

10/11/2024

# Major Assignment

Digital Forensics



Jophiel Arevalo Enriquez

S5391194 – MASTER'S OF CYBERSECURITY

## Task 1

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

The whole analysis process must have a special organisation, therefore, it is essential to create a folder and subfolders that will give us more control over the evidence. The 'mkdir' command makes it easy to create this type of folder with a single command (GeeksforGeeks, n.d.). The folder where we are going to work is '/cases/' and the subfolder created for this evidence will be called '/cases/EvidenceA/'.

To be able to interact with all the evidence, the downloaded documents must be analysed. Most of the evidence will be in a '.zip' format, this means that they will be compressed and must be decompressed with the help of the 'unzip' command which is used to extract documents from zip files, preserving the directory structure and permissions (GeeksforGeeks, n.d.).

When we open the folder where the 'evidence A' file has been unzipped we see that there are 11 documents from 'EvidenceA.001' to 'EvidenceA.011', we will join all the parts to create a single disk image file in .dd format to be able to analyse it in a comprehensive way. For this step we use the command 'cat' which simultaneously joins several documents and prints them in another one (GeeksforGeeks, n.d.), the name under which it will be printed is 'EvidenceA.dd'.

The hash of the created document (EvidenceA.dd) is e2163d35fb453047af7534d12de89055, in order to get this hash, we use 'md5sum' command, this command helps us to verify the integrity of the document, It generates and checks 128-bit MD5 hashes to ensure data is unchanged (TheLinuxCode, 2023).

On the other hand, to mount the Windows system that the evidence file has on our system we must verify the image information, a useful command for this is 'img\_stat' which highlights the image type, size and sector size (SleuthKit, n.d.). For our example we can look at image 1.

```
$ img_stat EvidenceA.dd
IMAGE FILE INFORMATION
-----
Image Type: raw

Size in bytes: 21474836480
Sector size: 512
```

*Figure 1, Image file EvidenceA.dd*

We also analyse the partitions of the disk image, to see the larger ones, as this is where the information is concentrated. SleuthKit (n.d.) in his article gives the functionality of this command that shows the structure of partitions within a volume system, including partition tables and disk labels. Basic data partition is the most interested one.

As a last step before we start interacting with the evidence itself, we must mount the disk file on our own system, for this, the command used is the mount command, which is utilized to attach the filesystem located on a device to the large hierarchical structure (Linux filesystem) that is rooted at '/'. It must be mounted with 'supeuser' or 'sudo' permission. We also need to calculate the offset since we are only going to mount the specific system within the partitions, for this we need the offset which is basically the start bit of the partition we want to mount (GeeksforGeeks, n.d.). For our case it is Basic data partition which starts at '673792'. This number multiplied by the sector size of each byte will give you the specific number of bits that the offset needs, in our case

it is '344981504'; In addition, you must have a folder where you will mount the system '/mnt/Windows\_mount'. The command to use is 'sudo mount -o ro,loop,offset=344981504 EvidenceA.dd /mnt/windows\_mount'.

### 1. Who is the owner of the computer?

Once we have mounted the image disk in our system, we can start to investigate the data that it shows us, to find out the owner of the computer or the registered name we can use the 'RegRipper' command 'rip.pl', this command extracts information from the hive files registers (Bajpai, 2014). Due to the massive amount of information that 'rip.pl' can present us with, we must use 'grep' which filters all the data; to see the owner of this computer we must filter rip.pl with grep looking for 'win' as 'rip.pl -l | grep win' to see the version of Windows that this system was running. As a result we have 'winver'; which is located in the software folder, the command to use is 'rip.pl -r /mnt/windows\_mount/Windows/System32/config/SOFTWARE -p winver', the result can be seen in the figure below, the registered owner of this computer is Windows User.

```
sansforensics@siftworkstation: /mnt/windows_mount/Windows/System32/config
$ rip.pl -r /mnt/windows_mount/Windows/System32/config/SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName           Windows 10 Pro N
ReleaseID              2009
BuildLab               19041.vb_release.191206-1406
BuildLabEx             19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID   EnterpriseN
RegisteredOrganization
RegisteredOwner        Windows User
InstallDate            2024-08-27 13:04:14Z
InstallTime            2024-08-27 13:04:14Z
```

*Figure 2, Registered owner*

Another way to verify or obtain the name of the user that used this computer is to search for name in 'rip.pl | grep name', the result is 'compname' which is located in the 'system' folder, the command used to obtain this information is 'rip.pl -r /mnt/windows\_mount/Windows/System32/config/SYSTEM -p compname', The hostname is 'DESKTOP-0N2DC4F' as you can see in the figure below.

```
$ rip.pl -r /mnt/windows_mount/Windows/System32/config/SYSTEM -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName          = DESKTOP-0N2DC4F
TCP/IP Hostname        = DESKTOP-0N2DC4F
```

*Figure 3, Host name*

Knowing this, we must verify the usernames that the owner used, for which we filter with grep username, with this we obtain the 'SAM' folder where we can obtain the users of the computer, the command used for this is 'rip.pl -r /mnt/windows\_mount/Windows/System32/config/SAM -p samparse | grep Username', the result yields 5 users and one of these is 'Alex Marshall' verifying that the owner of this computer is indeed Alex Marshall.

```
sansforensics@siftworkstation: /mnt/windows_mount/Windows/System32/config
$ rip.pl -r /mnt/windows_mount/Windows/System32/config/SAM -p samparse | grep Username
name
Launching samparse v.20200825
Username           : Administrator [500]
Username           : Guest [501]
Username           : DefaultAccount [503]
Username           : WDAGUtilityAccount [504]
Username           : Alex Marshall [1000]
```

