Project - Digital Forensics Project

Student Name: Bina Rani Paul

Date:31.08.2025

Introduction

- ## Purpose of the Project:

  The main purpose of this project is to gain hands-on experience in the field of Digital Forensics by analyzing forensic disk images using Autopsy. This includes recovering deleted data, investigating user activity, and solving cyber forensic Capture the Flag (CTF) challenges

- **Overview of Digital Forensics and Autopsy:**

"Digital Forensics" is the process of identifying, preserving, analyzing, and presenting digital evidence that can be used in court or during an investigation. It plays a vital role in cybercrime investigations, incident response, and ethical hacking.

"Autopsy"is an open-source digital forensic platform used by law enforcement, military, and corporate examiners. It provides modules for file system analysis, keyword searching, timeline creation, data recovery, and artifact extraction such as browser history, emails, and deleted files.

1. Lab Setup

Tools Used

- Operating system:Kali linux/Window 10
- Forensic Tool:Autopsy(latest version)
- Other tools :Tryhackeme platform
- Target Evidence: Forensic disk images from TryHackMe challenges

2.Installation Steps for Autopsy on Kali Linux:

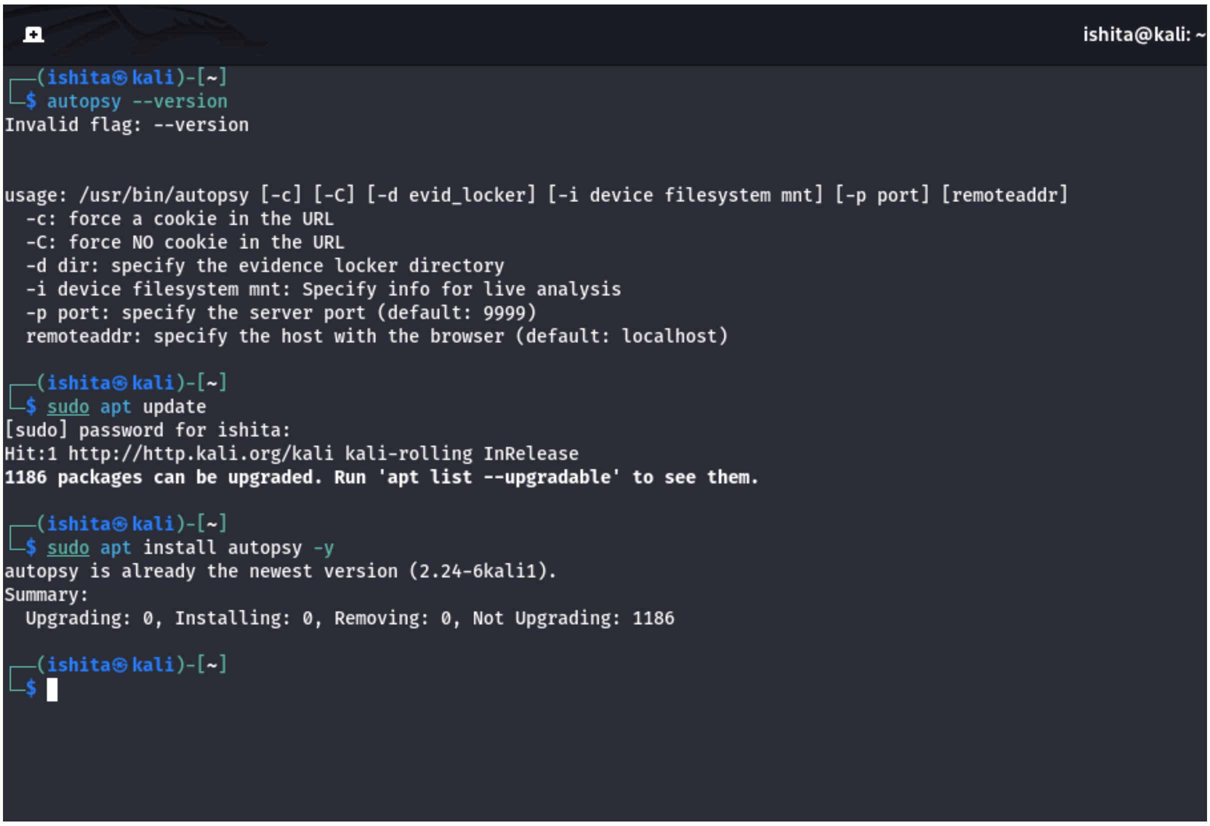
1. *Update the system:*

bash

sudo apt update && sudo apt upgrade -y

2. *Install Autopsy on Kali:* bash

sudo apt install autopsy -y



```
┌──(ishita㉿kali)-[~]
└─$ autopsy --version
Invalid flag: --version


usage: /usr/bin/autopsy [-c] [-C] [-d evid_locker] [-i device filesystem mnt] [-p port] [remoteaddr]
  -c: force a cookie in the URL
  -C: force NO cookie in the URL
