TryHackMe: Disk Analysis & Autopsy

Sean Dixon · Follow
7 min read · Jun 13, 2023

Overview: Disk Analysis & Autopsy is a Medium-difficulty forensics challenge. It involves analyzing a forensic disk image in Autopsy to determine what malicious software was installed, by which users, and to uncover various other artifacts.

Scenario: Your task is to perform a manual analysis of the artifacts discovered by Autopsy to answer the questions below.

This room should help to reinforce what you learned in the Autopsy room. Have fun investigating!

> *Q1*
>
> *What is the MD5 hash of the E01 image?*

We can find the hash of the image by selecting the appropriate data source in Autopsy and navigating to the Container tab under Summary.

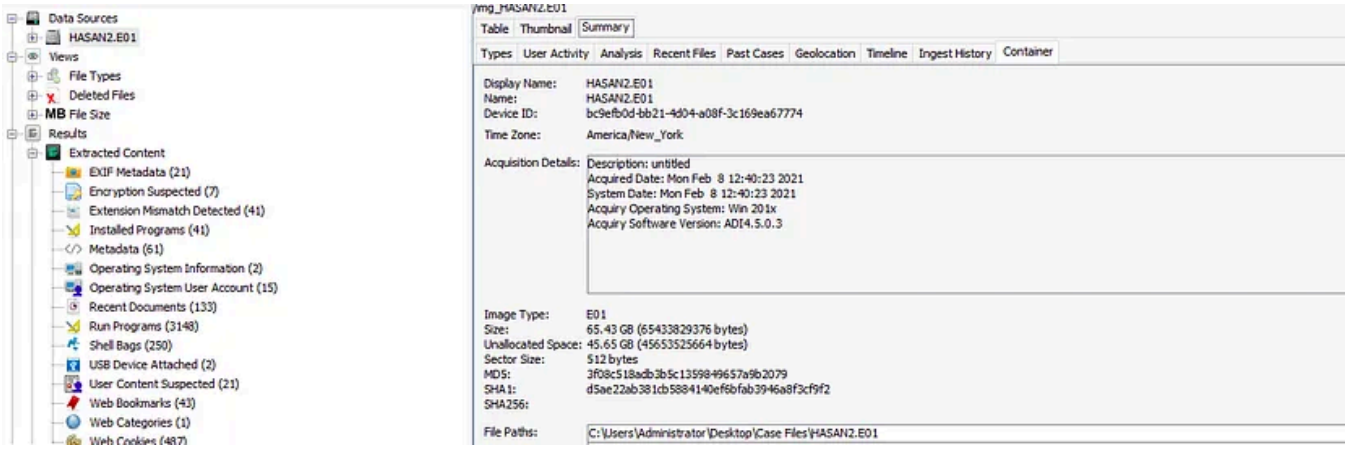
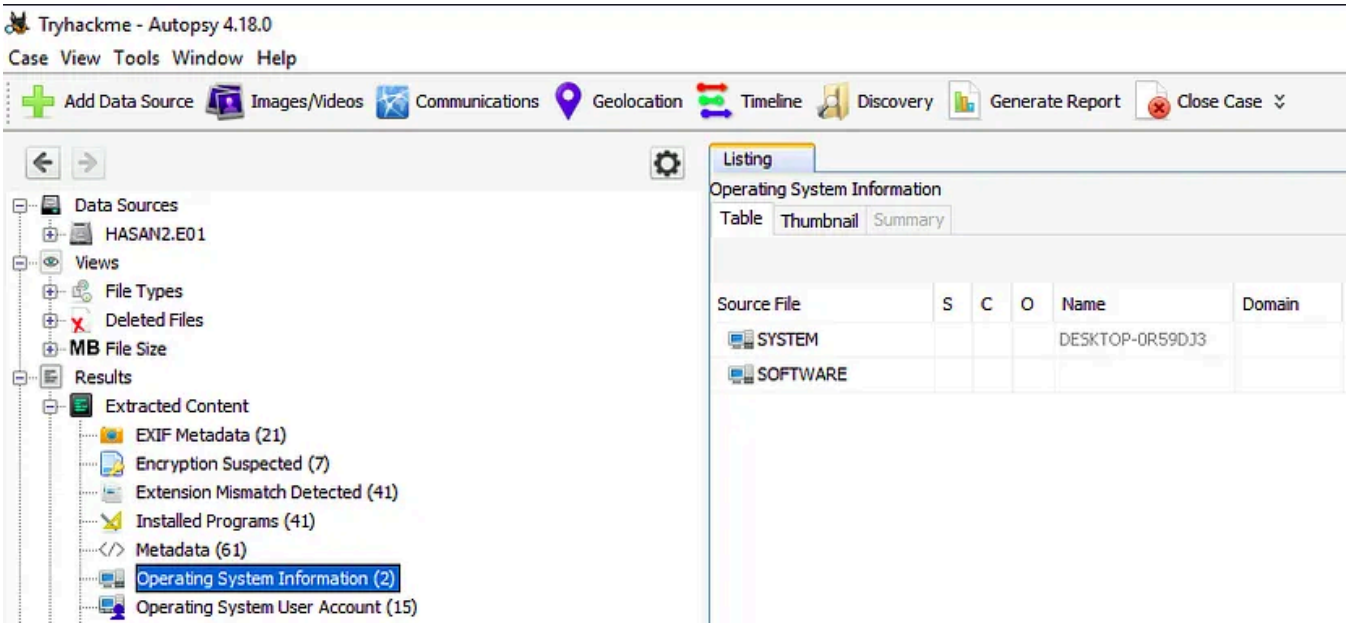


Image summary information, including hash values

Answer: 3f08c518adb3b5c1359849657a9b2079

> *Q2*
>
> *What is the computer account name?*

We can find the computer name under the results for *Operating System Information.*

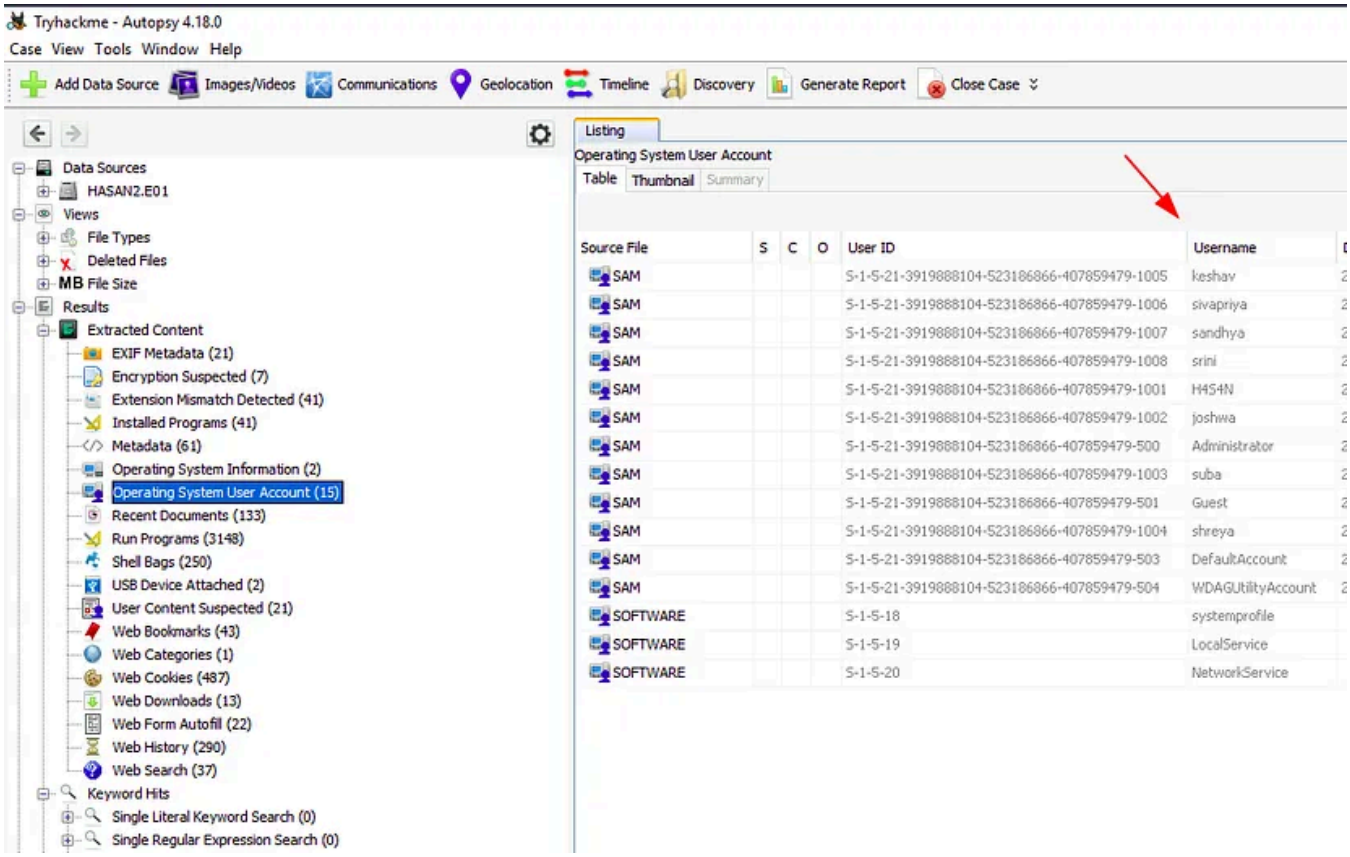


Computer name under the OS Information results.

Answer: DESKTOP-0R59DJ3

> *Q3*
>
> ***List all the user accounts. (alphabetical order)***

Just below the *Operating System Information* results, we see an option for *Operating System User Accounts*, we can get our answer from there.



List of user accounts

Note: We only need user accounts, so we can ignore Guest, LocalService, DefaultAccount, etc.

Answer: H4S4N,joshwa,keshav,sandhya,shreya,sivapriya,srini,suba

> *Q4*
>
> ***Who was the last user to log into the computer?***

We can sort the User Accounts by “Date Accessed” to get our answer.

Listing

Operating System User Account

Table | Thumbnail | Summary

Source File	S	C	O	User ID	Username	Date Created	Date Accessed	Count
SAM				S-1-5-21-3919888104-523186866-407859479-1006	sivapriya	2021-02-06 05:39:55 EST	2021-02-07 12:05:37 EST	10
SAM				S-1-5-21-3919888104-523186866-407859479-1001	H4S4N	2021-02-06 18:48:16 EST	2021-02-07 12:05:11 EST	24
SAM				S-1-5-21-3919888104-523186866-407859479-1004	shreya	2021-02-06 05:38:48 EST	2021-02-07 11:46:52 EST	13
SAM				S-1-5-21-3919888104-523186866-407859479-1003	suba	2021-02-06 05:38:22 EST	2021-02-07 11:46:01 EST	2
SAM				S-1-5-21-3919888104-523186866-407859479-1008	srini	2021-02-06 05:41:10 EST	2021-02-07 11:45:42 EST	2
SAM				S-1-5-21-3919888104-523186866-407859479-1007	sandhya	2021-02-06 05:40:42 EST	2021-02-07 11:45:11 EST	5
SAM				S-1-5-21-3919888104-523186866-407859479-1005	keshav	2021-02-06 05:39:20 EST	2021-02-07 11:45:00 EST	5
SAM				S-1-5-21-3919888104-523186866-407859479-1002	joshwa	2021-02-06 05:38:00 EST	2021-02-07 11:44:49 EST	5

User accounts, sorted by Date Accessed

Answer: sivapriya

> *Q5*
>
> *What was the IP address of the computer?*

Since we're working with an image of a Windows machine, we can find the IP address associated with network adapters in the Windows Registry. We can even access the registry from within Autopsy.

