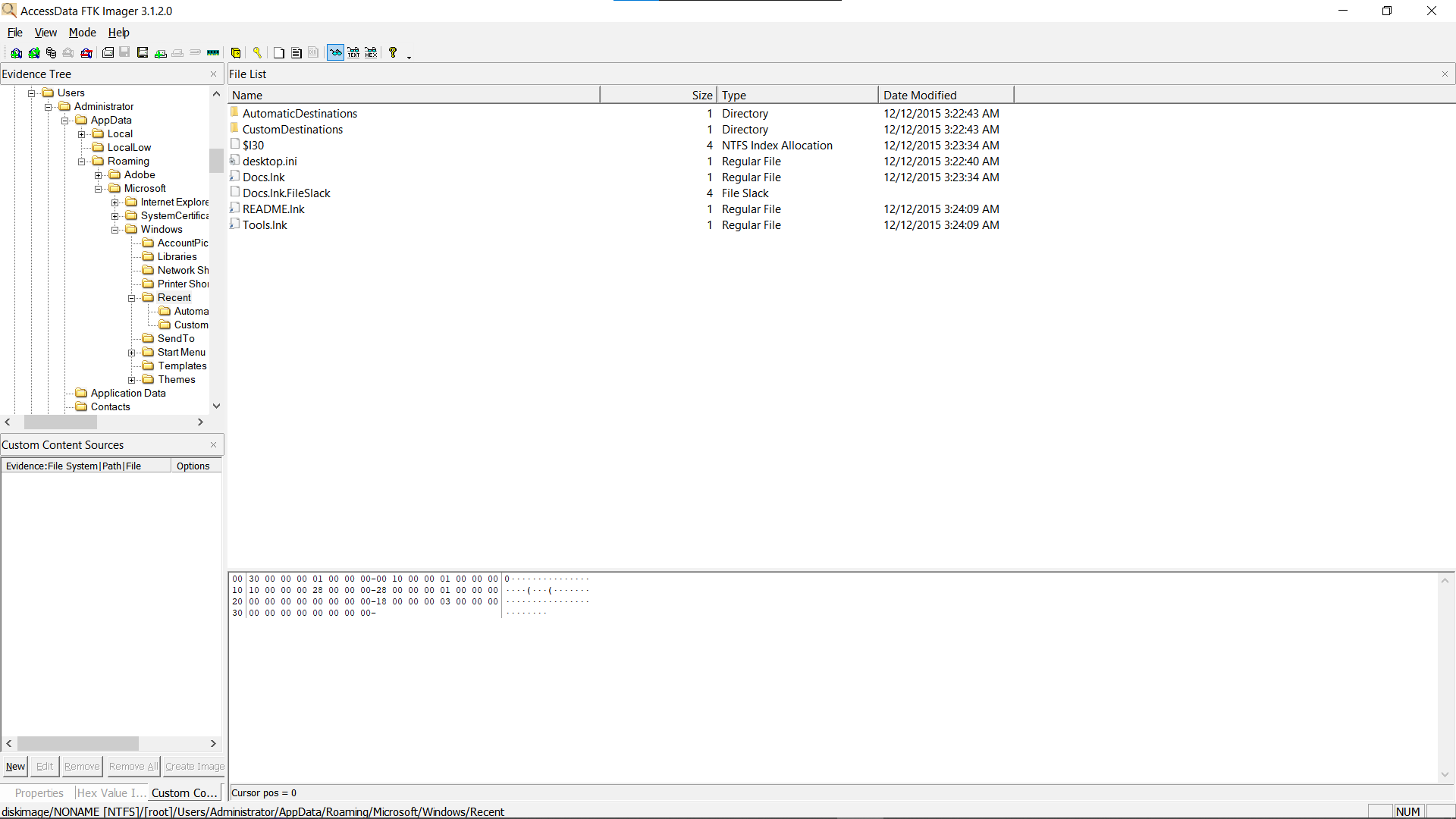
5:06 PM 11/27/2025 now we open $I30 in timeline explorar



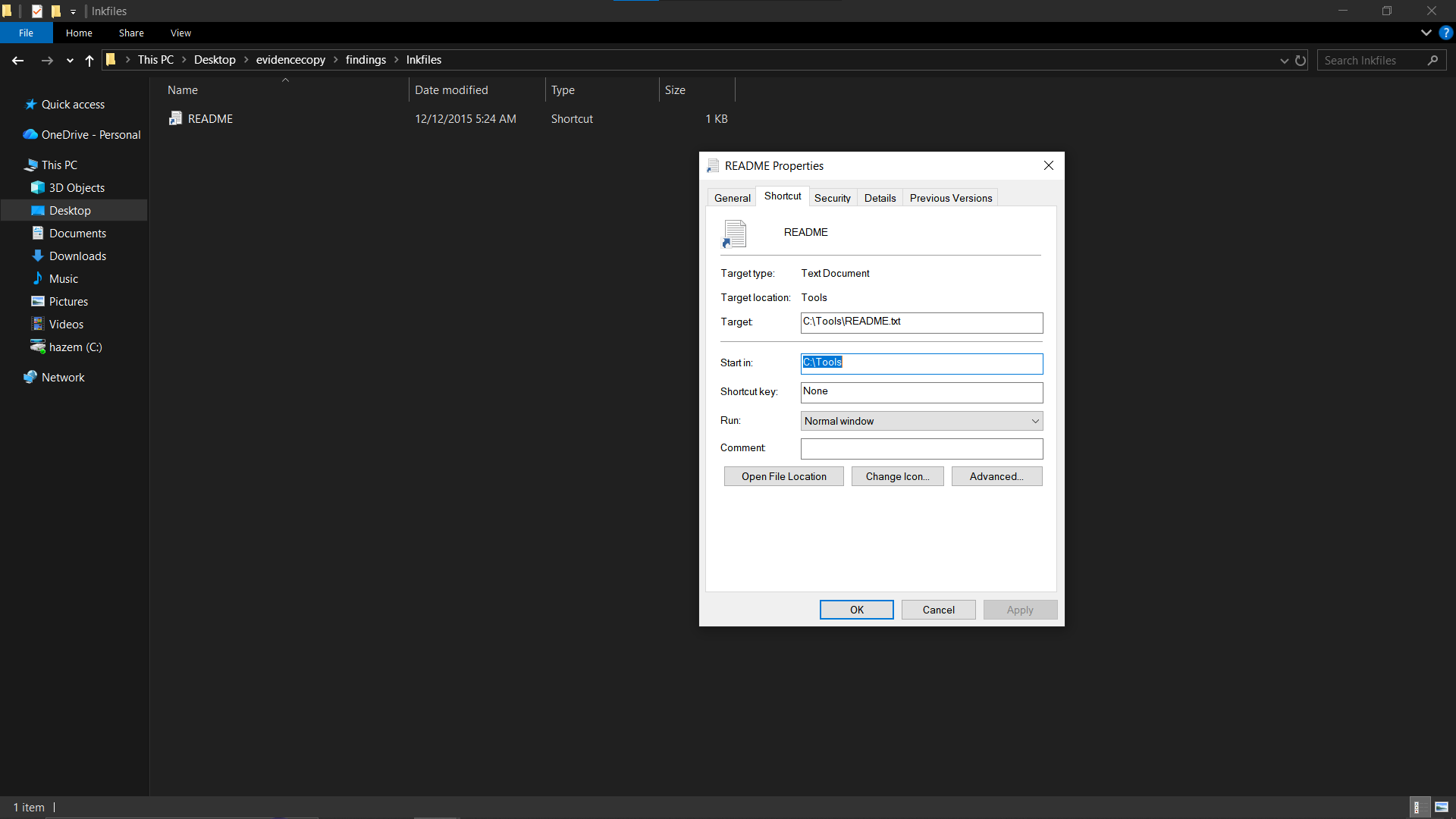
nothing important in it exept that we found the activeity on 12\12\2015 3 AM we have seen this a couple of times now

and its not the companys work hour ( sus )