  -d dir: specify the evidence locker directory
  -i device filesystem mnt: Specify info for live analysis
  -p port: specify the server port (default: 9999)
  remoteaddr: specify the host with the browser (default: localhost)

┌──(ishita㉿kali)-[~]
└─$ sudo apt update
[sudo] password for ishita:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1186 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(ishita㉿kali)-[~]
└─$ sudo apt install autopsy -y
autopsy is already the newest version (2.24-6kali1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1186

┌──(ishita㉿kali)-[~]
└─$ █
```

3. Run Autopsy (via browser interface): Bash autopsy

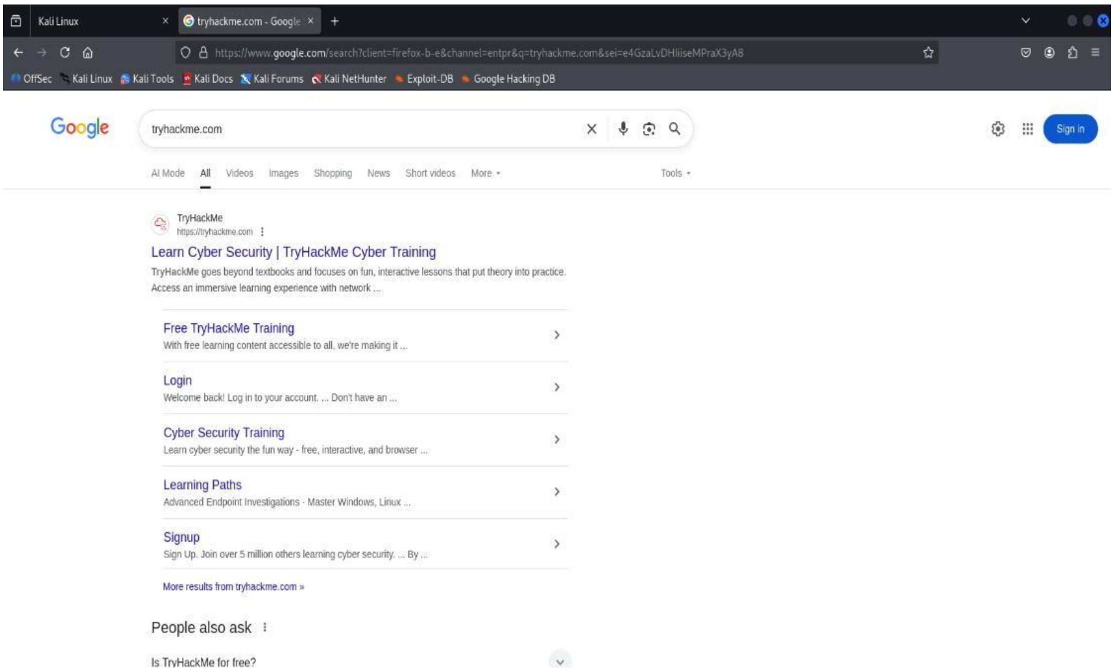
---***This starts the Autopsy server and provides a local web URL***

3.Case Analysis

- **Description of TryHackMe Challenge Used :**

For the case study, a forensic challenge from “TryHackMe”(e.g., "Investigating Windows" or "Autopsy" room) was used. The challenge provides a disk image file that simulates a compromised system for forensic analysis.

STEP 1: Search tryhackme.com/ on firefox broswer



TryHackMe
https://tryhackme.com

Learn Cyber Security | TryHackMe Cyber Training

TryHackMe goes beyond textbooks and focuses on fun, interactive lessons that put theory into practice. Access an immersive learning experience with network ...

Free TryHackMe Training
With free learning content accessible to all, we're making it ...

Login
Welcome back! Log in to your account. ... Don't have an ...

Cyber Security Training
Learn cyber security the fun way - free, interactive, and browser ...

Learning Paths
Advanced Endpoint Investigations · Master Windows, Linux ...

