Timeline Analysis of the Pieces of Evidence

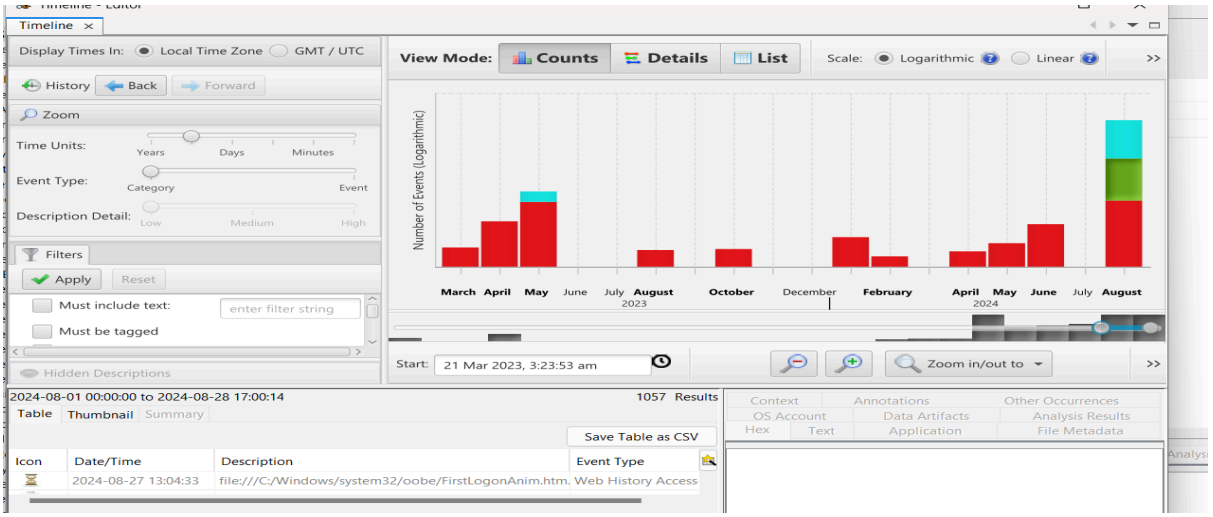
Tools Used: Autopsy, Wireshark, vol.py and memdump

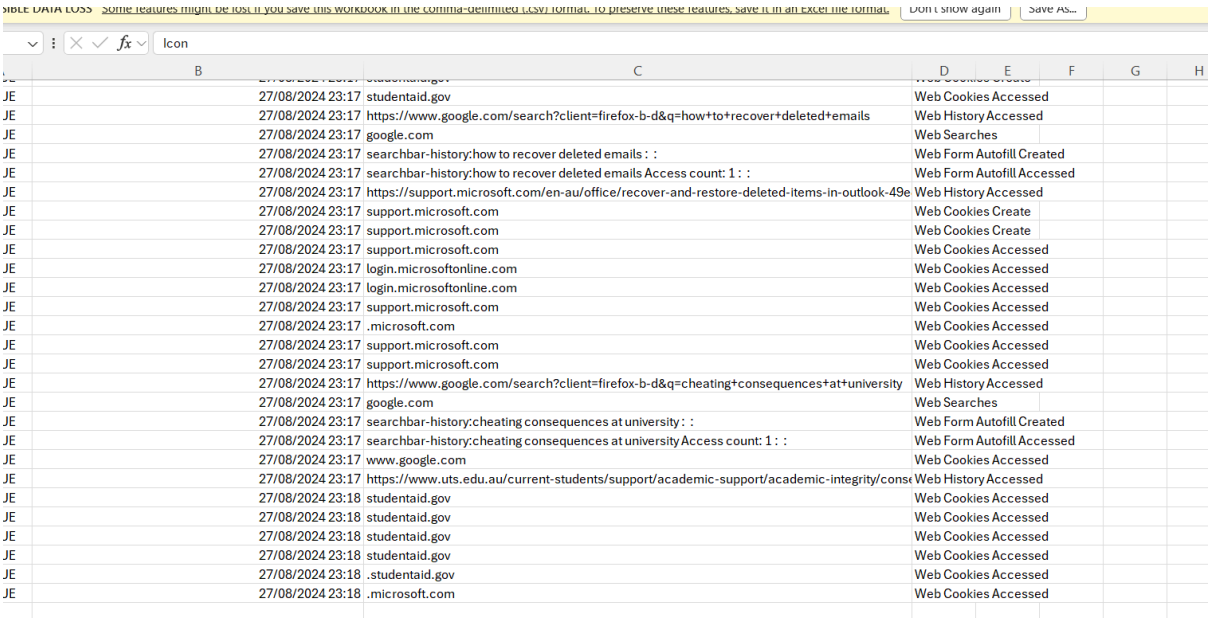
A timeline analysis was conducted to correlate events and actions associated with the evidence collected from Alex's computer, the dormitory network, the memory dump of the personal laptop, and the mobile phone. Below is a structured timeline that captures key events and interactions:

