TryHackMe Windows Forensics 1 Write-Up

Toumo · Follow

9 min read · Aug 6, 2023

Listen Share More

Image from tryhackme.com

For me, it's the final stretch to completing the SOC Level 1 learning path. I have completed all the phishing rooms already early on before thinking of doing write-ups to document my progress. That being said, I do want to complete most of the rooms and write the accompanying write-up. I plan on doing that in the future! Also, where is the DFIR: An Introduction room? I didn't want to create a write-up for rooms that don't have much hands on. As always, I'll document my thinking process, whether right or wrong, and will document if I looked for help or not. We're all learning together and I'm not afraid to say I am not an expert at all. Without furder ado, let's get started!

Task 1 Introduction to Windows Forensics

1: What is the most used Desktop Operating System right now?

This can be found in the reading.

Answer: Microsoft Windows

Task 2 Windows Registry and Forensics

1: What is the short form for HKEY_LOCAL_MACHINE?

This can be found in the reading. Also quite good information as to what the information in each of the five root keys hold.

Answer: HKLM

Task 3 Accessing registry hives offline

1: What is the path for the five main registry hives, DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM?

This can be found in the reading.

Answer: C:\Windows\System32\Config

2: What is the path for the AmCache hive?

This can be found in the reading.

Answer: C:\Windows\AppCompat\Programs\Amcache.hve

Task 6 System Information and System Accounts

1: What is the Current Build Number of the machine whose data is being investigated?

We will be using the screenshot provided in the reading. The OS Version section tells us to use the screenshot to answer question 1.

Answer: 19044

2: Which ControlSet contains the last known good configuration?

The screenshot in Current Control Set section will contain the answer we need.

Answer: 1

3: What is the Computer Name of the computer?

The screenshot in Computer Name section will contain the answer we need.

Answer: THM-4N6

4: What is the value of the TimeZoneKeyName?

The screenshot in Time Zone Information section will contain the answer we need.

Answer: Pakistan Standard Time

5: What is the DHCP IP address

The screenshot in Network Interface and Past Networks will contain the answer we need.

Answer: 192.168.100.58

6: What is the RID of the Guest User account?

The screenshot in SAM Hive and User Information section will contain the answer we need. Look at theUser ID colume in the screenshot.

Answer: 501

Task 7 Usage or knowledge of files/folders

1: When was EZtools opened?

The screenshot in Recent Files section will contain the answer we need.

Answer: 2021-12-01 13:00:34

2: At what time was My Computer last interacted with?

The screenshot in ShellBags section will contain the answer we need.

Answer: 2021-12-01 13:06:47

3: What is the Absolute Path of the file opened using notepad.exe?

The screenshot in Open/Save and LastVisited Dialog MRUs section will contain the answers we need for this question and the next.

Answer: C:\Program Files\Amazon\Ec2ConfigService\Settings

4: When was this file opened?

Answer: 2021-11–30 10:56:19

Task 8 Evidence of Execution

1: How many times was the File Explorer launched?

The screenshot in UserAssist section will contain the answer we need.

Answer: 26

2: What is another name for ShimCache?

The answer can be found in the reading. The shorter name is the answer.

Answer: AppCompatCache

3: Which of the artifacts also saves SHA1 hashes of the executed programs?

The answer can be found in the reading.

Answer: AmCache

4: Which of the artifacts saves the full path of the executed programs?

The answer can be found in the reading.

Answer: BAM/DAM

Task 9 External Devices/USB device forensics

1: What is the serial number of the device from the manufacturer 'Kingston'?

The screenshot in Device Identification section will contain the answers we need for this question and the next.

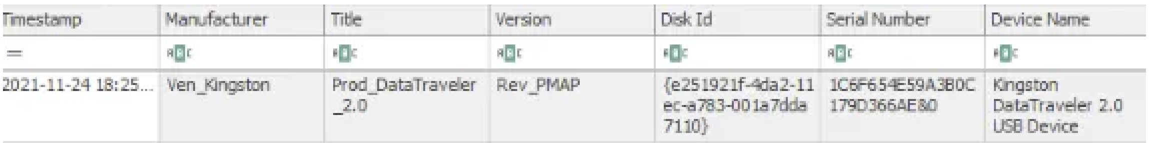
Answer: IC6F654E59A3B0C179D366AE&0

2: What is the name of this device?

Answer: Kingston DataTraveler 2.0 USB Device

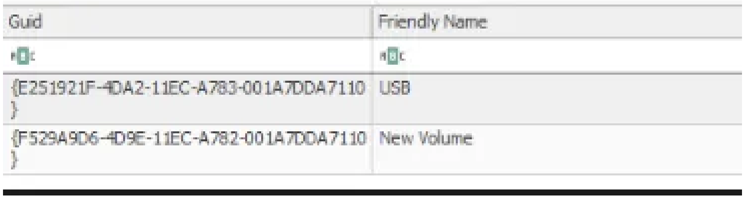
3: What is the friendly name of the device from the manufacturer ‘Kingston’?

Combining the information from both the first screenshot and the third from the reading, I can see the Disk Id from the first screenshot and Guid from the third screenshot shows a match. So the device name is Kingston DataTraveler 2.0 USB Device and the friendly name is USB.



Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name
2021-11-24 18:25...	Ven_Kingston	Prod_DataTraveler_2.0	Rev_PMAP	{e251921f-4da2-11ec-a783-001a7dda7110}	1C6F654E59A3B0C179D366AE80	Kingston DataTraveler 2.0 USB Device

First screenshot



Guid	Friendly Name
{E251921F-4DA2-11EC-A783-001A7DDA7110}	USB
{F529A9D6-4D9E-11EC-A782-001A7DDA7110}	New Volume

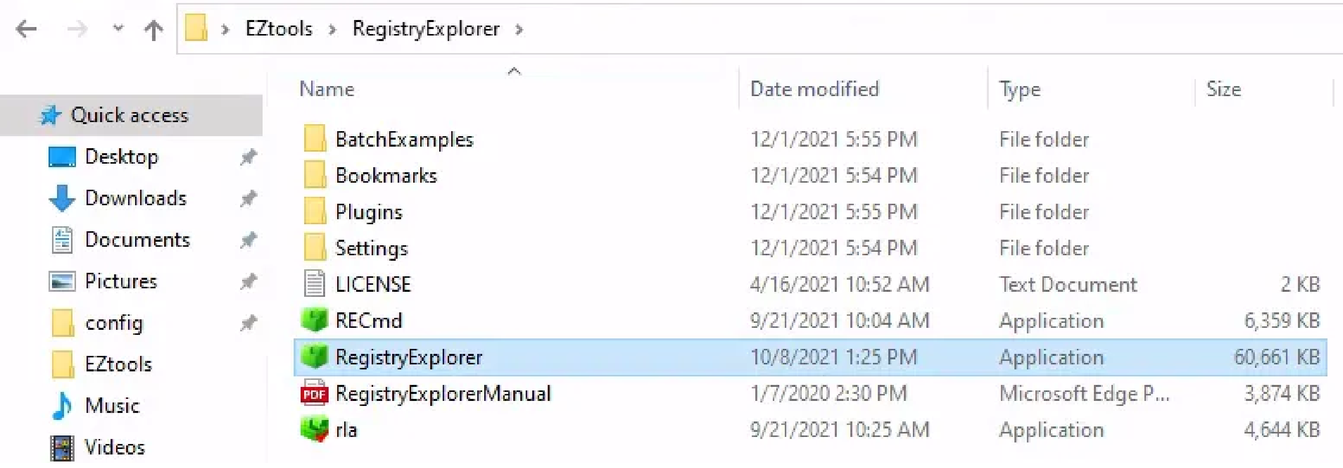
Third screenshot

Answer: USB

Task 10 Hands-on Challenge

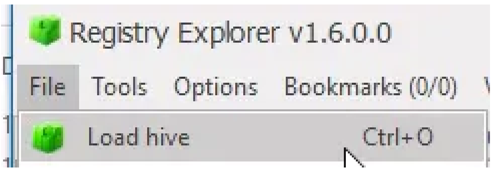
I will be RDPing into the machine. I wrote the instructions here on how I did it.

Loading the hives into RegistryExplorer took me about 20 minutes of searching and messing around with the interface. It was difficult when I didn’t even start on the actual questions yet! To load the hives into RegistryExplorer, we need to open it first. RegistryExplorer is located by going to EZTools folder -> RegistryExplorer -> RegistryExplorer. It may take a while for the application to load.