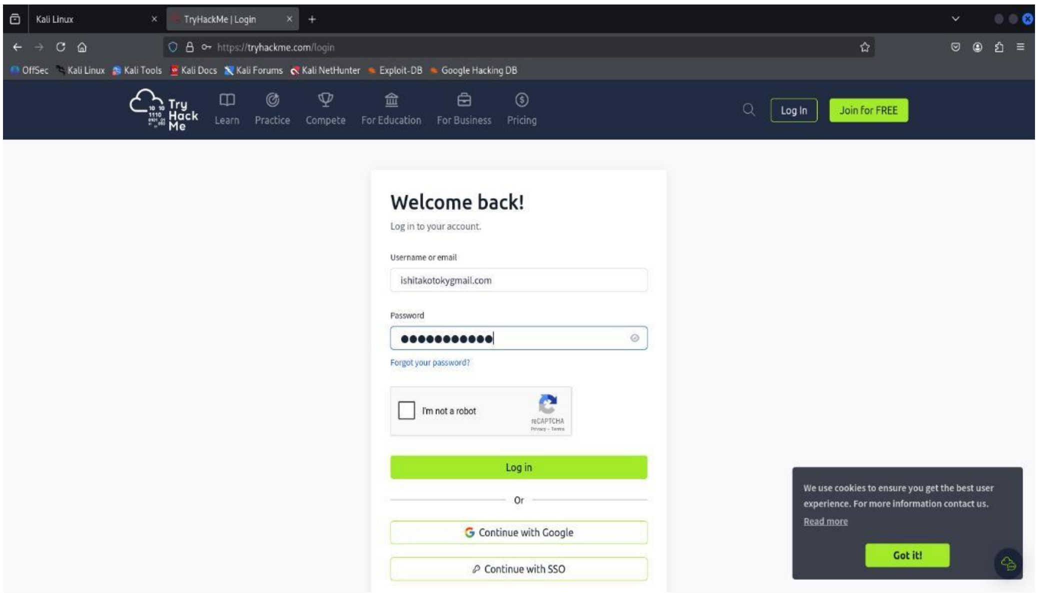
Signup
Sign Up. Join over 5 million others learning cyber security. ... By ...

More results from tryhackme.com »

People also ask

Is TryHackMe for free?

STEP 2 :Login configuration


Kali Linux
TryHackMe | Login
https://tryhackme.com/login
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Try Hack Me
Learn
Practice
Compete
For Education
For Business
Pricing
Log In
Join for FREE

Welcome back!

Log in to your account.

Username or email: ishitakotokygmail.com

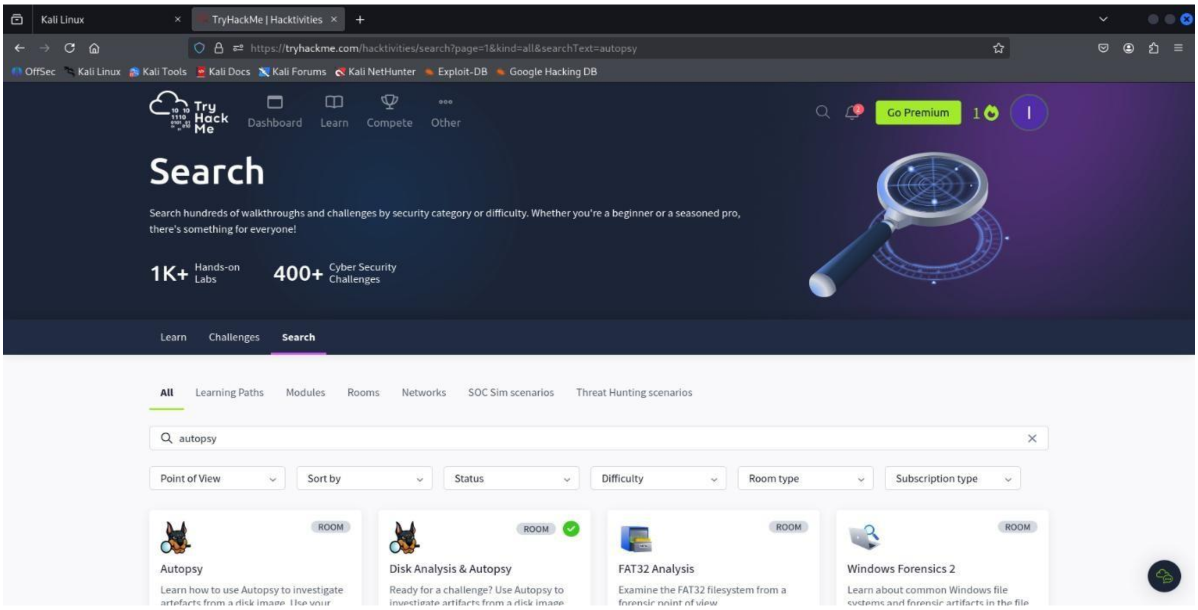
Password: ●●●●●●●●●●●

Forgot your password?