/img_HASAN2.E01/vol_vol3/Windows/System32/config/SYSTEM - Editor

/img_HASAN2.E01/vol_vol3/Windows/System32/config/SYSTEM | /img_HASAN2.E01/vol_vol3/Windows/System32/config/SOFTWARE

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

- SysMain
- SystemEventsBroker
- TabletInputService
- TapiSrv
- Tcpip
  - Linkage
  - Parameters
    - Adapters
    - DNSRegisteredAdapters
    - Interfaces
      - {df70681e-dcc3-4511-8a23-958c3ab03d
      - {e42cf5d6-2174-470f-9b1d-0d44858906
      - {f73911d8-68d4-11eb-b57e-806e6f6e69
    - NsiObjectSecurity
    - PersistentRoutes
    - Winsock
    - DataBasePath
    - Domain
    - ForwardBroadcasts
    - ICSDomain
    - IPEnableRouter
    - NameServer
    - SyncDomainWithMembership
    - NV Hostname
    - Hostname
    - TcpWindowSize

Metadata

Name: **{e42cf5d6-2174-470f-9b1d-0d448589066c}**
Number of subkeys: 0
Number of values: 18

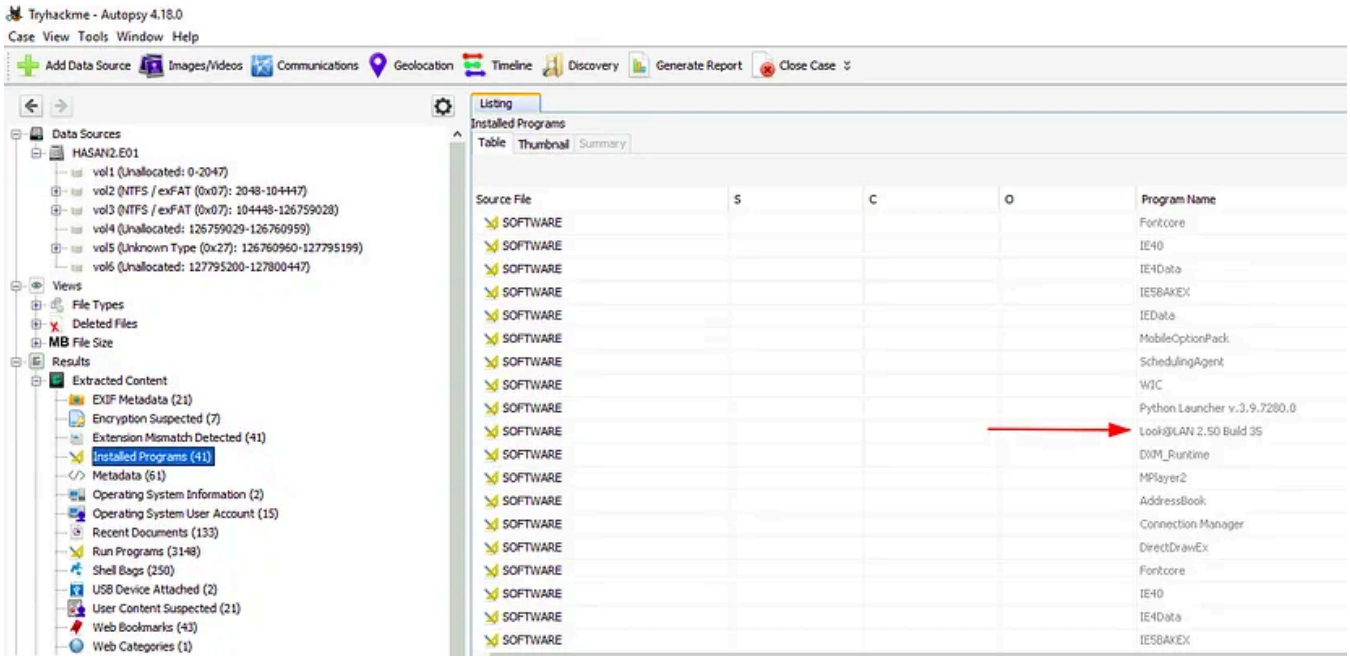
Values

Name	Type	Value
EnableDHCP	REG_DWORD	0x00000001 (1)
Domain	REG_SZ	(value not set)
NameServer	REG_SZ	(value not set)
DhcpIPAddress	REG_SZ	0.0.0.0
DhcpSubnetMask	REG_SZ	255.0.0.0
DhcpServer	REG_SZ	255.255.255.255
Lease	REG_DWORD	0x00000e0f (3599)
LeaseObtainedTime	REG_DWORD	0x60201dc4 (1612717508)
T1	REG_DWORD	0x602024cb (1612719307)
T2	REG_DWORD	0x60202a11 (1612720657)
LeaseTerminatesTime	REG_DWORD	0x60202bd3 (1612721107)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)
DhcpConnForceBroadcastFlag	REG_DWORD	0x00000000 (0)
DhcpInterfaceOptions	REG_BIN	FC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00...
DhcpIsMeteredDetected	REG_DWORD	0x00000001 (1)
DhcpGatewayHardware	REG_BIN	C0 A8 C6 21 06 00 00 00 7A B1 B8 86 E6 A7
DhcpGatewayHardwareCount	REG_DWORD	0x00000001 (1)

Network interface key, viewed in Autopsy

No such luck, the IP address is listed as 0.0.0.0. We'll have to find it elsewhere.

While looking through Autopsy's findings, we notice an unusual application installed on the device.

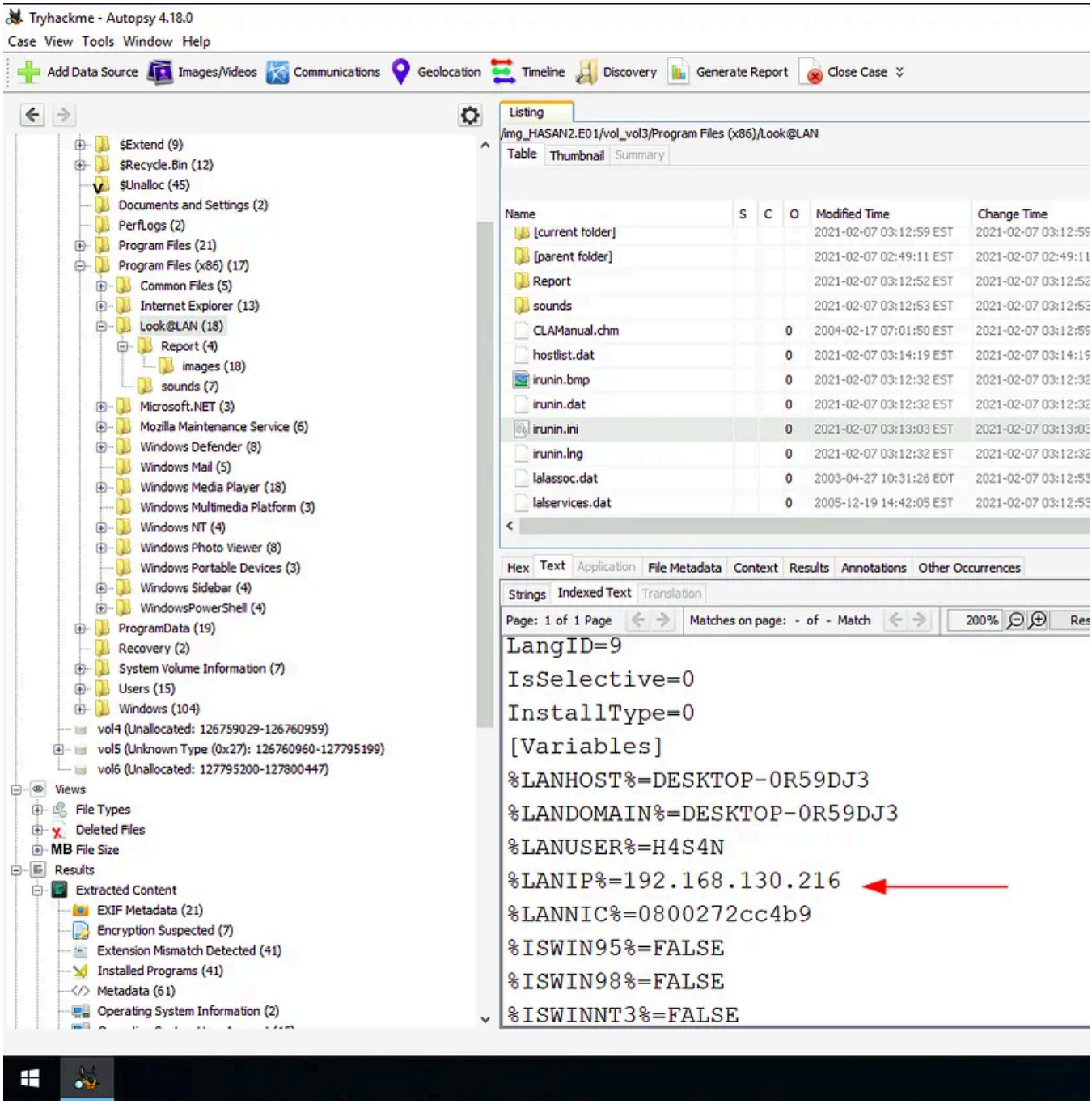


Look@LAN listed among the installed applications

Searching for the executable name tells us it is a network monitoring tool, so let's look for any logs it may have generated. We find its directory under *Program Files (x86)*. Among the files in the folder, only one stands out, a .ini file. We can view the file within Autopsy by selecting it.

Note: .ini files are used to set initial configurations.

Note: If you don't see the text after selecting the file, switch to the Indexed Text tab.