Evidence A

To understand Alex's state of mind, I focused on the private note he wrote and subsequently deleted. I extracted the creation and deletion timestamps, which are crucial for providing context regarding his mental state during that period.

Generating Timeline using Autopsy (Web searches)





Icon

	B	C	D
JE	27/08/2024 23:17	studentaid.gov	Web Cookies Accessed
JE	27/08/2024 23:17	https://www.google.com/search?client=firefox-b-d&q=how+to+recover+deleted+emails	Web History Accessed
JE	27/08/2024 23:17	google.com	Web Searches
JE	27/08/2024 23:17	searchbar-history:how to recover deleted emails : :	Web Form Autofill Created
JE	27/08/2024 23:17	searchbar-history:how to recover deleted emails Access count: 1 : :	Web Form Autofill Accessed
JE	27/08/2024 23:17	https://support.microsoft.com/en-au/office/recover-and-restore-deleted-items-in-outlook-49e	Web History Accessed
JE	27/08/2024 23:17	support.microsoft.com	Web Cookies Create
JE	27/08/2024 23:17	support.microsoft.com	Web Cookies Create
JE	27/08/2024 23:17	support.microsoft.com	Web Cookies Accessed
JE	27/08/2024 23:17	login.microsoftonline.com	Web Cookies Accessed
JE	27/08/2024 23:17	login.microsoftonline.com	Web Cookies Accessed
JE	27/08/2024 23:17	support.microsoft.com	Web Cookies Accessed
JE	27/08/2024 23:17	.microsoft.com	Web Cookies Accessed
JE	27/08/2024 23:17	support.microsoft.com	Web Cookies Accessed
JE	27/08/2024 23:17	support.microsoft.com	Web Cookies Accessed
JE	27/08/2024 23:17	https://www.google.com/search?client=firefox-b-d&q=cheating+consequences+at+university	Web History Accessed
JE	27/08/2024 23:17	google.com	Web Searches
JE	27/08/2024 23:17	searchbar-history:cheating consequences at university : :	Web Form Autofill Created
JE	27/08/2024 23:17	searchbar-history:cheating consequences at university Access count: 1 : :	Web Form Autofill Accessed
JE	27/08/2024 23:17	www.google.com	Web Cookies Accessed
JE	27/08/2024 23:17	https://www.uts.edu.au/current-students/support/academic-support/academic-integrity/conse	Web History Accessed
JE	27/08/2024 23:18	studentaid.gov	Web Cookies Accessed
JE	27/08/2024 23:18	studentaid.gov	Web Cookies Accessed
JE	27/08/2024 23:18	studentaid.gov	Web Cookies Accessed
JE	27/08/2024 23:18	studentaid.gov	Web Cookies Accessed
JE	27/08/2024 23:18	.studentaid.gov	Web Cookies Accessed
JE	27/08/2024 23:18	.microsoft.com	Web Cookies Accessed