□ I'm not a robot

We use cookies to ensure you get the best user experience. For more information contact us.

STEP 3: Join the room and click Disk Analysis & Autopsy and start the machine


Kali Linux
TryHackMe | Hacktivities
https://tryhackme.com/hacktivities/search?page=1&kind=all&searchText=autopsy
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Try Hack Me
Dashboard
Learn
Compete
Other
Go Premium
1
I

Search

Search hundreds of walkthroughs and challenges by security category or difficulty. Whether you're a beginner or a seasoned pro, there's something for everyone!

1K+ Hands-on Labs   400+ Cyber Security Challenges

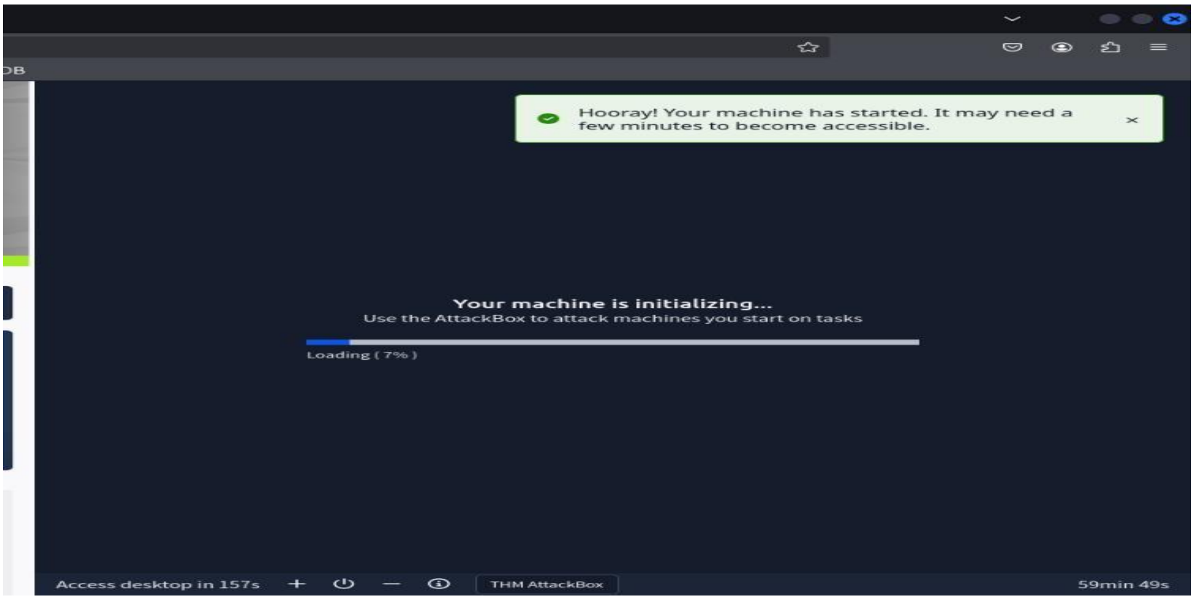
Search: autopsy

ROOM — Autopsy — Learn how to use Autopsy to investigate artefacts from a disk image. Use your

ROOM ✓ — Disk Analysis & Autopsy — Ready for a challenge? Use Autopsy to investigate artifacts from a disk image

ROOM — FAT32 Analysis — Examine the FAT32 filesystem from a forensic point of view

ROOM — Windows Forensics 2 — Learn about common Windows file systems and forensic artifacts in the file



Hooray! Your machine has started. It may need a few minutes to become accessible.

Your machine is initializing...