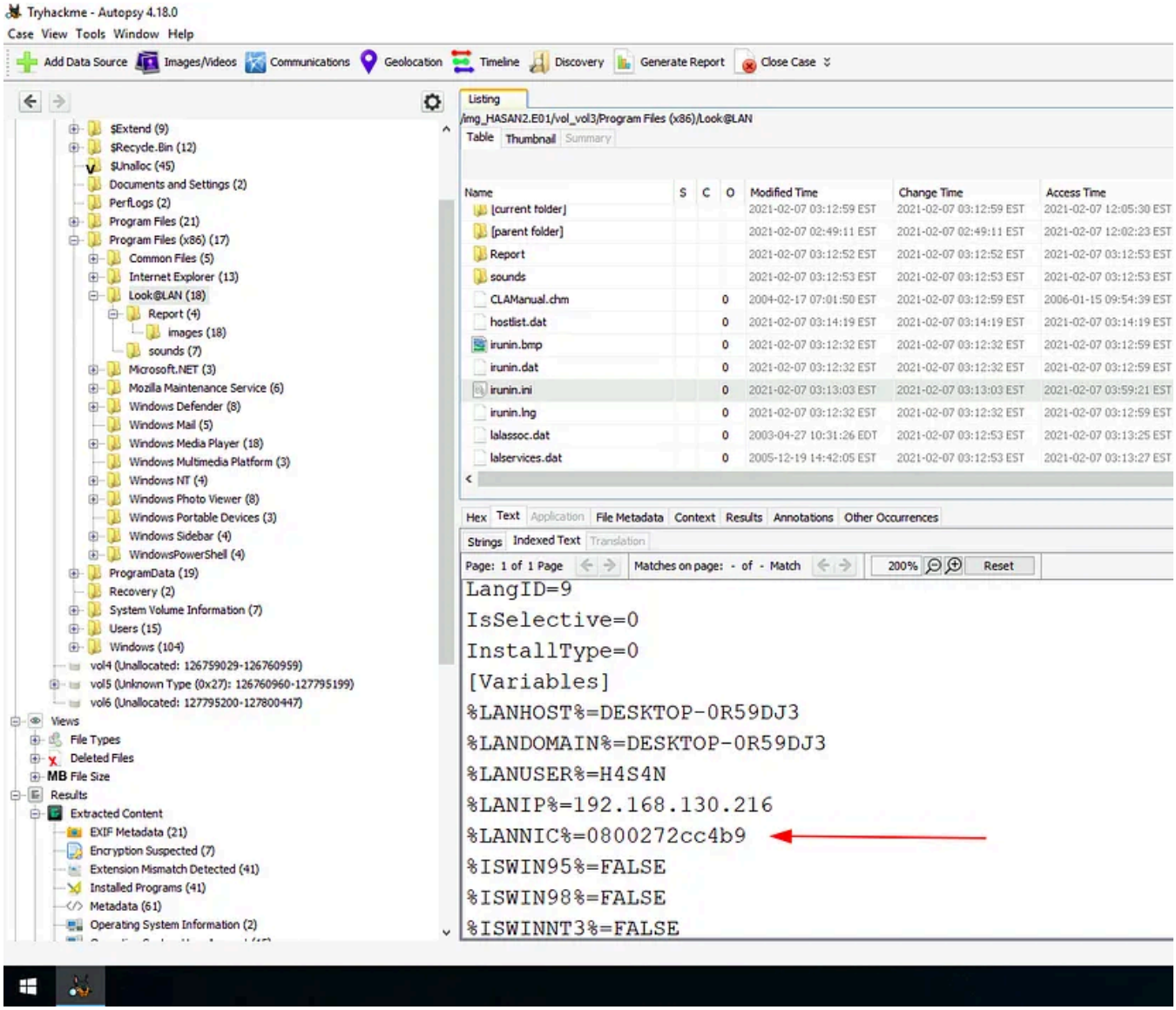


IP Address as listed in the Look@LAN .ini file

Answer: 192.168.130.216

> *Q6*
>
> *What was the MAC address of the computer? (XX-XX-XX-XX-XX-XX)*

The MAC address is easy to overlook, it wasn't present in the registry, and searching for the string "mac" within the .ini file returns no results. But, if we take a second look at the fields surrounding the IP address, we'll notice there is one for LANNIC.



LANNIC listed in the Look@LAN .ini file

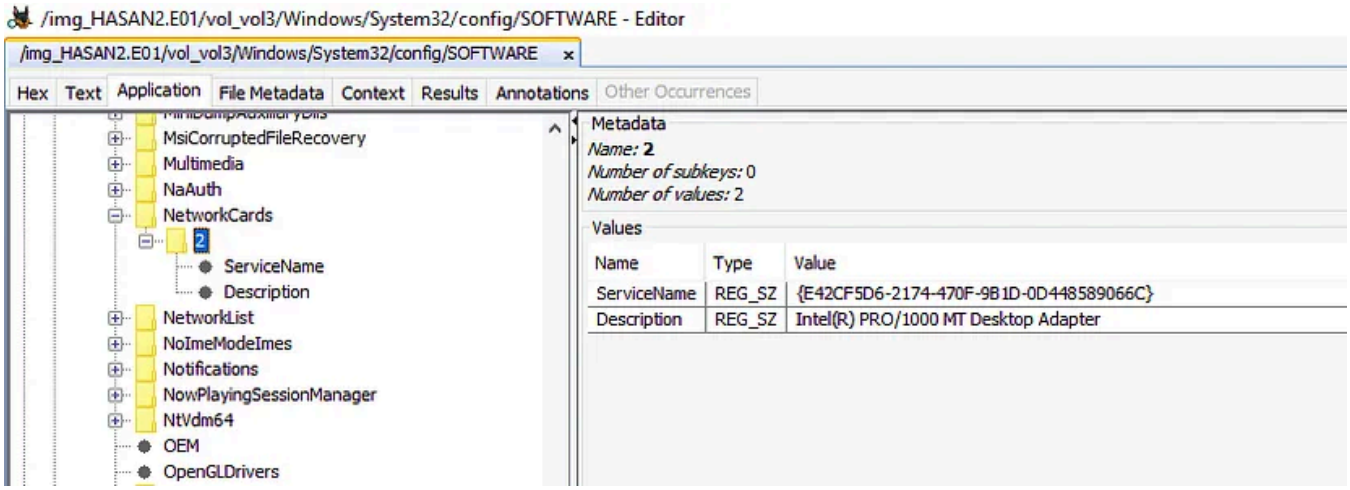
The answer is formatted to use hyphens, so we just have to format the string accordingly.

Answer: 08–00–27–2c-c4-b9

> *Q7*
>
> ***What is the name of the network card on this computer?***

We'll return to the registry to get the name of the NIC.

We can find the name of the NIC under the following path: *SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards*



NetworkCards registry key

Answer: Intel(R) PRO/1000 MT Desktop Adapter

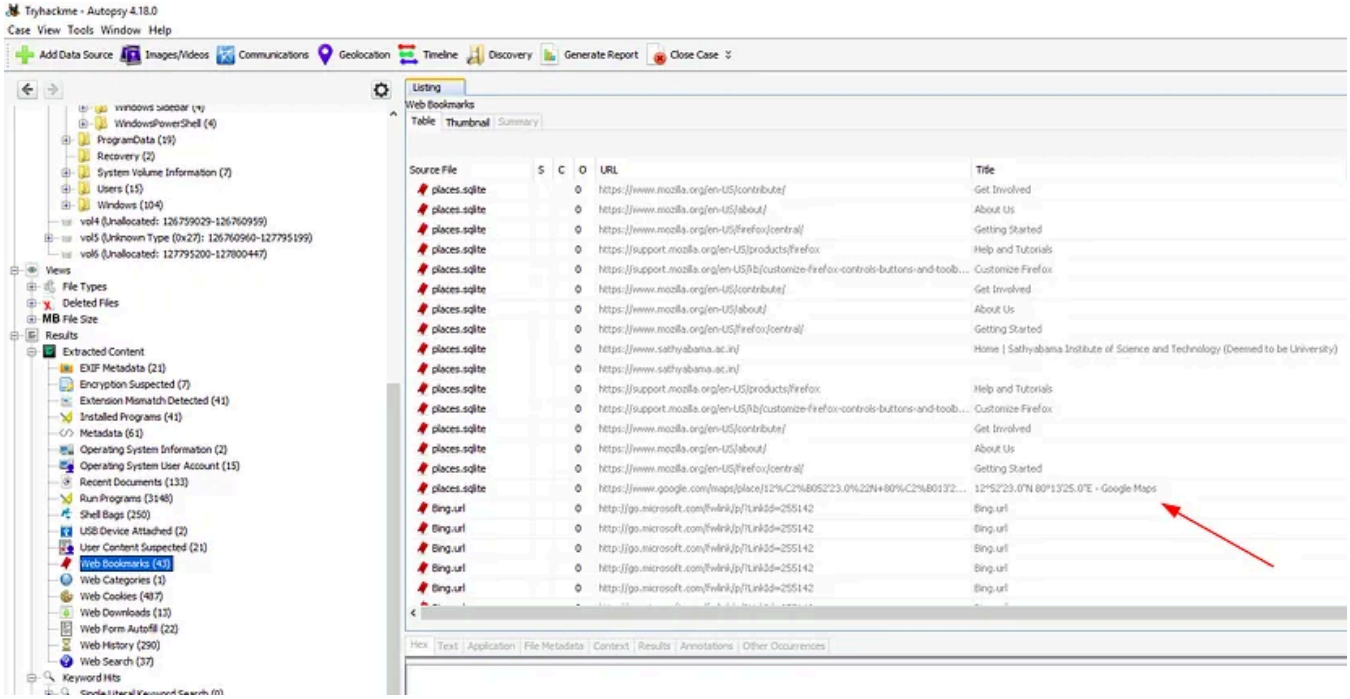
> *Q8*
>
> *What is the name of the network monitoring tool?*

As we've seen, the tool installed is Look@LAN.

Answer: Look@LAN

> *Q9*
>
> *A user bookmarked a Google Maps location. What are the coordinates of the location?*

Autopsy's *Web Bookmarks* results will give us the answer to this question.

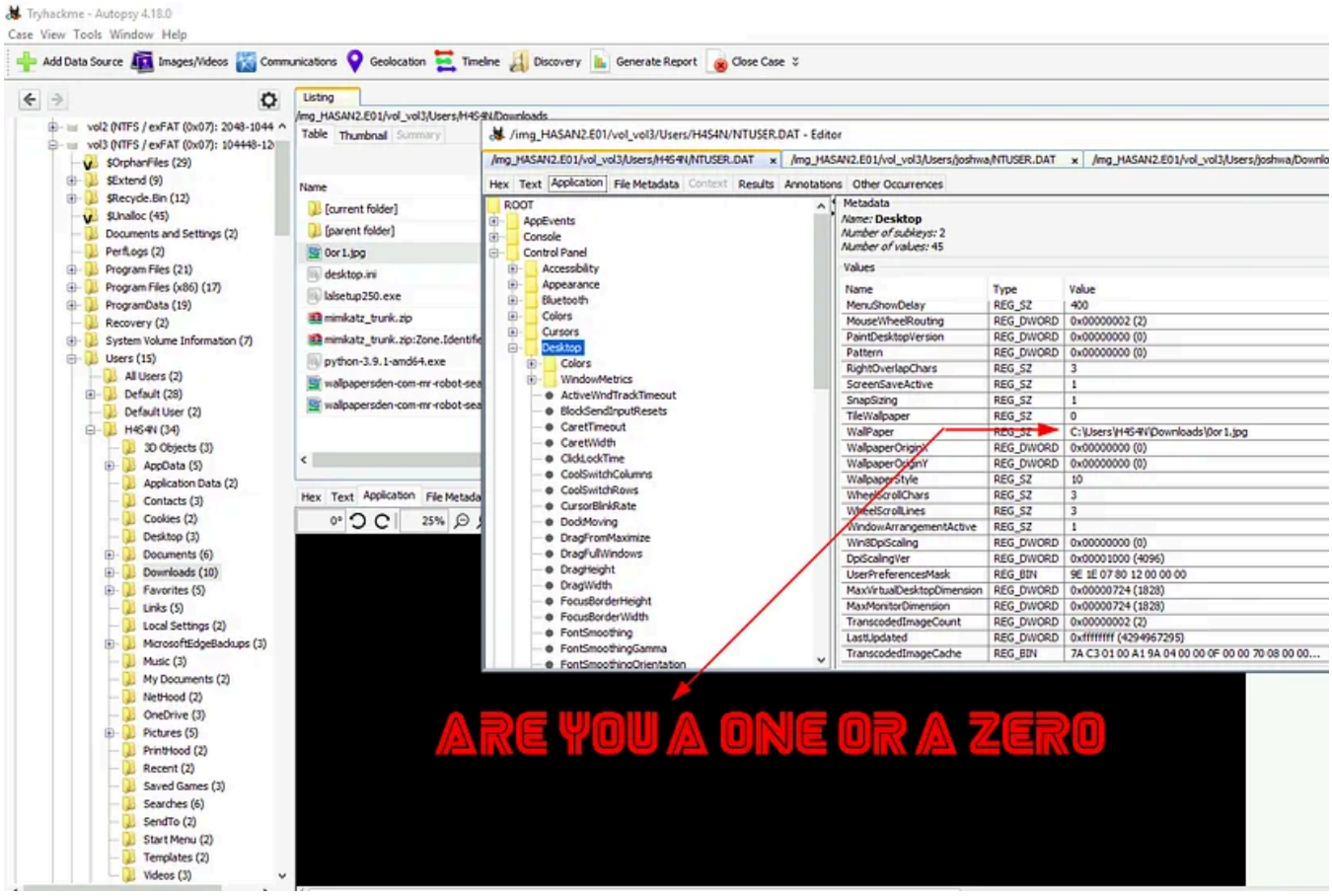


Autopsy results for Web Bookmarks

Answer: 12°52'23.0"N 80°13'25.0"E

> *Q10*
>
> *A user has his full name printed on his desktop wallpaper. What is the user's full name?*