Save Table as CSV

Domain	Text	Program Name	Date Accessed	Data Source
bing.com	firefox download	Microsoft Edge	2024-08-27 23:07:02 AEST	evidencea.dd
bing.com	firefox download	Microsoft Edge	2024-08-27 23:07:02 AEST	evidencea.dd
bing.com	firefox download	Microsoft Edge	2024-08-27 23:07:02 AEST	evidencea.dd
bing.com	firefox download	Microsoft Edge	2024-08-27 23:07:02 AEST	evidencea.dd
bing.com	firefox download	Microsoft Edge	2024-08-27 23:07:02 AEST	evidencea.dd
bing.com	firefox download	Microsoft Edge	2024-08-27 23:07:02 AEST	evidencea.dd
google.com	winzip download free	FireFox Analyzer	2024-08-27 23:08:32 AEST	evidencea.dd
google.com	vlc download	FireFox Analyzer	2024-08-27 23:09:15 AEST	evidencea.dd
google.com	winzip install failed	FireFox Analyzer	2024-08-27 23:09:57 AEST	evidencea.dd
google.com	winzip alternative	FireFox Analyzer	2024-08-27 23:10:10 AEST	evidencea.dd
google.com	zzip	FireFox Analyzer	2024-08-27 23:11:51 AEST	evidencea.dd
google.com	how to encrypt files on Windows	FireFox Analyzer	2024-08-27 23:17:01 AEST	evidencea.dd
google.com	symptoms of severe anxiety and stress	FireFox Analyzer	2024-08-27 23:17:16 AEST	evidencea.dd
google.com	student loan forgiveness programs 2024	FireFox Analyzer	2024-08-27 23:17:30 AEST	evidencea.dd
google.com	how to recover deleted emails	FireFox Analyzer	2024-08-27 23:17:43 AEST	evidencea.dd
google.com	cheating consequences at university	FireFox Analyzer	2024-08-27 23:17:54 AEST	evidencea.dd

/img_evidencea.dd/vol_vol6/Users/Alex Marshall/Documents 15 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Dad_Email_March.pdf			1	2024-08-18 13:48:38 AEST	2024-08-27 23:15:12 AEST	2024-08-27 23:15:14 AEST	2024-08-27 23:15:12
Debt_Tracker.csv			1	2024-08-17 12:39:30 AEST	2024-08-27 23:15:12 AEST	2024-08-27 23:15:14 AEST	2024-08-27 23:15:12
Expenses_March.csv			1	2024-08-17 12:38:52 AEST	2024-08-27 23:15:12 AEST	2024-08-27 23:15:14 AEST	2024-08-27 23:15:12
InternshipOffer_Reynolds.pdf			1	2024-08-18 14:48:56 AEST	2024-08-27 23:15:12 AEST	2024-08-27 23:15:13 AEST	2024-08-27 23:15:12
Mum_Email_April.jpg			1	2024-08-17 21:54:02 AEST	2024-08-27 23:15:12 AEST	2024-08-27 23:15:13 AEST	2024-08-27 23:15:12
My Music				2024-08-27 23:04:17 AEST	2024-08-27 23:04:17 AEST	2024-08-27 23:04:17 AEST	2024-08-27 23:04:17
My Pictures				2024-08-27 23:04:17 AEST	2024-08-27 23:04:17 AEST	2024-08-27 23:04:17 AEST	2024-08-27 23:04:17
My Videos				2024-08-27 23:04:17 AEST	2024-08-27 23:04:17 AEST	2024-08-27 23:04:17 AEST	2024-08-27 23:04:17
[current folder]				2024-08-27 23:15:35 AEST	2024-08-27 23:15:35 AEST	2024-08-27 23:19:12 AEST	2024-08-27 23:04:17
[parent folder]				2024-08-27 23:06:57 AEST	2024-08-27 23:06:57 AEST	2024-08-27 23:19:41 AEST	2024-08-27 23:04:17
desktop.ini			1	2024-08-27 23:04:25 AEST	2024-08-27 23:04:25 AEST	2024-08-27 23:19:17 AEST	2024-08-27 23:04:25
journal1.txt			1	2024-08-17 12:31:32 AEST	2024-08-27 23:15:12 AEST	2024-08-27 23:15:13 AEST	2024-08-27 23:15:12
journal2.txt			1	2024-08-17 12:36:22 AEST	2024-08-27 23:15:12 AEST	2024-08-27 23:15:13 AEST	2024-08-27 23:15:12
privatenotes.txt				2024-08-27 23:15:35 AEST	2024-08-27 23:15:35 AEST	2024-08-27 23:15:13 AEST	2024-08-27 23:15:12
rubbish.zip				2024-08-27 23:15:35 AEST	2024-08-27 23:15:35 AEST	2024-08-27 23:15:12 AEST	2024-08-27 23:15:12

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

Next, consider the timeline of other significant events in Alex's life:

Parents' Emails:

- Date: April 5, 2024
- Context: Evaluating the timestamps of emails from Alex's parents helps us assess their concern and support during this time.