5:28 PM 11/27/2025 now we look at LNK files

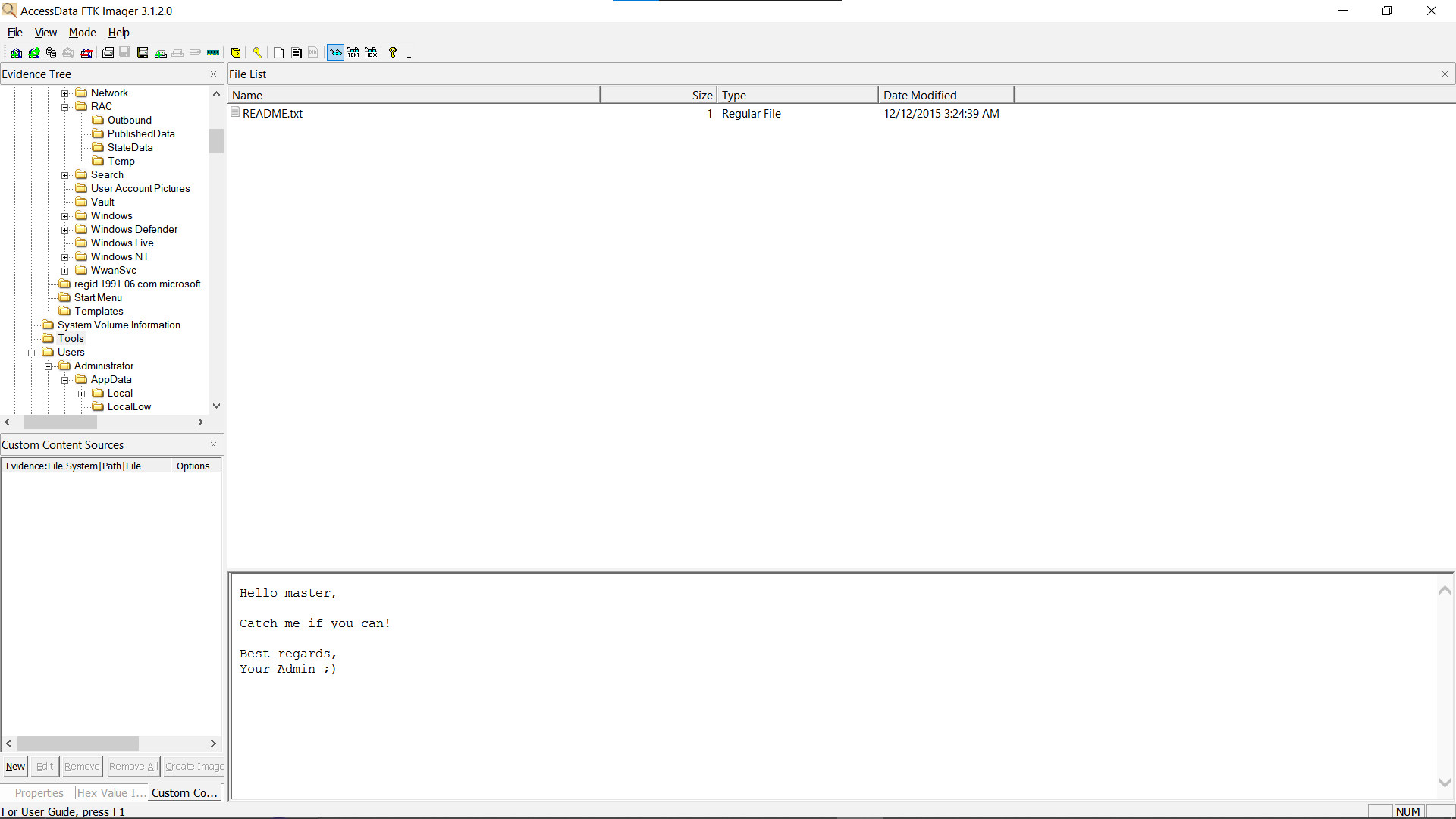


at C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent\ found a file called README



so the target of that file is c:\tools\README.txt

after going there it appers to be the message that the company found



6:21 PM 11/27/2025while looking at the doc of users on FTK imager found interesting files on the user called master so lets analyze the users in more details