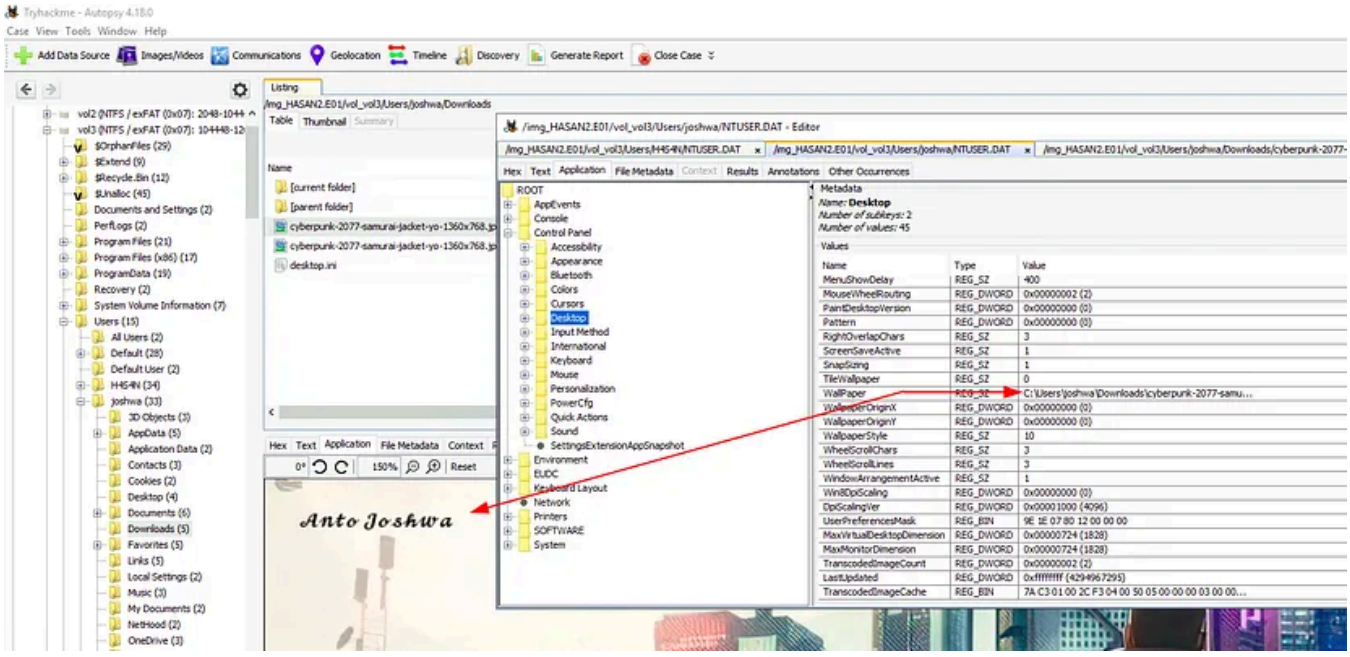
Windows stores user profile information in the NTUSER.dat file; located within their home directory. Knowing this, we can determine user wallpaper images and whether their name is visible in the image.



NTUSER.dat and wallpaper for the H4S4N user.

The first user in the list is H4S4N. After determining the wallpaper's source file in NTUSER.dat, we can check the image. The wallpaper image does not have a visible name, so we'll move on down the list.

Next on the user list is Joshwa, this time we've got a match.



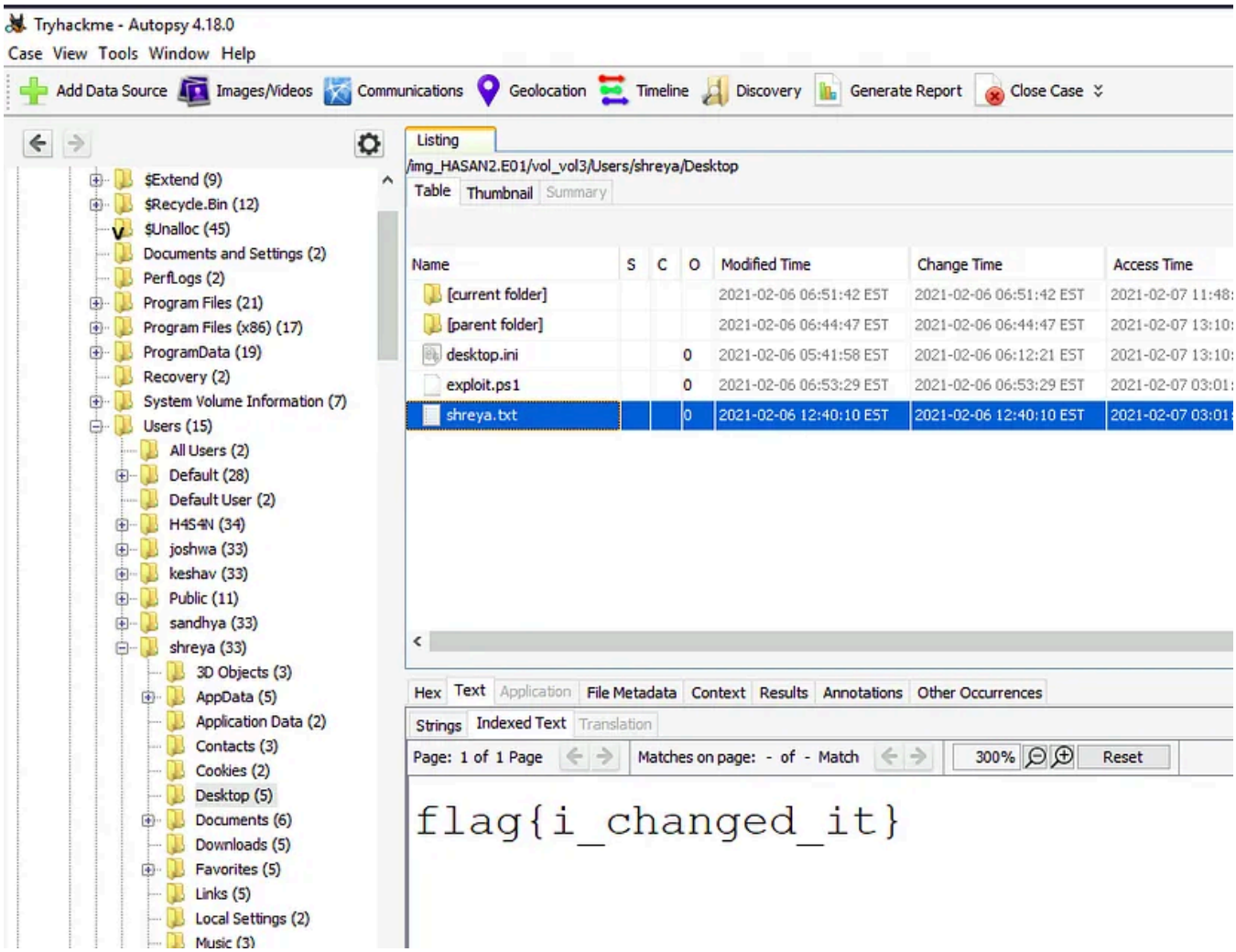
NTUSER.dat and wallpaper for Joshwa user

We can see a name in the image and the last name matches the username, so this looks like our answer.

Answer: Anto Joshwa

> *Q11*
>
> ***A user had a file on her desktop. It had a flag but she changed the flag using PowerShell. What was the first flag?***

PowerShell command history is stored in *APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt,* so that will be the focus of our search. Before we start there, however, let's determine what the file is named and who the user is.

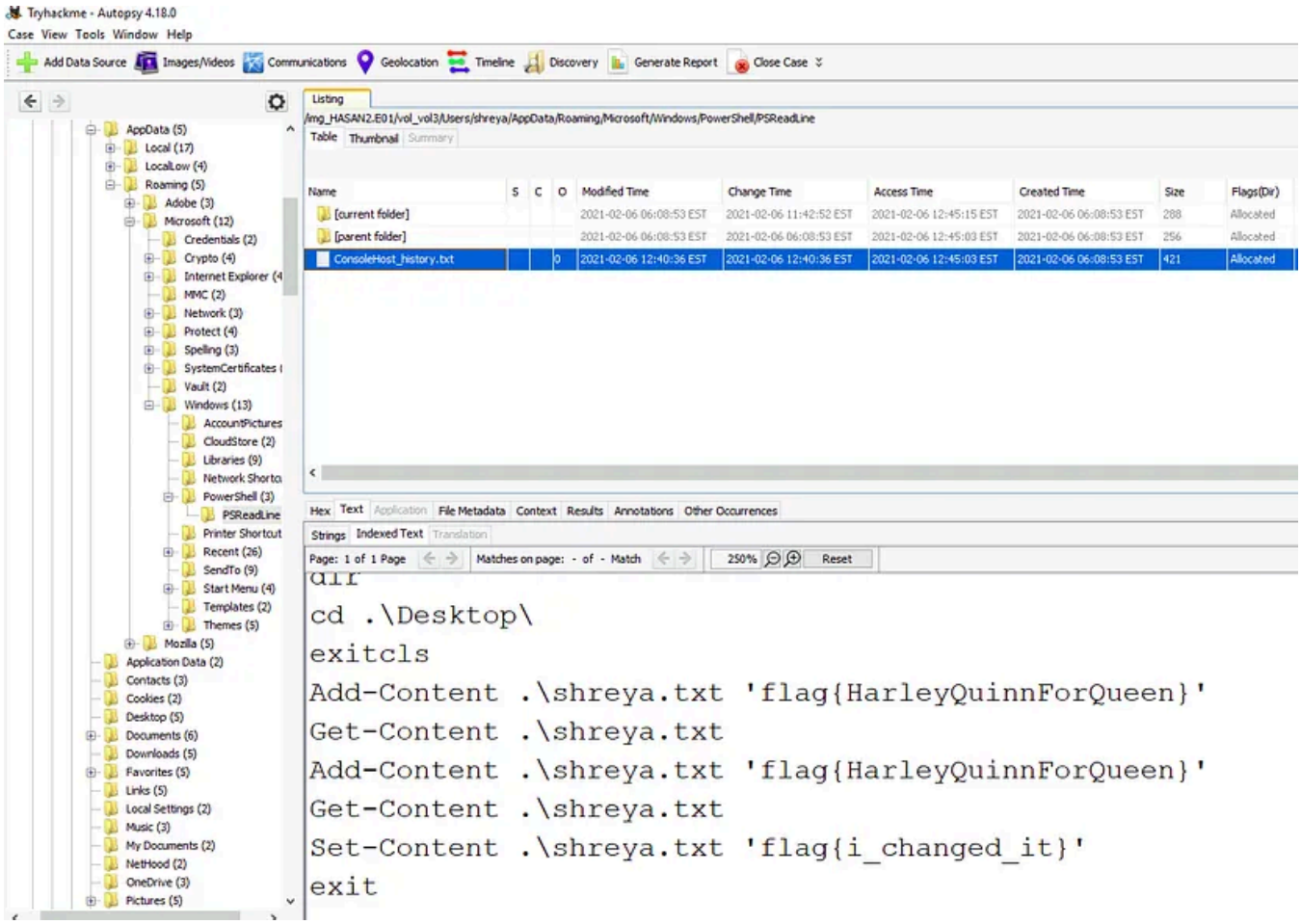


shreya.txt file on the shreya user's desktop

After checking some of the user's Desktops, we locate the flag within the shreya user's Desktop directory. Now that we know the user, we'll check the PowerShell history for the account.