*Figure 4, Usernames*

To verify the use of these users samparse helps us because it shows us the interaction that the users had along the time, the command used was 'rip.pl -r /mnt/windows\_mount/Windows/System32/config/SAM -p samparse', where it shows us the interaction that Alex's user had, it is important to say that he is the only user of the 5 that had interaction, that's why only this user is shown in the figure below.

```
Username      : Alex Marshall [1000]
Full Name     :
User Comment  :
Account Type  :
Account Created : 2024-08-27 13:02:28Z
Name         :
Last Login Date : 2024-08-27 13:05:43Z
Pwd Reset Date : 2024-08-27 13:02:28Z
Pwd Fail Date  : 2024-08-27 13:06:45Z
Login Count   : 2
Embedded RID   : 1000
--> Normal user account
```

*Figure 5, Alex user interactions*

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

Taking into account that the complete system image is mounted on our system we can go to the directory directly where the system programs are located with the command change directory to the program files folder 'Cd Program Files' inside this directory you can see the applications that this computer had such as '7-zip', 'internet explorer', 'Mozilla Firefox' among others as you can see in the folders 'Program Files', 'Program Files (x86)' and 'Downloads'.

```
$ ls
7-Zip                      'Windows Defender'
Common Files               'Windows Defender Advanced Threat Protection'
desktop.ini               'Windows Mail'
Internet Explorer         'Windows NT'
ModifiableWindowsApps    'Windows Photo Viewer'
Uninstall Information     'Windows PowerShell'
VMware                   'Windows Security'
WindowsApps              'Windows Sidebar'
```

*Figure 6, Program Files*

```
sansforensics@siftworkstation: /mnt/windows_mount/Program Files (x86)
$ ls
Common Files'      Microsoft      'Mozilla Maintenance Service'  'Windows Mail'      'WindowsPowerShell'
desktop.ini        Microsoft.NET  VideoLAN                     'Windows NT'        'Windows Sidebar'
Internet Explorer' 'Mozilla Firefox' 'Windows Defender'           'Windows Photo Viewer'
```

*Figure 7, Program Files (x86)*

```
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/Alex Marshall/Downloads
$ ls
7z2408-x64.exe  desktop.ini  'Firefox Installer.exe'  vlc-3.0.21-win32.exe  winzip76-downwz.exe
```

*Figure 8 Downloads*

3. Recover the content of any files in the recycle bin.

You can see that there are 4 documents inside the recycle bin. Using 'recbin.pl' which is designed to parse the contents of the \$I file in the Recycle Bin. The tool accepts the \$I file path as a command-line argument and retrieves details about the deleted file, including its filename, full

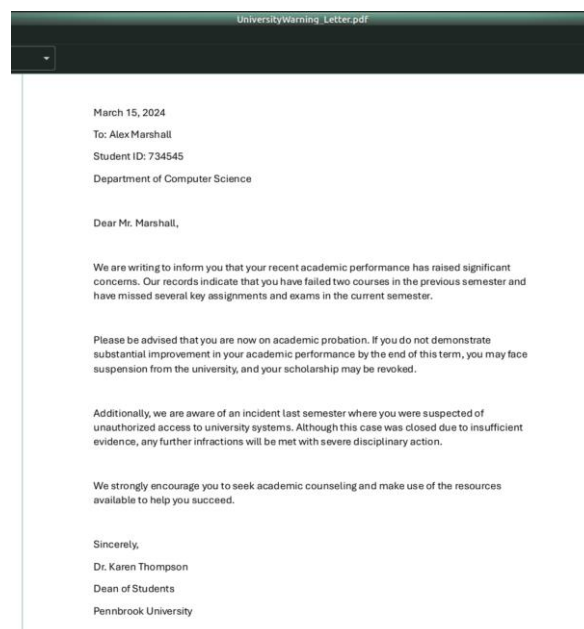
path, size, and the date and time of deletion (Mehrnoush, 2022). So, you can see the original name of the document, in this case he deleted some private notes, it also details the date that Alex deleted this document

C:\Alex Marshall\Documents\privatenotes.txt [14336 bytes] deleted on Tue Aug 27 13:15:35 2024 Z

You can also retrieve the name of a zip file that alex deleted called rubbish

C:\Alex Marshall\Documents\rubbish.zip [63400 bytes] deleted on Tue Aug 27 13:15:35 2024 Z

With the help of 'fcrackzip' we can try to recover the zip file, for this, we will need the help of 'rockyou.txt', It can crack password-protected zip files using either brute force or dictionary-based attacks. (Kali Linux, n. d.). The command used was 'fcrackzip -u -v -D -p /cases/EvidenceD/Sms/rockyou.txt "\$RLY0J7N.zip"' and the result was 'football' as the password, so we can unzip the document and see what Alex deleted. The file that was deleted was 'UniversityWarning\_Letter.pdf' where they explain to Alex that he is under review as he lost subjects and has allegations against him for selling test answers.