University Warning Letter:

- Date: March 15, 2024
- Context: Identifying the date of this warning letter provides insight into the academic pressure Alex was facing.

Internship Offer:

- Date: April 1, 2024
- Context: Noting the date of this offer sheds light on his career prospects and potential stress levels.

Journal Entries:

- Entry Dates:

- February 28 (first entry)
- April 5 (second entry)
- Context: These entries provide insights into Alex's thoughts and feelings during this critical period.

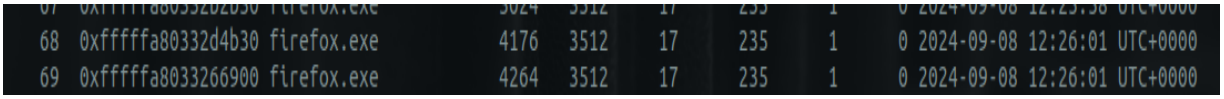
All relevant screenshots are included in the appendix.

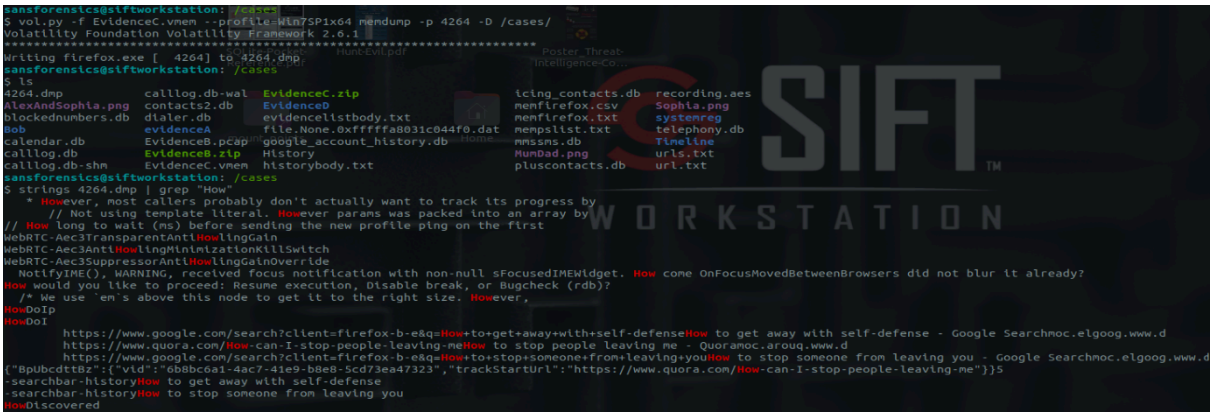
Evidence B

The PCAP file analysed in Wireshark has already been referenced in the questions related to Evidence B questions. The timestamps are given in local time (AES), while the actual message timestamps in the TCP stream are recorded in UTC. To maintain consistency with the other event times, I have chosen to use AES time for this analysis. Screenshots can be found in the previous Evidence B questions.

Evidence C

I used memdump to analyse the memory related to a specific process identified by its PID. The execution start time for this process can be obtained from the pslist, which offers important context for the analysis. The following screenshot displays web searches conducted at 12:26:01.





Evidence D

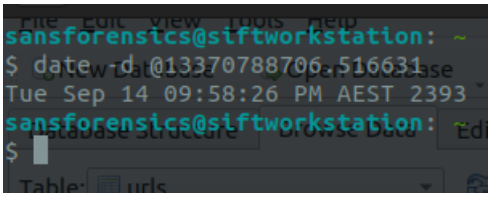
I am particularly interested in the dates and times of Alex's messages, web searches, and call logs.

Web Search: Using the command “date -d @13370788706.516631”, I determined that Alex searched for the nearest campus security office at 9:58:26 PM, just before Sophia arrived at his dorm.

Last Message from Sophia: The final message from Sophia was timestamped on September 14, 10:59:00 PM.

