

Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



TryHackMe: Disk Analysis & Autopsy



Sean Dixon · [Follow](#)

7 min read · Jun 13, 2023

Listen

Share

More

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.

Display Name: HASAN2.E01
 Name: HASAN2.E01
 Device ID: bc5e9b04-bb21-4d04-a08f-3c169ea67774
 Time Zone: America/New_York

Acquisition Details: Description: untitled
 Acquired Date: Mon Feb 8 12:40:23 2021
 System Date: Mon Feb 8 12:40:23 2021
 Acqury Operating System: Win 20 tx
 Acqury Software Version: AD14.5.0.3

Image Type: E01
 Size: 65.43 GB (65433829376 bytes)
 Unallocated Space: 45.65 GB (45653525664 bytes)
 Sector Size: 512 bytes
 MD5: 3f08c518adb3b5c1359849657a9b2079
 SHA1: d5ae22ab381cb5884140ef6fbab3946a8f3cf9f2
 SHA256: SHA256

File Paths: C:\Users\Administrator\Desktop\Case Files\HASAN2.E01

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*.

Source File	S	C	O	Name	Domain
SYSTEM				DESKTOP-0R59DJ3	
SOFTWARE					

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.

Source File	S	C	O	User ID	Username
SAM				S-1-5-21-3919888104-523106866-407859479-1005	keshav
SAM				S-1-5-21-3919888104-523106866-407859479-1006	sivapriya
SAM				S-1-5-21-3919888104-523106866-407859479-1007	sandhya
SAM				S-1-5-21-3919888104-523106866-407859479-1008	srini
SAM				S-1-5-21-3919888104-523106866-407859479-1001	H4S4N
SAM				S-1-5-21-3919888104-523106866-407859479-1002	joshwa
SAM				S-1-5-21-3919888104-523106866-407859479-500	Administrator
SAM				S-1-5-21-3919888104-523106866-407859479-1003	suba
SAM				S-1-5-21-3919888104-523106866-407859479-501	Guest
SAM				S-1-5-21-3919888104-523106866-407859479-1004	shreya
SAM				S-1-5-21-3919888104-523106866-407859479-503	DefaultAccount
SAM				S-1-5-21-3919888104-523106866-407859479-504	WDAGUtilityAccount
SOFTWARE				S-1-5-18	systemprofile
SOFTWARE				S-1-5-19	LocalService
SOFTWARE				S-1-5-20	NetworkService

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.

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	H454N	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.

The screenshot shows the Autopsy Forensic Browser interface with the Windows Registry Editor. The left pane displays a tree view of registry keys under 'Windows\System32\config\SYSTEM'. The right pane shows the details for the 'Tcp' key, specifically the 'Adapters' and 'Interfaces' subkeys, which contain information about network adapters. The 'Metadata' section shows the key name as '{e42cf5d6-2174-470f-9b1d-0d448589066c}' and its values. The 'Values' section lists various registry entries such as 'EnableDHCP', 'Domain', 'NameServer', 'DhcpIPAddress', 'DhcpSubnetMask', 'DhcpServer', 'Lease', 'LeaseObtainedTime', 'T1', 'T2', 'LeaseTerminatesTime', 'AddressType', 'IsServerNapAware', 'DhcpConnForceBroadcastFlag', 'DhcpInterfaceOptions', 'DhcpIsMeteredDetected', 'DhcpGatewayHardware', and 'DhcpGatewayHardwareCount'. The 'DhcpIPAddress' value is listed as '0.0.0.0'.

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.

The screenshot shows the Autopsy interface with the 'Installed Programs' section selected. The table lists various software entries, including 'Look@LAN 2.50 Build 36' which is highlighted with a red arrow.

Source File	S	C	O	Program Name
SOFTWARE				Fontcore
SOFTWARE				IE40
SOFTWARE				IE4Data
SOFTWARE				IE5BAKEX
SOFTWARE				IEData
SOFTWARE				MobileOptionPack
SOFTWARE				SchedulingAgent
SOFTWARE				WIC
SOFTWARE				Python Launcher v.3.9.7280.0
SOFTWARE				Look@LAN 2.50 Build 36
SOFTWARE				DMM_Runtime
SOFTWARE				MPlayer2
SOFTWARE				AddressBook
SOFTWARE				Connection Manager
SOFTWARE				DirectDrawEx
SOFTWARE				Fontcore
SOFTWARE				IE40
SOFTWARE				IE4Data
SOFTWARE				IE5BAKEX

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.

