Evidence A – A disk image of a desktop computer found in Student's dorm room.

Tools Used:

- Sleuth Kit: A collection of command-line tools for forensic analysis.
- Autopsy: A graphical interface (window). I used it to find out what programs have been installed and recover any content files in recycle bin. The usage will be in appendix.
- rip.pl: tool for forensic investigations, aiding in data recovery and analysis from disk images.

First, I combined all the disk images to one as evidencea.dd using “cat EvidenceA.001 to .011”. and then check the md5sum.

Then check the image stat and identify partitions

Calculate the offset 005.

Mount the partition, use “ro” mode to maintain the disk integrity and to prevent accidental changes make to the original disk.

Who is the owner of the computer?

I used rip.pl tool to grep “Username”, “Login Count” and “Last Login” to identify the owner of the computer. The screenshot illustrates in detail.

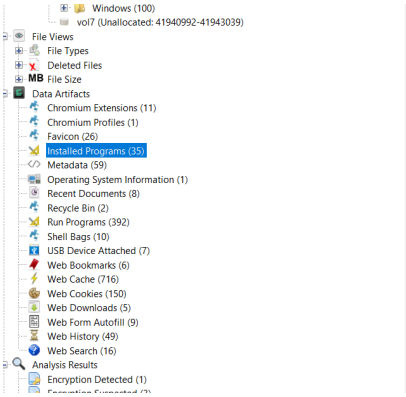
```
sansforensics@siftworkstation: /cases/evidenceA
$ rip.pl -r /mnt/windows_mount/Windows/System32/config/SAM -p samparse | grep Username
Launching samparse v.20220921
Username        : Administrator [500]
Username        : Guest [501]
Username        : DefaultAccount [503]
Username        : WDAGUtilityAccount [504]
Username        : Alex Marshall [1000]
sansforensics@siftworkstation: /cases/evidenceA
$ rip.pl -r /mnt/windows_mount/Windows/System32/config/SAM -p samparse | grep "Login Count"
Launching samparse v.20220921
Login Count     : 0
Login Count     : 0
Login Count     : 0
Login Count     : 0
Login Count     : 2
sansforensics@siftworkstation: /cases/evidenceA
$ rip.pl -r /mnt/windows_mount/Windows/System32/config/SAM -p samparse | grep "Last Login"
Launching samparse v.20220921
Last Login Date : Never
Last Login Date : Never
Last Login Date : Never
Last Login Date : Never
Last Login Date : Tue Aug 27 13:05:43 2024 Z
sansforensics@siftworkstation: /cases/evidenceA
$
```

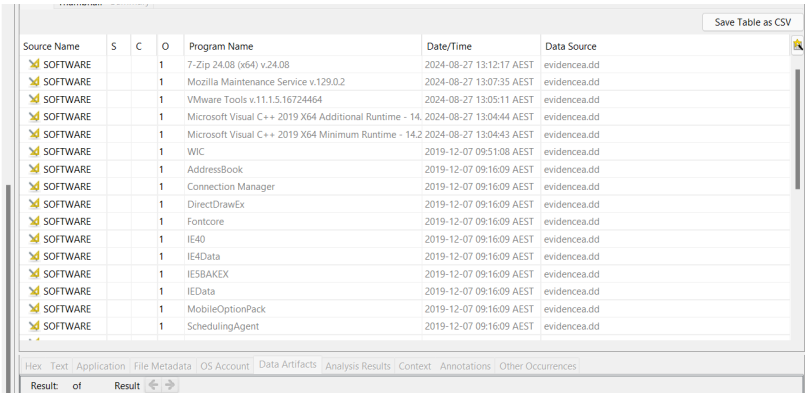
Alex Marshall is the owner of the computer.

What programs have been installed on the computer? What recent programs have been run?