We will open the master user on shellbag

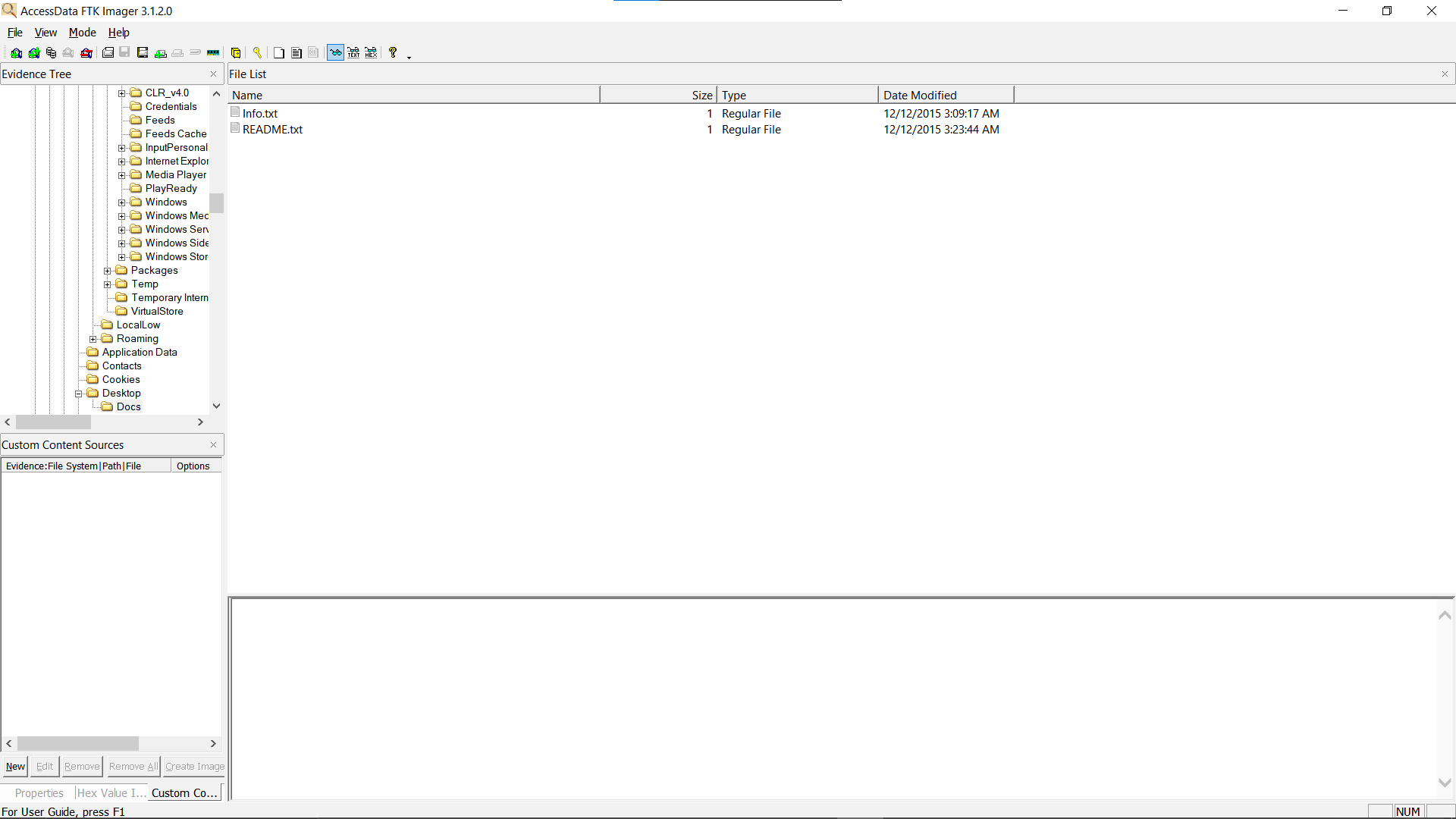


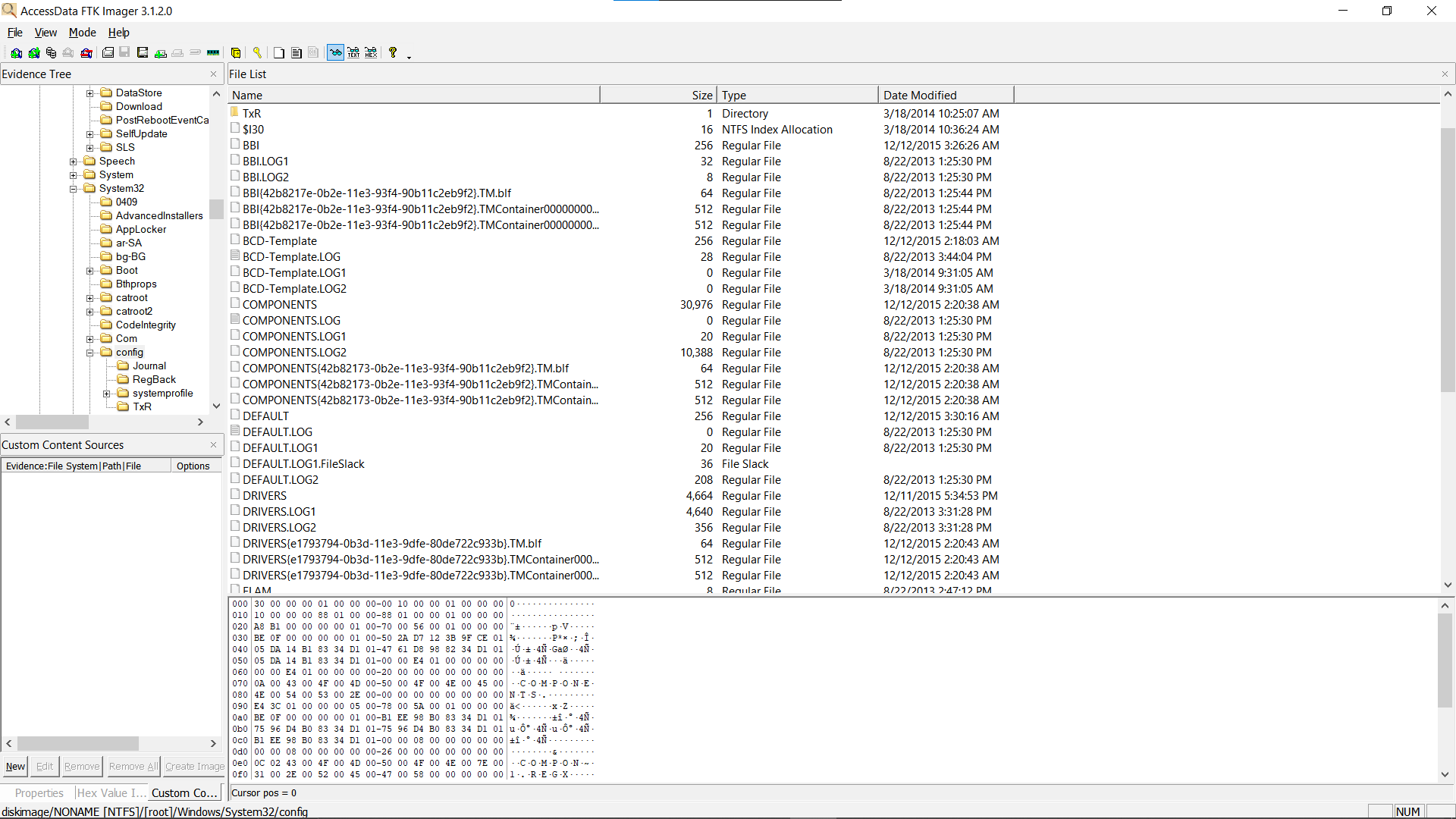
Now we should see what is on Docs

9:32 PM 11/27/2025 lets check the brefetch files

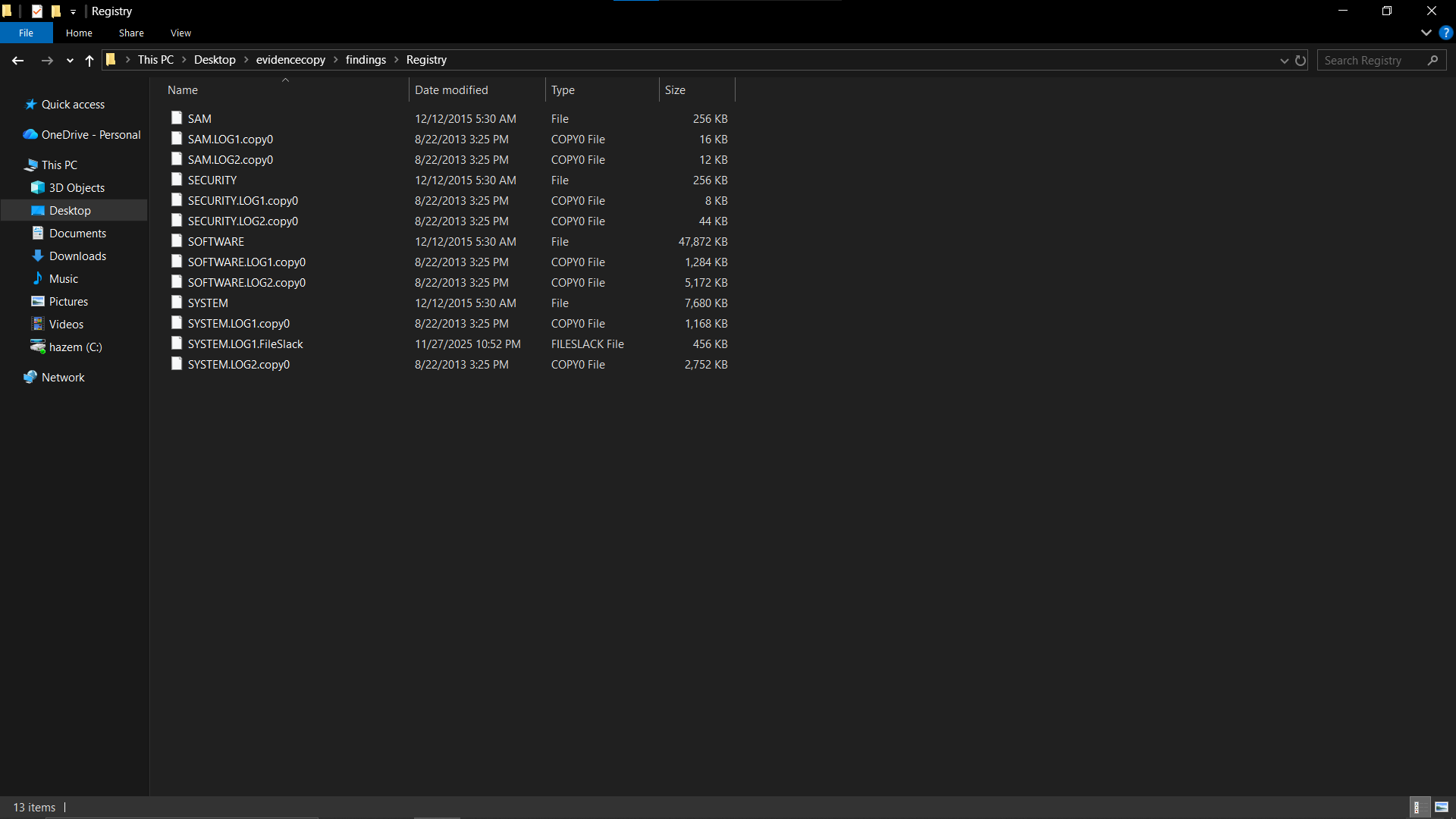
found nothing important

9:57 PM 11/27/2025 now would be a good idea to investigate the master user