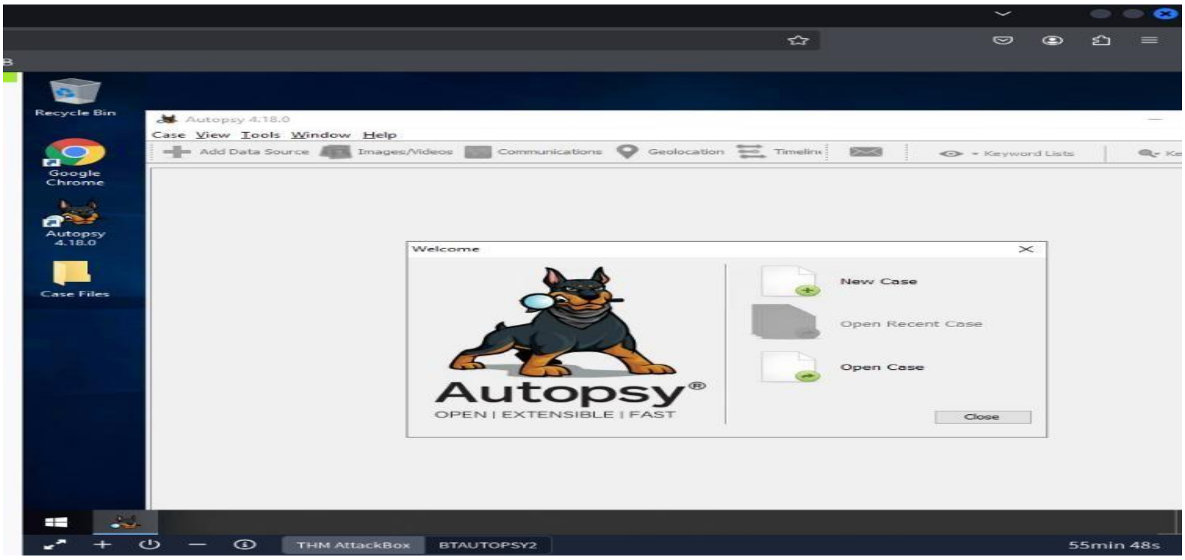
Use the AttackBox to attack machines you start on tasks

Loading (7%)

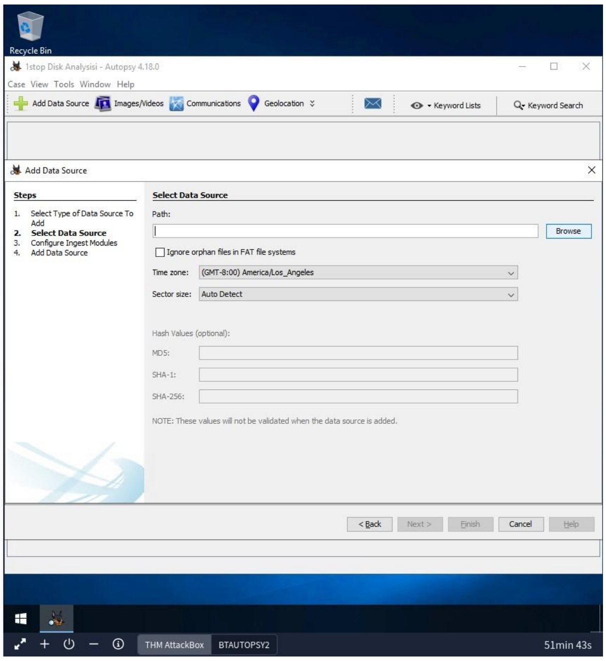
Access desktop in 157s

4.Steps followed:

1.Create a new case in Autopsy and create the Path



- **Creating the path**



1stop Disk Analysisi - Autopsy 4.18.0

Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path:

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-8:00) America/Los_Angeles

Sector size: Auto Detect

Hash Values (optional):

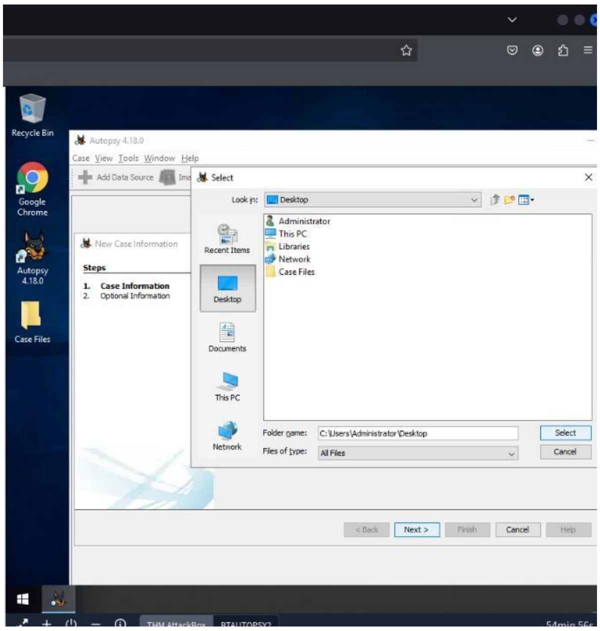
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