B	C	D	E	F	G	H
lessage T	Date/Time	Read	Direction	From Phor	To Phone N	Text
ndroid Me	2024-09-14 22:51:36 AEST	1	Incoming	6.14E+10	3ead5183-	Hey, can we talk tonight? We really need to sort this out.
ndroid Me	2024-09-14 22:51:55 AEST	1	Outgoing	3ead5183-	6.14E+10	Not tonight, Lily. Iâ€™m dealing with a lot right now.
ndroid Me	2024-09-14 22:52:08 AEST	1	Incoming	6.14E+10	3ead5183-	Alex, this is important. I canâ€™t keep going on like this, wonder
ndroid Me	2024-09-14 22:52:25 AEST	1	Outgoing	3ead5183-	6.14E+10	I know, I know. But I just canâ€™t tonight. Tomorrow?
ndroid Me	2024-09-14 22:52:38 AEST	1	Incoming	6.14E+10	3ead5183-	Tomorrow might be too late, Alex. If you donâ€™t end this with h
ndroid Me	2024-09-14 22:52:50 AEST	1	Outgoing	3ead5183-	6.14E+10	Lily, please donâ€™t do anything rash. Iâ€™ll figure it out, I prom
ndroid Me	2024-09-14 22:53:03 AEST	1	Incoming	6.14E+10	3ead5183-	You better. Iâ€™m done waiting.
ndroid Me	2024-09-14 22:53:34 AEST	1	Incoming	6.14E+10	3ead5183-	Alex, Iâ€™m outside your dorm. Can we talk?
ndroid Me	2024-09-14 22:53:56 AEST	1	Outgoing	3ead5183-	6.14E+10	Sophia, nowâ€™s not a good time. Iâ€™m swamped.
ndroid Me	2024-09-14 22:54:08 AEST	1	Incoming	6.14E+10	3ead5183-	Itâ€™ll only take a minute. Please, I really need to see you.
ndroid Me	2024-09-14 22:54:22 AEST	1	Outgoing	3ead5183-	6.14E+10	Fine, come up. But I donâ€™t have long.
ndroid Me	2024-09-14 22:54:36 AEST	1	Incoming	6.14E+10	3ead5183-	Thank you. I justâ€¦ I need to know where we stand. I canâ€™t k
ndroid Me	2024-09-14 22:54:55 AEST	1	Outgoing	3ead5183-	6.14E+10	Weâ€™ll talk when you get here.
ndroid Me	2024-09-14 22:55:07 AEST	1	Incoming	6.14E+10	3ead5183-	Okay, Iâ€™m on my way.
ndroid Me	2024-09-14 22:55:30 AEST	1	Incoming	6.15E+10	3ead5183-	Youâ€™re overdue on the payment. We agreed youâ€™d have it
ndroid Me	2024-09-14 22:55:51 AEST	1	Outgoing	3ead5183-	6.15E+10	Iâ€™m working on it. I just need a bit more time.
ndroid Me	2024-09-14 22:56:03 AEST	1	Incoming	6.15E+10	3ead5183-	Timeâ€™s up, Alex. You donâ€™t want to see what happens if yo
ndroid Me	2024-09-14 22:56:14 AEST	1	Outgoing	3ead5183-	6.15E+10	Iâ€™ll have it by tomorrow. Please, just one more day.
ndroid Me	2024-09-14 22:56:28 AEST	1	Incoming	6.15E+10	3ead5183-	Fine. One day. But after that, weâ€™re done talking.
ndroid Me	2024-09-14 22:56:42 AEST	1	Outgoing	3ead5183-	6.15E+10	Thank you. I wonâ€™t let you down.
ndroid Me	2024-09-14 22:58:08 AEST	1	Incoming	6.14E+10	3ead5183-	Iâ€™m just outside. I canâ€™t take this anymore, Alex. You prom
ndroid Me	2024-09-14 22:58:25 AEST	1	Outgoing	3ead5183-	6.14E+10	Sophia, please, I need time. Weâ€™ll talk, but not like this.
ndroid Me	2024-09-14 22:58:36 AEST	1	Incoming	6.14E+10	3ead5183-	No, I need to know now. Itâ€™s either me or her.
ndroid Me	2024-09-14 22:58:49 AEST	1	Outgoing	3ead5183-	6.14E+10	Come up, weâ€™ll talk. But you need to calm down.
ndroid Me	2024-09-14 22:59:00 AEST	1	Incoming	6.14E+10	3ead5183-	Iâ€™m calm, but I donâ€™t think you understand what this mear
ndroid Me	2024-09-14 22:59:21 AEST	1	Outgoing	3ead5183-	6.14E+10	Iâ€™m not tossing you aside. Letâ€™s talk when you get here.

