

# Disk Analysis & Autopsy

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

Here I will perform a manual analysis of the artifacts discovered by Autopsy to answer the module questions below.

## 1. What is the MD5 hash of the E01 image?

Select the E01 datasource in the Container tab under Summary.

**Answer:** 3f08c518adb3b5c1359849657a9b2079

The screenshot shows the Autopsy interface with the 'HASAN2.E01' datasource selected. The 'Summary' tab is active. In the 'Extracted Content' section, 'Operating System Information' is highlighted. The 'Operating System User Account' item under it is also highlighted. The 'File Paths' field shows the path: C:\Users\Administrator\Desktop\Case Files\HASAN2.E01.

## 2. What is the computer account name?

The computer name is under the results for “Operating System Information”.

**Answer:** DESKTOP-0R59DJ3

The screenshot shows the 'Operating System Information' listing. The 'SYSTEM' row has 'Name' set to 'DESKTOP-0R59DJ3'. The 'Domain' column is empty.

# Disk Analysis & Autopsy

### 3. List all the user accounts

Below the Operating System Information results I see an option for Operating System User Accounts which is where the usernames are listed.

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

The screenshot shows the 'Operating System User Account' listing in the Autopsy interface. The left sidebar shows various data sources and views, including 'Extracted Content' which is expanded to show categories like EXIF Metadata, Encryption Suspected, Extension Mismatch Detected, Installed Programs, Metadata, Operating System Information, and Operating System User Account (15). The main pane displays a table of user accounts with columns for Source File, S, C, O, User ID, Username, and Count. A red arrow points to the 'Username' column, highlighting the list of users: H4S4N, joshwa, keshav, sandhya, shreya, sivapriya, srini, and suba.

Source File	S	C	O	User ID	Username	Count
SAM				S-1-5-21-3919888104-523186866-407859479-1005	keshav	2
SAM				S-1-5-21-3919888104-523186866-407859479-1006	sivapriya	2
SAM				S-1-5-21-3919888104-523186866-407859479-1007	sandhya	2
SAM				S-1-5-21-3919888104-523186866-407859479-1008	srini	2
SAM				S-1-5-21-3919888104-523186866-407859479-1001	H4S4N	2
SAM				S-1-5-21-3919888104-523186866-407859479-1002	joshwa	2
SAM				S-1-5-21-3919888104-523186866-407859479-500	Administrator	2
SAM				S-1-5-21-3919888104-523186866-407859479-1003	suba	2
SAM				S-1-5-21-3919888104-523186866-407859479-501	Guest	2
SAM				S-1-5-21-3919888104-523186866-407859479-1004	shreya	2
SAM				S-1-5-21-3919888104-523186866-407859479-503	DefaultAccount	2
SAM				S-1-5-21-3919888104-523186866-407859479-504	WDAGUtilityAccount	2
SOFTWARE				S-1-5-18	systemprofile	
SOFTWARE				S-1-5-19	LocalService	
SOFTWARE				S-1-5-20	NetworkService	

### 4. Who was the last user to log into the computer?

Sort the User Accounts by “Date Accessed” to get the answer.

**Answer:** sivapriya

The screenshot shows the 'Operating System User Account' listing in the Autopsy interface, similar to the previous one but sorted by Date Accessed. The table now has an additional column 'Date Accessed'. A red arrow points to this column. The data remains the same as in the previous screenshot, with sivapriya having the most recent access date.

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 18:46:16 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

# Disk Analysis & Autopsy

## 5. What was the IP address of the computer?

Answer: 192.168.130.216

With an image of a Windows machine, find the IP address associated with network adapters in the Windows Registry, which can also be accessed from the registry within Autopsy.