The screenshot shows the TryHackMe - Autopsy 4.18.0 interface. On the left is a tree view of the file system, showing volumes like \$Extend, \$Recycle.Bin, \$Unalloc, and various Windows system folders. On the right is a 'Listing' panel showing a table of files from the Look@LAN folder. Below it is a text editor displaying the contents of the Look@LAN.ini file. The file contains the following text:

```

LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=DESKTOP-0R59DJ3
%LANDOMAIN%=DESKTOP-0R59DJ3
%LANUSER%=H4S4N
%LANIP%=192.168.130.216 ←
%LANNIC%=0800272cc4b9
%ISWIN95%=false
%ISWIN98%=false
%ISWINNT3%=false

```

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.

The screenshot shows the Autopsy 4.18.0 interface. On the left, the file tree shows a directory structure including Program Files (x86), Internet Explorer, Look@LAN, and various system folders. The Look@LAN folder is expanded, showing subfolders like Report and sounds. The sounds folder contains images and sounds files. The right side displays a table of files from the Look@LAN folder. Below the table is a text pane showing the contents of a file, likely an .ini file. The text pane includes tabs for Hex, Text, Application, File Metadata, Context, Results, Annotations, and Other Occurrences. The Text tab is selected, showing the following text:

```

LangID=9
IsSelective=0
InstallType=0
[Variables]
%LANHOST%=DESKTOP-0R59DJ3
%LANDomain%=DESKTOP-0R59DJ3
%LANUSER%=H4S4N
%LANIP%=192.168.130.216
%LANNIC%=0800272cc4b9 ←
%ISWIN95%=FALSE
%ISWIN98%=FALSE
%ISWINNT3%=FALSE

```

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

The screenshot shows the Autopsy software interface with the title bar "img_HASAN2.E01/vol_vols/Windows/System32/config/SOFTWARE - Editor". The main pane displays a tree view of registry keys under "Software". One key, "NetworkCards", is selected and expanded, showing two sub-values: "ServiceName" and "Description". To the right of the tree view is a panel titled "Metadata" which shows the key has 2 subkeys and 2 values. Below this is a table titled "Values" with two rows:

Name	Type	Value
ServiceName	REG_SZ	{E42CF5D6-2174-470F-9B1D-0D448589066C}
Description	REG_SZ	Intel(R) PRO/1000 MT Desktop Adapter

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.

The screenshot shows the Autopsy interface with the 'Web Bookmarks' section selected. The left sidebar shows various analysis categories like Windows Registry, ProgramData, and Results. The main pane displays a table of bookmark entries from a 'places.sqlite' database. One entry, which is highlighted with a red arrow, corresponds to the coordinates provided in the question.

Source File	S	C	O	URL	Title
places.sqlite				https://www.mozilla.org/en-US/contribute/	Get Involved
places.sqlite				https://www.mozilla.org/en-US/about/	About Us
places.sqlite				https://www.mozilla.org/en-US/refox/central/	Getting Started
places.sqlite				https://support.mozilla.org/en-US/products/refox	Help and Tutorials
places.sqlite				https://support.mozilla.org/en-US/b/customize-firefox-controls-buttons-and-toob...	Customize Firefox
places.sqlite				https://www.mozilla.org/en-US/contribute/	Get Involved
places.sqlite				https://www.mozilla.org/en-US/about/	About Us
places.sqlite				https://www.mozilla.org/en-US/refox/central/	Getting Started
places.sqlite				https://www.sathyabama.ac.in/	Home Sathyabama Institute of Science and Technology (Deemed to be University)
places.sqlite				https://www.sathyabama.ac.in/	
places.sqlite				https://support.mozilla.org/en-US/products/refox	Help and Tutorials
places.sqlite				https://support.mozilla.org/en-US/b/customize-firefox-controls-buttons-and-toob...	Customize Firefox
places.sqlite				https://www.mozilla.org/en-US/contribute/	Get Involved
places.sqlite				https://www.mozilla.org/en-US/about/	About Us
places.sqlite				https://www.mozilla.org/en-US/refox/central/	Getting Started
places.sqlite				https://www.google.com/maps/place/12%2C16%2B05223.0%22N+80%2C80132...	12°52'23.0"N 80°13'25.0"E - Google Maps
Bing.url				http://go.microsoft.com/fwlink/p/LinkId=255142	Bing.url
Bing.url				http://go.microsoft.com/fwlink/p/LinkId=255142	Bing.url
Bing.url				http://go.microsoft.com/fwlink/p/LinkId=255142	Bing.url
Bing.url				http://go.microsoft.com/fwlink/p/LinkId=255142	Bing.url
Bing.url				http://go.microsoft.com/fwlink/p/LinkId=255142	Bing.url

