

Disk Analysis & Autopsy

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.

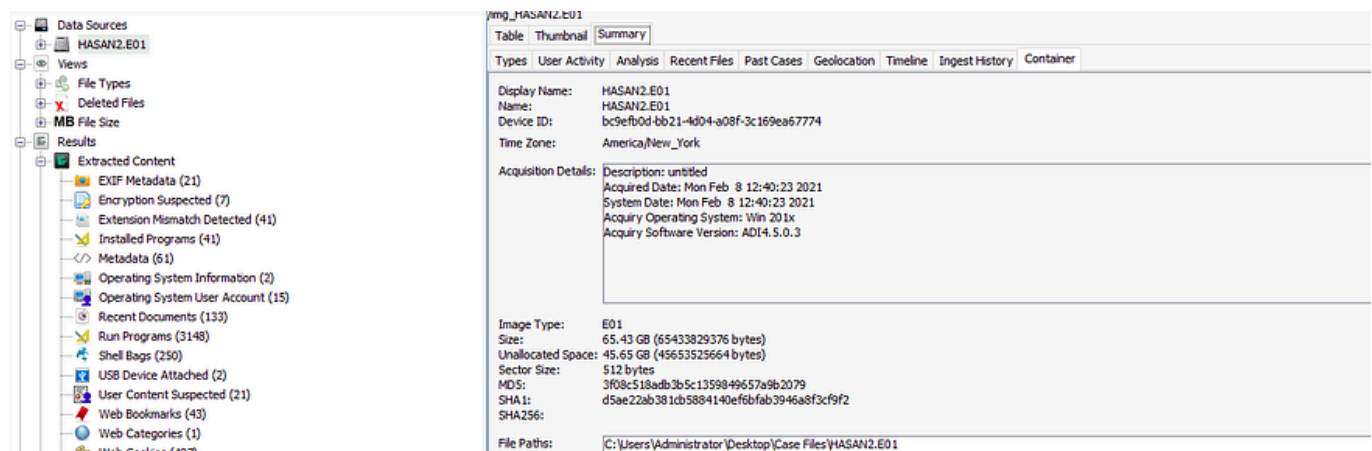
Scenario: Your task is to perform a manual analysis of the artifacts discovered by Autopsy to answer the questions below.

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.

Press enter or click to view image in full size



The screenshot shows the Autopsy interface with the 'HASAN2.E01' image selected. The left sidebar shows the 'Data Sources' tree with 'Extracted Content' expanded. The right pane shows the 'Summary' tab for the image. The 'Image Type' is E01, and the 'MD5' hash is 3f08c518adb3b5c1359849657a9b2079.

Types	User Activity	Analysis	Recent Files	Past Cases	Geolocation	Timeline	Ingest History	Container
Display Name: HASAN2.E01								
Name: HASAN2.E01								
Device ID: bc9efb0d-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 Acquiry Operating System: Win 201x Acquiry Software Version: ADI4.5.0.3								
Image Type: E01								
Size: 65.43 GB (65433829376 bytes)								
Unallocated Space: 45.65 GB (45653525664 bytes)								
Sector Size: 512 bytes								
MD5: 3f08c518adb3b5c1359849657a9b2079								
SHA1: d5ae22ab381cb5884140ef6bfab3946a8f3cf9f2								
SHA256:								
File Paths: C:\Users\Administrator\Desktop\Case Files\HASAN2.E01								

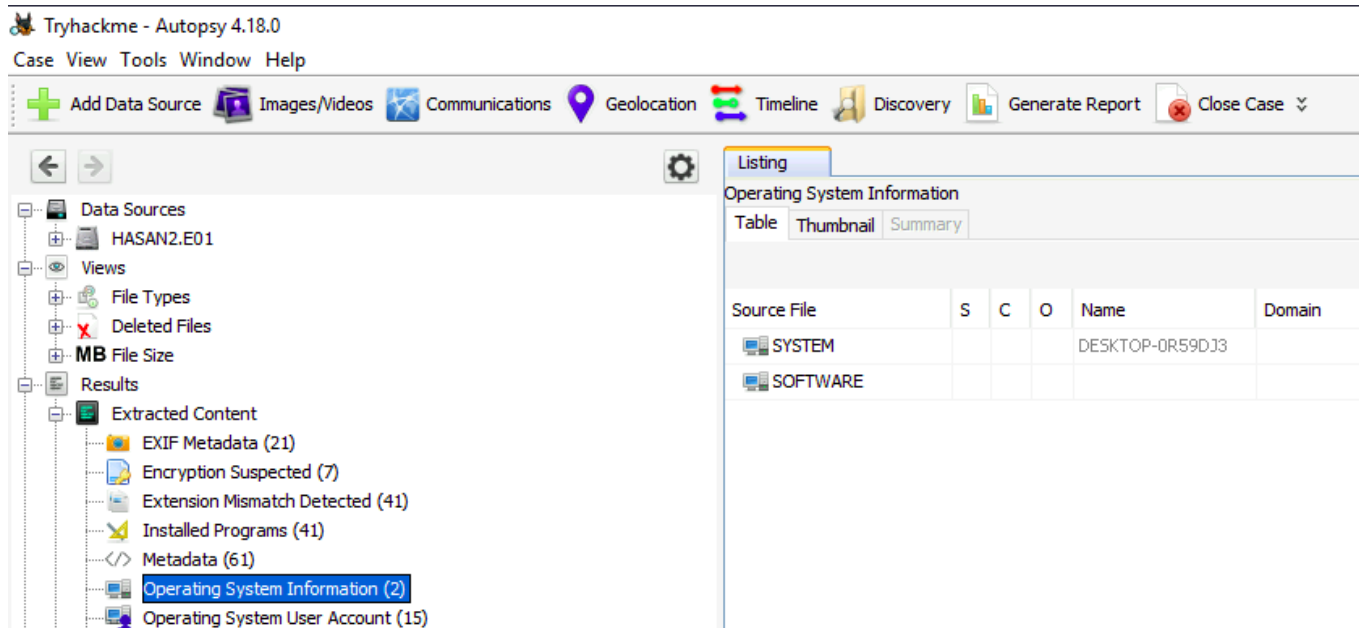
Image summary information, including hash values