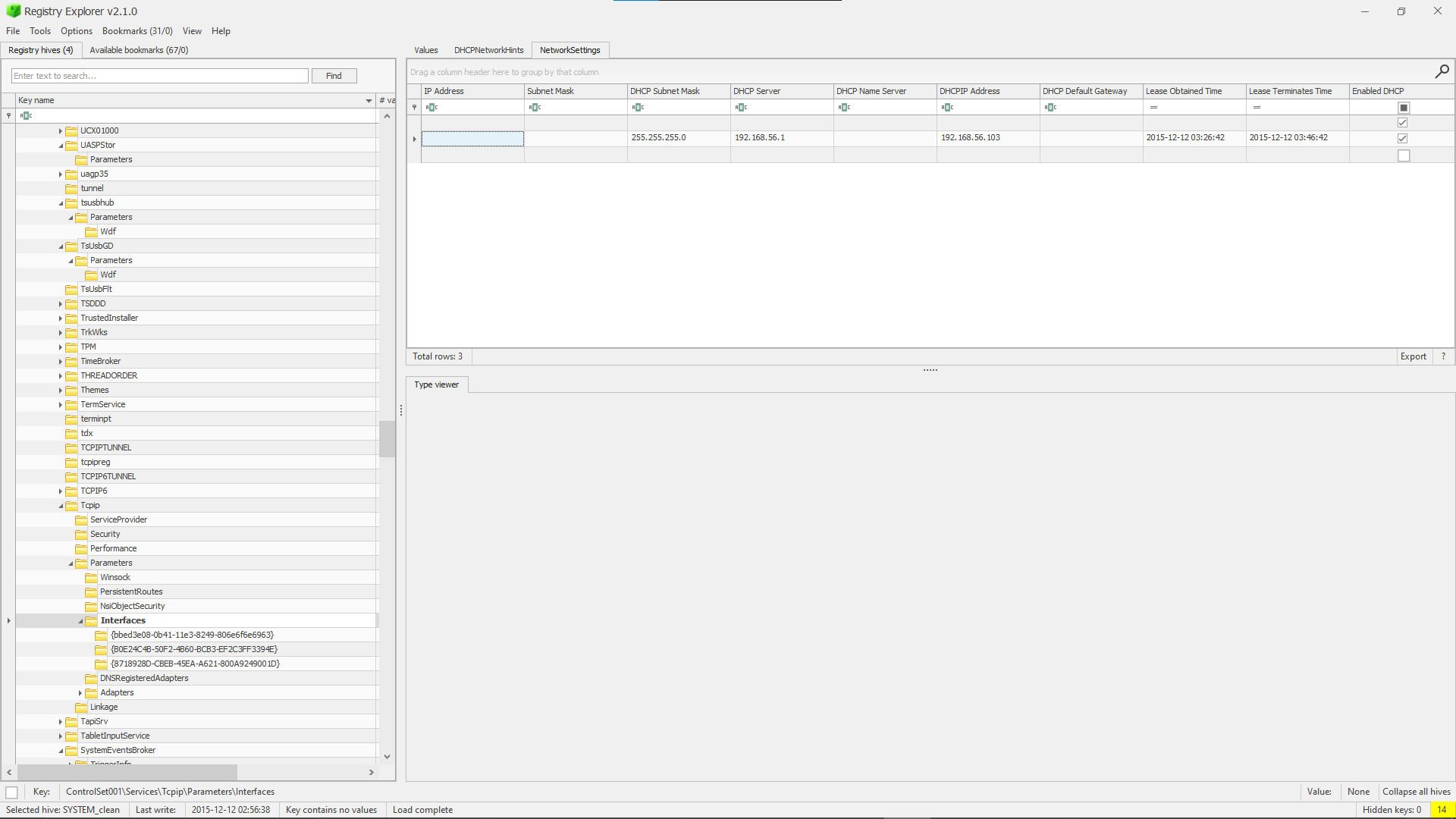


after geting the registary hives we open them on registary explorar



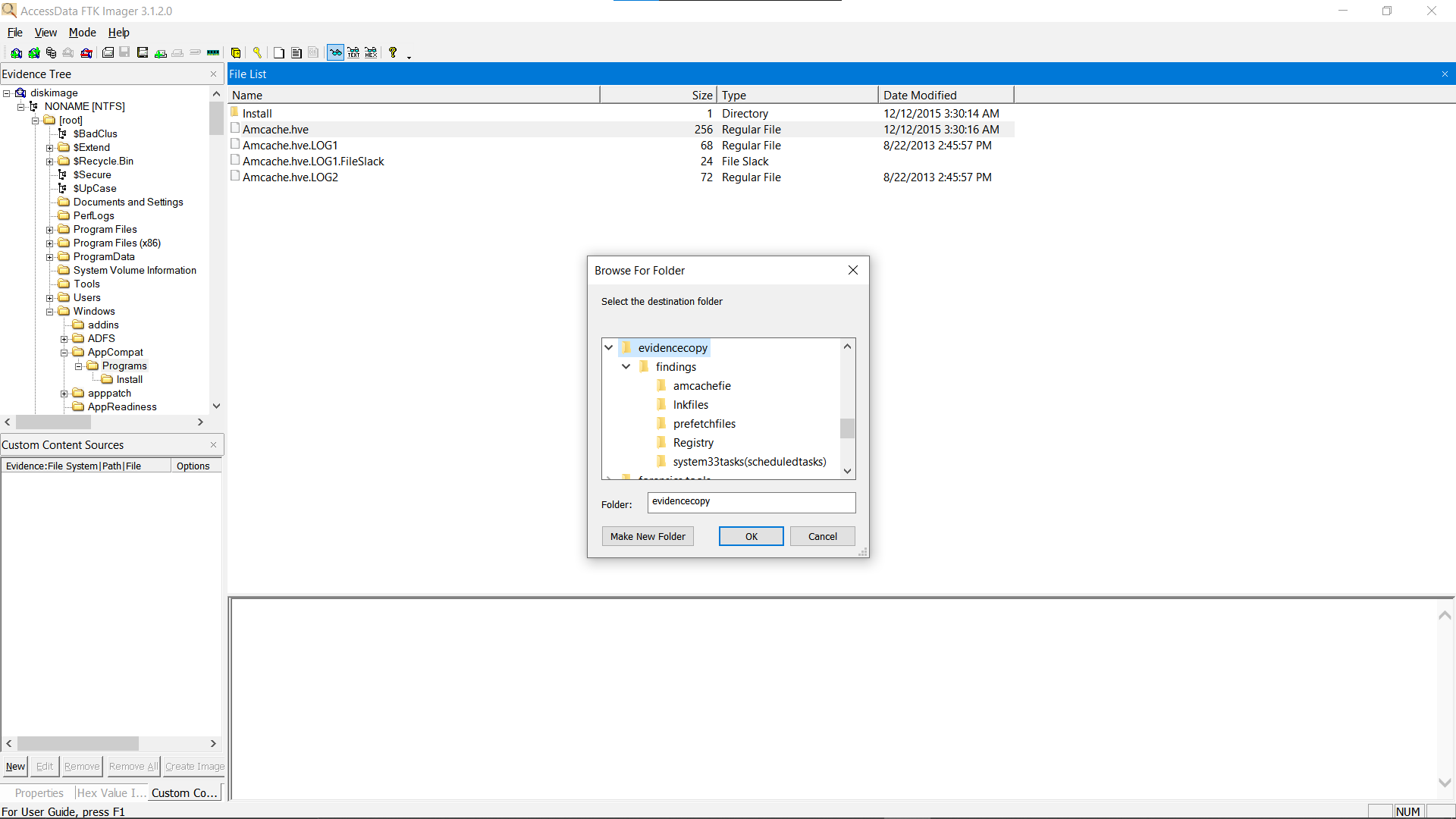
checked for USP device history but nothing important

while looking at system registary at SYSTEM → CurrentControlSet → Services → Tcpip → Parameters → Interfaces we found weird connection at the same time of the message