	id	url	title	visit_count	typed_count	last_visit_time	hidden
	F...	Filter	Filter	Filter	Filter	Filter	Filter
	16	https://www.google.com/search?...	google - Google Search	1	0	13370788735144663	0
	14	https://www.google.com/url?q=https://...	Clery Act Policy | California Community ...	1	0	13370788713635512	0
	15	https://www.cccco.edu/About-Us/...	Clery Act Policy | California Community ...	1	0	13370788713635512	0
	13	https://www.google.com/search?...	nearest campus security office - Google ...	1	0	13370788706516631	0
	11	https://www.google.com/url?q=https://...	Archive or delete messages, calls, or ...	1	0	13370788691003586	0
	12	https://support.google.com/voice/answer/...	Archive or delete messages, calls, or ...	1	0	13370788691003586	0
	10	https://www.google.com/search?...	how to delete messages permanently on ...	1	0	13370788687758765	0
	8	https://www.google.com/url?q=https://...	Block or unblock a phone number - Phone ...	1	0	13370788664517820	0
	9	https://support.google.com/phoneapp/...	Block or unblock a phone number - Phone ...	1	0	13370788664517820	0
0	7	https://www.google.com/search?...	how to block calls from a specific number -...	1	0	13370788660077873	0
1	5	https://www.google.com/url?q=https://...	403 Forbidden	1	0	13370788644456745	1
2	6	https://www.elfi.com/emergency-student-...	403 Forbidden	1	0	13370788644456745	1
3	4	https://www.google.com/search?...	emergency loan options for students - ...	1	0	13370788640678041	0
4	3	https://www.walmart.com/browse/cell-...	Prepaid Phones in Phones With Plans - ...	2	0	13370788625109302	0
5	2	https://www.google.com/url?q=https://...	Prepaid Phones in Phones With Plans - ...	1	0	13370788622951288	0
6	1	https://www.google.com/search?...	cheap burner phones near me - Google ...	1	0	13370788616325874	0



Final Analysis and Conclusions

The analysis of the collected evidence reveals a complicated relationship, mental health challenges, and social pressures surrounding Alex in the time leading up to his death. Key findings include:

- Owner Identification: Alex Marshall is confirmed as the owner of the desktop computer based on user account details extracted from the disk image.
- Psychological State: SMS and web searches strongly suggest Alex was suffering from anxiety and stress caused by academic pressures and financial troubles. His deleted notes, including a will, indicate he was in a deeply troubled state of mind.
- Network Interactions: Dormitory network activity reflects Alex's interactions with his friends and his girlfriend, Sophia. The PCAP file reveals suspicious network activity involving two individuals, "DormKing" and "PartyDude," with whom Alex had been involved in selling exam papers for $200. DormKing expresses reluctance to pay Alex the agreed $200 for the answers. The chat

logs show DormKing instructing PartyDude to retrieve a session key from Alex's PC while Alex was supposed to be out of his room. However, PartyDude mistakenly accessed DormKing's room and uploaded an SSL key to the FTP server. PartyDude later reports seeing Alex, talking to some girls likely Sophia and Lily.

- Relationships: Alex was in a complex situation with two girlfriends, Sophia and Lily, as revealed by messages in the mmssms.db database. Both women sent him SMS pressuring him to choose between them, adding to the emotional strain. Sophia even went to Alex's dorm room, making her the last person to have seen him.
- Financial Pressure: Alex was also being harassed by someone over overdue payments, with threatening warnings about what would happen if he continued stalling. However, Alex requested an extra day, and both parties seemed to agree.
- Digital Footprint: The analysis of the memory dump and mobile phone data reveals significant connections to Sophia, who was an important figure in Alex's life. Her presence in emails, SMS messages, and physical interactions with Alex shortly before his death suggests that she may have been more aware of his struggles than others. Notably, her web searches after arriving at Alex’s room, including "how to get away with self-defense," raise concerns about her motives and intentions, implying that she might have been seeking justification for harming Alex.

In conclusion, Alex faced various pressures, including academic, financial, and personal challenges, which contributed to his emotional distress. His relationships with Sophia and Lily intensified his struggles, and financial difficulties added to his stress. Furthermore, a memory dump from Sophia's personal laptop indicates her presence in his room, and her web searches conducted while at Alex’s place suggest her likely involvement at the scene.