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.

ARE YOU A ONE OR A ZERO

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.

Anto Joshwa

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.

The screenshot shows the Autopsy 4.18.0 interface. The left pane displays a file system tree for the volume `/img_HASAN2.E01/vol_vol3`. The `Users\shreya\Desktop` folder is selected. The right pane shows a table of files found in this folder. The table has columns: Name, S, C, O, Modified Time, Change Time, and Access Time. The data is as follows:

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2021-02-06 06:51:42 EST	2021-02-06 06:51:42 EST	2021-02-07 11:48:
[parent folder]				2021-02-06 06:44:47 EST	2021-02-06 06:44:47 EST	2021-02-07 13:10:
desktop.ini	0			2021-02-06 05:41:58 EST	2021-02-06 06:12:21 EST	2021-02-07 13:10:
exploit.ps1	0			2021-02-06 06:53:29 EST	2021-02-06 06:53:29 EST	2021-02-07 03:01:
shreya.txt	0			2021-02-06 12:40:10 EST	2021-02-06 12:40:10 EST	2021-02-07 03:01:

At the bottom of the interface, a search bar contains the text `flag{i_changed_it}`.

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.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)
[current folder]				2021-02-06 06:08:53 EST	2021-02-06 11:42:52 EST	2021-02-06 12:45:15 EST	2021-02-06 06:08:53 EST	208	Allocated
[parent folder]				2021-02-06 06:08:53 EST	2021-02-06 06:08:53 EST	2021-02-06 12:45:03 EST	2021-02-06 06:08:53 EST	256	Allocated
ConsoleHost_history.txt		0		2021-02-06 12:40:36 EST	2021-02-06 12:40:36 EST	2021-02-06 12:45:03 EST	2021-02-06 06:08:53 EST	421	Allocated

```

cd .\Desktop\
exitcls
Add-Content .\shreya.txt 'flag{HarleyQuinnForQueen}'
Get-Content .\shreya.txt
Add-Content .\shreya.txt 'flag{HarleyQuinnForQueen}'
Get-Content .\shreya.txt
Set-Content .\shreya.txt 'flag{i_changed_it}'
exit

```

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.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location
{current folder}				2021-02-06 06:51:42 EST	2021-02-06 06:51:42 EST	2021-02-07 11:48:09 EST	2021-02-06 05:41:55 EST	360	Allocated	Allocated	unknown	/img_HASAN2.E01/vol_v03/Users/shreya/Desktop
[parent folder]				2021-02-06 06:44:47 EST	2021-02-06 06:44:47 EST	2021-02-07 13:10:05 EST	2021-02-06 05:41:59 EST	256	Allocated	Allocated	unknown	/img_HASAN2.E01/vol_v03/
desktop.ini			O	2021-02-06 05:41:58 EST	2021-02-06 06:12:21 EST	2021-02-07 13:10:05 EST	2021-02-06 05:41:59 EST	282	Allocated	Allocated	unknown	/img_HASAN2.E01/vol_v03/
exploit.ps1			O	2021-02-06 06:53:29 EST	2021-02-06 06:53:29 EST	2021-02-07 03:01:54 EST	2021-02-06 06:22 EST	766	Allocated	Allocated	unknown	/img_HASAN2.E01/vol_v03/
shreya.txt			O	2021-02-06 12:40:10 EST	2021-02-06 12:40:10 EST	2021-02-07 03:01:49 EST	2021-02-06 05:42:42 EST	20	Allocated	Allocated	unknown	/img_HASAN2.E01/vol_v03/

```

if(((System.Security.Principal.WindowsIdentity)GetCurrent()).groups -eq "Administrators") {
    #Payload goes here
    #It'll run as Administrator
    New-Item "C:\Users\H4S4N\Desktop\hacked.txt"
    Add-Content C:\Users\H4S4N\Desktop\hacked.txt 'Flag{I-hacked-you}'
    ##### https://youtu.be/C9GfMFFjhYI
}

```

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.