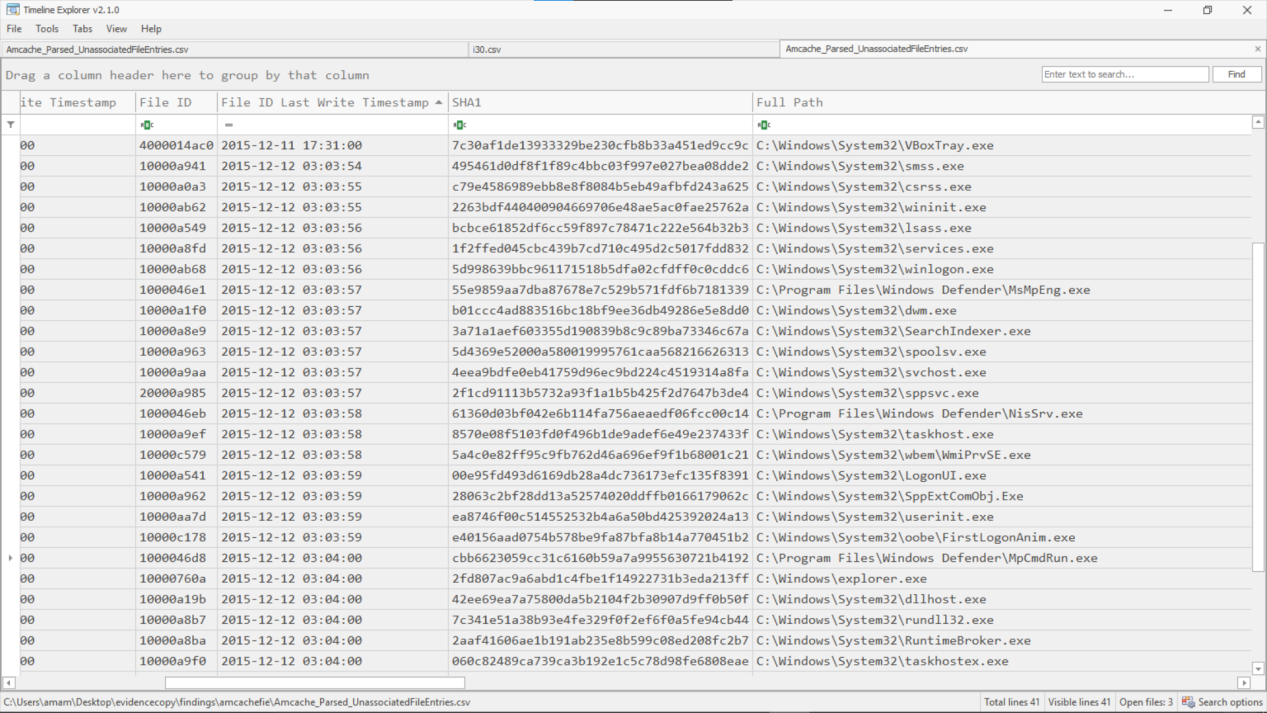
7:18 AM 11/28/2025 now lets work on the amcache files

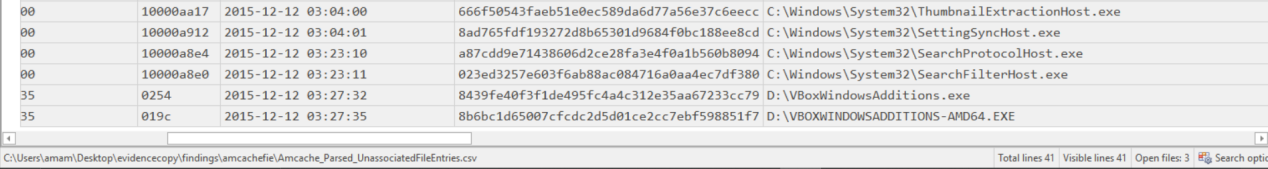
extracting it using ftk imager from C:\Windows\appcompat\Programs\Amcache.hve

.

now we use a tool called the Amcache Parser to turn it to a csv

7:31 AM 11/28/2025 opening the amcache file on timeline explorar





so what we found is theat the windows logged in at 12\12\20215 3:3:56 then a couple of events happend then a new user account was created found that by C:\Windows\System32\oobe\FirstLogonAnim.exe which means A legitimate Windows OOBE (Out-Of-Box Experience) component. Which was not found in the security log

It runs the first logon animation after:

A new user account is created

A fresh Windows installation is completed

A new profile is loaded for the first time

This is the animation that says:

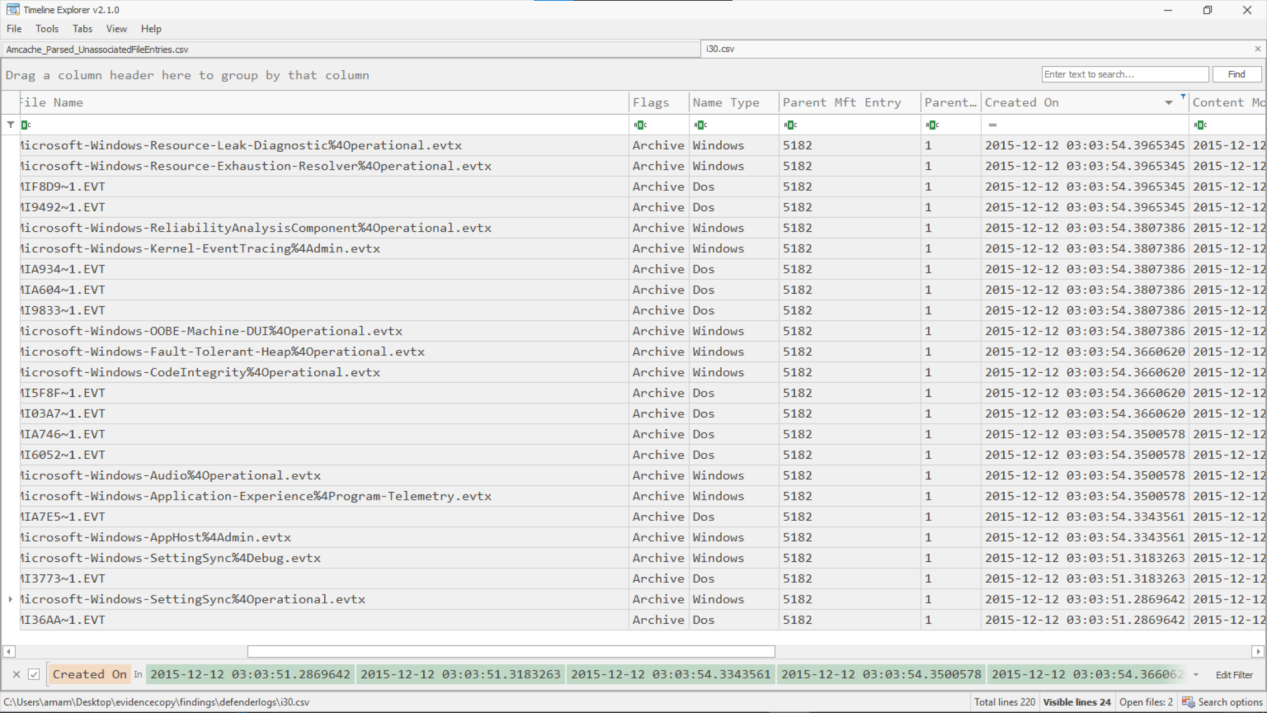
“Hi”, “We’re getting things ready for you”, etc.

then C:\Program Files\Windows Defender\MpCmdRun.exe was opend due to the activity on the defender i found hear i wanted to look at its log

beforen keeping going with the amcache we going to check C:\Windows\System32\winevt\Logs\

the logs of events at the time we found on amcache wasnt there so we tried with $I30