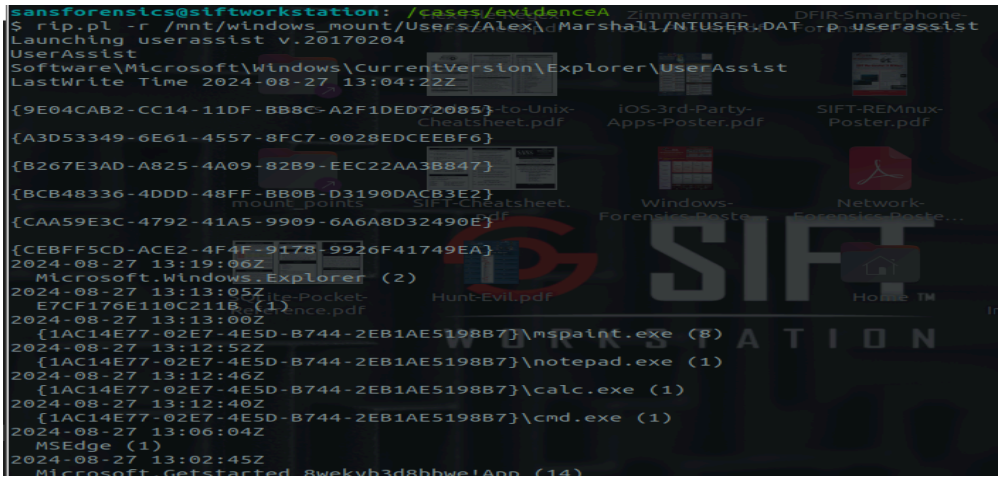
The following screenshots demonstrate how I get the result using autopsy and rip.pl.

Installed Programs on the Computer:





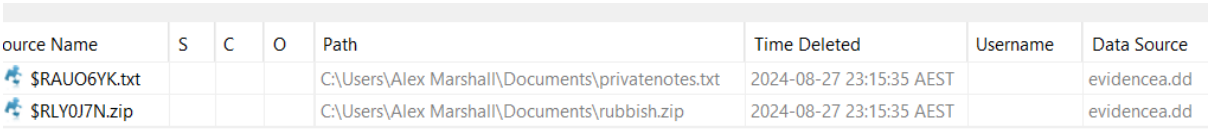
Recent Programs:



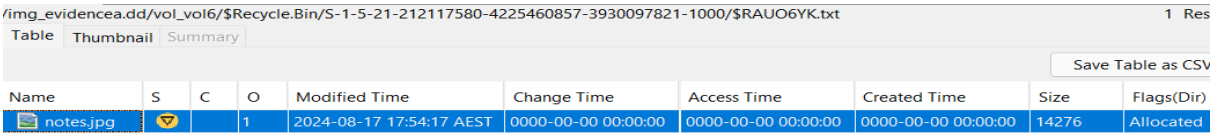
Recover the content of any files in the recycle bin

I use autopsy (GUI) on window to check the content of any files in the recycle bin.

$RAUO6YK.txt (notes.jpg (Iextracted the file to my computer and open with Microsoft word to see the content) and $RLY0J7N.zip (rubbish.zip) (its password protected pdf file and the password is football). I used fccrack and rockyou to crack the zip file.



ource Name	S	C	O	Path	Time Deleted	Username	Data Source
$RAUO6YK.txt				C:\Users\Alex Marshall\Documents\privatenotes.txt	2024-08-27 23:15:35 AEST		evidencea.dd
$RLY0J7N.zip				C:\Users\Alex Marshall\Documents\rubbish.zip	2024-08-27 23:15:35 AEST		evidencea.dd

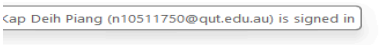


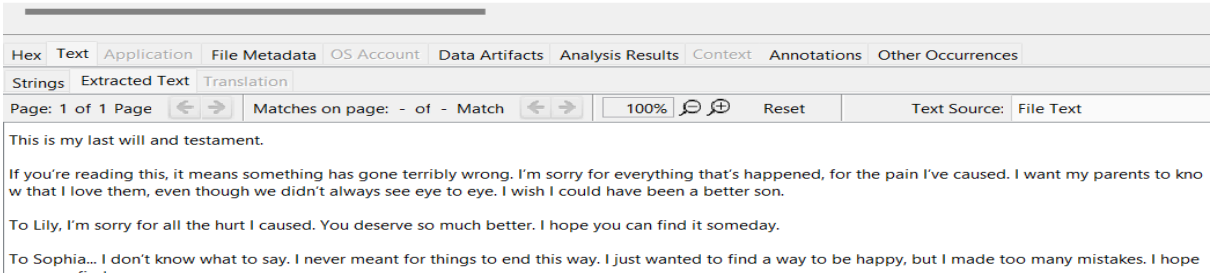
/img_evidencea.dd/vol_vol6/$Recycle.Bin/S-1-5-21-212117580-4225460857-3930097821-1000/$RAUO6YK.txt 1 Res