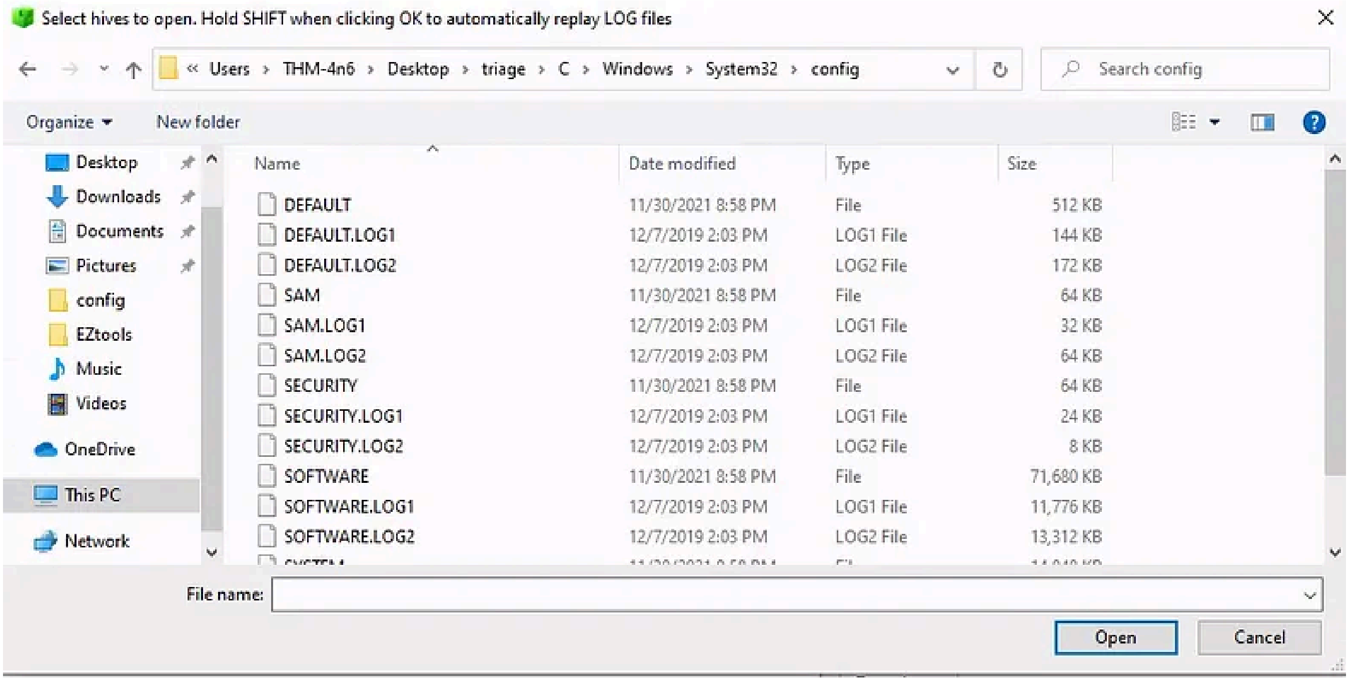


Name	Date modified	Type	Size
BatchExamples	12/1/2021 5:55 PM	File folder	
Bookmarks	12/1/2021 5:54 PM	File folder	
Plugins	12/1/2021 5:55 PM	File folder	
Settings	12/1/2021 5:54 PM	File folder	
LICENSE	4/16/2021 10:52 AM	Text Document	2 KB
RECmd	9/21/2021 10:04 AM	Application	6,359 KB
RegistryExplorer	10/8/2021 1:25 PM	Application	60,661 KB
RegistryExplorerManual	1/7/2020 2:30 PM	Microsoft Edge P...	3,874 KB
rla	9/21/2021 10:25 AM	Application	4,644 KB

Once Registry Explorer loads, we will load the hive. Do this by going to File -> Load hive.

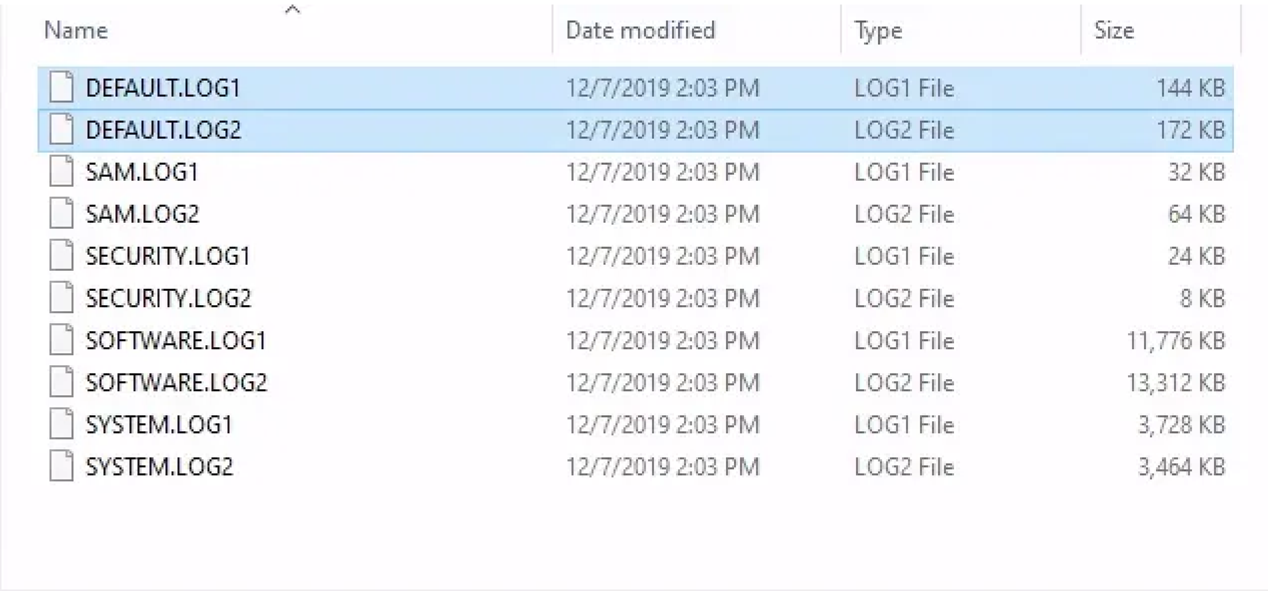


From here, go to triage -> C -> Windows -> System 32 -> config to access the registry files.


Select hives to open. Hold SHIFT when clicking OK to automatically replay LOG files

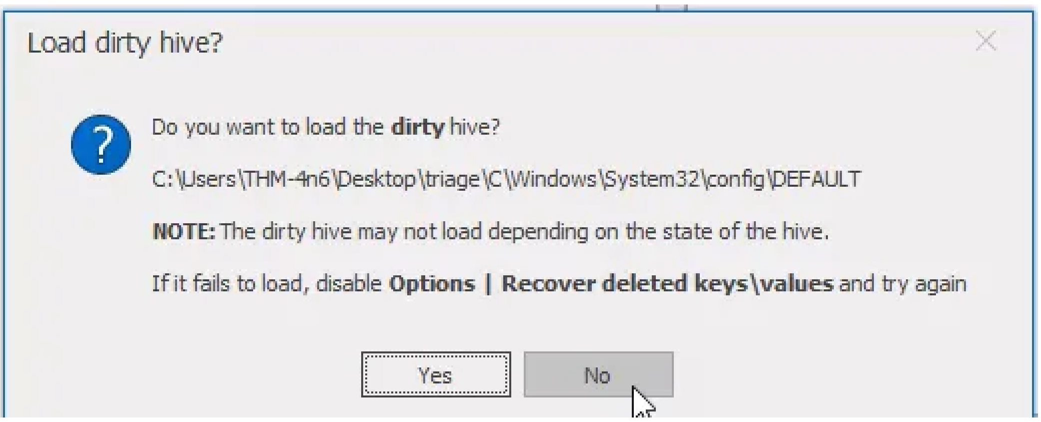
Name	Date modified	Type	Size
DEFAULT	11/30/2021 8:58 PM	File	512 KB
DEFAULT.LOG1	12/7/2019 2:03 PM	LOG1 File	144 KB
DEFAULT.LOG2	12/7/2019 2:03 PM	LOG2 File	172 KB
SAM	11/30/2021 8:58 PM	File	64 KB
SAM.LOG1	12/7/2019 2:03 PM	LOG1 File	32 KB
SAM.LOG2	12/7/2019 2:03 PM	LOG2 File	64 KB
SECURITY	11/30/2021 8:58 PM	File	64 KB
SECURITY.LOG1	12/7/2019 2:03 PM	LOG1 File	24 KB
SECURITY.LOG2	12/7/2019 2:03 PM	LOG2 File	8 KB
SOFTWARE	11/30/2021 8:58 PM	File	71,680 KB
SOFTWARE.LOG1	12/7/2019 2:03 PM	LOG1 File	11,776 KB
SOFTWARE.LOG2	12/7/2019 2:03 PM	LOG2 File	13,312 KB

I loaded each file one at a time starting with “DEFAULT.” A warning should pop up about sequence numbers not matching. Do not worry. Just press Yes. Next, it says select transaction logs. We will select both DEFAULT.LOG1 and DEFAULT.LOG2 files. To select more than one file, you can click on the first file, then hold CTRL and click on the second file.



Name	Date modified	Type	Size
DEFAULT.LOG1	12/7/2019 2:03 PM	LOG1 File	144 KB
DEFAULT.LOG2	12/7/2019 2:03 PM	LOG2 File	172 KB
SAM.LOG1	12/7/2019 2:03 PM	LOG1 File	32 KB
SAM.LOG2	12/7/2019 2:03 PM	LOG2 File	64 KB
SECURITY.LOG1	12/7/2019 2:03 PM	LOG1 File	24 KB
SECURITY.LOG2	12/7/2019 2:03 PM	LOG2 File	8 KB
SOFTWARE.LOG1	12/7/2019 2:03 PM	LOG1 File	11,776 KB
SOFTWARE.LOG2	12/7/2019 2:03 PM	LOG2 File	13,312 KB
SYSTEM.LOG1	12/7/2019 2:03 PM	LOG1 File	3,728 KB
SYSTEM.LOG2	12/7/2019 2:03 PM	LOG2 File	3,464 KB

We should get a pop up saying to select a location for our new and updated hive. I just saved it at the default location, which should be our Desktop. Next, it should ask if you want to load the **updated** hive. Select Yes. Now it should ask if we want to load the dirty/original hive. Select No.



Load dirty hive?