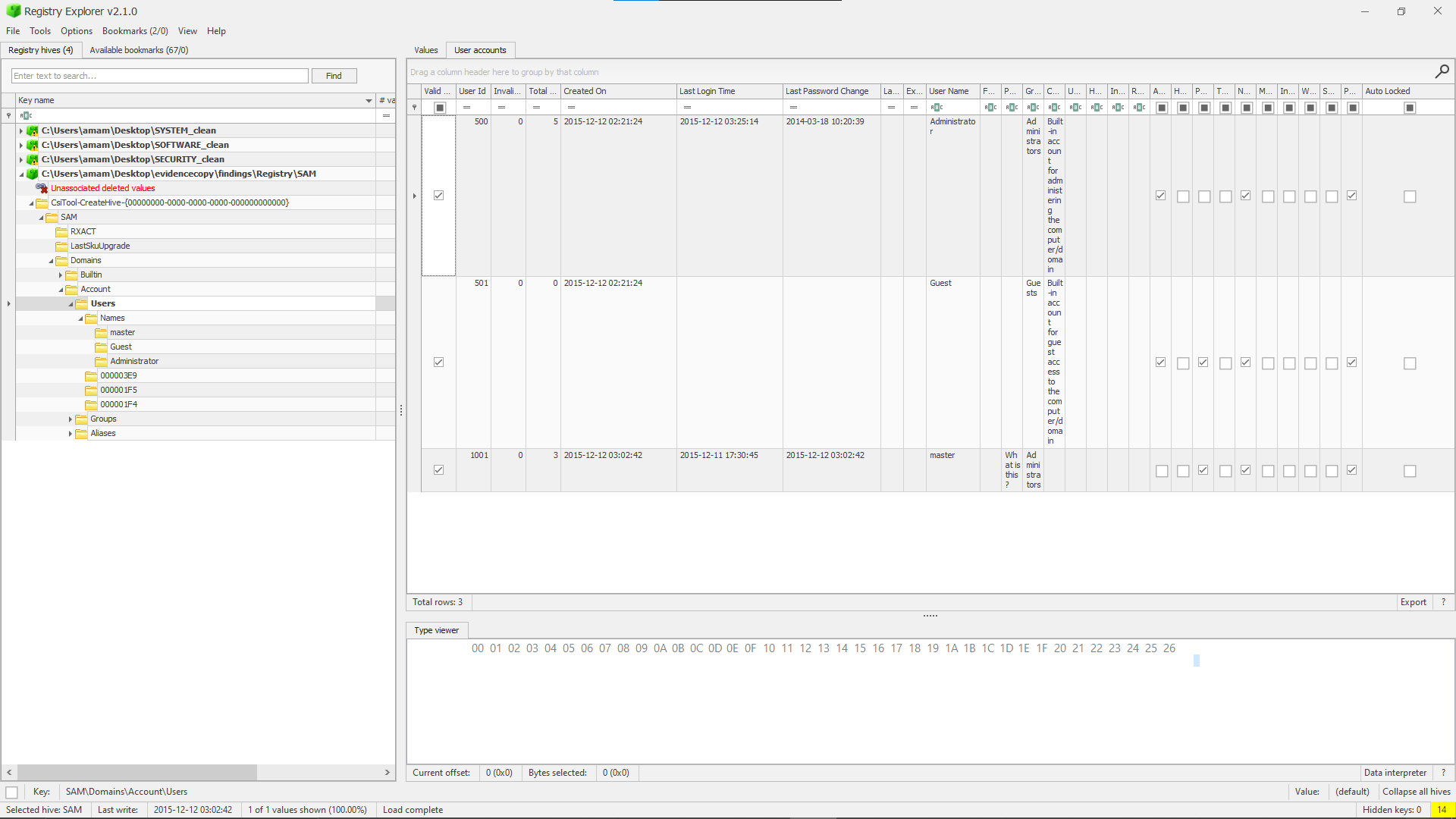
the files we are loking for cant be found any where so this looks like anti forensics



8:23 AM 11/28/2025 now we go back to the amcache files

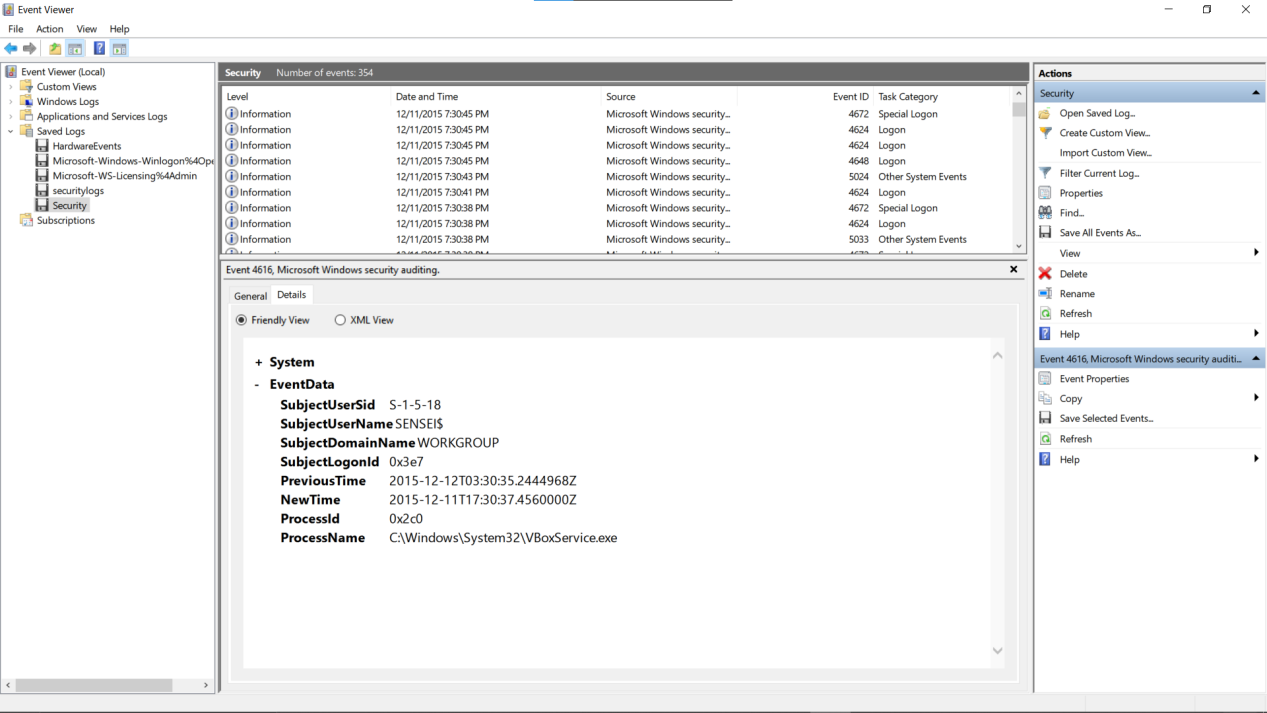
9:32 AM 11/28/2025 we can find C:\Windows\System32\ThumbnailExtractionHost.exe at 3:4 whcih could indicate malicious