○ Enter Case Information



Autopsy 4.18.0

New Case Information

Steps

1. **Case Information**
2. Optional Information

Select

Look in: Desktop

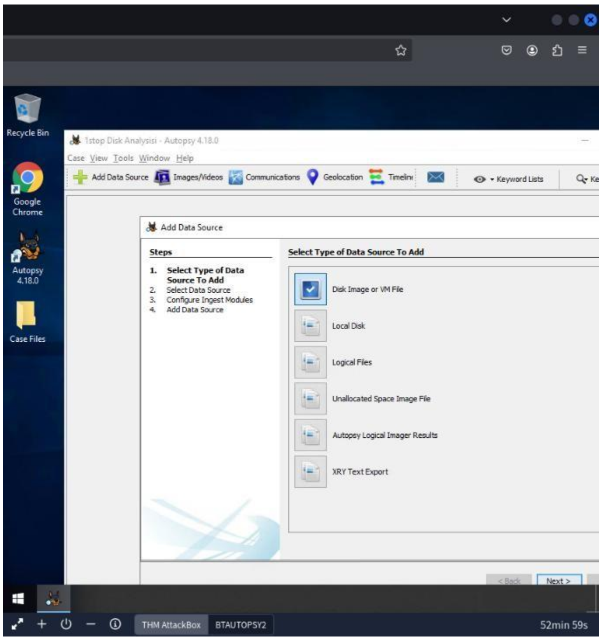
- Administrator
- This PC
- Libraries
- Network
- Case Files

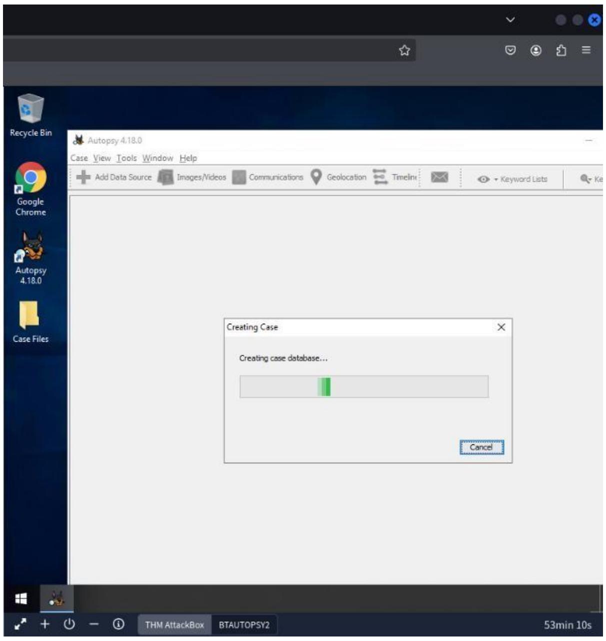
Folder name: C:\Users\Administrator\Desktop

Files of type: All Files

Case processing

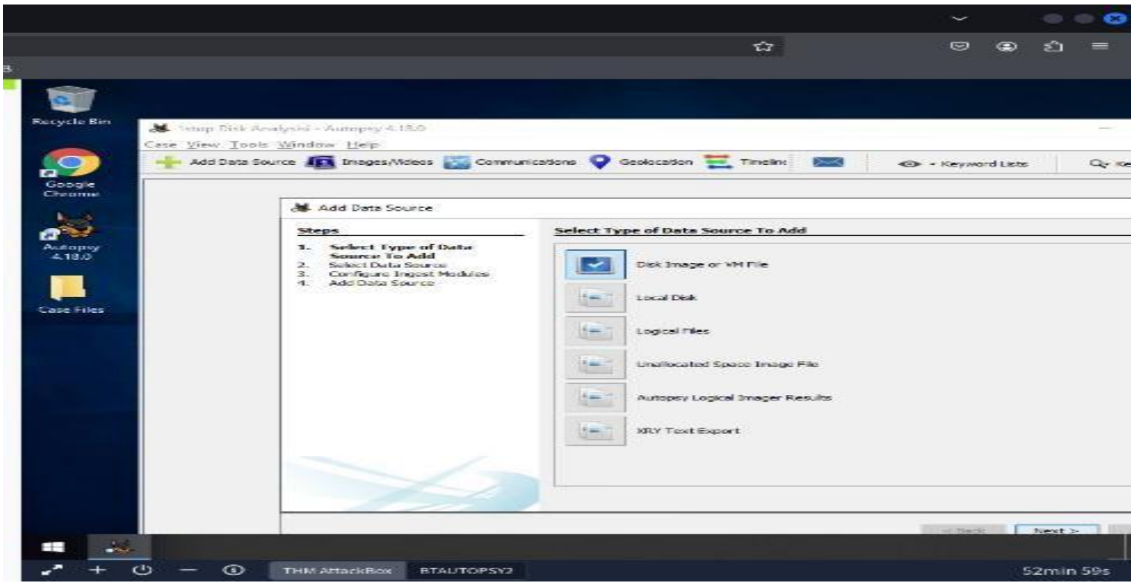
Add the data source





Creating case database...