Tryhackme - Autopsy 4.18.0

Case View Tools Window Help

The screenshot shows the Autopsy interface with the following details:

- Left Panel (File Tree):** Shows a hierarchical view of the file system. The current path is `/img_HASAN2.E01/vol_vol3/Users/H4S4N/Downloads`. Key folders include Support (11), Windows NT (4), Windows Security Health (4), WinMSIPC (3), WwanSvc (4), Microsoft OneDrive (3), Mozilla (5), Package Cache (14), Packages (10), regid.1991-06.com.microsoft (3), SoftwareDistribution (2), ssh (2), Start Menu (2), Templates (2), USOPrivate (3), USOShared (3), WindowsHolographicDevices (3), Recovery (2), System Volume Information (7), and Users (15). The `H4S4N` folder is expanded, showing All Users (2), Default (28), Default User (2), and `H4S4N` (34).
- Right Panel (File Listing):** The `Listing` tab is selected, showing a table of files in the `Downloads` folder. The table has columns: Name, S, C, O, Modified Time, and CI.
- Table Data:**

Name	S	C	O	Modified Time	CI
[current folder]				2021-02-07 02:49:01 EST	2C
[parent folder]				2021-02-06 18:51:57 EST	2C
Oor1.jpg	0			2020-10-01 14:17:08 EDT	2C
desktop.ini	0			2021-02-06 18:49:17 EST	2C
lalsetup250.exe	0			2021-02-07 02:47:16 EST	2C
mimikatz_trunk.zip	0			2021-02-06 09:56:28 EST	2C
mimikatz_trunk.zip:Zone.Identifier	0			2021-02-06 09:56:28 EST	2C
python-3.9.1-amd64.exe	0			2021-02-06 10:27:17 EST	2C
wallpapersden-com-mr-robot-season-4-7500x3708.jpg	0			2021-02-06 11:42:50 EST	2C
wallpapersden-com-mr-robot-season-4-7500x3708.jpg:Zone.Iden	0			2021-02-06 11:42:50 EST	2C
- Bottom Panel (File Details):** Shows tabs for Hex, Text, Application, File Metadata, Context, Results, Annotations, and Other Occurrences. The Application tab is selected, displaying the contents of the mimikatz_trunk.zip file.

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.

The screenshot shows the TryHackMe - Autopsy 4.18.0 interface. The left sidebar displays a file tree of the analyzed disk volume, including sections like Features, LocalCopy, Network Inspection System, Platform, Quarantine, Scans, BackupStore, History, Results, Service, DetectionHistory, Store, Scans, and Support. The main pane is titled 'Listing' and shows a table of log entries from the path '/img_HASAN2.E01/vol_vvol3/ProgramData/Microsoft/Windows Defender/Scans/History/Service/DetectionHistory/02'. The table has columns for Name, S, C, O, Modified Time, Change Time, and Access Time. One entry is selected, showing details in the bottom pane: 'Name' is '8363AFD9-AF2E-453A-BB2D-766E1C57A8BA', 'Modified Time' is '2021-02-07 02:49:01 EST', 'Change Time' is '2021-02-07 02:49:01 EST', and 'Access Time' is '2021-02-07 12:10:57 EST'. Below the table are tabs for Hex, Text, Application, File Metadata, Context, Results, Annotations, Other Occurrences, Strings, Indexed Text, and Translation. The 'Text' tab is active, displaying the log entry content.