*Figure 9, University warning*

In order to decipher the following document, we must open it with the help of 'Bless hex editor' and find the magic number that tells us what type of document it is in order to remove the header of it and thus be able to see the content, this document is a Word document so the magic number that we must find is 50 4B 03 04, once we find it, we remove all the data that are above it and save it. Alex saved this document as if it were 'notes.jpg' but when we check in the terminal what kind of document it is, it shows us that it is a Word document, so we open it as text and we can see that it is 'last Will and testament'.

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

Figure 10, Last will and testament

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

Digging into Alex's profile we can find several documents that can help us to begin to make assumptions about the case, within his personal documents folder we can find emails from his father detailing on March 10, 2024 that his student report is not what should be expected from the Marshall family, that if he continues like this the financial support will be cut off.

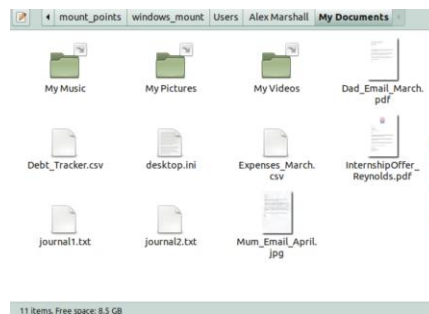


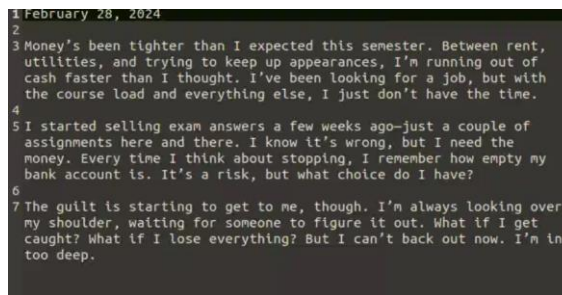
Figure 11 Alex's personal documents

In addition, we can see that Alex had a budget set up and a document to track debts where he has debts to Lily Parker, on credit cards and on a private loan that is urgent.

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

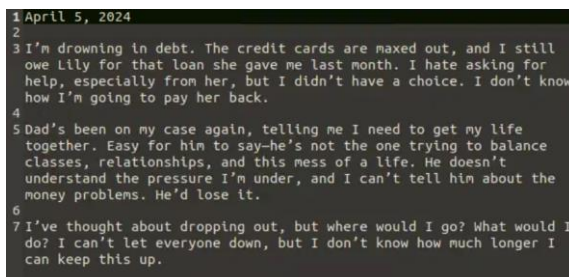
Figure 12 Alex's debt file

Alex's notes show that he has a business selling exam answers, but he doesn't enjoy it, he knows he is not doing well, but money and debt force him to keep doing it.



1 February 28, 2024  
2  
3 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.  
4  
5 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?  
6  
7 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.

*Figure 13 Alex's Journal 1*



1 April 5, 2024  
2  
3 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.  
4  
5 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.  
6  
7 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.

*Figure 14 Alex's journal 2*

There is also an email from Alex's mother in which she supports her son and encourages him to continue, explaining that his father has a bit of a temperament, but it is because she wants to see him achieve his goals.



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.

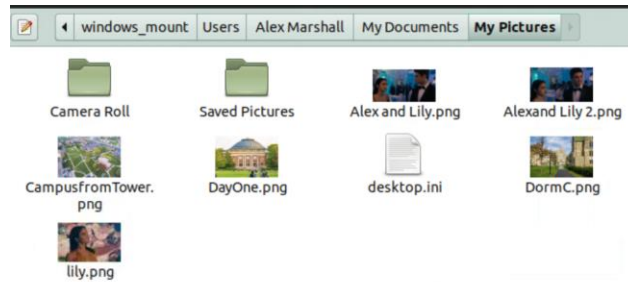
If you ever feel like you need someone to talk to, please don't hesitate to reach out. I'm worried about you, and I hope you're taking care of yourself. Life can be challenging, but you're strong, and I know you'll find your way.

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

Love,  
Mum

*Figure 15 Alex's mom letter*

We can also find an internship offer that should be accepted until April 10th with TechVision, Professor Mark Reynolds is the person who is offering her this opportunity. In the photo folder we can find some pictures with Lily and of the university campus.



*Figure 16 Alex's Pictures*

These findings show that Alex had several debts from credit cards to loans with unknown people that were urgent, the semester was not going in the best way as we can see from his father's letter that his grades were not good. In addition, he was giving exam answers to classmates, which he was not proud of, but he was doing it because of the debts he himself had. This may give way to important evidence and justification for some behavior that can be found later. Finally, we can see the last will and testament, meaning that Alex knew something bad could happen.

#### **Evidence B – Network capture of the dormitory network.**

By downloading and unzipping this evidence and creating, as with the first evidence, a specific folder to maintain an integrated organisation of all the documents (EvidenceB) we can see that it is a pcap document, it means that it contains network packet data that Wireshark intercepted and logged while monitoring a network.

As in the first part, the integrity of the document must be analysed, for this we use the md5sum command and the hash it gives us is b383bb9ae1dce23a4e72a0c192aafe80.

5. Who are the people communicating in the transmission? When does the first transmission begin and the last transmission finish?