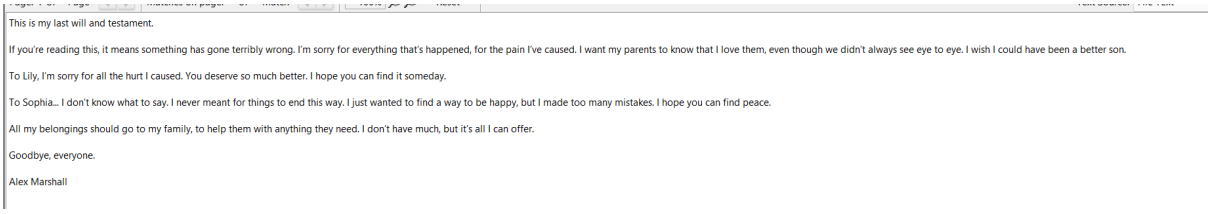
Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
notes.jpg			1	2024-08-17 17:54:17 AEST	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14276	Allocated







This is my last will and testament.

If you're reading this, it means something has gone terribly wrong. I'm sorry for everything that's happened, for the pain I've caused. I want my parents to know that I love them, even though we didn't always see eye to eye. I wish I could have been a better son.

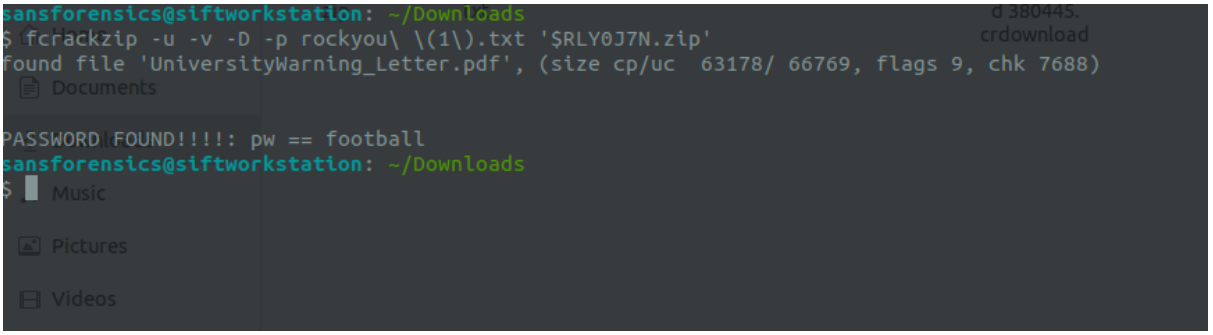
To Lily, I'm sorry for all the hurt I caused. You deserve so much better. I hope you can find it someday.

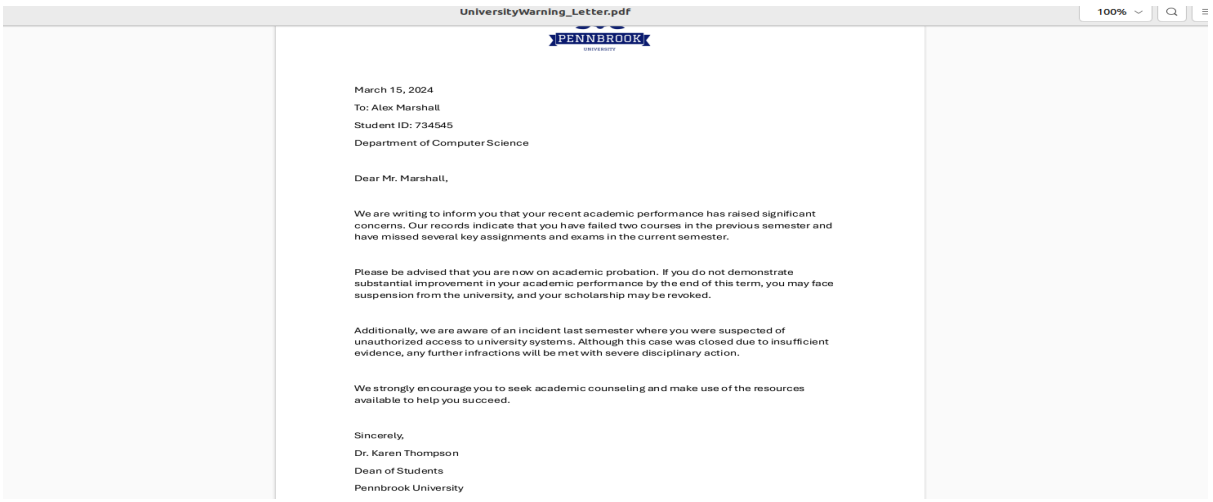
To Sophia... I don't know what to say. I never meant for things to end this way. I just wanted to find a way to be happy, but I made too many mistakes. I hope you can find peace.