The screenshot shows the Windows Registry Editor with the path `/img_HASAN2.E01/vol_vol3/Windows/System32/config/SYSTEM`. The `Tcpip` key is expanded, showing subkeys like `Linkage`, `Parameters`, `Adapters`, and `Interfaces`. The `Adapters` key contains several entries, including `{df70681e-dcc3-4511-8a-23-958c3ab03d}` and `{e42cf5d6-2174-470f-9b1d-0d44858906}`. The `Interfaces` key contains entries like `{f73911d8-68d4-11eb-b57e-806e6f6e69}`. The `Parameters` key contains values such as `EnableDHCP` (REG\_DWORD), `Domain` (REG\_SZ), `NameServer` (REG\_SZ), `DhcpIPAddress` (REG\_SZ), `DhcpSubnetMask` (REG\_SZ), `DhcpServer` (REG\_SZ), `Lease` (REG\_DWORD), `LeaseObtainedTime` (REG\_DWORD), `T1` (REG\_DWORD), `T2` (REG\_DWORD), `LeaseTerminatesTime` (REG\_DWORD), `AddressType` (REG\_DWORD), `IsServerNapAware` (REG\_DWORD), `DhcpConnForceBroadcastFlag` (REG\_DWORD), `DhcpInterfaceOptions` (REG\_BIN), `DhcpIsMeteredDetected` (REG\_DWORD), `DhcpGatewayHardware` (REG\_BIN), and `DhcpGatewayHardwareCount` (REG\_DWORD).

The IP address is listed as 0.0.0.0. While looking through Autopsy, I see an unusual application installed on the device.

The screenshot shows the Autopsy Forensic Browser interface. The left sidebar shows the `Data Sources` section with `HASAN2.E01` selected, displaying various volumes and their file systems. The `Views` section includes `File Types`, `Deleted Files`, and `MB File Size`. The `Results` section is expanded, showing categories like `Extracted Content`, `Metadata`, and `Operating System Information`. The `Installed Programs` category is selected and expanded, showing a table of installed software. A red arrow points to the entry for `Look@LAN 2.50 Build 35`.

Source File	S	C	O	Program Name
SOFTWARE				Fontcore
SOFTWARE				IE40
SOFTWARE				IESBAKEX
SOFTWARE				IEData
SOFTWARE				MobileOptionPack
SOFTWARE				SchedulingAgent
SOFTWARE				WIC
SOFTWARE				Python Launcher v.3.9.7280.0
SOFTWARE				Look@LAN 2.50 Build 35
SOFTWARE				DXM_Runtime
SOFTWARE				MPlayer2
SOFTWARE				AddressBook
SOFTWARE				Connection Manager
SOFTWARE				DirectDrawEx
SOFTWARE				Fontcore
SOFTWARE				IE40
SOFTWARE				IE4Data
SOFTWARE				IESBAKEX

Searching for the executable name tells me it is a network monitoring tool, so check for any generated logs. Finding its directory under Program Files (x86). Among the files in the folder, an .ini file appears (.ini files are used to set configurations).

# Disk Analysis & Autopsy

The screenshot shows the Autopsy 4.18.0 interface with the following details:

- File System Tree:** Shows a tree view of the file system, including:
  - \$Extend (9)
  - \$Recycle.Bin (12)
  - \$Unalloc (45)
  - Documents and Settings (2)
  - Perflogs (2)
  - Program Files (21)
  - Program Files (x86) (17)
    - Common Files (5)
    - Internet Explorer (13)
      - Look@LAN (18)
        - Report (4)
          - images (18)
        - sounds (7)
    - Microsoft.NET (3)
    - Mozilla Maintenance Service (6)
    - Windows Defender (8)
    - Windows Mail (5)
    - Windows Media Player (18)
    - Windows Multimedia Platform (3)
    - Windows NT (4)
    - Windows Photo Viewer (8)
    - Windows Portable Devices (3)
    - Windows Sidebar (4)
    - WindowsPowerShell (4)
  - ProgramData (19)
  - Recovery (2)
  - System Volume Information (7)
  - Users (15)
  - Windows (104)
  - vol4 (Unallocated: 126759029-126760959)
  - vol5 (Unknown Type (0x27): 126760960-127795199)
  - vol6 (Unallocated: 127795200-127800447)
- Results Panel:** Displays extracted content, including:
  - Extracted Content
    - EXIF Metadata (21)
    - Encryption Suspected (7)
    - Extension Mismatch Detected (41)
    - Installed Programs (41)
    - Metadata (61)
    - Operating System Information (2)
- Variables Panel:** Shows environment variables:
  - %LANHOST% = DESKTOP-0R59DJ3
  - %LANDOMAIN% = DESKTOP-0R59DJ3
  - %LANUSER% = H4S4N
  - %LANIP% = 192.168.130.216 ← (highlighted with a red arrow)
  - %LANNIC% = 0800272cc4b9
  - %ISWIN95% = FALSE
  - %ISWIN98% = FALSE
  - %ISWINNT3% = FALSE