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2021-02-07 02:48:21 EST	2021-02-07 02:48:21 EST	2021-02-07 12:10:57 EST
[parent folder]				2021-02-06 11:19:43 EST	2021-02-07 02:29:18 EST	2021-02-07 12:10:57 EST
2B18887D-B94C-4E51-934B-654F69FAE7E2	0			2021-02-07 11:05:20 EST	2021-02-07 11:05:20 EST	2021-02-07 12:10:57 EST
7F334C0D-CED8-4268-8096-CE083CD29441	0			2021-02-07 11:05:20 EST	2021-02-07 11:05:20 EST	2021-02-07 12:10:57 EST
8363AFD9-AF2E-453A-BB2D-766E1C57A8BA	0			2021-02-07 02:49:01 EST	2021-02-07 02:49:01 EST	2021-02-07 12:10:57 EST

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.

File Search by Attributes

Name: .yar

*Note: Name match is case insensitive and matches any part of the file name. Regular expressions are not currently supported.

Date: ... to ...
*Empty fields mean "No Limit" *The date format is mm/dd/yyyy
Timezone: (GMT-5:00) America/New_York

Modified Accessed Created Changed

Known Status:
 Unknown Known (NSRL or other) Notable

MIME Type:
 application/activemessage
 application/andrew-inset
 application/applefile
 application/appixware
 application/atom+xml

*Note: Multiple MIME types can be selected

MD5:

SHA-256:

Data Source:
HASAN2.E01

*Note: Multiple data sources can be selected

Search

Searching for filenames containing .yar

TryHackMe - Autopsy 4.18.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing File Search Results 1 File Search Results 2

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
kiwi_passwords.yar.link	0			2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	836	Allocated
kiwi_passwords.yar.link-dock				2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	2021-02-06 10:05:17 EST	3260	Allocated
kiwi_passwords.yar	0			2020-09-16 21:04:34 EDT	0000-00-00 00:00:00	2020-09-16 21:04:34 EDT	2020-09-16 21:04:34 EDT	2834	Allocated

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 200% Reset

```
/*
 Benjamin DELPY `gentilkiwi`
 https://blog.gentilkiwi.com
 benjamin@gentilkiwi.com
 Licence : https://creativecommons.org/licenses/by/4.0/
 */

rule mimikatz
{
    meta:
        description      = "mimikatz"
        author           = "Benjamin DELPY (gentilkiwi)"
        tool_author      = "Benjamin DELPY (gentilkiwi)"
}
```

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.

The screenshot shows the Autopsy 4.18.0 interface. The left sidebar displays a tree view of the case contents, including Windows (104), Views (File Types, Deleted files, File System, All), MB File System, Results (Extracted Content, EXIF Metadata, Encryption Suspected, Extension Mismatch Detected, Installed Programs, Metadata, Operating System Information, Operating System User Account, Recent Documents, Run Programs, Shell Bags, USB Device Attached, User Content Suspected, Web Browsers, Web Categories, and Web Cookies). The main pane shows a listing of found artifacts. A red arrow points to the artifact '2.2.0 20200918 Zerologon encrypted.lnk'. The table columns include Name, Keyword Preview, Location, and Modified Time.

Name	Keyword Preview	Location	Modified Time
1112_0H3H4E_CU1YV4_VU4[Users\sandhya\AppData\Local\Temp\1401-1401-1401-1401-1401-1401]	1112_0H3H4E_CU1YV4_VU4[Users\sandhya\AppData\Local\Temp\1401-1401-1401-1401-1401-1401]	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2021-02-07 13:10:07 EST
0	0	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2020-09-18 13:19:18 EDT
0	0	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2020-09-18 00:00:00:00
WebCacheV01.dat	ds/2.0%20200918%20zerologon%20encrypted.zip	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2021-02-07 13:10:07 EST
mimkatz.exe	rrentpostzerologon\zerologon\pad\agesask.a dt	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2020-09-18 13:19:18 EDT
2.2.0 20200918 Zerologon encrypted.lnk	2.2.0 20200918 %20zerologon%20encrypted.ln	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2021-02-06 09:26:25 EST
Recent Documents Artifact	oadis2.2.0 20200918%20zerologon%20encrypted.zippath	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2021-02-06 09:26:25 EST
2.2.0 20200918 Zerologon encrypted.lnk-slac	2.2.0 20200918 %20zerologon%20encrypted.lnk-slac	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2021-02-06 09:26:25 EST
Web Cookies Artifact	ix(2.0%20200918%20zerologon%20encrypted.zip)opro	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2021-02-06 09:54:44 EST
B57146C2B88B714BF6353A884EA1A2171857E5D6	ix(2.0%20200918%20zerologon%20encrypted.zip)	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2021-02-06 09:25:31 EST
places.sqlite	ix(2.0%20200918%20zerologon%20encrypted.zip)	/img_HASAN2_E01/vol_v01/Users/sandhya/AppData/Local/Temp/1401-1401-1401-1401-1401-1401	2021-02-06 09:54:44 EST
RegRipper /img_HASAN2_E01/vol_v01/	23 = 2.2.0 20200918%20zerologon%20encrypted.zip 22	RegRipper /img_HASAN2_E01/vol_v01/Users/sandhya/NT...	