Note: There is also a PowerShell script on the user's desktop named exploit.ps1, we should take a note of this for later.

As expected, we find the PowerShell history in the path mentioned previously.

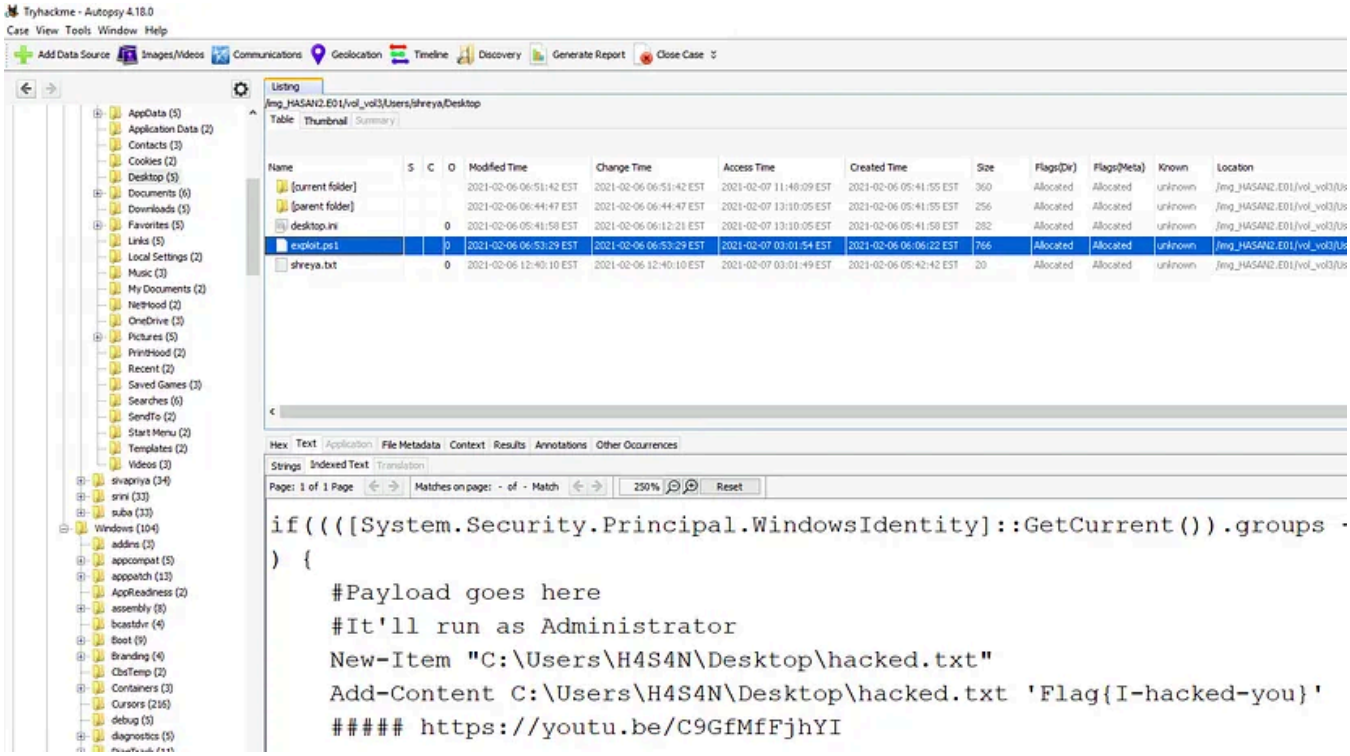


PowerShell history for the shreya user

Answer: flag{HarleyQuinnForQueen}

> *Q12*
>
> *The same user found an exploit to escalate privileges on the computer. What was the message to the device owner?*

We noted a PowerShell script named exploit in the previous question, so we'll go back and look at its contents now.

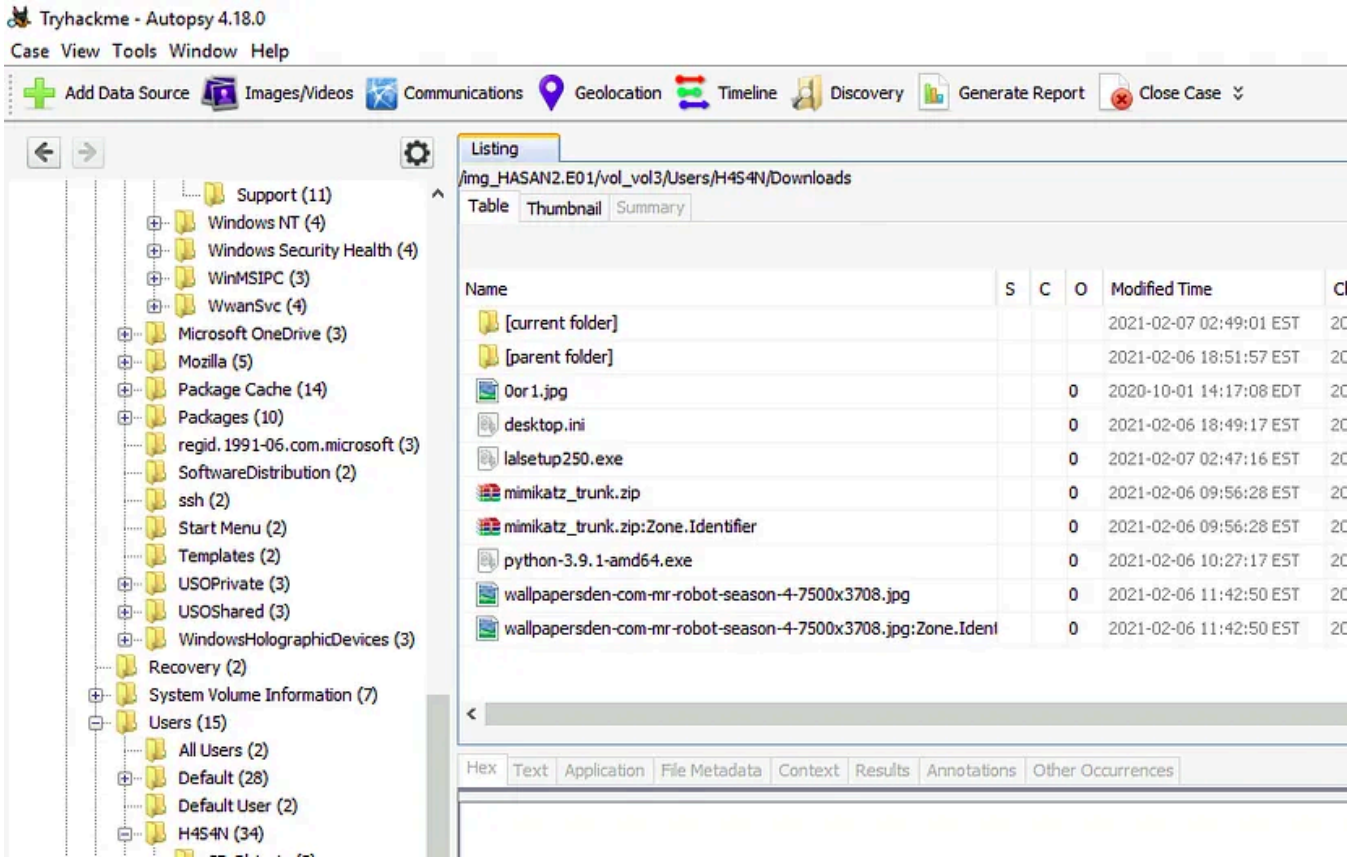


contents of exploit.ps1

Answer: flag{I-hacked-you}

> *Q13*
>
> *2 hack tools focused on passwords were found in the system. What are the names of these tools? (alphabetical order)*

There are multiple signs of Mimikatz on the image which we've likely already noticed, and the zip file is located in H4S4N's Downloads folder.

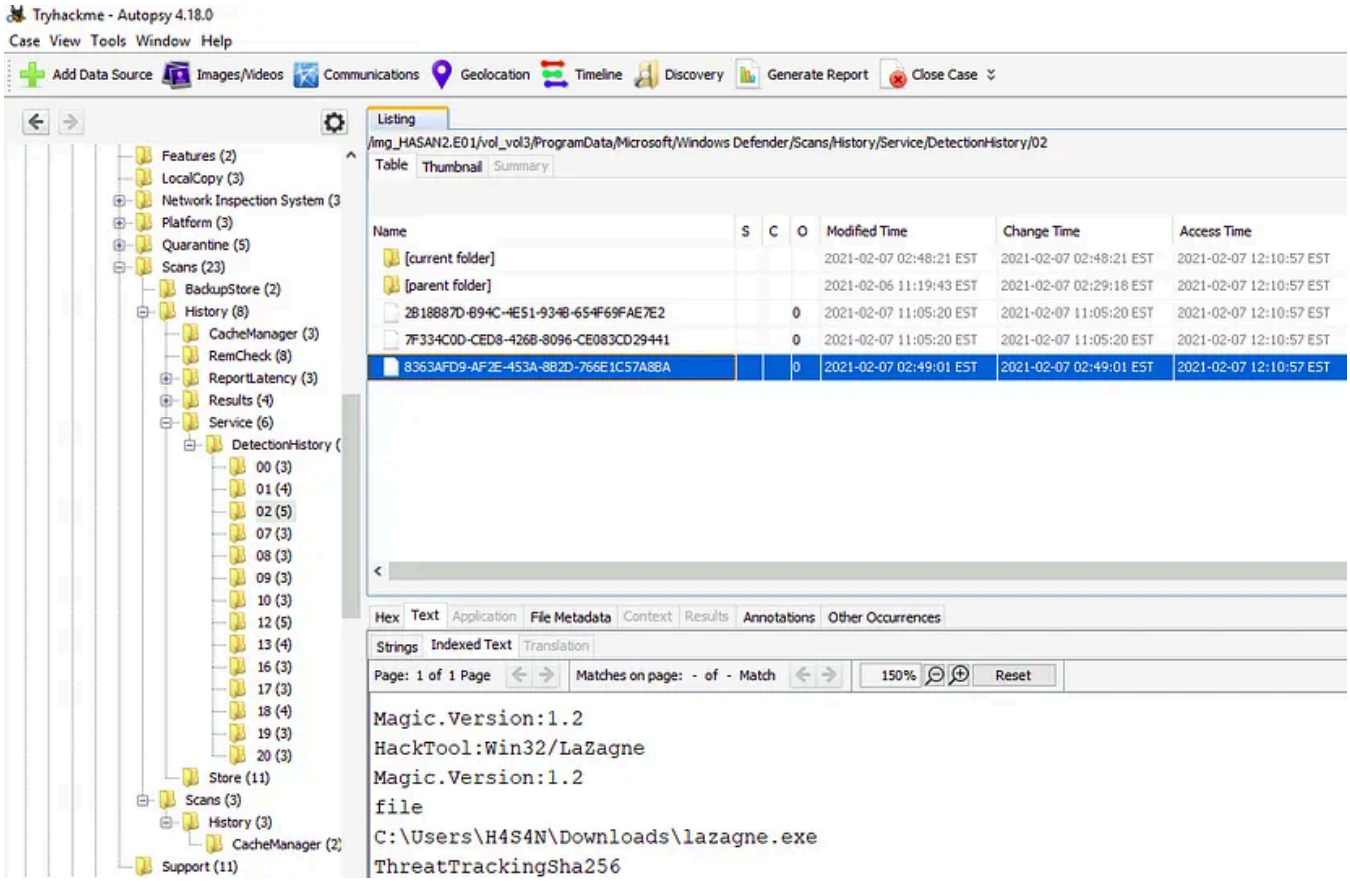


mimikatz_trunk.zip in H4S4N's Downloads folder.