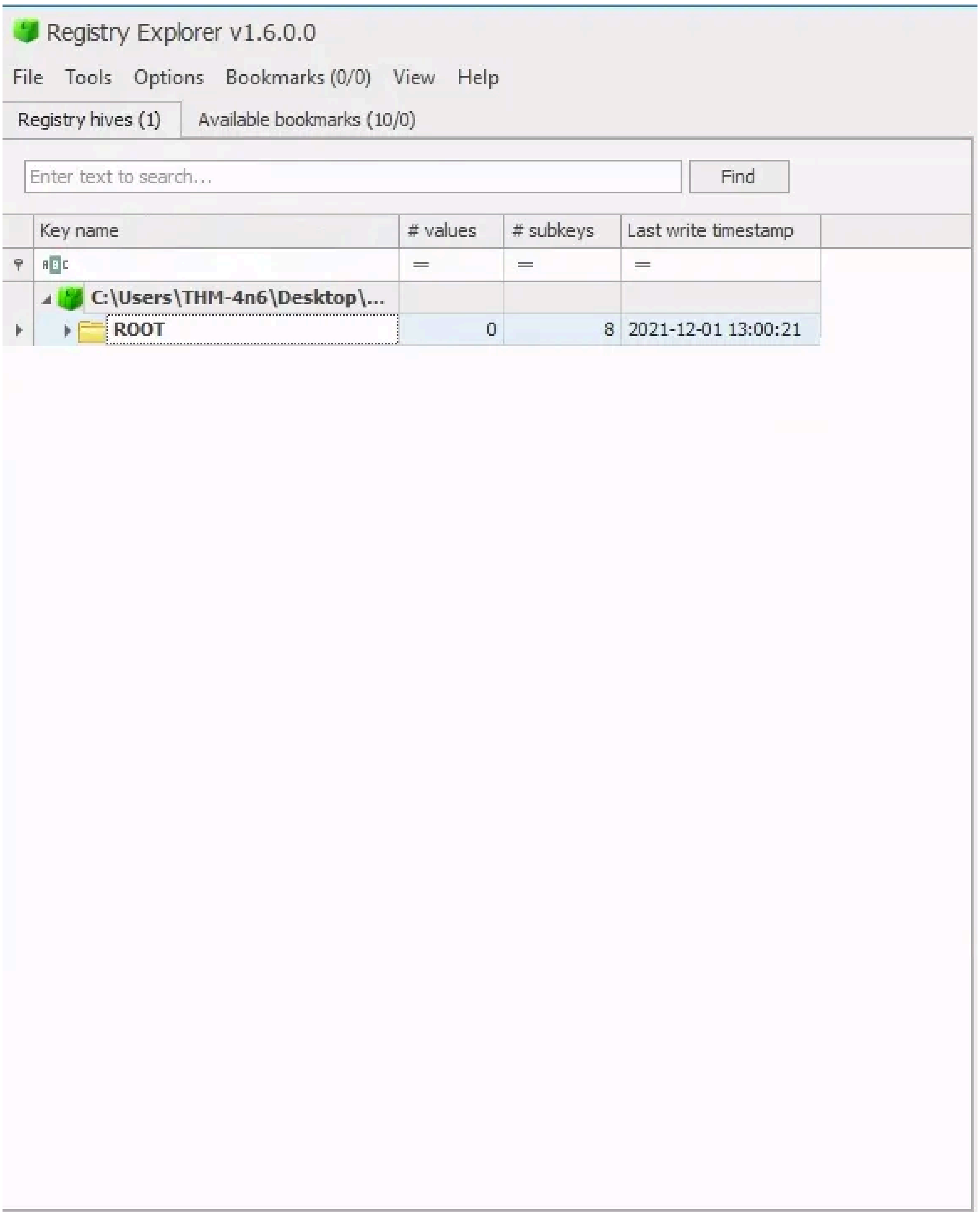
Do you want to load the **dirty** hive?

C:\Users\THM-4n6\Desktop\triage\C\Windows\System32\config\DEFAULT

NOTE: The dirty hive may not load depending on the state of the hive.

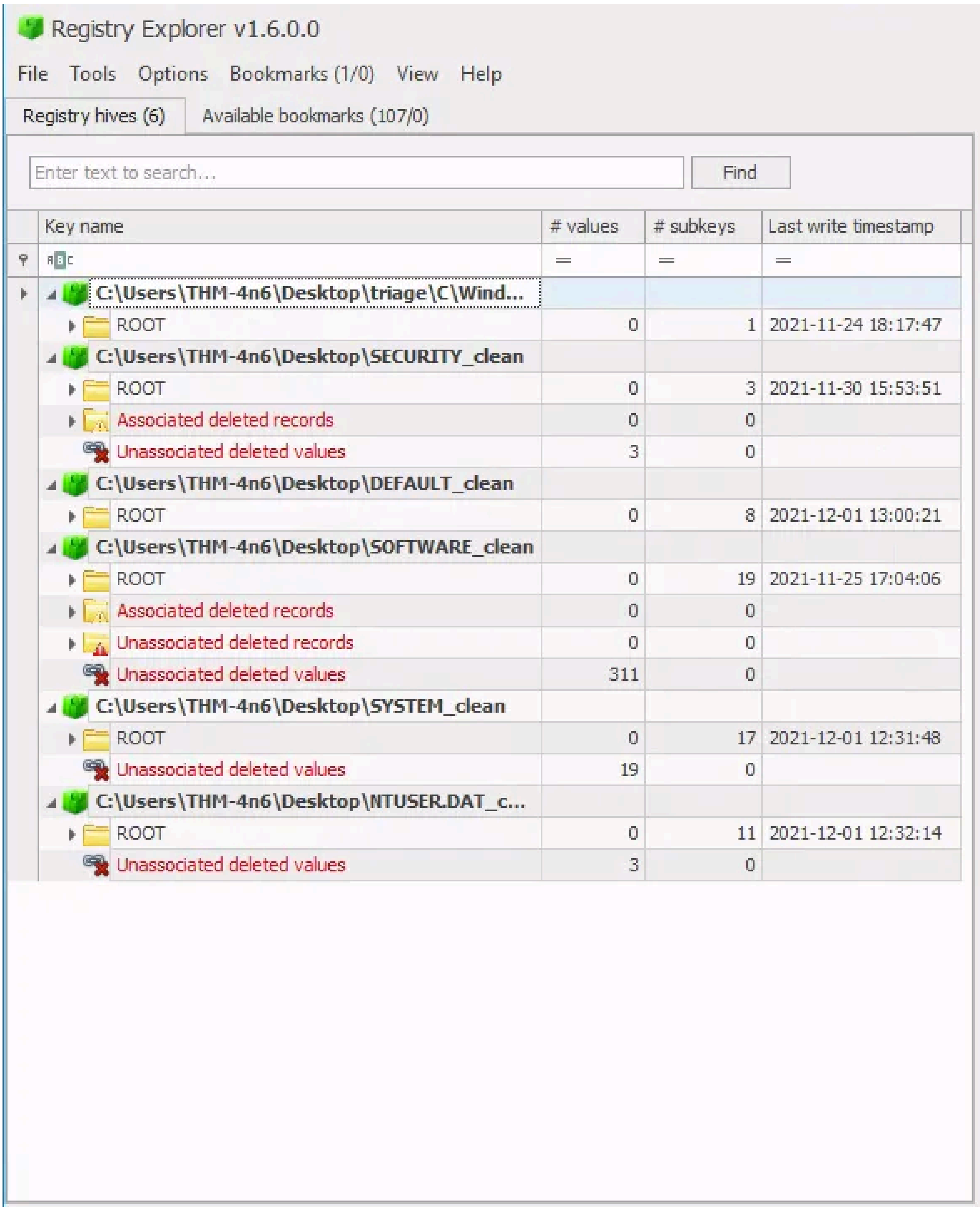
If it fails to load, disable **Options | Recover deleted keys\values** and try again

Congratulations! We loaded our first hive!


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (0/0) View Help
Registry hives (1) Available bookmarks (10/0)
Enter text to search...
Find

Key name	# values	# subkeys	Last write timestamp
C:\Users\THM-4n6\Desktop\...			
ROOT	0	8	2021-12-01 13:00:21

Now do it again for the hives, which are SAM, SECURITY, SOFTWARE, and SYSTEM. SAM was the only one that didn't seem to have any trouble with it being "dirty" but I'm not sure if it's just me. I also loaded NTUSER.DAT since I think I might need it later on. NTUSER.DAT is located at a different folder. It is found in triage -> C -> Users -> THM-4n6 -> NTUSER.DAT. Once you finish loading everything, it should look like this.

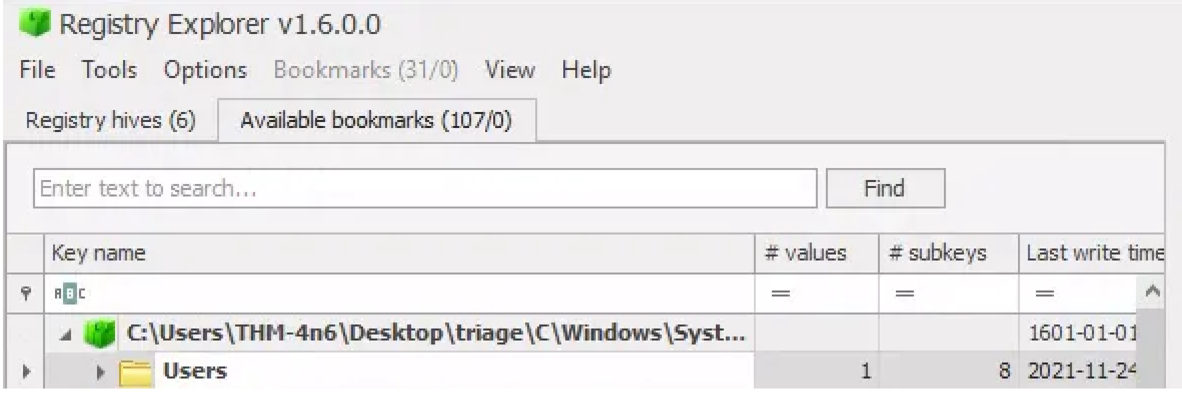


Key name	# values	# subkeys	Last write timestamp
C:\Users\THM-4n6\Desktop\triage\C\Wind...			
ROOT	0	1	2021-11-24 18:17:47
C:\Users\THM-4n6\Desktop\SECURITY_clean			
ROOT	0	3	2021-11-30 15:53:51
Associated deleted records	0	0	
Unassociated deleted values	3	0	
C:\Users\THM-4n6\Desktop\DEFAULT_clean			
ROOT	0	8	2021-12-01 13:00:21
C:\Users\THM-4n6\Desktop\SOFTWARE_clean			
ROOT	0	19	2021-11-25 17:04:06
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	311	0	
C:\Users\THM-4n6\Desktop\SYSTEM_clean			
ROOT	0	17	2021-12-01 12:31:48
Unassociated deleted values	19	0	
C:\Users\THM-4n6\Desktop\NTUSER.DAT_c...			
ROOT	0	11	2021-12-01 12:32:14
Unassociated deleted values	3	0	

Now we’re ready to begin!