Wireshark is the leading network protocol analyzer globally, allowing you to observe network activity at a detailed level. It is the de facto, and often official, standard used across various industries and educational institutions. (Wireshark Foundation, n.d.).

Following the TCP communications that were in this web capture we found some communications along the capture, for this we can filter in wireshark TCP and follow the stream, another way to filter and interact with these documents is to go to the statistics tab and see the conversations that the activity had, so we can see the TCP interaction within the ethernet or TCP, we can also see the duration that these had and filter the longest or the communications that had more interaction, with that we can get the following packets. In addition to those listed below we found the captures of the conversations, but with the other endpoint, for reasons of not redundant in the same information we specify below the capture that Alex made from his computer and the only extra communication between Dormking and Partydude.

Packet 272 TCP stream laptop Alex Marshall

**CheatChat:**

AlexM21: message, time: 2024-09-01T07:57:11.087Z: "Alright, the files are ready. Bio101 answers, top tier. Who's in?"

DormKing: message, time: 2024-09-01T07:57:51.403Z: "I'm in. How much are we talking?"

DormKing: message, time: 2024-09-01T07:58:26.944Z: "\$200 for the full set. Same as last time."

PartyDude: message, time: 2024-09-01T07:59:02.387Z: "Dude you're saving my life. Finals are killing me."

AlexM21: message, time: 2024-09-01T08:01:38.498Z: "Done. You won't get the answers better anywhere else. Also not going to give you a 7, just a 6, but that will get you through and no suspicions."

DormKing: message, time: 2024-09-01T08:02:00.463Z: "Same drop as before?"

AlexM21: message, time: 2024-09-01T08:02:32.887Z: "Yep I'll leave it on the ftp server. Make sure you delete everything after."

BookWorm: message, time: 2024-09-01T08:03:22.472Z: "Careful guys. Heard the faculty is cracking down on this."

AlexM21: message, time: 2024-09-01T08:03:59.968Z: "Relax, they'll never trace it back. Just keep it quiet and the profs will never know it is happening."

AlexM21: message, time: 2024-09-01T08:06:56.418Z: "Who's up for pizza tonight?"

DormKing: message, time: 2024-09-01T08:07:16.015Z: "Always. Where from?"

BookWorm: message, time: 2024-09-01T08:07:34.483Z: "Count me out. Too much studying to do."

PartyDude: message, time: 2024-09-01T08:08:00.203Z: "Bro, you need to take a break. You're gonna burn out."

AlexM21: message, time: 2024-09-01T08:08:17.322Z: "Domino's? Easy and fast."

DormKing: message, time: 2024-09-01T08:08:32.057Z: "Works for me. Same room as last time?"

AlexM21: message, time: 2024-09-01T08:08:45.416Z: "Yeah, meet you there in 10."

#### **PrivateChat with Sophia alias ArtLover99:**

ArtLover99: message, time: 2024-09-01T08:09:28.019Z: "Alex, we need to talk."

AlexM21: message, time: 2024-09-01T08:09:44.742Z: "About what? I'm busy."

ArtLover99: message, time: 2024-09-01T08:10:02.913Z: "About us. I can't keep doing this if your not serious."

AlexM21: message, time: 2024-09-01T08:10:31.914Z: "Sophia, I told you. I need time. It's complicated with Lily."

ArtLover99: message, time: 2024-09-01T08:10:55.862Z: "You always say that. It's like I don't even matter to you."

AlexM21: message, time: 2024-09-01T08:11:23.321Z: "That's not true. I care about you. But you know how things are right now."

ArtLover99: message, time: 2024-09-01T08:11:43.159Z: "Then show it. Make a decision. Alex I'm not going to wait forever."

AlexM21: message, time: 2024-09-01T08:12:06.324Z: "I'll figure it out, OK? Just give me a little more time."

ArtLover99: message, time: 2024-09-01T08:12:26.410Z: "Fine. But I won't be strung along. I deserve better."

### Private Chat with Lily:

Packet 371 from Lily's chat

LilyLaw: message, time: 2024-09-01T08:20:53.197Z: "Where were you tonight? I waited at the library."

AlexM21: message, time: 2024-09-01T08:21:10.311Z: "Sorry something came up. I'll make it up to you."

LilyLaw: message, time: 2024-09-01T08:21:22.511Z: "Something or someone?"

AlexM21: message, time: 2024-09-01T08:21:34.821Z: "What's that supposed to mean?"

LilyLaw: message, time: 2024-09-01T08:22:09.353Z: "You know exactly what I mean. Are you seeing someone else?"

AlexM21: message, time: 2024-09-01T08:22:36.051Z: "Lily, come on. You're over thinking this. I was just busy. It's finals."

LilyLaw: message, time: 2024-09-01T08:23:14.633Z: "I'm not stupid, Alex. I know there's someone else. If you don't end it, I will. And it won't be pretty."

AlexM21: message, time: 2024-09-01T08:23:39.431Z: "There's no one else, I swear. Let's talk about this in person, OK?"

LilyLaw: message, time: 2024-09-01T08:23:51.649Z: "Fine, but this isn't over.",

### Private chat between DormKing and PartyDude capture TCP stream 3 from PartyDude endpoint:

DormKing: message, time: 2024-09-01T08:16:09.877Z: "Hey Dude, I'm not going to pay \$200! Alex will be out of his room in 10. See if you can get to his PC and grab the session key from his PC."