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

Hosts (1)	Sources (8)	Sourcetypes (8)
		<input type="text" value="filter"/> <input type="button" value="Search"/>
Sourcetype	Count	Last Update
Perfmon:Available Memory	1,668	5/16/22 1:47:03.000 PM
Perfmon:CPU Load	3,194	5/16/22 1:47:02.000 PM
Perfmon:Free Disk Space	12	5/13/22 9:06:02.000 PM
Perfmon:Network Interface	3,336	5/16/22 1:47:03.000 PM
WinEventLog:Application	109	5/16/22 1:42:31.000 PM
WinEventLog:Microsoft-Windows-Sysmon/Operational	7,004	5/16/22 1:46:40.000 PM
WinEventLog:Security	1,651	5/16/22 1:45:14.000 PM
WinEventLog:System	104	5/16/22 1:46:39.000 PM

 Sean Dixon

TryHackMe: PS Eclipse

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

Jun 7, 2023  3


.. 0x85d74030:lsm.exe	512	396	9	135	2021-01-31	18:01:11 UTC+0000
.. 0x85d5f030:services.exe	496	396	8	205	2021-01-31	18:01:11 UTC+0000
.. 0x85e6d548:svchost.exe	896	496	42	1148	2021-01-31	18:01:11 UTC+0000
.. 0x85ed6030:spoolsv.exe	1196	496	14	277	2021-01-31	18:01:12 UTC+0000
.. 0x84c80a48:VGAAuthService.	1560	496	3	83	2021-01-31	18:01:12 UTC+0000
.. 0x85d5a450:svchost.exe	2380	496	10	322	2021-01-31	18:03:15 UTC+0000
.. 0x85ed91c8:svchost.exe	2204	496	11	143	2021-01-31	18:03:14 UTC+0000
.. 0x85e0fd40:svchost.exe	688	496	8	271	2021-01-31	18:01:11 UTC+0000
.. 0x85ea9030:svchost.exe	1068	496	16	470	2021-01-31	18:01:12 UTC+0000
.. 0x84e81d40:dllhost.exe	1740	496	13	194	2021-01-31	18:01:14 UTC+0000
.. 0x84d11030:vmtoolsd.exe	1720	496	10	278	2021-01-31	18:01:13 UTC+0000
.. 0x85d975b0:svchost.exe	2508	496	5	87	2021-01-31	18:21:28 UTC+0000
.. 0x85f32cb0:taskhost.exe	1348	496	8	157	2021-01-31	18:01:12 UTC+0000
.. 0x84dc1d40:SearchIndexer.	2232	496	10	704	2021-01-31	18:01:18 UTC+0000
.. 0x84f0a030:SearchFilterHo	3008	2232	5	108	2021-01-31	18:23:00 UTC+0000
.. 0x84f5ead8:SearchProtocol	2304	2232	8	449	2021-01-31	18:01:18 UTC+0000
.. 0x83ebc0f0:sppsvc.exe	2432	496	4	147	2021-01-31	18:03:14 UTC+0000
.. 0x85e58030:svchost.exe	856	496	14	307	2021-01-31	18:01:11 UTC+0000
.. 0x98ff9b88:dwm.exe	1424	856	3	69	2021-01-31	18:01:12 UTC+0000
.. 0x85e22520:svchost.exe	736	496	18	457	2021-01-31	18:01:11 UTC+0000
.. 0x85f07290:svchost.exe	1252	496	19	332	2021-01-31	18:01:12 UTC+0000
.. 0x85e424a0:svchost.exe	2032	496	6	92	2021-01-31	18:01:13 UTC+0000
.. 0x85e92a88:svchost.exe	1000	496	11	529	2021-01-31	18:01:11 UTC+0000
.. 0x85de2b08:svchost.exe	620	496	12	364	2021-01-31	18:01:11 UTC+0000
.. 0x84f3d940:WmiPrvSE.exe	208	620	8	120	2021-01-31	18:24:23 UTC+0000
.. 0x84e3ea58:WmiPrvSE.exe	1296	620	10	202	2021-01-31	18:01:14 UTC+0000
.. 0x84d28a78:msdtc.exe	2044	496	12	148	2021-01-31	18:01:16 UTC+0000
.. 0x85d72958:lsass.exe	504	396	6	566	2021-01-31	18:01:11 UTC+0000