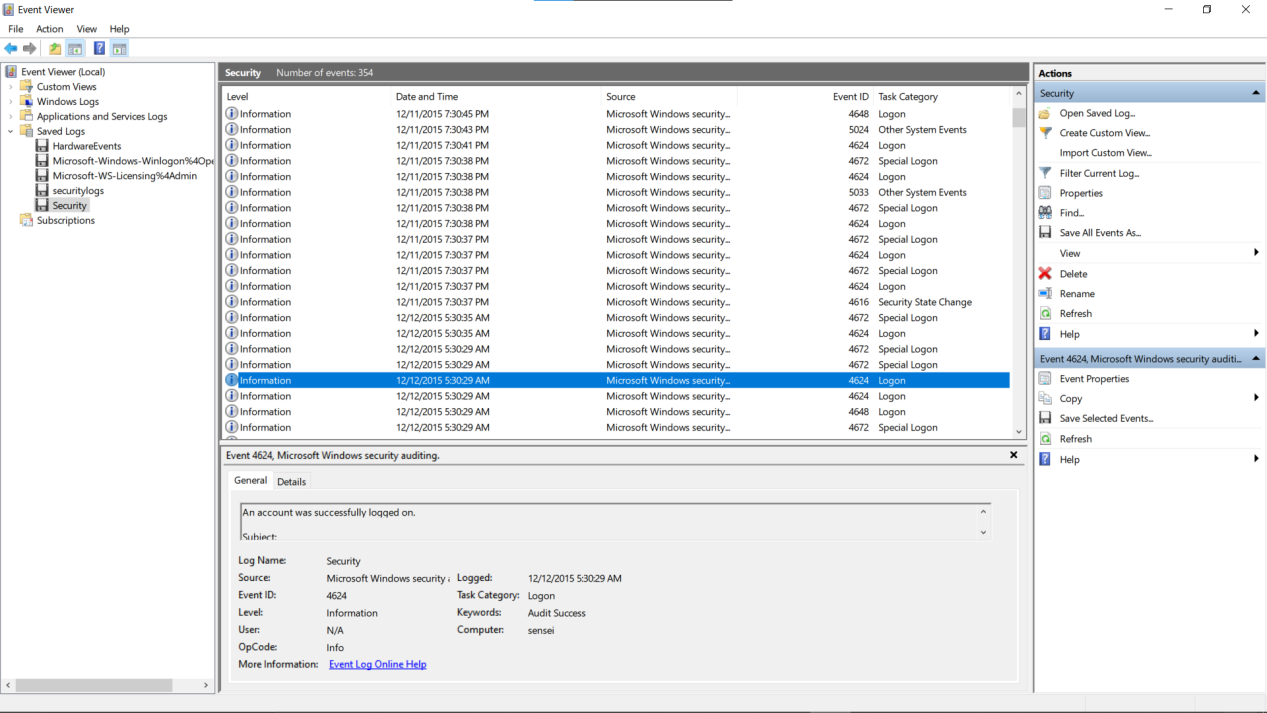
10:03 AM 11/28/2025 looking back at the SAM hive found that the dates changes for a user called master and administrator

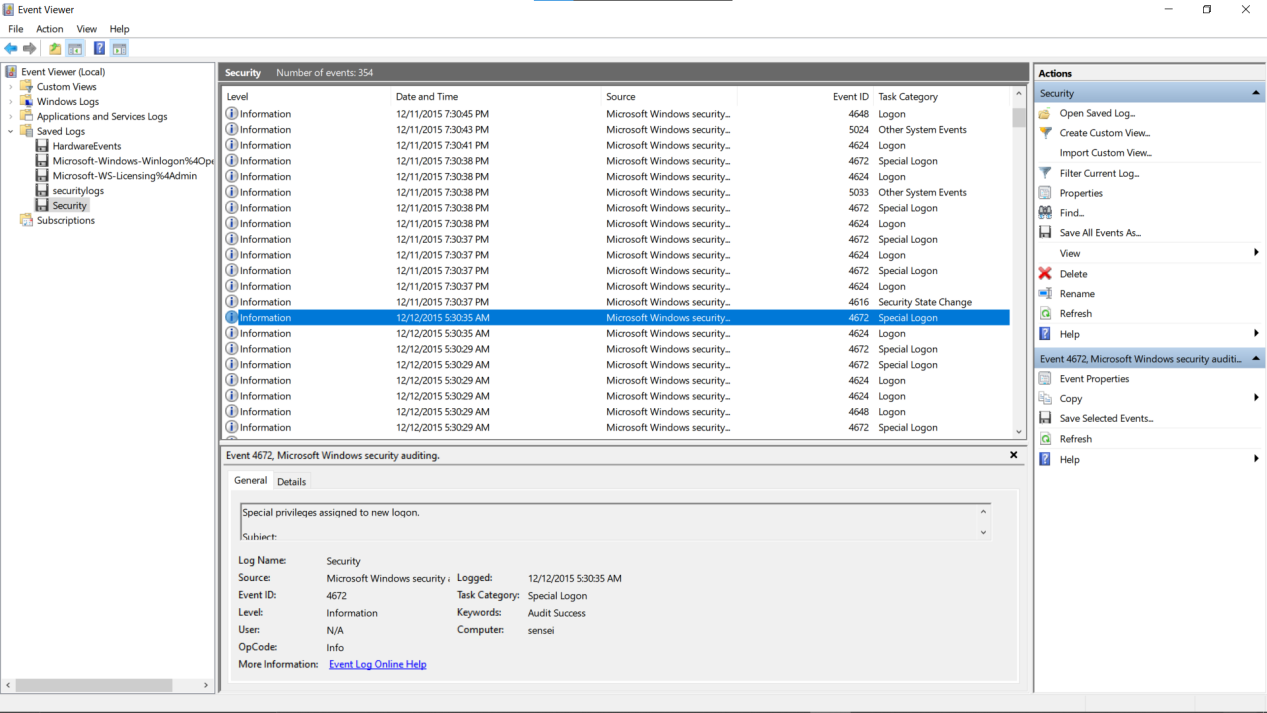


2:17 PM 11/28/2025 found in securtiy log that system time was changed at 2015-12-12T03:30:35.2444968Z and necame 2015-12-11T17:30:37.4560000Z

that heppend after a log in had happend and Special privileges assigned to new logon.