Answer: 3f08c518adb3b5c1359849657a9b2079

Q2: What is the computer account name?

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

Press enter or click to view image in full size



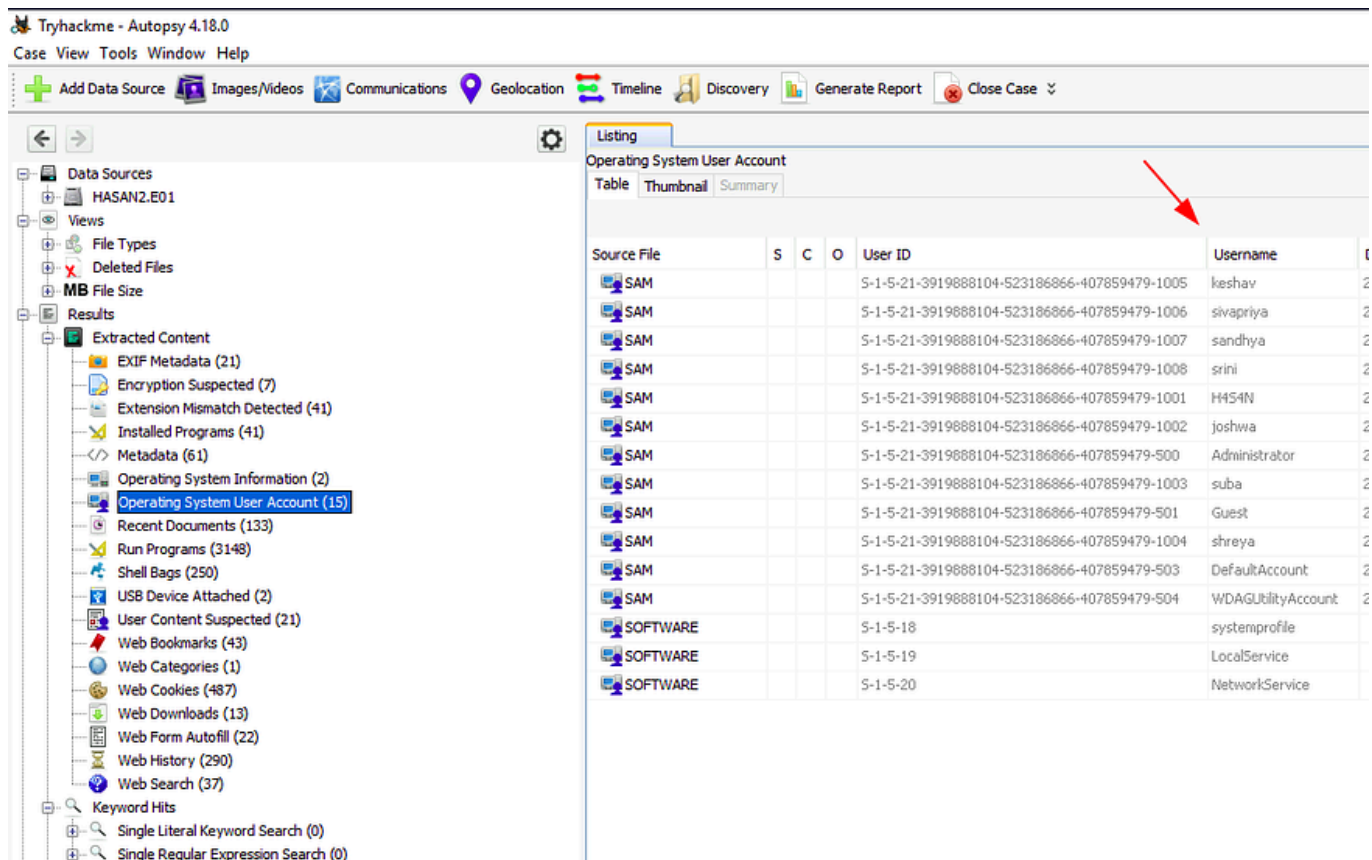
Computer name under the OS Information results.

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.

Press enter or click to view image in full size



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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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*

Press enter or click to view image in full size

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.

Get Sean Dixon's stories in your inbox

Join Medium for free to get updates from this writer.

Subscribe

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

Searching for filenames containing .yar

Press enter or click to view image in full size

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.

Press enter or click to view image in full size

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