All my belongings should go to my family, to help them with anything they need. I don't have much, but it's all I can offer.

Goodbye, everyone.

Alex Marshall





Is there evidence that gives an indication of the state of mind of the owner of the computer?

The computer owner's troubled mental state is evident from his email exchanges with his parents. His father puts pressure on him, while his mother is supportive. He is facing financial problems and has started selling exam answers to make money, which has increased his anxiety. He deleted a warning letter from the university about his poor grades and unauthorised access, as well as private notes that include his last will and testament, showing how distressed he is.

His journal entries show:

- February 28, 2024: He is struggling with money, trying to pay for rent and utilities while selling exam answers. He feels guilty and worries about getting caught.
- April 5, 2024: He feels overwhelmed by debt and pressure from his father to improve his life. He can’t talk to anyone about his financial issues. He thinks about dropping out of school but is afraid of letting others down.

All relevant screenshots will be included in the appendix.

Appendix

Evidence A

From: Oliver Marshall <oliver.marshall@email.com>

To: Alex Marshall <alex.marshall@university.edu>

Date: March 10, 2024

Subject: Your Future

Alex,

I've just received your latest report card, and I'm deeply disappointed. This is not the level of performance I expect from my son. You have all the potential in the world, but you're throwing it away by not applying yourself.

I've warned you before that you're running out of chances. If you don't get your act together, I will have no choice but to cut off your financial support. You need to understand that the Marshall family has a reputation to uphold, and you're not living up to it.

You need to focus on your studies and start making decisions that reflect the kind of man you want to become. I didn't work my entire life for you to squander these opportunities.

Consider this your final warning.

Dad

Debt_tracker.csv

A1 Creditor

	A	B	C	D	E
1	Creditor	Amount	Owed	Due Date	Notes
2	Credit Card 1	1200	15/04/2024	Maxed out	
3	Credit Card 2	800	20/04/2024	Maxed out	
4	Lily Parker	300	10/04/2024	Personal loan, urgent	
5	Private Loan	5000	30/04/2024	From unknown source, urgent	
6	Friends	150	25/04/2024	Various small loans	
7	Total	7450			
8					
9					
10					

UNIVERSITY

April 1, 2024

To: Alex Marshall

Student ID: 734545

Department of Computer Science

Dear Alex,

I am pleased to offer you an internship position with TechVision, a leading company in the field of artificial intelligence and cybersecurity. This opportunity is extended to you based on your demonstrated skills and potential in computer science.

The internship is a highly competitive program that could be a pivotal step in your career. However, I must stress the importance of staying focused and avoiding any distractions that may impede your progress.

This internship will require full commitment and excellence in both your academic and professional pursuits. I trust you will take this opportunity seriously and make the most of it.

Please confirm your acceptance of this offer by April 10, 2024.

Journal1

February 28, 2024

Money's been tighter than I expected this semester. Between rent, utilities, and trying to keep up appearances, I'm running out of cash faster than I thought. I've been looking for a job, but with the course load and everything else, I just don't have the time.

I started selling exam answers a few weeks ago—just a couple of assignments here and there. I know it's wrong, but I need the money. Every time I think about stopping, I remember how empty my bank account is. It's a risk, but what choice do I have?

The guilt is starting to get to me, though. I'm always looking over my shoulder, waiting for someone to figure it out. What if I get caught? What if I lose everything? But I can't back out now. I'm in too deep.