2.After that add the forensic disk image from TryHackMe challenge.



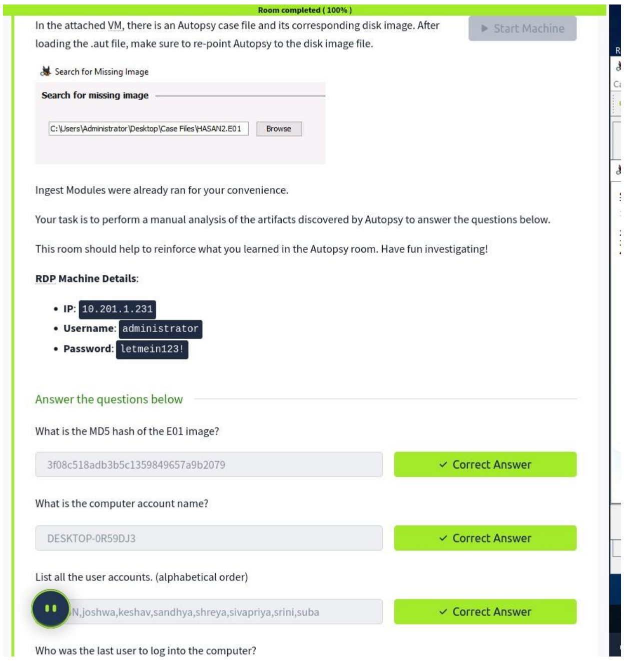
3. Run ingest modules (File Analysis, Keyword Search, Web Artifacts, Registry Analysis, etc.)

4. Browse recovered evidence under different categories.

5. Answer challenge questions based on finding

6.After starting the machine we have to answers the questions like this

- Using Autopsy, we examined the case image and found the answers to all the given questions through this process.



In the attached VM, there is an Autopsy case file and its corresponding disk image. After loading the .aut file, make sure to re-point Autopsy to the disk image file.

Search for Missing Image

Search for missing image

C:\Users\Administrator\Desktop\Case Files\HASAN2.E01 Browse

Ingest Modules were already ran for your convenience.

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!

RDP Machine Details:

- **IP**: `10.201.1.231`
- **Username**: `administrator`
- **Password**: `letmein123!`

Answer the questions below

What is the MD5 hash of the E01 image?

3f08c518adb3b5c1359849657a9b2079 ✓ Correct Answer

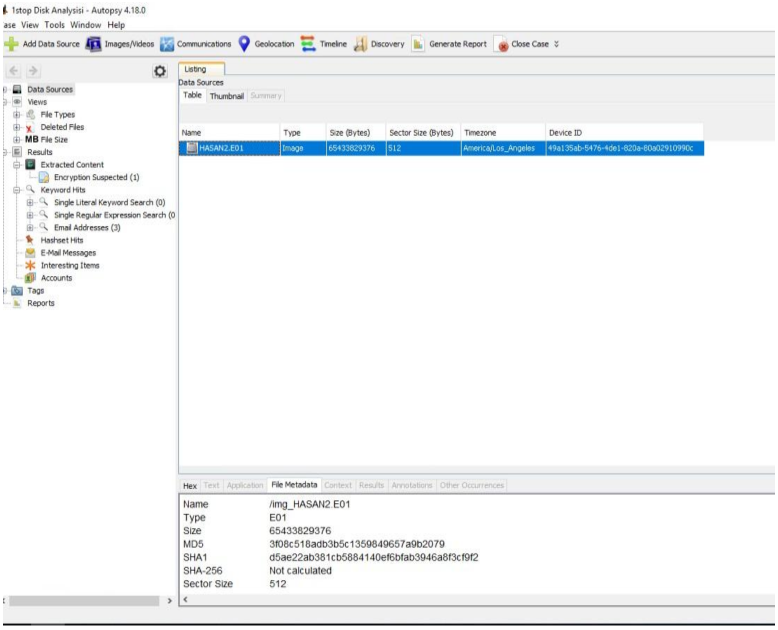
What is the computer account name?