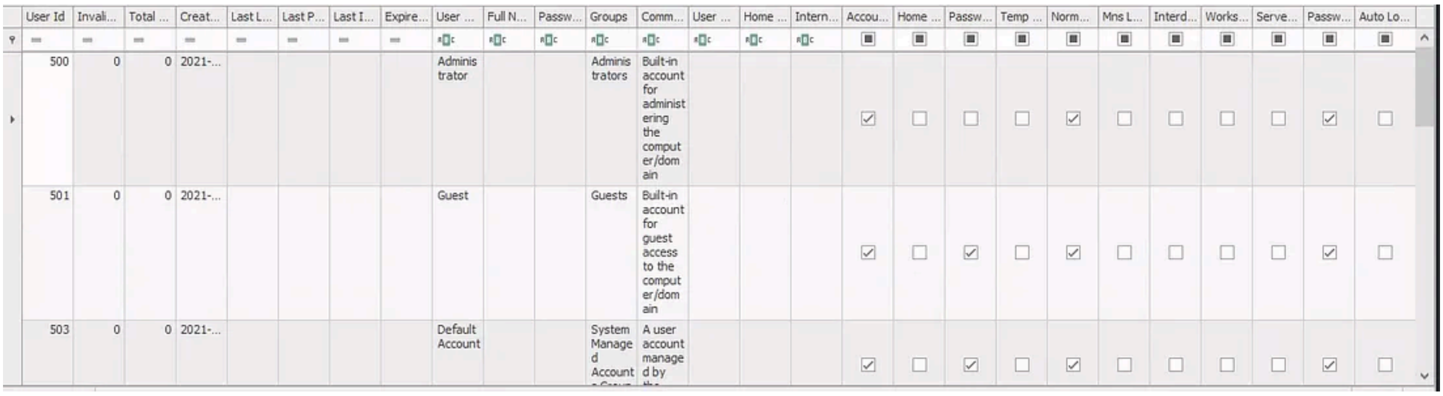
1: How many user created accounts are present on the system?

On the top left, I clicked on “Available bookmarks” and then clicked on “Users” which should display the list of users associated on this computer.


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (31/0) View Help
Registry hives (6)
Available bookmarks (107/0)
Enter text to search...
Find

Key name	# values	# subkeys	Last write time
C:\Users\THM-4n6\Desktop\triage\C\Windows\Syst...			1601-01-01
Users	1	8	2021-11-24

The right handed side should then show something similar to this. Look at "User Id" column and look for IDs starting with 10. That means it's a user created account. I only knew that because I checked the hint.

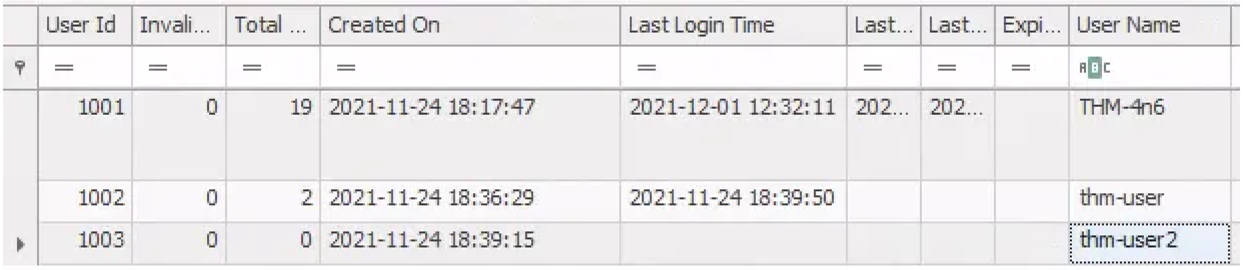


User Id	Invali...	Total ...	Creat...	Last L...	Last P...	Last I...	Expire...	User ...	Full N...	Passw...	Groups	Comm...	User ...	Home ...	Intern...	Accou...	Home ...	Passw...	Temp ...	Norm...	Mns L...	Interd...	Works...	Serve...	Passw...	Auto Lo...
500	0	0	2021-...					Administrator			Administrators	Built-in account for administering the computer/domain				☑	□	□	□	☑	□	□	□	□	☑	□
501	0	0	2021-...					Guest			Guests	Built-in account for guest access to the computer/domain				☑	□	☑	□	☑	□	□	□	□	☑	□
503	0	0	2021-...					Default Account			System Managed Account	A user account managed by				☑	□	☑	□	☑	□	□	□	□	☑	□

Answer: 3

2: What is the username of the account that has never been logged in?

After the above, I extended some of the columns so I can see what the column headers were. From here, we can see one user never logged on.

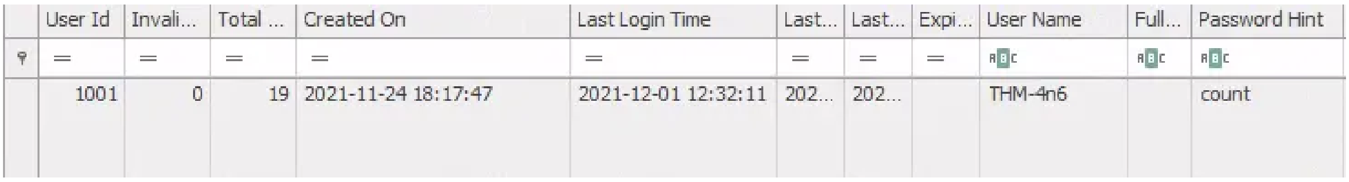


User Id	Invali...	Total ...	Created On	Last Login Time	Last...	Last...	Expi...	User Name
1001	0	19	2021-11-24 18:17:47	2021-12-01 12:32:11	202...	202...		THM-4n6
1002	0	2	2021-11-24 18:36:29	2021-11-24 18:39:50				thm-user
1003	0	0	2021-11-24 18:39:15					thm-user2

Answer: thm-user2

3: What's the password hint for the user THM-4n6?

Similar to question 2, I looked at the columns to see which one gives me the answer I need and extended it for better visibility.

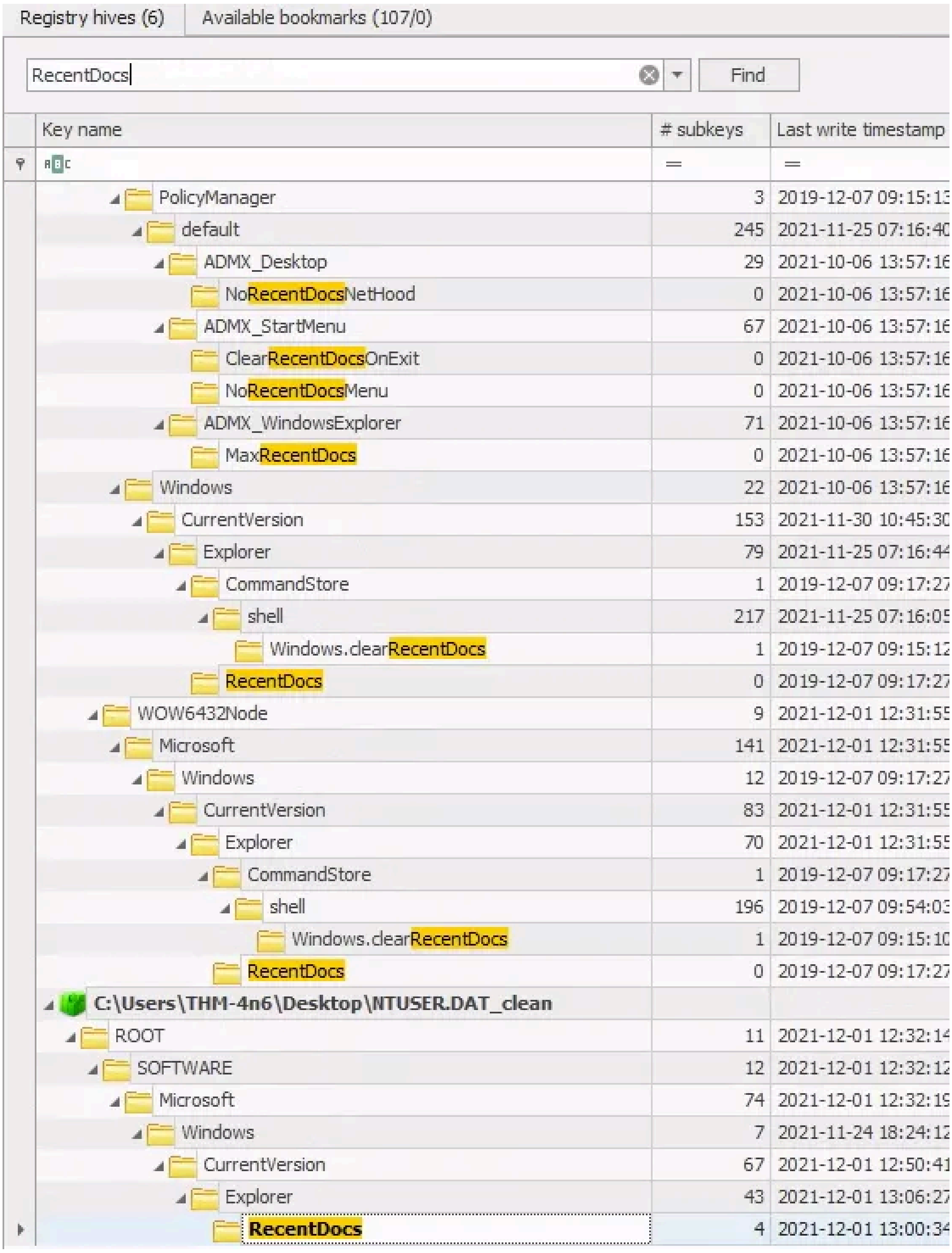


User Id	Invali...	Total ...	Created On	Last Login Time	Last...	Last...	Expi...	User Name	Full...	Password Hint
1001	0	19	2021-11-24 18:17:47	2021-12-01 12:32:11	202...	202...		THM-4n6		count

Answer: count

4: When was the file ‘Changelog.txt’ accessed?