PartyDude: message, time: 2024-09-01T08:16:54.068Z: "The one on the ftp server? I thought that was where the drop was?"

DormKing: message, time: 2024-09-01T08:17:37.982Z: "Nah, the drop will be on the web server like last time, didn't you hear? Load the key on the ftp server."

PartyDude: message, time: 2024-09-01T08:17:52.411Z: "Uhhh OK."

DormKing: message, time: 2024-09-01T08:18:25.656Z: "Man. No wonder you need the answers."

DormKing: message, time: 2024-09-01T08:44:49.709Z: "Hey did I see you just come out of my room?!"

PartyDude: message, time: 2024-09-01T08:45:39.918Z: "Yeah, I did as you said. Waited till you left and then uploaded to the ssl key to the ftp server."

DormKing: message, time: 2024-09-01T08:46:03.006Z: "You idiot! Alex's room Alex's PC"

PartyDude: message, time: 2024-09-01T08:46:20.141Z: "Oh nah, he is still there talking to some girl."

6. What browsers, operating systems, and IP addresses are used by the communication endpoints?

Using the tools that wireshark gives us we can filter and verify the connections that were with the protocol 'http' which gives us information of IPs used and the user agent that had that connection, with this we can see what devices and operating systems used the owners of those connections, the following are the IPs and user agents that were used. With the help of useragents.net we can verify the details of the system that was used.

- IP: 10.10.10.33  
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36  
Browser: Chrome  
OS: Windows 7
- IP: 10.10.10.1  
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36  
Browser: Chrome  
OS: Windows7
- IP: 10.10.10.56  
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_2) AppleWebKit/601.3.9 (KHTML, like Gecko) Version/9.0.2 Safari/601.3.9  
Browser: Safari  
OS: Mac OS X
- IP: 10.10.10.22  
User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11\_2) AppleWebKit/601.3.9 (KHTML, like Gecko) Version/9.0.2 Safari/601.3.9  
Browser: Safari  
OS: Mac OS X
- IP: 10.10.10.44  
User Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:15.0) Gecko/20100101 Firefox/15.0.1  
Browser: Firefox  
OS: Ubuntu
- All also communicate via a local network with the ip 10.10.10.254 via:  
User Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:129.0) Gecko/20100101 Firefox/129.0  
Browser: Firefox  
OS: Ubuntu

## 7. What files were transmitted on the local network?

Filtering by FTP protocol and following the TCP stream we can find that the documents that were transferred were as follows

ftp stream 694:

```

220 (vsFTPd 3.0.5)
USER anonymous
230 Login successful.
SYST
215 UNIX Type: L8
TYPE I
200 Switching to Binary mode.
PORT 10,10,10,22,211,95
200 PORT command successful. Consider using PASV.
STOR sslkeyfile
553 Could not create file.
TYPE A
200 Switching to ASCII mode.
PORT 10,10,10,22,137,9
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
CWD pub
250 Directory successfully changed.
PORT 10,10,10,22,162,39
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 10,10,10,22,205,3
200 PORT command successful. Consider using PASV.
STOR sslkeyfile
150 Ok to send data.
226 Transfer complete.
QUIT
221 Goodbye.

```

```

# SSL/TLS secrets log file, generated by NSS
CLIENT_HANDSHAKE_TRAFFIC_SECRET
7eb7aa304379b70109738e04a08b548856f1efaf0d245966fb4dd24f8d9d7d42
10b7a548166d4d0030ef819588efee47d85e4fbc1b307670bbdefe28d8aea790
SERVER_HANDSHAKE_TRAFFIC_SECRET
7eb7aa304379b70109738e04a08b548856f1efaf0d245966fb4dd24f8d9d7d42
2b4c0eecd27e54df3c815903402f13a76e50caf2864bc209e1e79c81d9348d4
CLIENT_HANDSHAKE_TRAFFIC_SECRET
7eb7aa304379b70109738e04a08b548856f1efaf0d245966fb4dd24f8d9d7d42
50d9e26b5d9d51c42d51f13707674fc14c8eb342b64885530ec8ad1307ad5d4
SERVER_HANDSHAKE_TRAFFIC_SECRET
7eb7aa304379b70109738e04a08b548856f1efaf0d245966fb4dd24f8d9d7d42
5292a58d4fe774317fcd05d6d64f286d1593bfc39803221ecff844f7f3d14ce
EXPORTER_SECRET 7eb7aa304379b70109738e04a08b548856f1efaf0d245966fb4dd24f8d9d7d42
552cfd619a3ddd6213374f8329c65b90fcfee98155c5687f7a2c9195e2c31c7c
CLIENT_HANDSHAKE_TRAFFIC_SECRET
db75f172d0879ab8d42c7efae0e3b40091560f7be596022ab448eac447970500
818f2273e0c5bfcbf2b167c4b0ffff8b52c9f34d3666cc17c26d53cbb5c2c97e
SERVER_HANDSHAKE_TRAFFIC_SECRET
db75f172d0879ab8d42c7efae0e3b40091560f7be596022ab448eac447970500
80a8119cdee88f02a8b8eaa732a7e35cc69160a10ebffee11f824294cbbc2db
CLIENT_HANDSHAKE_TRAFFIC_SECRET
db75f172d0879ab8d42c7efae0e3b40091560f7be596022ab448eac447970500
d82923398b872af8fbcefe4699d29f6b26bb2e106cfb6945241715bf56fa04
SERVER_HANDSHAKE_TRAFFIC_SECRET
db75f172d0879ab8d42c7efae0e3b40091560f7be596022ab448eac447970500
39983d3505c846a1a05118e094b455d61f92c6e08ef77009a46d0694dfb7a837
EXPORTER_SECRET db75f172d0879ab8d42c7efae0e3b40091560f7be596022ab448eac447970500
cf4acc430f6248e6a508a12e6b0e6f226b434eac6d6f79742d89f72c1582bb6
CLIENT_RANDOM 38016bc94ae0826412f45f2a7e0d826697cf1a8e396df56fb4634e9534bfcff5
201cddb82cb83a8c3a3e8d8323055d135a20b68c1107f78f6610821eb10ca506669c3b0b5199a29be5
b5412a7386460
CLIENT_RANDOM 72d3bab0ca2aedac7cd4b842b1d3d0410a0e36428c7823e590e80e3c9e747644
f83e24701a8f09e658104ed422c870565e24b8e12b857046e044e1a99d29296b688cf6bfde704cdc93
9cc740cf10da5
CLIENT_HANDSHAKE_TRAFFIC_SECRET
87bdc31f6fca9c3618a060038ae29462e02f35613624745ca0a3e1ffc65fd789
5ec3b1cd3a472a21cce88f1d59b594d01bbca8a13d30680c341d9b26f01d5682
SERVER_HANDSHAKE_TRAFFIC_SECRET
87bdc31f6fca9c3618a060038ae29462e02f35613624745ca0a3e1ffc65fd789
8214a82c800acdcac3c223995b3c879d78095167c5505dcf61d444c2152a7dc