The other executable, however, is elusive. Checking the browser history, downloads, web searches, run programs, installed programs, recent documents, etc. leaves us without any clues.

There was one log source I hadn't thought to utilize before, Windows Defender. With a goal in mind, we'll have to determine where Defender records its alerts.

With enough Googling we find a reference to *C:\ProgramData\Microsoft\Windows Defender\Scans\History, so we'll try there.*



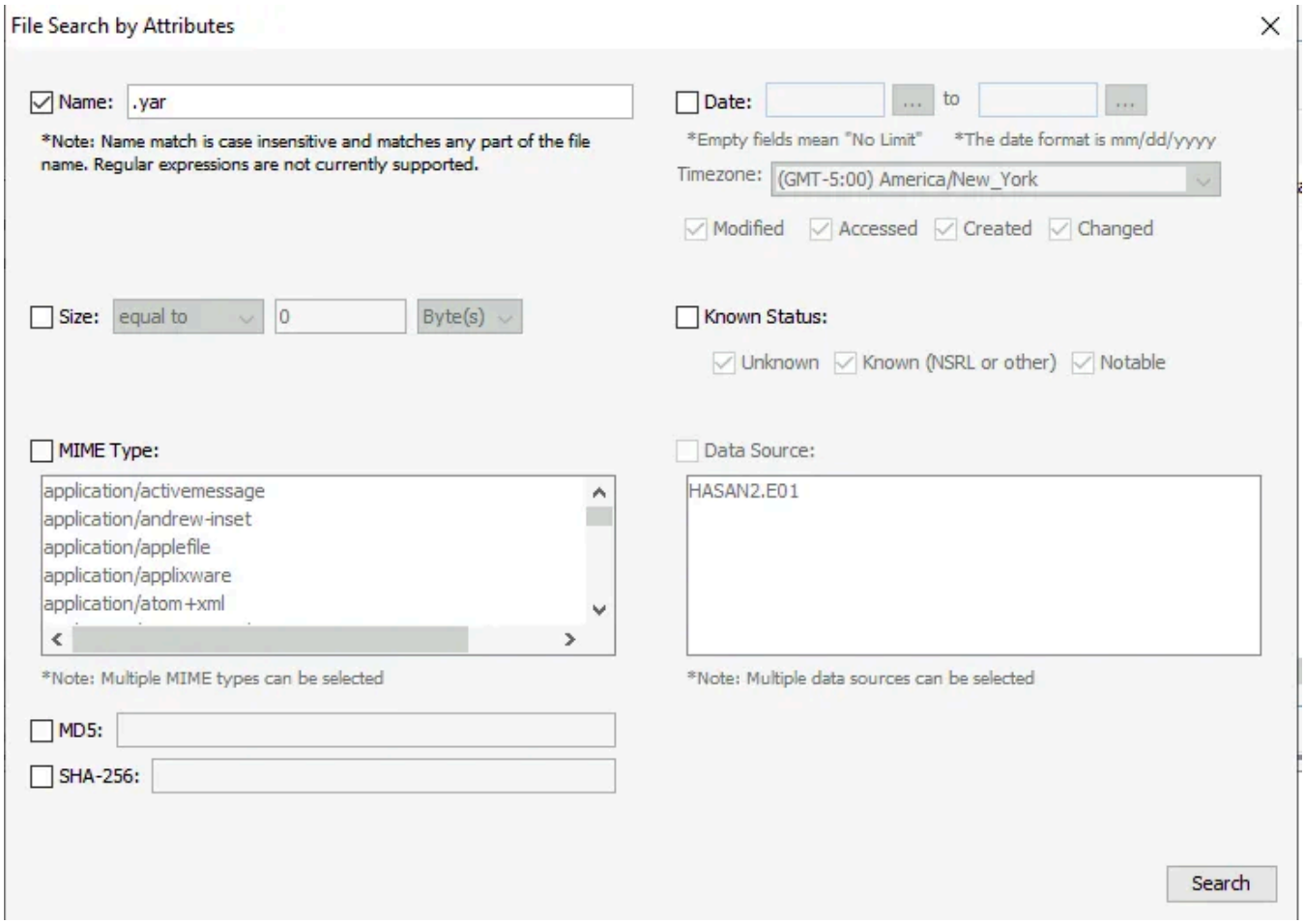
Windows Defender log showing an alert for lazagne.exe

Going through the files in this directory we come across multiple alerts for mimikatz preceding an alert for lazagne.exe. A quick Google informs us it is another password-dumping tool.

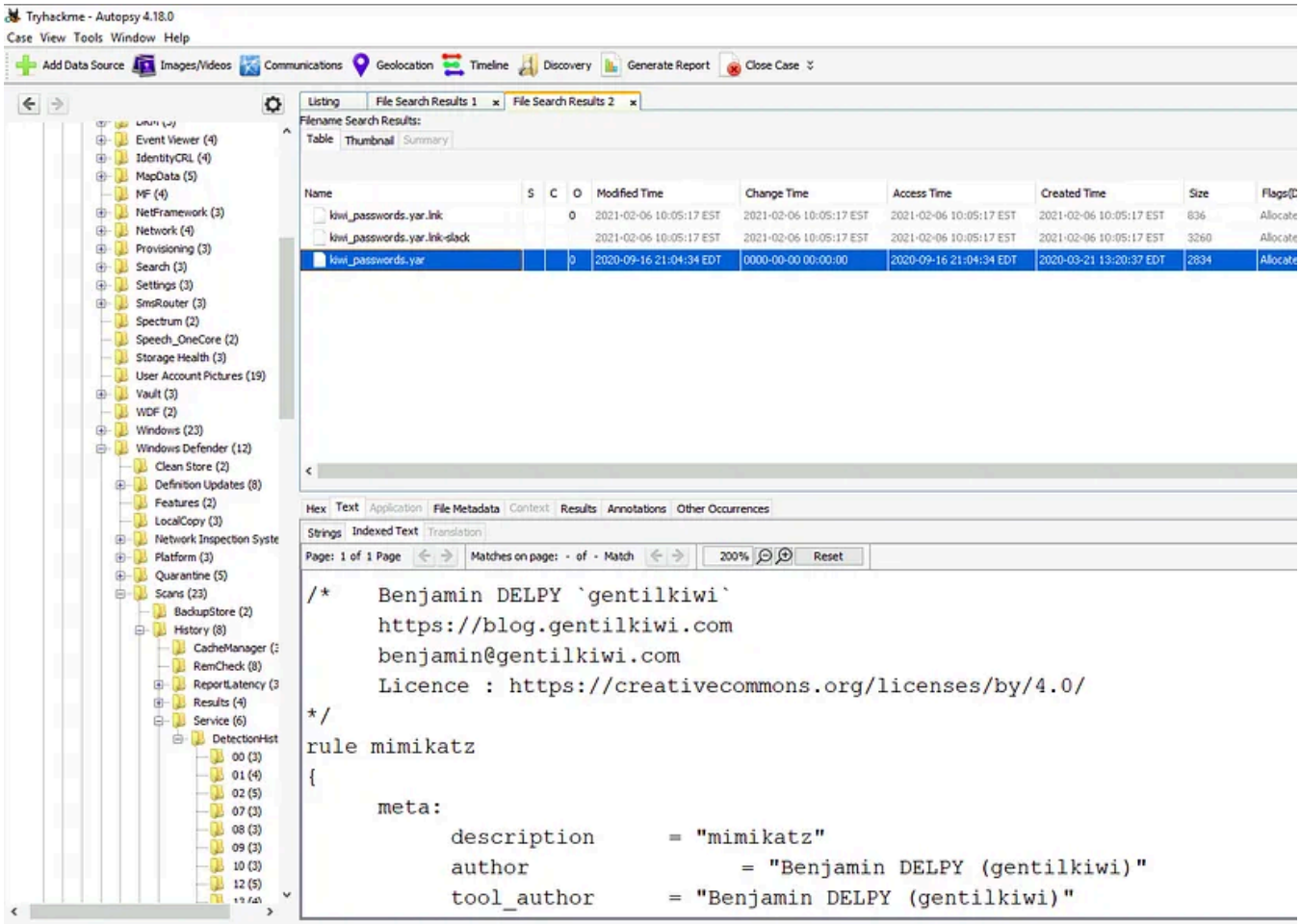
Answer: Lazagne,Mimikatz

> *Q14*
>
> *There is a YARA file on the computer. Inspect the file. What is the name of the author?*

We can use the File Search By Attribute tool (located in the Tools drop-down menu) to search .yar and .yara files.



Searching for filenames containing .yar



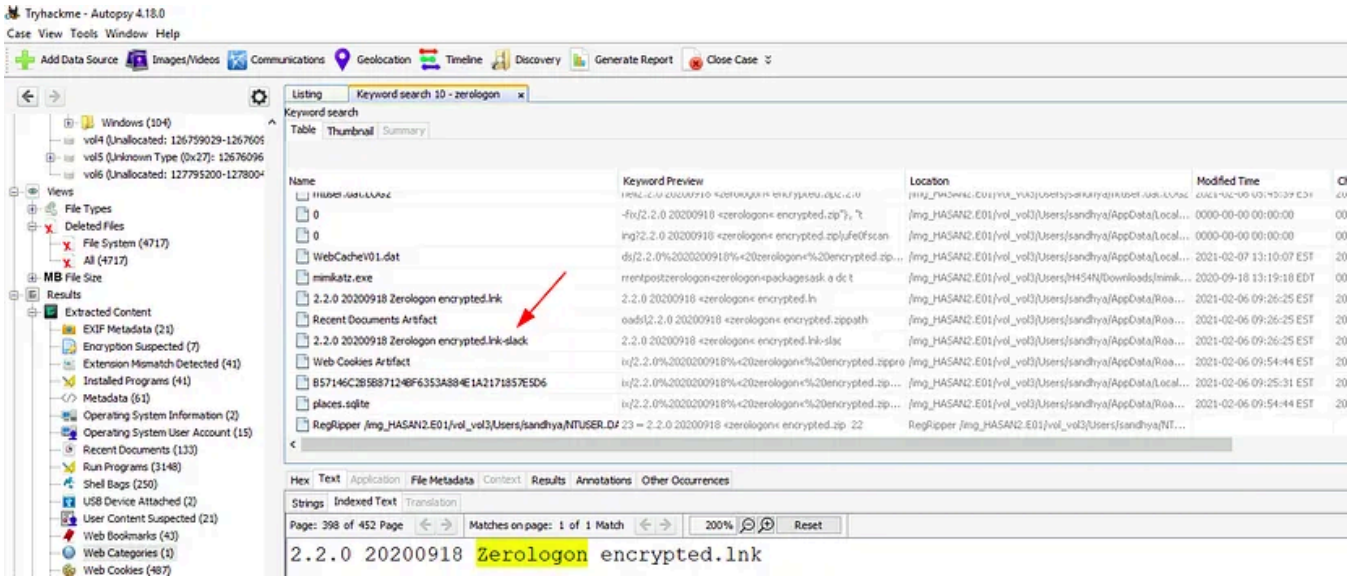
Results of the file name search

The file search returns three references to a single .yar file, so we'll inspect the data they hold to get our answer.

Answer: Benjamin DELPY (gentilkiwi)

> *Q15*
>
> *One of the users wanted to exploit a domain controller with an MS-NRPC based exploit. What is the filename of the archive that you found? (include the spaces in your answer)*

If we look up MS-NRPC exploits, there are many results for the exploit known as Zerologon. We'll see if we get lucky with a keyword search.