I went back to one of the reading sections as I recalled learning where to find recent files. It’s in Task 7. The location to find where a file was last accessed is at NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs. Alternatively, you can type “RecentDocs” in the search bar and then look for the result that is under NTUSER.DAT. I was practicing navigating it and didn’t use the search bar.

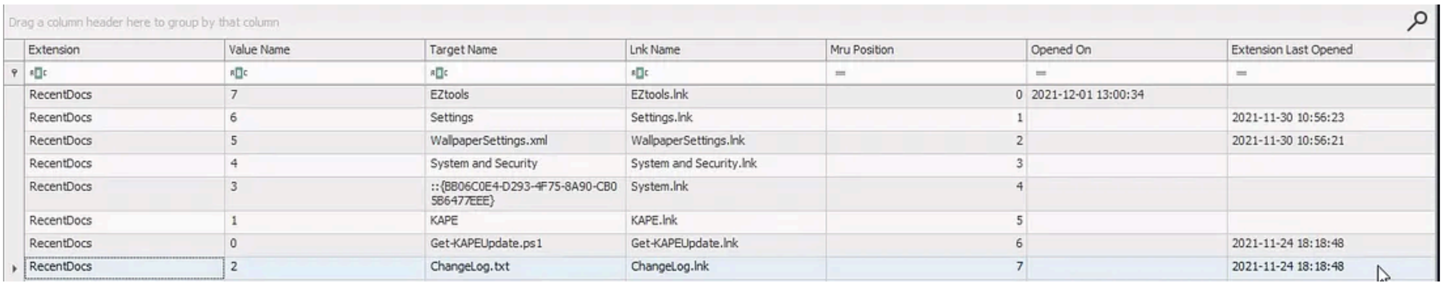


Registry hives (6) | Available bookmarks (107/0)

RecentDocs

Key name	# subkeys	Last write timestamp
PolicyManager	3	2019-12-07 09:15:13
default	245	2021-11-25 07:16:40
ADMX_Desktop	29	2021-10-06 13:57:16
NoRecentDocsNetHood	0	2021-10-06 13:57:16
ADMX_StartMenu	67	2021-10-06 13:57:16
ClearRecentDocsOnExit	0	2021-10-06 13:57:16
NoRecentDocsMenu	0	2021-10-06 13:57:16
ADMX_WindowsExplorer	71	2021-10-06 13:57:16
MaxRecentDocs	0	2021-10-06 13:57:16
Windows	22	2021-10-06 13:57:16
CurrentVersion	153	2021-11-30 10:45:30
Explorer	79	2021-11-25 07:16:44
CommandStore	1	2019-12-07 09:17:27
shell	217	2021-11-25 07:16:05
Windows.clearRecentDocs	1	2019-12-07 09:15:12
RecentDocs	0	2019-12-07 09:17:27
WOW6432Node	9	2021-12-01 12:31:55
Microsoft	141	2021-12-01 12:31:55
Windows	12	2019-12-07 09:17:27
CurrentVersion	83	2021-12-01 12:31:55
Explorer	70	2021-12-01 12:31:55
CommandStore	1	2019-12-07 09:17:27
shell	196	2019-12-07 09:54:03
Windows.clearRecentDocs	1	2019-12-07 09:15:10
RecentDocs	0	2019-12-07 09:17:27
C:\Users\THM-4n6\Desktop\NTUSER.DAT_clean		
ROOT	11	2021-12-01 12:32:14
SOFTWARE	12	2021-12-01 12:32:12
Microsoft	74	2021-12-01 12:32:19
Windows	7	2021-11-24 18:24:12
CurrentVersion	67	2021-12-01 12:50:41
Explorer	43	2021-12-01 13:06:27
RecentDocs	4	2021-12-01 13:00:34

Once you find the right folder, look at the right side for "ChangeLog.txt" and information that seems like the answer.



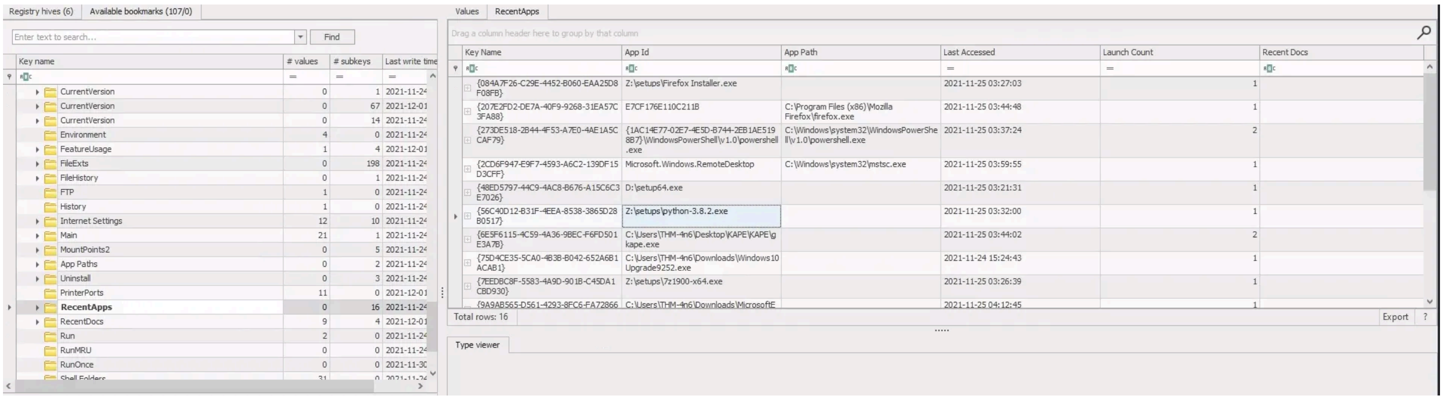
Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	7	EZtools	EZtools.lnk	0	2021-12-01 13:00:34	
RecentDocs	6	Settings	Settings.lnk	1		2021-11-30 10:56:23
RecentDocs	5	WallpaperSettings.xml	WallpaperSettings.lnk	2		2021-11-30 10:56:21
RecentDocs	4	System and Security	System and Security.lnk	3		
RecentDocs	3	::{BB06C0E4-D293-4F75-8A90-CB05B6477EEE}	System.lnk	4		
RecentDocs	1	KAPE	KAPE.lnk	5		
RecentDocs	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.lnk	6		2021-11-24 18:18:48
RecentDocs	2	ChangeLog.txt	ChangeLog.lnk	7		2021-11-24 18:18:48

Answer: 2021–11–24 18:18:48

5: What is the complete path from where the python 3.8.2 installer was run?

Admittedly, I found this on a whim. I clicked on the Available bookmarks tab on the top left and then just looked around for a bit. I limited myself to only NTUSER.DAT since it'll limit ourselves to only user THM-4n6. From there, I checked if the answer could be there judging from the folder names only. I saw something interesting when I clicked on RecentApps.

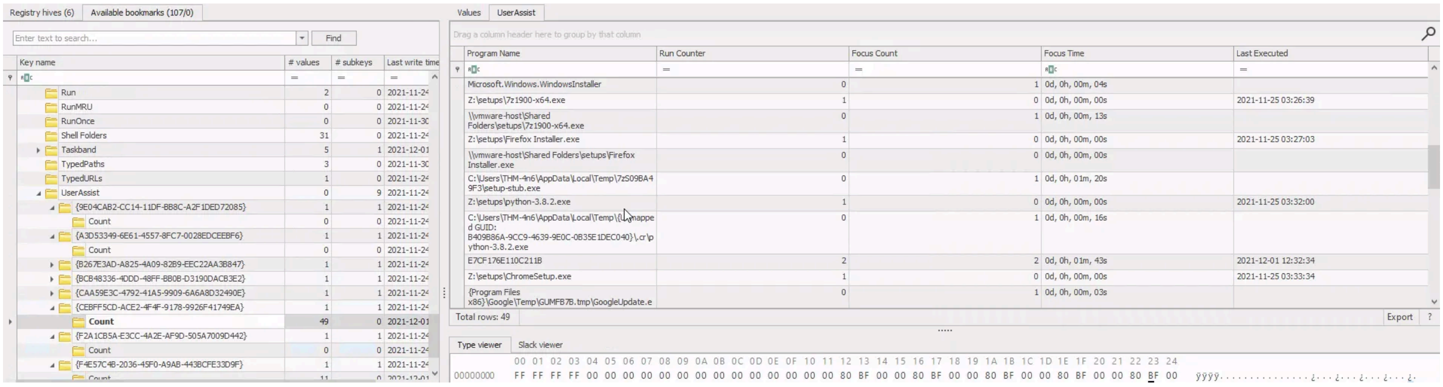


Key name	# values	# subkeys	Last write time
CurrentVersion	0	1	2021-11-24
CurrentVersion	0	67	2021-12-01
CurrentVersion	0	14	2021-11-24
Environment	4	0	2021-11-24
FeatureUsage	1	4	2021-12-01
FileExts	0	198	2021-11-24
FileHistory	0	1	2021-11-24
FTP	1	0	2021-11-24
History	1	0	2021-11-24
Internet Settings	12	10	2021-11-24
Main	21	1	2021-11-24
MountPoints2	0	5	2021-11-24
App Paths	0	2	2021-11-24
Uninstall	0	3	2021-11-24
PrinterPorts	11	0	2021-12-01
RecentApps	0	16	2021-11-24
RecentDocs	9	4	2021-12-01
Run	2	0	2021-11-24
RunMRU	0	0	2021-11-24
RunOnce	0	0	2021-11-30
Shell Folders	31	0	2021-11-24