```

Figure 17, TCP stream 694

Analysing the 'FTP' protocol within this server there is a folder called 'pub' and there are also two documents that were not transferred but are there, 'test.txt' and 'upload.txt'.

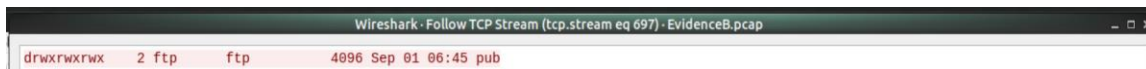


Figure 18, pub Directory

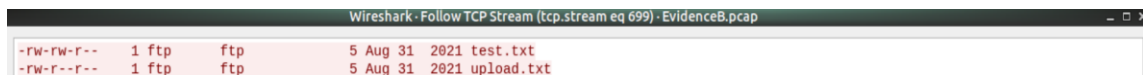


Figure 19 Test.txt file

- What is the relationship of the people communicating in the network capture? How are they related to the victim?

There are 3 communications where Alex interacts, the first is in a group chat called 'Cheat Chat' where there are 4 involved: Alex, Party Dude, DormKing, and WormBook. This chat shows Alex's intentions to sell the Bio101 exam answers. It has been found in TCP communication package 3 which is the same chat conversation but from PartyDude's endpoint, where he has another private conversation with DormKing telling him to go into Alex's room and steal the exam answers. However, in the same chat it is evident that the plan was unsuccessful as DormKing misunderstood.

The second chat we can see that Alex had with Sophia aka 'ArtLover99', where we can see a discussion between her and Alex related to Lily, demanding him to leave her and asking for explanations as to why he is still with her.

The last conversation captured on the network related to Alex is with Lily, where she asks him if there is anyone else in Alex's life, there he responds by assuring her that there is no one else, they agree to meet in person to talk about the situation.

**Evidence C** – A memory dump of a personal laptop found in Alex's bedroom.

The next piece of evidence is a memory dump of a personal laptop found in Alex's bedroom. To be able to analyse it we need to create a folder inside our cases folder with 'mkdir' in order not to lose the continuity of organisation that we have been managing, in the same way when unzipping the Evidence C in its respective folder we can see that there is a 'vmem' file, in other words, it is a 'Virtual Memory' and contains a backup of a main memory of a system (File Info Base, 2024). In addition to this, thanks to the previously explained function 'md5sum' we can see that the hash of this document is 610278c68947d89a587ea64987af5b85.

A functional tool to be able to analyse this type of document is volatility, is an entirely open-source set of tools, developed in Python under the GNU General Public License, designed for extracting digital artifacts from volatile memory (RAM) samples (Volatility Foundation, 2024).

In the figure below we can see the type of image that the evidence c gives us, the operating system that this backup handled, which most likely was a 'Win7SP1x64' system.

```

$ vol.py -f EvidenceC.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win200
8R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsX86X64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/cases/EvidenceC/EvidenceC.vmem)
PAE type : No PAE
DTB : 0x1870000
KDBG : 0xf00029f40a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KDBG for CPU 0 : 0xfffff800029f5000L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2024-09-08 12:26:34 UTC+0000
Image local date and time : 2024-09-08 22:26:34 +1000