Keyword search results for 'zerologon'

And we got a hit for a zipped Zerologon exploit. Though the file appears to have been deleted, we have plenty of evidence that it was located in sandhya's download folder.

Answer: 2.2.0 20200918 Zerologon encrypted.zip

Conclusion: This was an interesting challenge, though some of the questions were simple, others involved deeper dives into the user activity, registry, and alternative sources of evidence. Q13 was a tough one, but I won't forget to keep Windows Defender's scan history in mind for future investigations.

Follow

Written by Sean Dixon

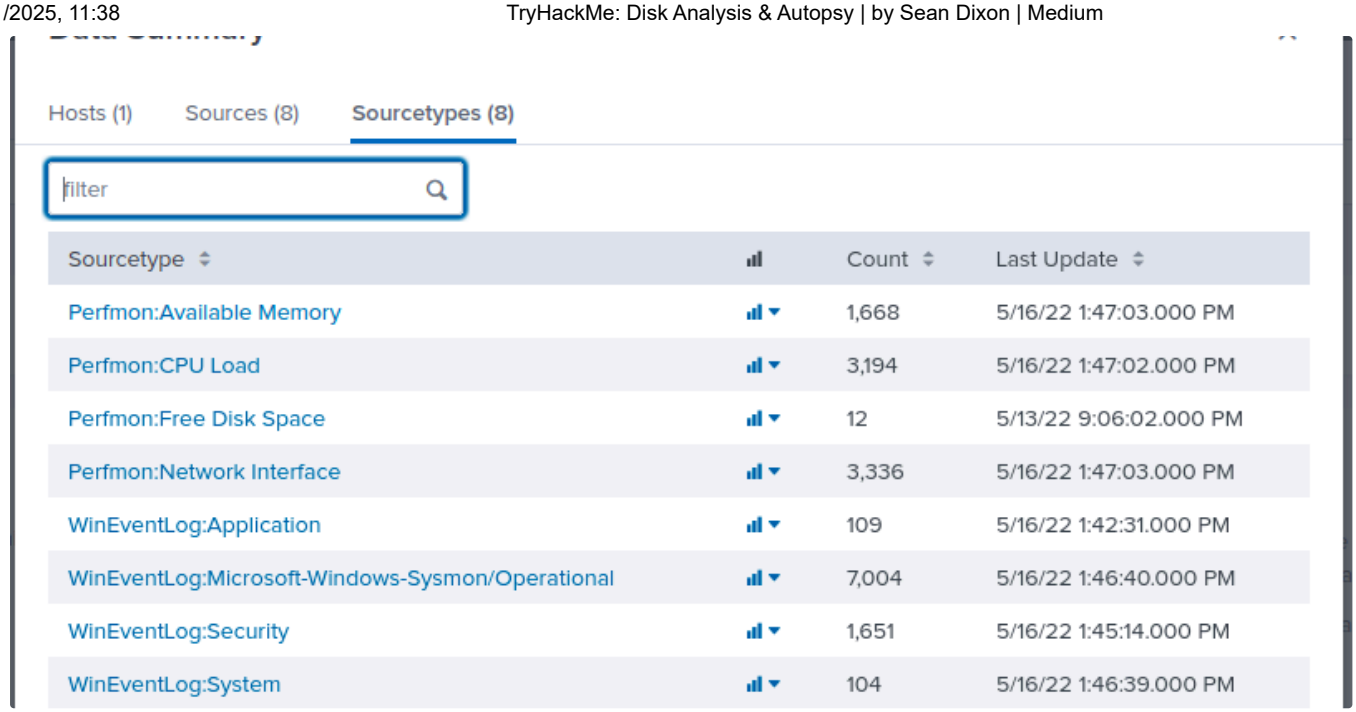
7 Followers · 1 Following

No responses yet

What are your thoughts?

Respond

More from Sean Dixon

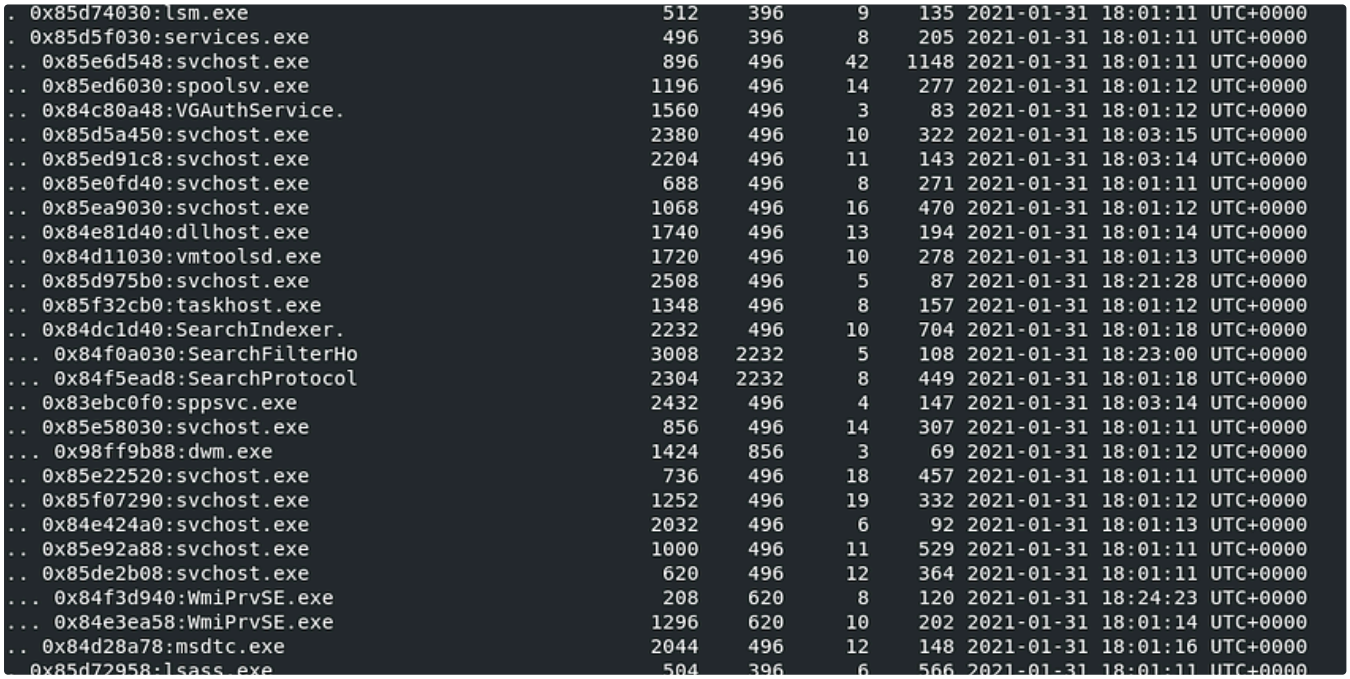


Sean Dixon

TryHackMe: PS Eclipse

Medium-difficulty Splunk challenge. Tools/Topics: Splunk, CyberChef, PowerShell Execution, Malicious Downloads, Ransomware, BlackSun

Jun 7, 2023 3

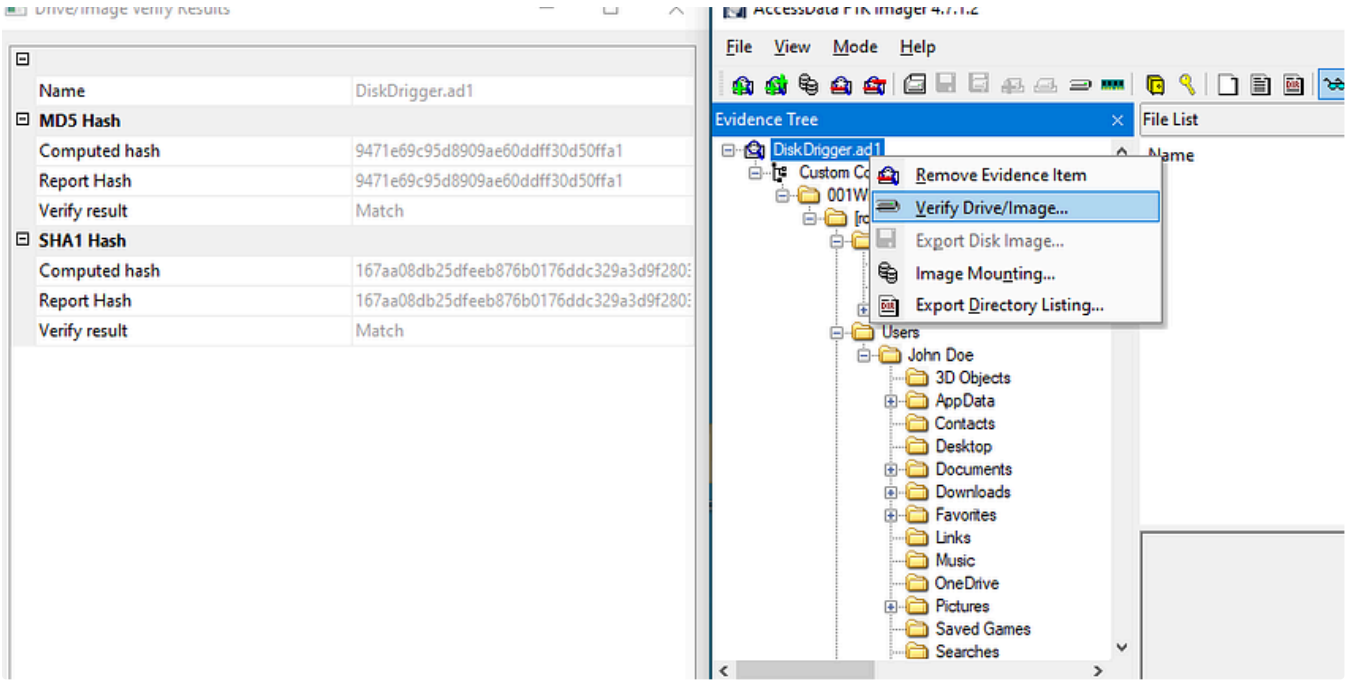


Sean Dixon

BTLO: Memory Analysis—Ransomware

Medium-difficulty memory forensics challenge. Tools/Topics: Volatlity, Process Hierarchy, Hidden Processes, Malware.