Key Name	App Id	App Path	Last Accessed	Launch Count	Recent Docs
{084A7F26-C29E-4452-B060-EAA25D8F08FB}	Z:\setups\Firefox Installer.exe		2021-11-25 03:27:03	1	
{207E2FD2-DE7A-40F9-9268-31EA57C3FA88}	E7CF176E110C211B	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	2021-11-25 03:44:48	1	
{273DE518-2B44-4F53-A7E0-4AE1A5CCAF79}	{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe	2021-11-25 03:37:24	2	
{2CD6F947-E9F7-4593-A6C2-139DF15D3CFF}	Microsoft.Windows.RemoteDesktop	C:\Windows\system32\mstsc.exe	2021-11-25 03:59:55	1	
{48ED5797-44C9-4AC8-B676-A15C6C3E7026}	D:\setup64.exe		2021-11-25 03:21:31	1	
{56C40D12-B31F-4EEA-8538-3865D28B0517}	Z:\setups\python-3.8.2.exe		2021-11-25 03:32:00	1	
{6E5F6115-4C59-4A36-9BEC-F6FD501E3A7B}	C:\Users\THM-4n6\Desktop\KAPE\KAPE\gkape.exe		2021-11-25 03:44:02	2	
{75D4CE35-5CA0-4B3B-B042-652A6B1ACAB1}	C:\Users\THM-4n6\Downloads\Windows10Upgrade9252.exe		2021-11-24 15:24:43	1	
{7EEDBC8F-5583-4A9D-901B-C45DA1CBD930}	Z:\setups\7z1900-x64.exe		2021-11-25 03:26:39	1	
{9A9AB565-D561-4293-8FC6-FA72866	C:\Users\THM-4n6\Downloads\MicrosoftE		2021-11-25 04:12:45	1	

Total rows: 16

I checked the hint to see how to do this section properly. It said to look at UserAssist to look for any execution artifacts. I ended up doing that and looking through each of the folder in UserAssist. Found python again!



Key name	# values	# subkeys	Last write time
Run	2	0	2021-11-24
RunMRU	0	0	2021-11-24
RunOnce	0	0	2021-11-30
Shell Folders	31	0	2021-11-24
Taskband	5	1	2021-12-01
TypedPaths	3	0	2021-11-30
TypedURLs	1	0	2021-11-24
UserAssist	0	9	2021-11-24
{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}	1	1	2021-11-24
Count	0	0	2021-11-24
{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}	1	1	2021-11-24
Count	0	0	2021-11-24
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}	1	1	2021-11-24
{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}	1	1	2021-11-24
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}	1	1	2021-11-24
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2021-11-24
Count	49	0	2021-12-01
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2021-11-24
Count	0	0	2021-11-24
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	1	1	2021-11-24
Count	11	0	2021-12-01

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
Microsoft.Windows.WindowsInstaller	0	1	0d, 0h, 00m, 04s	
Z:\setups\7z1900-x64.exe	1	0	0d, 0h, 00m, 00s	2021-11-25 03:26:39
\\vmware-host\Shared Folders\setups\7z1900-x64.exe	0	1	0d, 0h, 00m, 13s	
Z:\setups\Firefox Installer.exe	1	0	0d, 0h, 00m, 00s	2021-11-25 03:27:03
\\vmware-host\Shared Folders\setups\Firefox Installer.exe	0	0	0d, 0h, 00m, 00s	
C:\Users\THM-4n6\AppData\Local\Temp\7zS09BA49F3\setup-stub.exe	0	1	0d, 0h, 01m, 20s	
Z:\setups\python-3.8.2.exe	1	0	0d, 0h, 00m, 00s	2021-11-25 03:32:00
C:\Users\THM-4n6\AppData\Local\Temp\{Unmapped GUID: B409B86A-9CC9-4639-9E0C-0B35E1DEC040}\.cr\python-3.8.2.exe	0	1	0d, 0h, 00m, 16s	
E7CF176E110C211B	2	2	0d, 0h, 01m, 43s	2021-12-01 12:32:34
Z:\setups\ChromeSetup.exe	1	0	0d, 0h, 00m, 00s	2021-11-25 03:33:34
{Program Files x86}\Google\Temp\GUMFB7B.tmp\GoogleUpdate.e	0	1	0d, 0h, 00m, 03s	

Total rows: 49

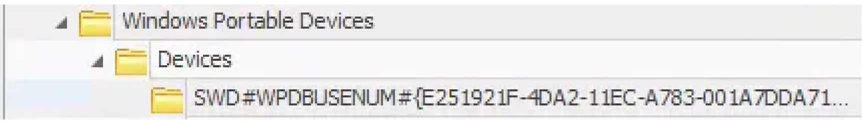
```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24
00000000  FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00   ÿÿÿÿ..............¿...¿...¿...¿...¿.
```

Answer: Z:\setups\python-3.8.2.exe

6: When was the USB device with the friendly name 'USB' last connected?

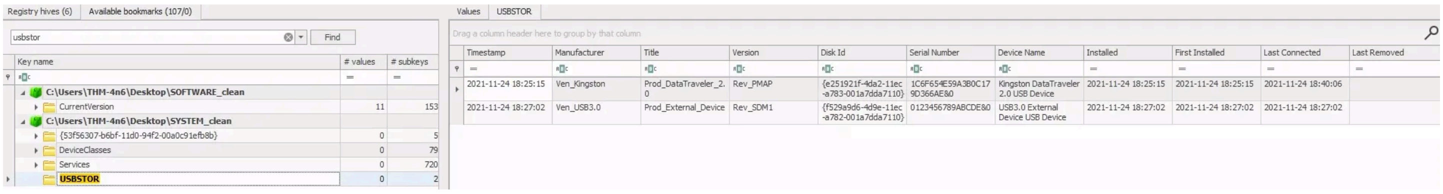
I reread task 9 to jog my memory on how to get the device name. I went to SOFTWARE\Microsoft\Windows Portable Devices\Devices first. Unfortunately, Microsoft folder didn't exist, so the path I used was SOFTWARE\Windows Portable

Devices\Devices. I saw that one of the two folders had a FriendlyName value of USB. I took note of, what I believe to be, the serial number in the folder name.



Windows Portable Devices
Devices
SWD#WPDBUSENUM#{E251921F-4DA2-11EC-A783-001A7DDA71...

Now I searched for "USBSTOR" and looked at the right side to compare values. It looks like the value I took note of wasn't the serial number but disk ID instead.



Registry hives (6)
Available bookmarks (107/0)
Find
Values
USBSTOR
Drag a column header here to group by that column

usbstor

Key name	# values	# subkeys
C:\Users\THM-4n6\Desktop\SOFTWARE_clean		
CurrentVersion	11	153
C:\Users\THM-4n6\Desktop\SYSTEM_clean		
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}	0	5
DeviceClasses	0	79
Services	0	720
USBSTOR	0	2

Timestamp	Manufacturer	Title	Version	Disk Id	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
2021-11-24 18:25:15	Ven_Kingston	Prod_DataTraveler_2.0	Rev_PMAP	{e251921f-4da2-11ec-a783-001a7dda7110}	1C6F654E59A3B0C179D366AE&0	Kingston DataTraveler 2.0 USB Device	2021-11-24 18:25:15	2021-11-24 18:25:15	2021-11-24 18:40:06	
2021-11-24 18:27:02	Ven_USB3.0	Prod_External_Device	Rev_SDM1	{f529a9d6-4d9e-11ec-a782-001a7dda7110}	0123456789ABCDE&0	USB3.0 External Device USB Device	2021-11-24 18:27:02	2021-11-24 18:27:02	2021-11-24 18:27:02	

Answer: 2021–11–24 18:40:06

Thoughts:

I personally felt like this was the right difficulty for me. I've used EnCase and Autopsy before but never even heard of Registry Explorer. I love getting exposed to more tools as you'll never know what your organization will be using. Definitely took me a while to get started as the hardest part for me was understanding how to load the files into Registry Explorer. I enjoyed digging around trying to look for the answer. I even saved the cheat sheet that was given at the end of the room. There is absolutely no way I remembered everything I've read so the cheat sheet will definitely be useful. Excited to see what the next room entails!

Cybersecurity Tryhackme Digital Forensics Dfir Registry

Follow

Written by Toumo

152 Followers · 1 Following

Responses (1)

What are your thoughts?

Respond

Samar
about 2 months ago

thanks

Reply

More from Toumo

Toumo

TryHackMe Redline Write-Up

We just finished the Autopsy room and now we will be learning how to use Redline. I've never used it, nor have I heard of it before, so...