## 6. What was the IP address of the computer?

It wasn't present in the registry, and searching for the string "mac" within the .ini file returns no results. A second look at the fields surrounding the IP address, notice there is one for LANNIC.

**Answer:** 08-00-27-2c-c4-b9

The screenshot shows the Autopsy 4.18.0 interface with the following details:

- File System Tree:** Shows a tree view of the file system, including:
  - \$Extend (9)
  - \$Recycle.Bin (12)
  - \$Unalloc (45)
  - Documents and Settings (2)
  - Perflogs (2)
  - Program Files (21)
  - Program Files (x86) (17)
    - Common Files (5)
    - Internet Explorer (13)
      - Look@LAN (18)
        - Report (4)
          - images (18)
        - sounds (7)
    - Microsoft.NET (3)
    - Mozilla Maintenance Service (6)
    - Windows Defender (8)
    - Windows Mail (5)
    - Windows Media Player (18)
    - Windows Multimedia Platform (3)
    - Windows NT (4)
    - Windows Photo Viewer (8)
    - Windows Portable Devices (3)
    - Windows Sidebar (4)
    - WindowsPowerShell (4)
  - ProgramData (19)
  - Recovery (2)
  - System Volume Information (7)
  - Users (15)
  - Windows (104)
  - vol4 (Unallocated: 126759029-126760959)
  - vol5 (Unknown Type (0x27): 126760960-127795199)
  - vol6 (Unallocated: 127795200-127800447)
- Results Panel:** Displays extracted content, including:
  - Extracted Content
    - EXIF Metadata (21)
    - Encryption Suspected (7)
    - Extension Mismatch Detected (41)
    - Installed Programs (41)
    - Metadata (61)
    - Operating System Information (2)
- Variables Panel:** Shows environment variables:
  - %LANHOST% = DESKTOP-0R59DJ3
  - %LANDOMAIN% = DESKTOP-0R59DJ3
  - %LANUSER% = H4S4N
  - %LANIP% = 192.168.130.216 ← (highlighted with a red arrow)
  - %LANNIC% = 0800272cc4b9
  - %ISWIN95% = FALSE
  - %ISWIN98% = FALSE
  - %ISWINNT3% = FALSE

# Disk Analysis & Autopsy

## 7. What is the name of the network card on this computer?

Return to the registry to get the name of the NIC, and find the name of the NIC under the following path:

*SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\NetworkCards*

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

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

## 8. What is the name of the network monitoring tool?

**Answer:** Look@LAN

## 9. A user bookmarked a Google Maps location. What are the coordinates of the location?

Check Autopsy's Web Bookmarks results **Answer:** 12°52'23.0"N 80°13'25.0"E

Source File	S	C	O	URL	Title
places.sqlite	0			https://www.mozilla.org/en-US/contribute/	Get Involved
places.sqlite	0			https://www.mozilla.org/en-US/	About Us
places.sqlite	0			https://www.mozilla.org/en-US/firefox/central/	Getting Started
places.sqlite	0			https://support.mozilla.org/en-US/products/firefox	Help and Tutorials
places.sqlite	0			https://support.mozilla.org/en-US/b/customize-firefox-controls-buttons-and-toolbars/	Customize Firefox
places.sqlite	0			https://www.mozilla.org/en-US/contribute/	Get Involved
places.sqlite	0			https://www.mozilla.org/en-US/about/	About Us
places.sqlite	0			https://www.mozilla.org/en-US/firefox/central/	Getting Started
places.sqlite	0			https://www.sathyabama.ac.in/	Home   Sathyabama Institute of Science and Technology (Deemed to be University)
places.sqlite	0			https://support.mozilla.org/en-US/products/firefox	Help and Tutorials
places.sqlite	0			https://support.mozilla.org/en-US/b/customize-firefox-controls-buttons-and-toolbars/	Customize Firefox
places.sqlite	0			https://www.mozilla.org/en-US/contribute/	Get Involved
places.sqlite	0			https://www.mozilla.org/en-US/about/	About Us
places.sqlite	0			https://www.mozilla.org/en-US/firefox/central/	Getting Started
places.sqlite	0			https://www.google.com/maps/place/12%2252'23.0%22N+80%2613'25.0%26E+Google+Maps	12°52'23.0"N 80°13'25.0"E - Google Maps
Bing.url	0			http://go.microsoft.com/fwlink/?LinkId=255142	Bing.url
Bing.url	0			http://go.microsoft.com/fwlink/?LinkId=255142	Bing.url
Bing.url	0			http://go.microsoft.com/fwlink/?LinkId=255142	Bing.url
Bing.url	0			http://go.microsoft.com/fwlink/?LinkId=255142	Bing.url
Bing.url	0			http://go.microsoft.com/fwlink/?LinkId=255142	Bing.url

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

**Answer:** Anto Joshwa

# Disk Analysis & Autopsy

The screenshot shows the TryHackme Autopsy 4.18.0 interface. On the left, a file tree is displayed with various volumes and folders. The 'vol2 (NTFS / exFAT) (0x07): 2048-10444' volume contains several folders like 'OrphanFiles', 'Recycle.Bin', 'Unalloc', 'Documents and Settings', 'Perflogs', 'Program Files', 'Program Files (x86)', 'Program Data', 'Recovery', and 'System Volume Information'. The 'vol3 (NTFS / exFAT) (0x07): 104448-12' volume contains 'cyberpunk-2077-samurai-jacket-yo-1360x768.jp' and 'desktop.ini'. The main pane shows the contents of 'NTUSER.DAT' files from both volumes. A red arrow points from the 'Keyboard Layout' section of the registry editor to the 'Keyboard Layout' section of the file list.

11. 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 the search. Firstly, determine what the file is named and who the user is.

**Answer:** flag{HarleyQuinnForQueen}

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

I took note of a PowerShell script named exploit in the previous question.

**Answer:** flag{I-hacked-you}

TryHackme - Autopsy 4.18.0

Case View Tools Window Help

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

**Listing**  
Ang\_H454N2\_E01\vol\_vo3\Users\shreya\Desktop

Table Thumbnail Comments

Name	S	C	Modified Time	Change Time	Access Time
[current folder]			2021-02-06 05:51:42 EST	2021-02-06 05:51:42 EST	2021-02-07 11:48
[parent folder]			2021-02-06 05:44:47 EST	2021-02-06 05:44:47 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 13:01
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

All Users (2)  
Default (28)  
Default User (2)  
H454N (34)  
joshua (33)  
keshav (33)  
Public (11)  
sandhya (33)  
shreya (33)  
3D Objects (3)  
AppData (5)  
Application Data (2)  
Contacts (3)  
Cookies (2)  
Desktop (5)  
Downloads (5)  
Favorites (5)  
Links (5)  
Local Settings (2)

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page ⏪ ⏩ Matches on page: - of - Match ⏪ ⏩ 300% ⏪ ⏩ Reset

flag{i\_changed\_it}

# Disk Analysis & Autopsy

13. 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, and the zip file is located in H4S4N's \Downloads folder.