Jun 10, 2023

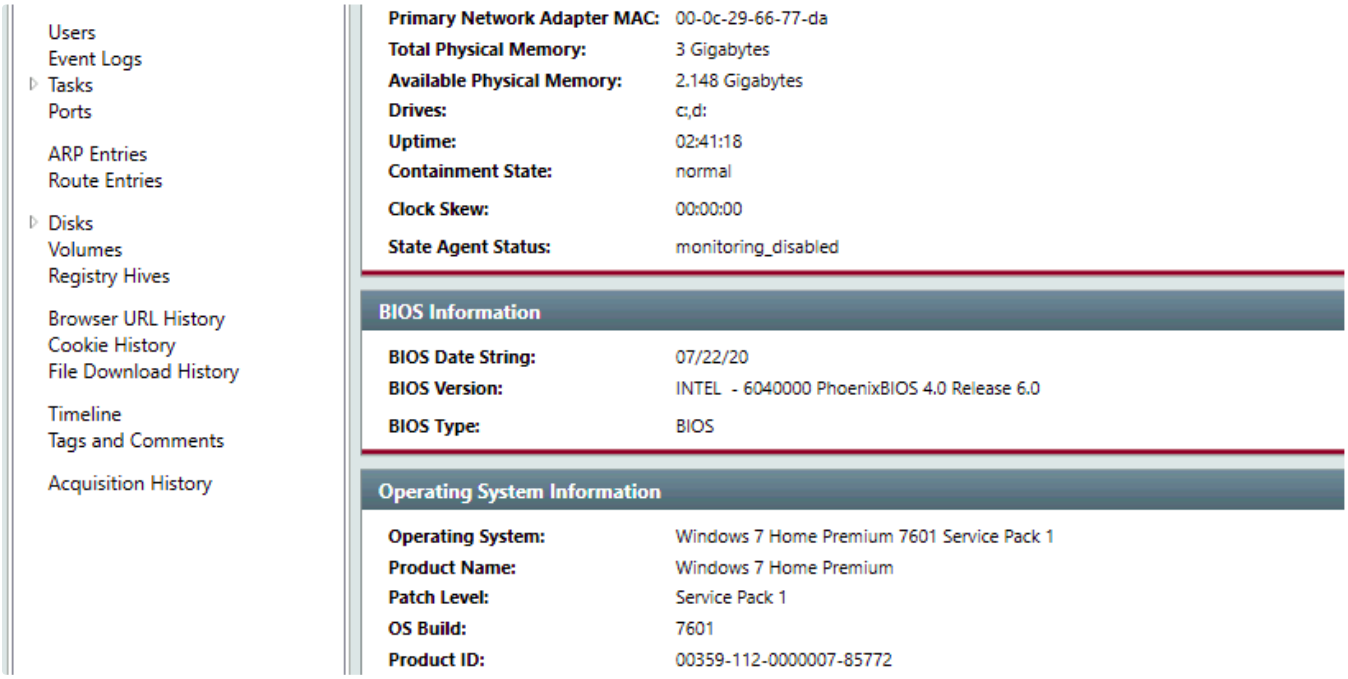


Sean Dixon

CyberDefenders: AfricanFalls

Medium-difficulty forensics challenge. Tools/Topics: FTK Imager, Windows Registry, ShellBags, Prefetch, Browser History, Password...

Jun 12, 2023 1



Sean Dixon

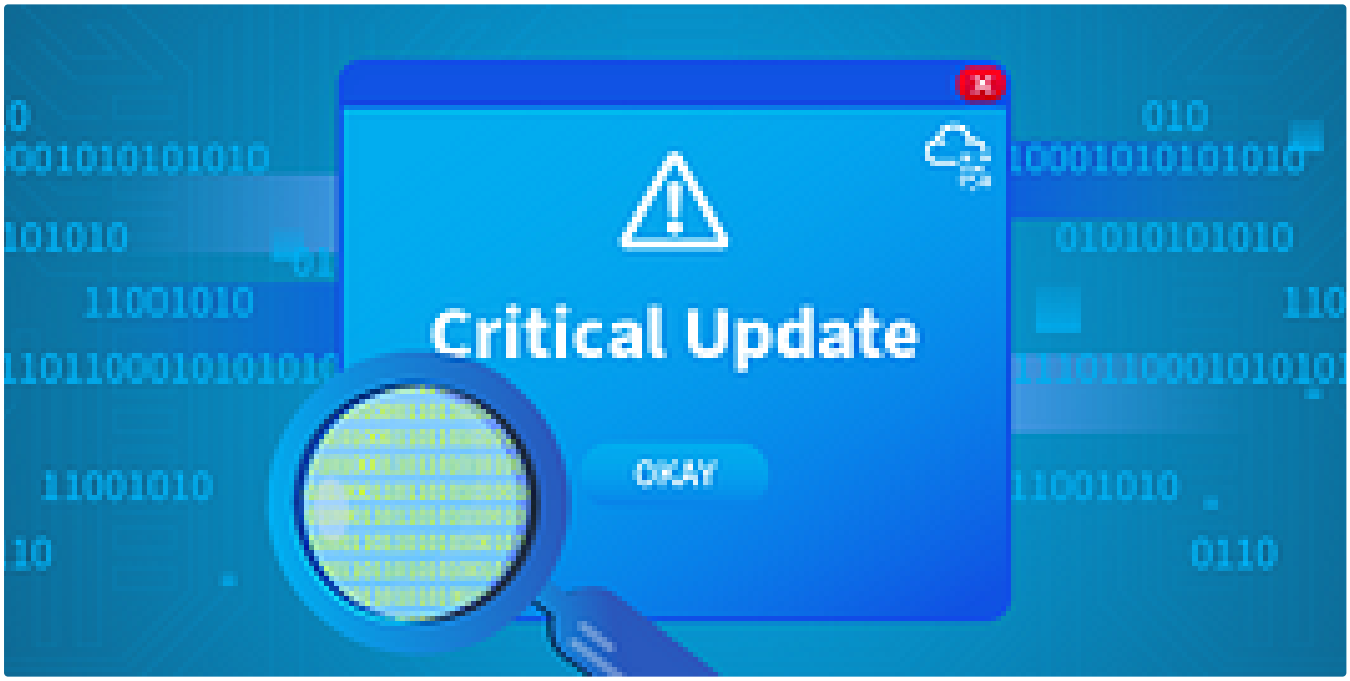
TryHackMe: REvil Corp

Medium-difficulty forensics challenge. Tools/Topics: Redline, Ransomware, File Changes, Download History, Browser History.

Jun 14, 2023 6

See all from Sean Dixon

Recommended from Medium

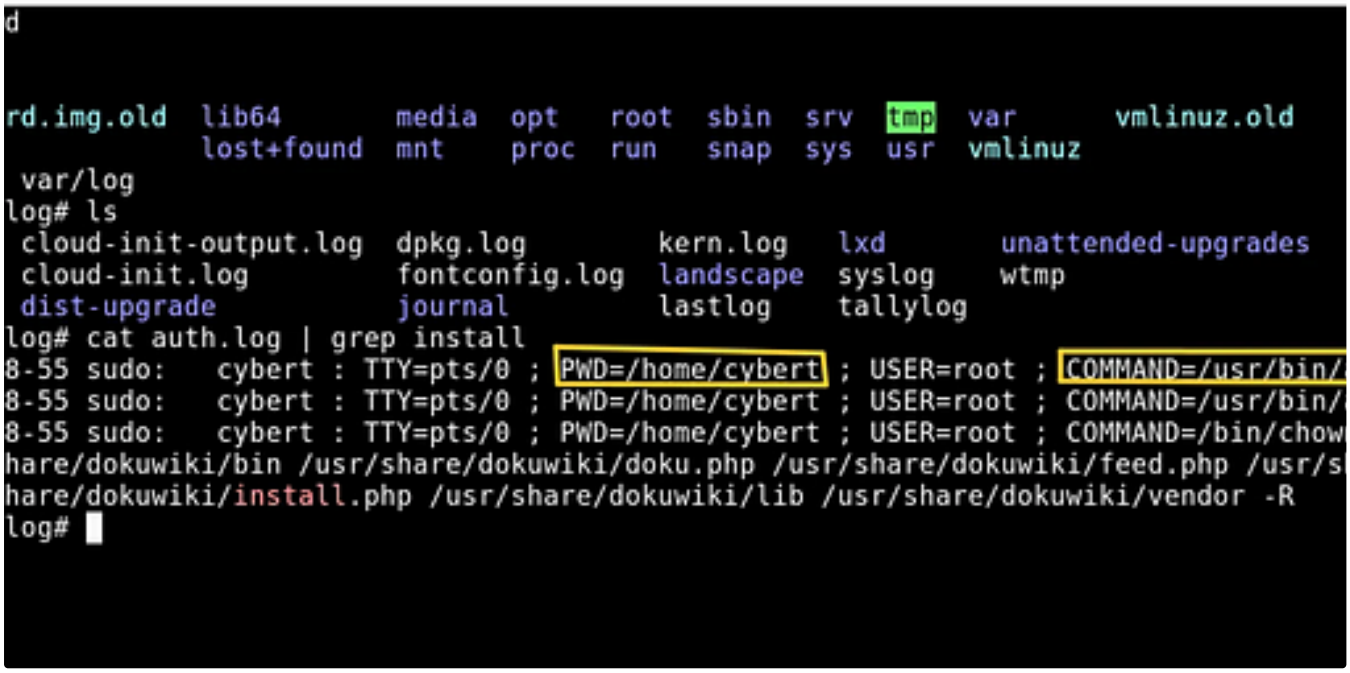


In T3CH by Axoloth

TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

Jul 21, 2024 104



Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here: https://tryhackme.com/room/disgruntled

Oct 22, 2024

Lists

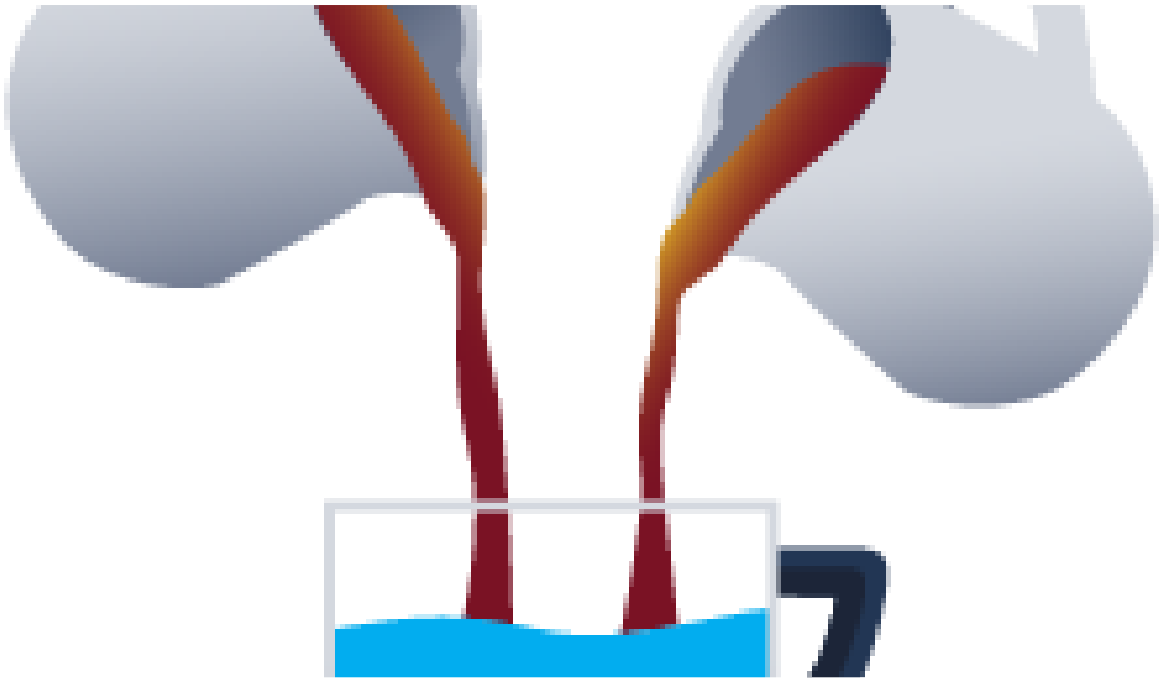
Staff picks
796 stories · 1561 saves

Stories to Help You Level-Up at Work
19 stories · 912 saves

Self-Improvement 101

Open in app ↗

Medium Search



MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024 2

Zach Gillespie

Conti: Ransomware Investigation with Splunk

In this Tryhackme challenge, an organization exchange server has been compromised with ransomware.

Aug 26, 2024 1

Fritzadriano

Retracted—TryHackMe WriteUp

IInvestigate the case of the missing ransomware. After learning about Wazuh previously, today's task is a bit different.

Sep 4, 2024 50

Mustapha Ait Ichou

Disgruntled Tryhackme

Hi All, i hope you are doing well thank for taking your time to read my writup i hope it’s will be usuful for you. In this write-up, I will...

Aug 14, 2024