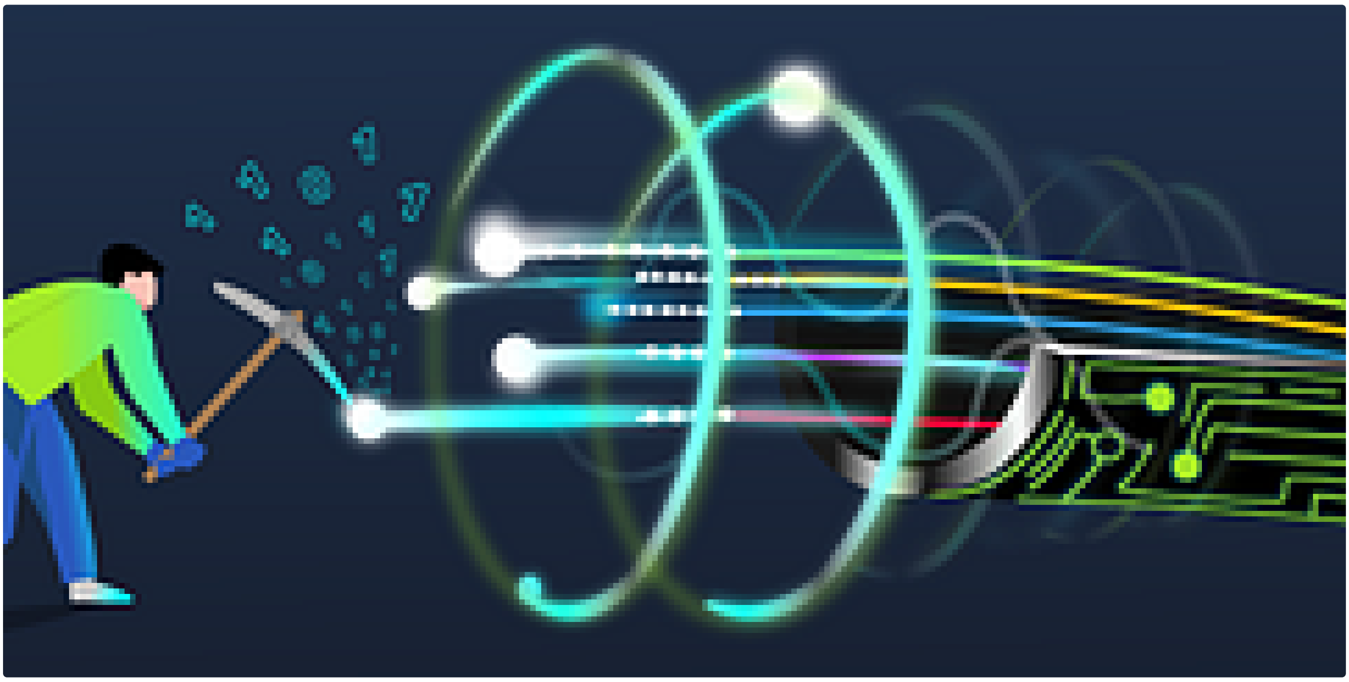
Aug 8, 2023 45 4

Toumo

TryHackMe Velociraptor Write-Up

We'll be learning about Velociraptor now. Another tool that I never heard of but I wonder how this will be different compared to the rest...

Aug 9, 2023 20 1

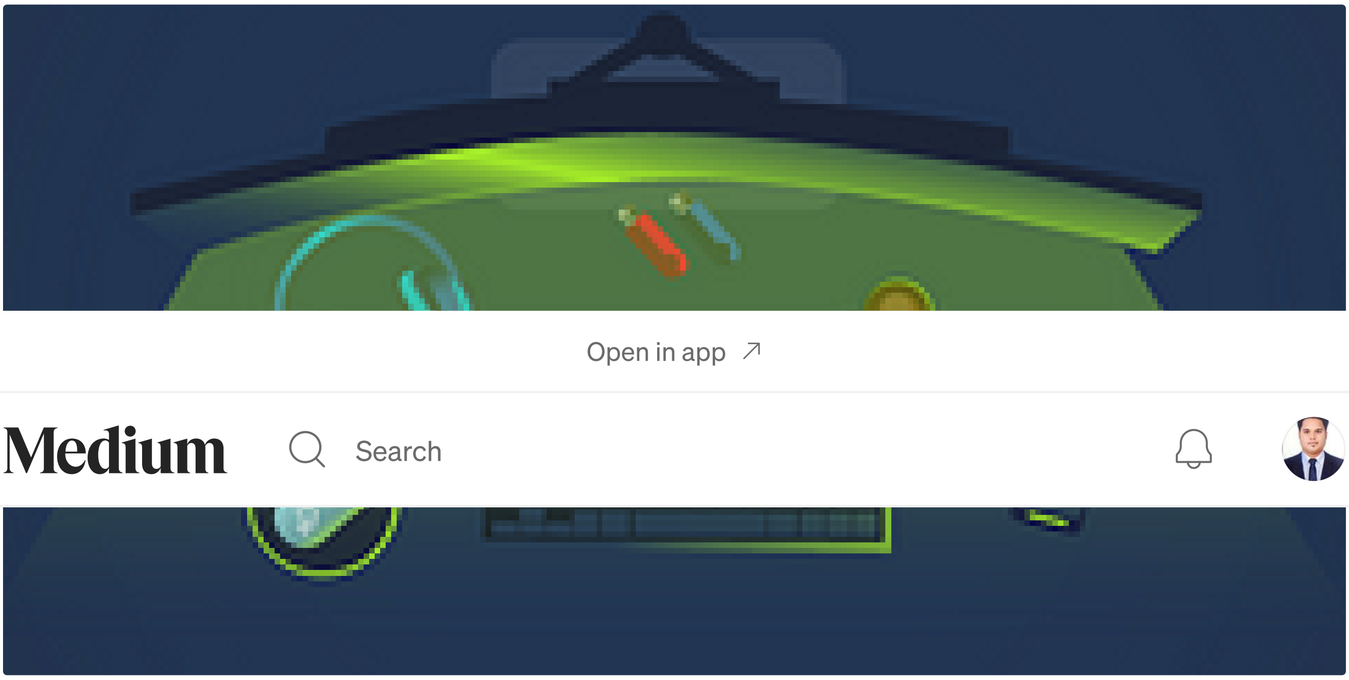


Toumo

TryHackMe NetworkMiner Write-Up

This time, we will be using a new tool called NetworkMiner. My assumption is that we're being exposed to many tools as we do not know what...

Jul 5, 2023 6 1



Toumo

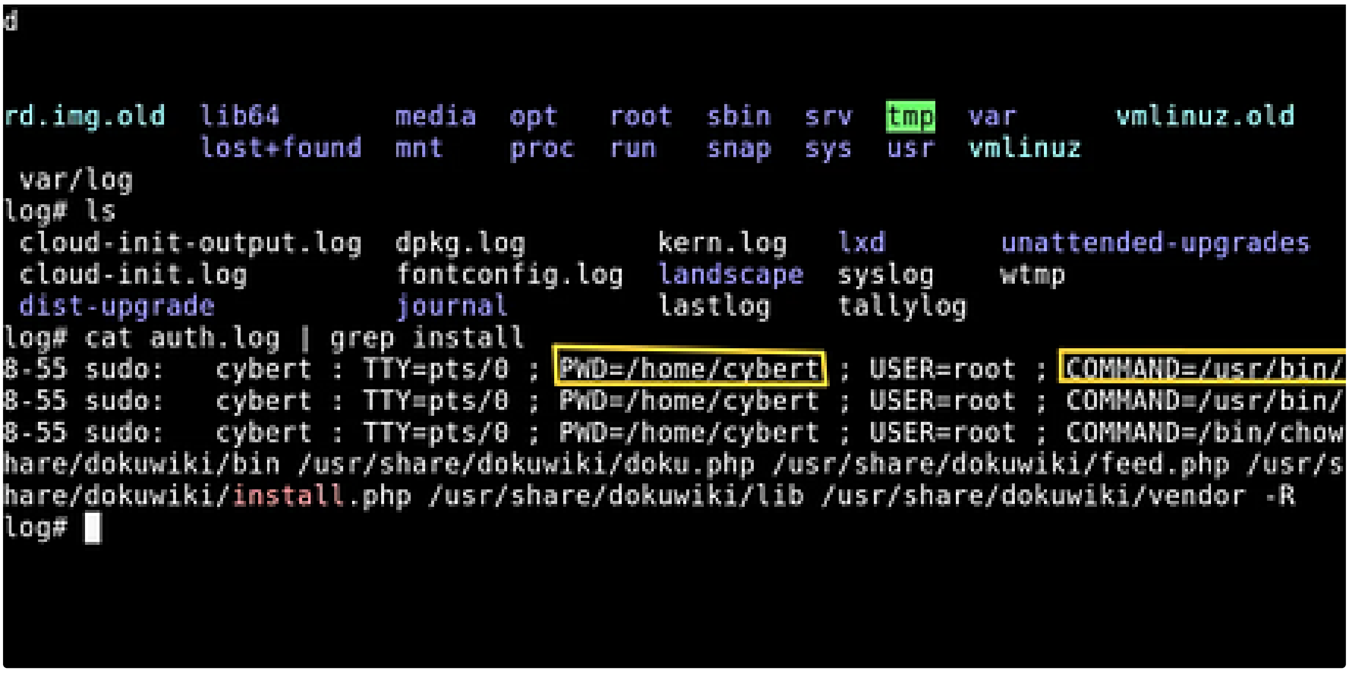
TryHackMe Windows Forensics 2 Write-Up

This is the second part of Windows Forensics. The write-up I did for the first part can be found here. I enjoyed the difficulty last time...