 Sean Dixon

BTLO: Memory Analysis—Ransomware

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

Jun 10, 2023



This screenshot of the Autopsy interface shows the 'Evidence Tree' pane on the right, which displays a hierarchical view of files and folders from the 'DiskDigger.ad1' image. The 'File List' pane on the right shows a detailed list of files with columns for Name, Type, Size, and MD5 Hash. The 'Evidence Tree' pane has a context menu open over a folder, with 'Verify Drive/Image...' selected.

Sean Dixon

CyberDefenders: AfricanFalls

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

Jun 12, 2023 1



This screenshot of the Autopsy interface shows the 'System Information' panel on the left, listing various system components and their status. To the right, there are three expandable sections: 'Primary Network Adapter MAC', 'BIOS Information', and 'Operating System Information'. The 'Operating System Information' section is expanded, showing details about the Windows 7 Home Premium operating system.

Sean Dixon

TryHackMe: REvil Corp

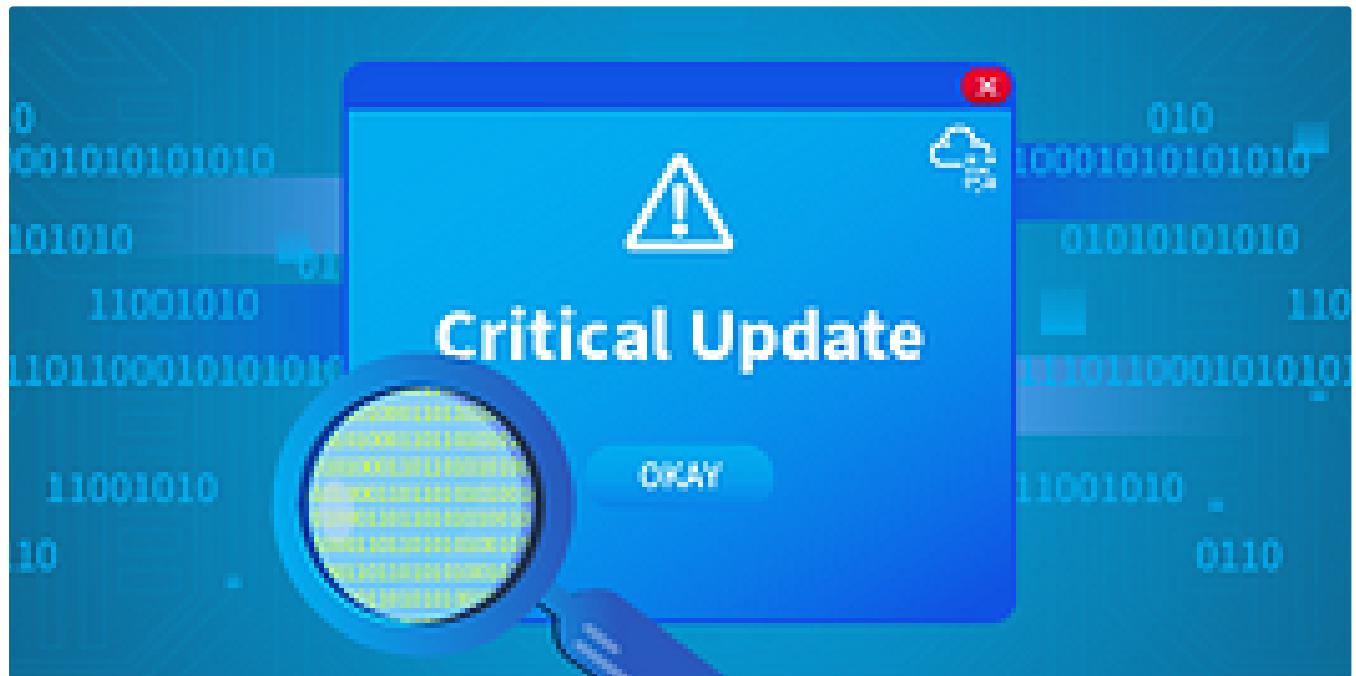
Medium-difficulty forensics challenge. Tools/Topics: Redline, Ransomware, File Changes, Download History, Browser History.