Answer: Lazagne,Mimikatz

The screenshot shows the Autopsy interface with the following details:

- File System Tree:** Shows the directory structure of the image file, including 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), Users (15), All Users (2), Default (28), Default User (2), and H4S4N (34).
- Table View:** The main pane displays a table of files in the /img\_HASAN2.E01/vol\_vo3/Users/H4S4N/Downloads directory. The table includes columns for Name, S, C, O, Modified Time, and Cl. Key entries include:
  - [current folder]
  - [parent folder]
  - 0or1.jpg
  - desktop.ini
  - lalsetup250.exe
  - mimikatz\_trunk.zip
  - mimikatz\_trunk.zip:Zone.Identifier
  - python-3.9.1-amd64.exe
  - wallpapersden-com-mr-robot-season-4-7500x3708.jpg
  - wallpapersden-com-mr-robot-season-4-7500x3708.jpg:Zone.Identifier
- Bottom Panel:** Includes tabs for Hex, Text, Application, File Metadata, Context, Results, Annotations, and Other Occurrences.

The other executable, however, is elusive. Checking the browser history, downloads, web searches, run programs, installed programs, recent documents, etc. leaves no clues. But there's a log source 'Windows Defender.' We'll have to determine where Defender records its alerts. Google finds a reference to

The screenshot shows the Autopsy interface with the following details:

- File System Tree:** Shows the directory structure of the image file, including Features (2), LocalCopy (3), Network Inspection System (3), Platform (3), Quarantine (5), Scans (23), BackupsStore (2), History (8), CacheManager (3), RemCheck (8), ReportLatency (3), Results (4), Service (6), DetectionHistory (20), and Store (11).
- Table View:** The main pane displays a table of files in the /img\_HASAN2.E01/vol\_vo3/ProgramData/Microsoft/Windows Defender/Scans/History/Service/DetectionHistory/02 directory. The table includes columns for Name, S, C, O, Modified Time, Change Time, and Access Time. A single entry is listed:
  - 8963AFD9-AF1E-453A-8B2D-766EFC57A8EA
- Bottom Panel:** Includes tabs for Hex, Text, Application, File Metadata, Context, Results, Annotations, and Other Occurrences. The Text tab shows the following log entry:

```
Magic.Version:1.2
HackTool:Win32/Lazagne
Magic.Version:1.2
file
C:\Users\H4S4N\Downloads\lazagne.exe
ThreatTrackingSha256
```

# Disk Analysis & Autopsy

C:\ProgramData\Microsoft\Windows Defender\Scans\History. Multiple alerts for mimikatz preceding an alert for lazagne.exe. Google informs us it is another password-dumping tool.

## 14. There is a YARA file on the computer. Inspect the file. What is the name of the author?

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

**Answer:** Benjamin DELPY (gentilkiwi)

The screenshot shows the Autopsy Forensic Browser interface. At the top, there's a 'File Search by Attributes' dialog box with various filters like 'Name: .yar', 'Modified', and 'Known Status: Unknown'. Below the dialog is a main window titled 'File Search Results 2' showing a table of search results. The table has columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags. Three entries are listed:

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-slack				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	2020-09-21 13:20:37 EDT	2834	Allocated

Below the table, the 'Hex' tab of the file viewer is open, displaying the YARA rule code:

```
/* 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)"
```

## 15. 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)

And we got a hit for a zipped Zerologon exploit. Though the file has been “deleted”, there’s evidence that it was located in sandhya’s download folder.

**Answer:** 2.2.0 20200918 Zerologon encrypted.zip

# Disk Analysis & Autopsy

## Conclusion

This involved a deep dive into the user activity, registry, and additional sources of evidence. I learned in other walkthroughs to keep Windows Defender's scan history in mind for future investigations and incident response.