Aug 7, 2023 3 1

See all from Toumo

Recommended from Medium



```
d

rd.img.old  lib64        media  opt   root  sbin  srv  tmp  var      vmlinuz.old
            lost+found   mnt    proc  run   snap  sys  usr  vmlinuz
 var/log
log# ls
 cloud-init-output.log  dpkg.log         kern.log   lxd        unattended-upgrades
 cloud-init.log         fontconfig.log   landscape  syslog     wtmp
 dist-upgrade           journal          lastlog    tallylog
log# cat auth.log | grep install
8-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log# 
```

T 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

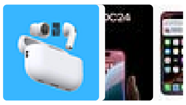
In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

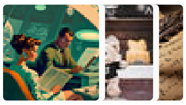
Nov 5, 2024 60

Lists



Tech & Tools

22 stories · 380 saves

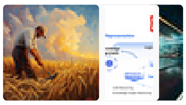


Medium's Huge List of Publications Accepting Submissions

377 stories · 4345 saves

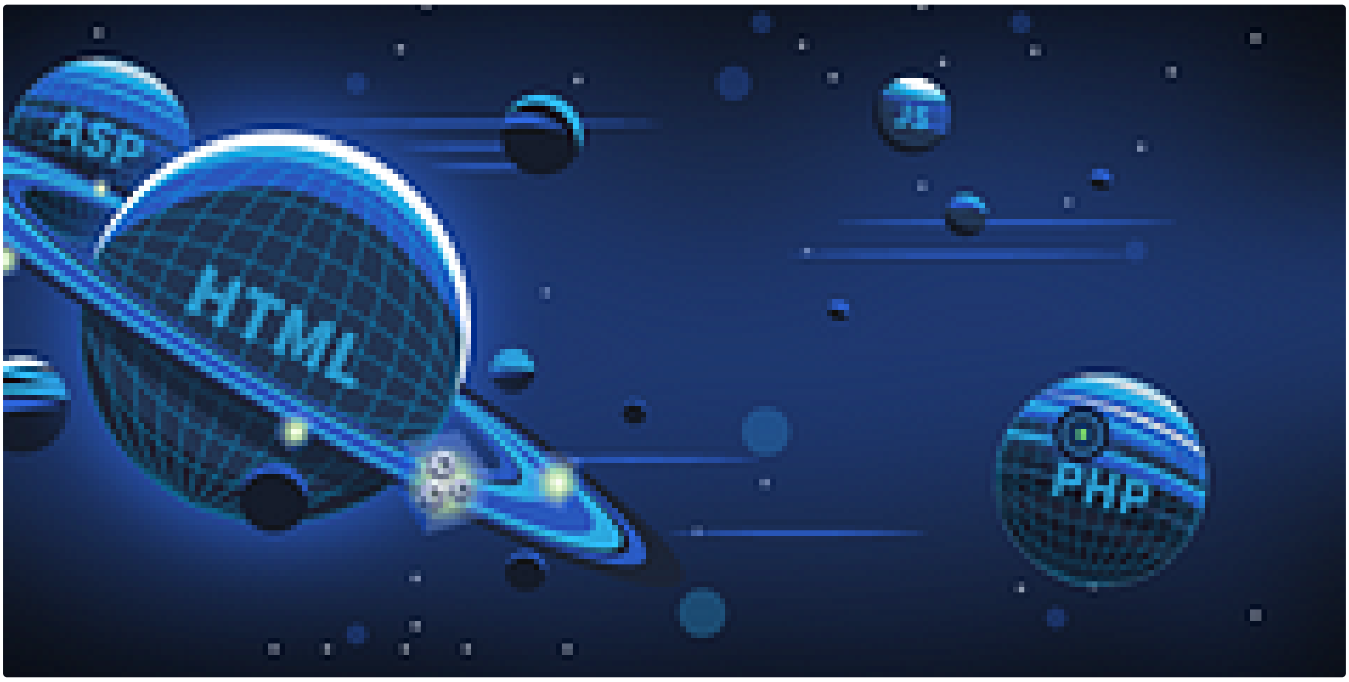
Staff picks

796 stories · 1561 saves



Natural Language Processing

1884 stories · 1529 saves

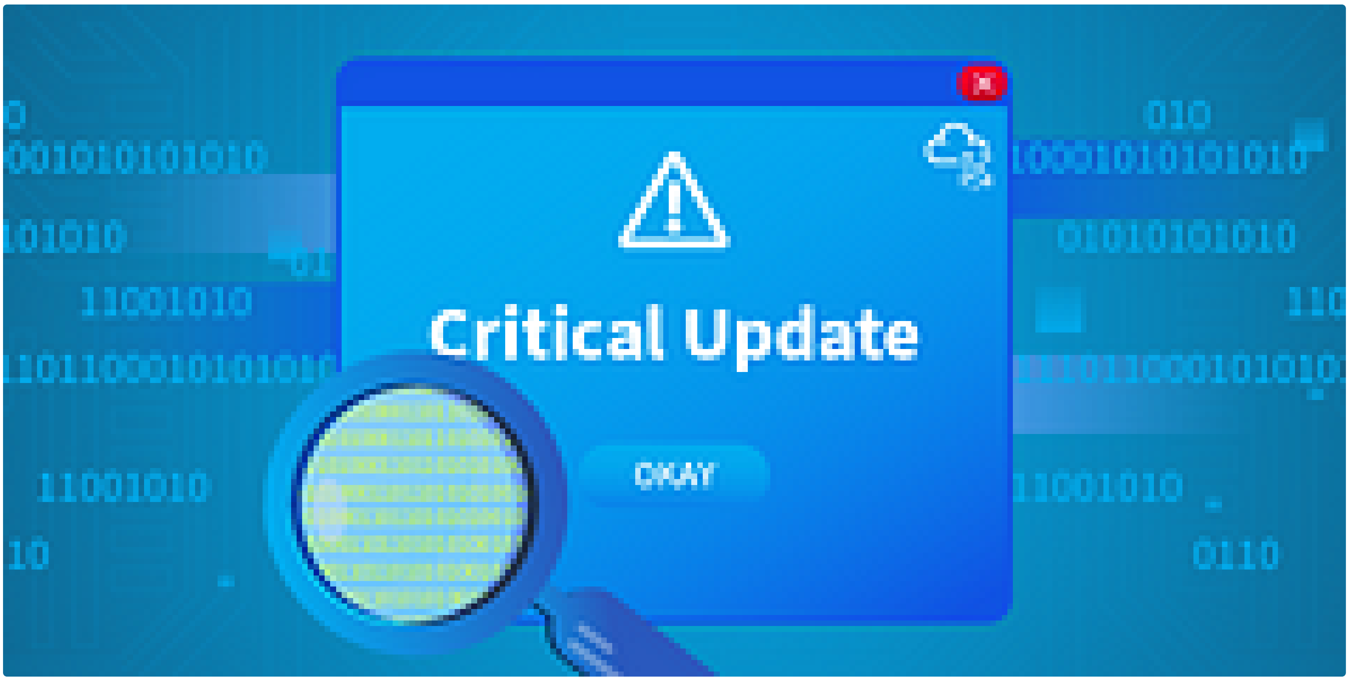


In T3CH by Axoloth

TryHackMe | Web Application Basics | WriteUp

Learn the basics of web applications: HTTP, URLs, request methods, response codes, and headers

Oct 26, 2024 56



In T3CH by Axoloth

TryHackMe | Critical | WriteUp

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

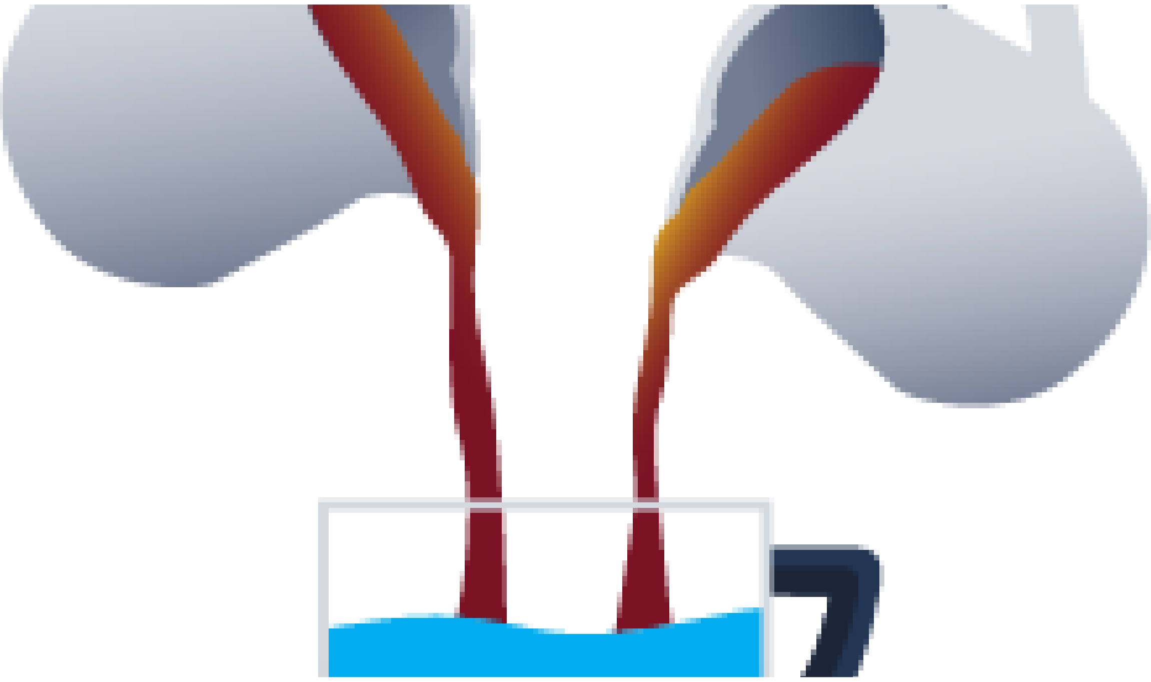
Jul 21, 2024 104

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



MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024 2

See more recommendations