```

Figure 20, ImageType EvidenceC

Another functionality that allows us to see volatility are the Registry hives, now of running the command with the EvidenceC file and the profile that gave us the type of image previously investigated we can see the list of the registers of the memory. This gives us a little hint of who can be this memory because inside the User folder is the name of 'Sophia Bennet'.

```

$ vol.py -f EvidenceC.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual Physical Name
-----
0xfffff800000f010 0x00000000a95e4010 [no name]
0xfffff8000024010 0x00000000a972f010 \Registry\Machine\System
0xfffff80000061010 0x00000000a96ee010 \Registry\Machine\Hardware
0xfffff80000b0410 0x00000000a66fd410 \Device\HarddiskVolume1\Boot\BCD
0xfffff80000b98010 0x00000000a520010 \SystemRoot\System32\Config\SOFTWARE
0xfffff80000cd7010 0x00000000dddb010 \SystemRoot\System32\Config\SECURITY
0xfffff80000e43010 0x00000000d738010 \SystemRoot\System32\Config\SAM
0xfffff80000f5c410 0x00000000d0e6410 ??[C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff80000f62010 0x00000000d36c010 ??[C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff800011ea010 0x0000000098c1d010 ??[C:\Users\Sophia Bennett\ntuser.dat
0xfffff800013d4010 0x0000000095148010 ??[C:\Users\Sophia Bennett\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff80001bf0370 0x000000007b1a9370 ??[C:\System Volume Information\Syscache.hve
0xfffff80001af010 0x00000000a991c010 \SystemRoot\System32\Config\DEFAULT

```

Figure 21, registry hives

## 9. What applications are running on the memory dump computer?

To list the processes of a system within volatility, the pslist command takes us into the processes that are currently open. The command used is 'vol.py -f EvidenceC.vmem --profile=Win7SP1x64 pslist' (Volatility Foundation, 2024), yielding the following applications which have open processes in memory:

Man	Firefox	Thunderbird	Mynotepad++
Helper	Dllhost	Csrss	Winlogon
Taskhost	Dwm	Explorer	Vmtoolsd

10. What web pages has the memory dump computer visited recently?

Netscan identifies TCP and UDP endpoints and listeners, distinguishing between IPv4 and IPv6. It displays the local and remote IP (if applicable), local and remote ports (if applicable), the time the socket was bound or the connection was established, and the current state (for TCP connections only). (Volatility Foundation, 2024). The command used was 'vol.py -f EvidenceC.vmem --profile=Win7SP1x64 netscan' noting that the applications being used were 'Firefox' 'Thunderbird' and 'svchost'.

0x13eee68f0	TCPv4	192.168.194.210:49577	142.250.66.195:443	ESTABLISHED	3512	firefox.exe
0x13eefc750	TCPv4	192.168.194.210:49676	18.155.216.27:443	ESTABLISHED	3512	firefox.exe
0x13f041010	TCPv4	192.168.194.210:49565	74.125.130.109:993	ESTABLISHED	1892	thunderbird.exe
0x13f046630	TCPv4	127.0.0.1:49504	127.0.0.1:49503	ESTABLISHED	1892	thunderbird.exe
0x13f05cc30	TCPv4	192.168.194.210:49576	172.217.167.100:443	ESTABLISHED	3512	firefox.exe
0x13f282390	TCPv4	127.0.0.1:49264	127.0.0.1:49263	ESTABLISHED	3512	firefox.exe
0x13f2cd8b0	TCPv4	127.0.0.1:49267	127.0.0.1:49266	ESTABLISHED	3800	firefox.exe
0x13f2cf010	TCPv4	127.0.0.1:49263	127.0.0.1:49264	ESTABLISHED	3512	firefox.exe
0x13f325540	TCPv4	127.0.0.1:49266	127.0.0.1:49267	ESTABLISHED	3800	firefox.exe
0x13f33f010	TCPv4	192.168.194.210:49575	172.217.167.100:443	ESTABLISHED	3512	firefox.exe
0x13f341010	TCPv4	192.168.194.210:49609	142.250.71.70:443	ESTABLISHED	3512	firefox.exe
0x13f7f73c0	UDPv4	0.0.0.0:63790	*:*		992	svchost.exe
09-08 07:11:13 UTC+0000						
0x13f7f73c0	UDPv6	:::63790	*:*		992	svchost.exe
09-08 07:11:13 UTC+0000						
0x13f72bb00	TCPv4	0.0.0.0:3587	0.0.0.0:0	LISTENING	2780	svchost.exe
0x13f72bb00	TCPv6	:::3587	:::0	LISTENING	2780	svchost.exe
0x13fb54cf0	TCPv4	192.168.194.210:49637	18.155.212.56:443	ESTABLISHED	3512	firefox.exe

Figure 22, Recent used apps

11. What is email address of the owner of the memory dump computer and how are they connected to the case?

Using the command string and knowing that the owner of the memory is Sophia, the following was used 'strings EvidenceC.vmem | grep mail.com'

Vb9945311@gmail.com Sophia Bennet

Extracting the Notepad extract from Sophia's memory with memdump which extracts all memory resident pages in a process into an individual file (Volatility Foundation, 2024). The command used was 'vol.py -f EvidenceC.vmem --profile=Win7SP1x64 memdump -p 4360 -D Notepad/' we can see some journals she wrote with the help of GHex editor and searching String for 'Alex'; making it known that she had an obsessive love affair with Alex and couldn't stand him having a seemingly perfect relationship with Lily.