DESKTOP-0R59DJ3 ✓ Correct Answer

List all the user accounts. (alphabetical order)

N,joshwa,keshav,sandhya,shreya,sivapriya,srini,suba ✓ Correct Answer

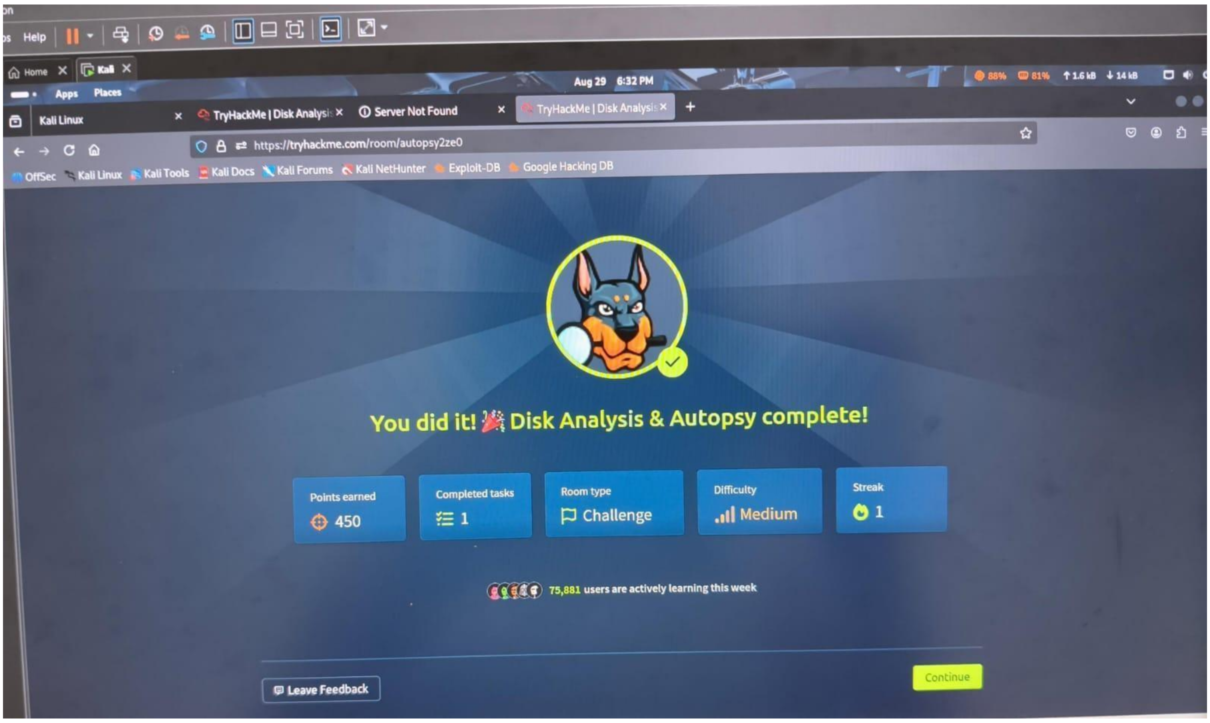
Who was the last user to log into the computer?



Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
HASAN2.E01	Image	65433829376	512	America/Los_Angeles	49a135ab-5476-4de1-820a-80a02910990c

Name	/img_HASAN2.E01
Type	E01
Size	65433829376
MD5	3f08c518adb3b5c1359849657a9b2079
SHA1	d5ae22ab381cb5884140ef6bfab3946a8f3cf9f2
SHA-256	Not calculated
Sector Size	512

- ***Anwers all the question then clicked submit: Disk Analysis & Autopsy completed***



You did it! 🎉 Disk Analysis & Autopsy complete!

Points earned 450

Completed tasks 1

Room type Challenge

Difficulty Medium

Streak 1

75,881 users are actively learning this week

Completed Disk Analysis & Autopsy

6.Recover data:

1. Browser History :Visited websites,downloads
2. Deleted Flies: Recovered using file carving.
3. **Registry Hives:** Extracted user information, installed applications, system configuration.
4. **Metadata:** File creation, modification, and deletion timestamps (MAC times).

7.Key Findings

- Recovered Files:Images, documents, and deleted data.
- User Activity: Logins, browsing history, file access records.
- Metadata: File timestamps, system logs.

- Techniques Used:Timeline analysis, keyword searching, deleted file recovery, browsing history extraction.

8. Conclusions

- Lessons Learned: Digital forensic analysis requires structured methodology, patience, and attention to detail. Autopsy simplifies the investigation process with its GUI.
- Tool Effectiveness: Autopsy proved effective in analyzing forensic images, automating data extraction, and categorizing evidence.
- Challenges Faced & Resolved:
    - Large image files slowed analysis → resolved by allocating more memory.
    - Difficulty in interpreting registry entries → cross-checked with documentation.

References

- Autopsy Official Site: https://www.autopsy.com
- The Sleuth Kit Documentation: https://sleuthkit.org/sleuthkit/
- TryHackMe Rooms:
    - Introduction to Digital Forensics ○ Investigating Windows ○ DFIR Room