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



```
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



...

Lists



Staff picks

796 stories · 1561 saves



Stories to Help You Level-Up at Work

19 stories · 912 saves



Self-Improvement 101

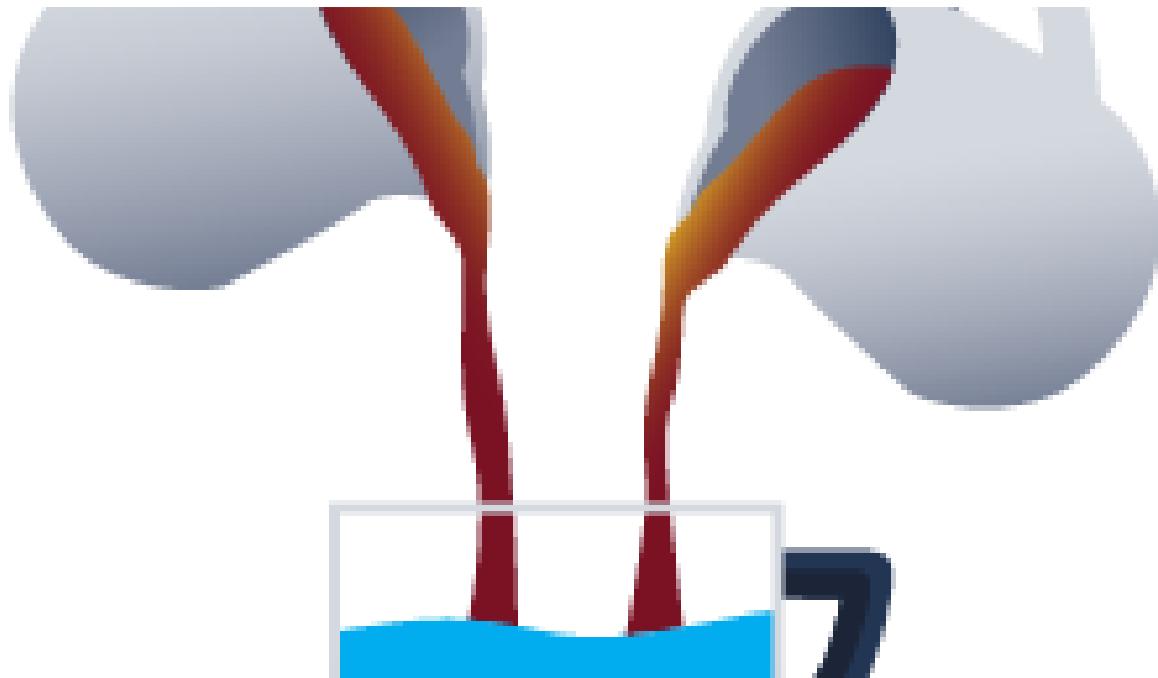
Open in app ↗

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

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

Sep 4, 2024  50

...

**Try
Hack
Me**

NEW CHALLENGE ROOM!

Disgruntled

Use your Linux forensics knowledge to investigate an incident

tryhackme.com/room/disgruntled

Difficulty: **Easy** Platform: **Linux**

 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 useful for you. In this write-up, I will...

Aug 14, 2024



...

See more recommendations