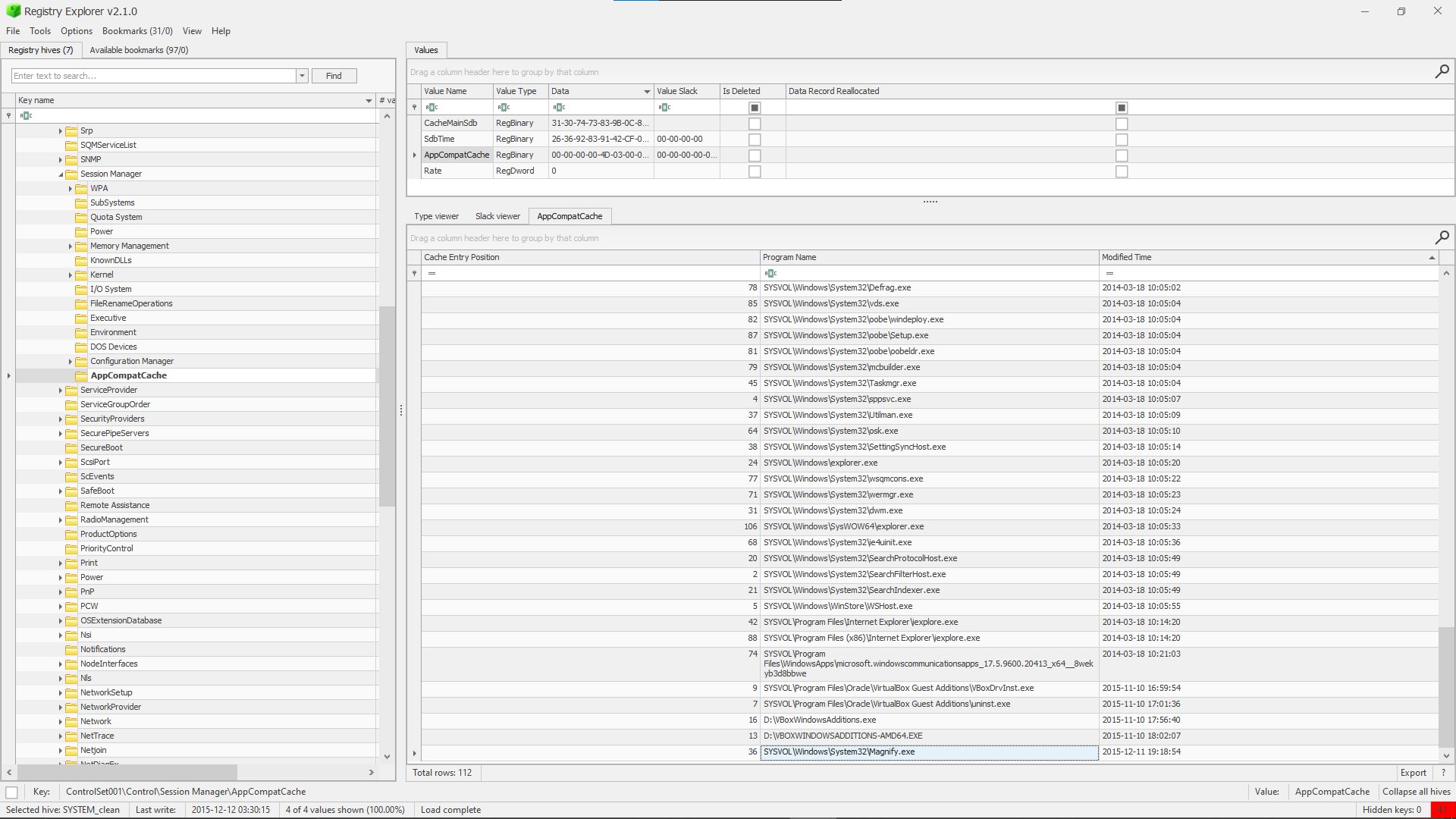




The susoucios thing here now that the master user that we found involved in a couple of thing s was created at 15\12\12 3:2:42 and was last login time 2015\12\11 17:30:45 the exact same time that the time chacnge which means that it was him who changed it that was supported by the files found in it and the idea of it created in one day and all of that happened after its creation we also know that the message was created at 2015\12\12 3:24:39

So due to the time change we can say that it was changed for something that happened but that is not supported because the rest of the files still have the same date or some thing that is going to happen and the user want to make look as if its old maybe a malicpus payload since the user have access to the device looked back in amache but nothing

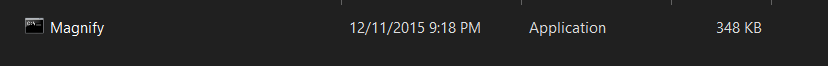
So we opend AppCompatCahe on SYSTEM hive this is used for tracks applications that were **executed or attempted to run** on the system even if it was deleted we locked for the changed time and after it 2015\12\11 17:30:45 at 2015\12\11 19:18:54 we found that the application magnify.exe was opend that appliction literley have no tecknical use so lets check it



We will open its path on ftk imger

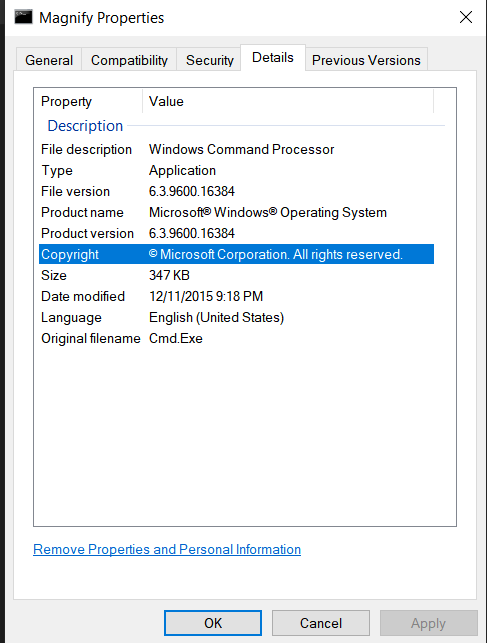
Found lets just do a fast google search on it nothing important online so lets open it on a my private pc

magnifier on my pc



That it it’s a malicous payload could be a trusion

This is an **Ease of Access privilege escalation attack**



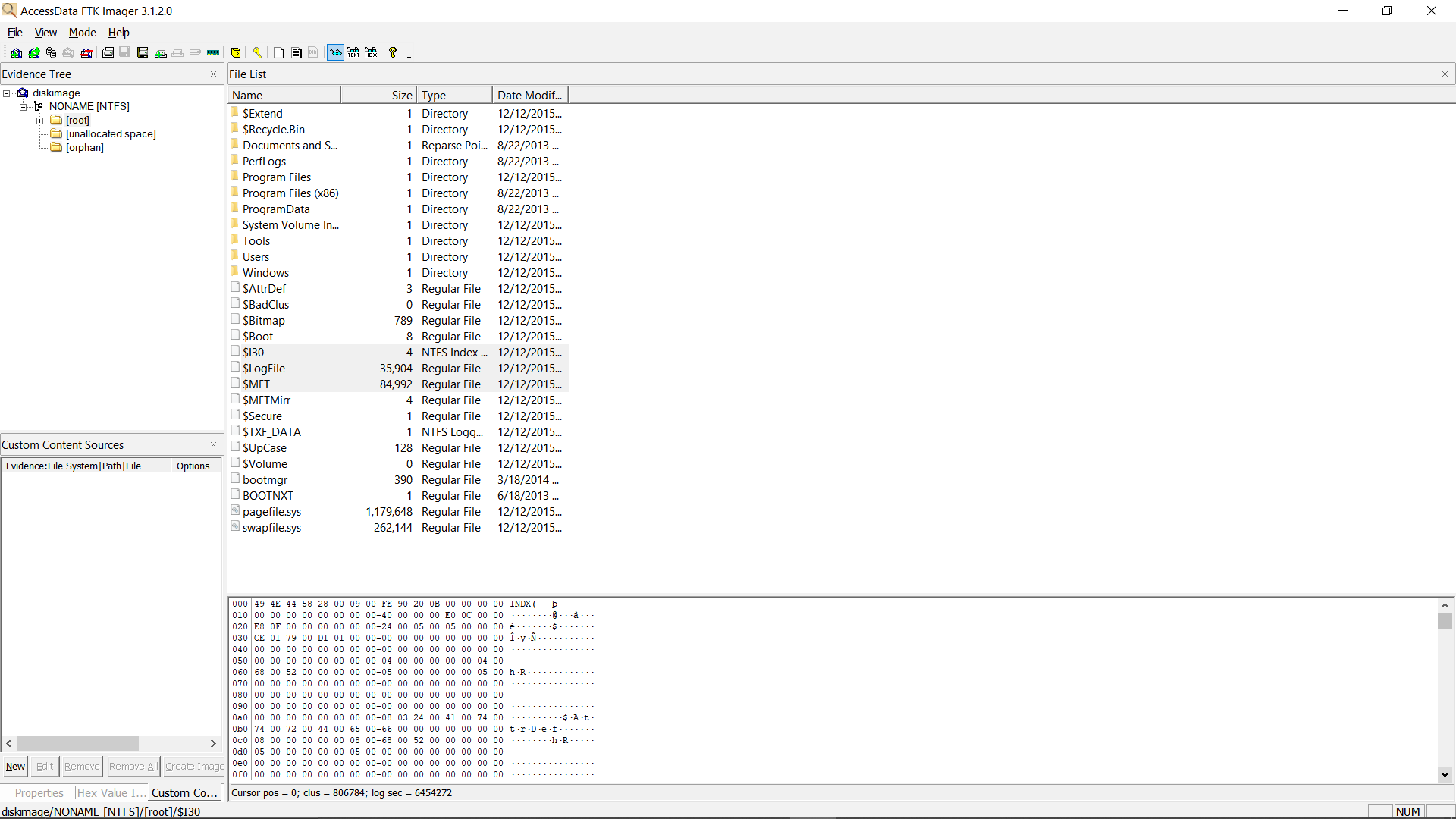
That is what was used to hack into the system

Now we finished the investigation lets use easue

couldn’t recover anything because it needs a subscribtion

While using the mmls on the diskimage nothing showed because the file consist of one partition so the sleuthkit wouldn’t have any meaning we need to mount the disk image so I found it useful to use ftk imager for the investigation

BY PROCESSING the $MFT file



We found the time line for accessing the magnify