Journal2

April 5, 2024

I'm drowning in debt. The credit cards are maxed out, and I still owe Lily for that loan she gave me last month. I hate asking for help, especially from her, but I didn't have a choice. I don't know how I'm going to pay her back.

Dad's been on my case again, telling me I need to get my life together. Easy for him to say—he's not the one trying to balance classes, relationships, and this mess of a life. He doesn't understand the pressure I'm under, and I can't tell him about the money problems. He'd lose it.

I've thought about dropping out, but where would I go? What would I do? I can't let everyone down, but I don't know how much longer I can keep this up.

April 5, 2024

Dear Alex,

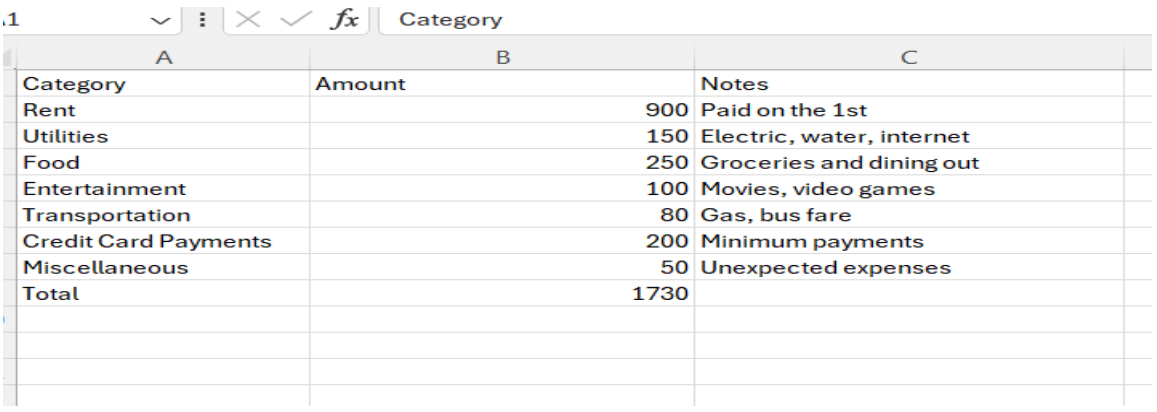
I hope you're doing well. I've been thinking about you a lot lately and wanted to write you a quick note to check in.

I know things have been tough with school, and your father can be hard on you. He just wants what's best for you, but I understand it can be overwhelming. I want you to know that I'm here for you, no matter what.

If you ever feel like you need someone to talk to, please don't hesitate to reach out. I'm worried about you, and I hope you're taking care of yourself. Life can be challenging, but you're strong, and I know you'll find your way.

Remember that we love you very much, and we're always here for you.

Love,
Mum



	A	B	C
1	Category	Amount	Notes
2	Rent	900	Paid on the 1st
3	Utilities	150	Electric, water, internet
4	Food	250	Groceries and dining out
5	Entertainment	100	Movies, video games
6	Transportation	80	Gas, bus fare
7	Credit Card Payments	200	Minimum payments
8	Miscellaneous	50	Unexpected expenses
9	Total	1730	

Autopsy

Step 1: Download and Install Autopsy

- Go to the Autopsy website and download the Windows installer.
- Run the installer and follow the prompts to install Autopsy on your computer.

Step 2: Launch Autopsy

- After installation, open Autopsy from the Start Menu or desktop shortcut.
- The main screen will give options to open or create a new case.

Step 3: Create a New Case

- Click "Create New Case" on the home screen.
- Enter a case name, number (optional), and the case directory where all case files will be stored.
- Fill in the examiner details and click "Next".

Step 4: Add Data Source

- Choose the type of data source to analyse (e.g., disk image, local disk).
- Browse to the location of the data source (e.g., a .dd or. E01 file) and select it.
- Click "Next" and follow the prompts.

Step 5: Analyse the Data

- Once the data is added, Autopsy will process it and display the results in various tabs, such as:
- File Types: Shows the types of files found.
- Timeline: Displays a timeline of file activity.
- Web Artifacts: Lists browser history, cookies, and cached files.
- Keyword Search: Allows you to search for specific terms within the data.

Use these tabs to navigate and analyse the evidence.

Merging Images on Window

Cmd : “ copy /b EvidenceA.001 + …… + EvidenceA.011 evidencea.dd”