#### Note 1 Sophia:

It's getting harder to control my thoughts about Alex. I've started keeping track of where he goes, who he talks to, what he does when he's not with me. I need to know everything about him. It's the only way I can make sure that no one else gets in the way of what we have. He's pulling away, I can feel it, and it terrifies me. If I lose him, I don't know what I'll do.

I saw them together again today, Lily and Alex, and it was like a knife in my heart. I wanted to scream, to grab him and make him understand that she doesn't deserve him. But I didn't. I just watched, and I felt this rage building up inside of me, this desperate need to do something,

anything, to bring him back to me. He belongs with me. I know he does. I just need to find a way to make him see it. That perfect smile, making me feel like I'm the only person in the world who matters. But then I see him with her. Lily, with her perfect hair and perfect life, and it makes me sick. How can he not see that I'm the one who truly understands him! We're meant to be together. She doesn't know him like I do. She can't possibly love him the way I do.

I watch them sometimes, just to see how they interact. It's all so superficial! There's no depth, no real connection. It's like he's just going through the motions with her, but with me? With me, it's real. I know it is. I just need to show him that. I need to make him see that I'm the one who can make him happy. I'll do whatever it takes to make sure he realizes that we're meant to be together.

### **Professor Kane Email for Sophia:**

Professor Kane:

It seems you've found yourself in quite the predicament. A word of advice: your friends in high places are not to be trusted. They have their own agendas, and you are but a pawn in their game.

I've been instructed to extend an offer. Come with me, and your work will be appreciated, protected, and rewarded. Or you can continue down your current path and face the consequences alone. The choice is yours, but know this: time is running out, and your enemies are closing in.

Consider this a friendly warning, from one professional to another. You have talents that are too valuable to be wasted. Don't let your pride be your downfall.

-IvanovA Friendly WarningVictor Ivanov <vb9945311@gmail.com>

### **Conversation between Alex and Sophia through email**

Hi Alex,

It felt so good to see you the other day. I could tell you're feeling torn, and I get it! I really do. But you know you don't have to keep pretending with her, Alex. I see how you look when you're with me, how relaxed you seem. You deserve to be with someone who understands you, who supports you without all the strings attached.

I keep thinking about what you said, about needing something different, someone who gets it. I think we both know that's me. I'm here for you, no matter what. I hope you see that sooner rather than later. I just want you to be happy, Alex. And I think we both know where that happiness is.

Always,

SophieYou and MeSophia Bennett <vb9945311@gmail.com>

Hey Soph,

Thanks for checking in. I've been feeling a bit overwhelmed with everything. Lily's been more intense lately, and I don't know how to handle it. I'm starting to think I need a change, something different, maybe even someone who gets it, you know? Someone who doesn't expect me to be perfect all the time.

I feel like I can be more honest with you than anyone else. You don't make things complicated. It's... nice. Let's grab that coffee. I think I could use the break and some time to clear my head. I appreciate you being there.

See you soon,

**Alex Feeling Overwhelmed** Alex Marshall <sr8640171@gmail.com>

Hey Alex,

I missed you in class today. I kept looking over at your usual spot, hoping you'd walk in with that goofy smile of yours. It's strange how quickly I've gotten used to seeing you around, like you're a part of my day I don't want to go without. I guess that sounds a bit silly, but It's true. I know things have been a bit... complicated lately, but I feel like we're getting closer, and I really like that. You make things feel a little less overwhelming, even when it feels like everything else is falling apart. I hope you're doing okay. Let me know if you want to grab coffee or just talk sometime. I'm here.

Take care,

Sophie Missed You Today Sophia Bennett <vb9945311@gmail.com>

12. What is password of the memory dump computer?

To extract LSA secrets from the registry, use the lsadump command. This reveals details such as the default password (for systems with autologin enabled), the RDP public key, and credentials used by DPAPI. (Volatility Foundation, 2024). We used the following command 'vol.py -f EvidenceC.vmem --profile=Win7SP1x64 lsadump' y la respuesta es la siguiente:

Alexisbeautiful

**Evidence D** – A disk image of a damaged mobile phone found in Alex's apartment apartment under some furniture.

To be able to analyse this evidence first we must unzip the file, this contrary to the previous evidences is a 7zip, for this reason the command that will be used to free all the content of the image of the mobile phone is '7zip', When we see the documents that we will work with we see that they have been decompressed several that are usual in an Android system, when analyzing the sizes of each one we see that the one we are most interested in is dm-1 and has a hash md5sum cbf84de09de09b0143ebddefcdae2e3d9a7c.

These types of images must be mounted on the system to be analysed, so the command used was 'sudo mount -o loop dm-1 /mnt/e01/'.

13. What are the non-stock applications installed on the phone?

After having mounted the Linux system, we can start to analyse the mobile phone found in the scene, a useful command to find things more efficiently in the Android system is 'find' It can search for files and directories using a whole raft of different criteria (How-To Geek, 2023). The command to see the non-stock applications is 'Find /mnt/e01 -name "\*.apk"' and the result we got was:

Facebook	Angrybirds	Tencent	Twitter
Bubble Shotter			

14. Who is in the contacts list? What messages and calls have been sent and received by the phone?

For this question we use 'find' in the same way and focus on the databases that are returned as Android uses databases to store information on the device 'Find /mnt/e01 -name "\*call\*"'. The most probable database with call History: /mnt/e01/data/com.android.providers.contacts/databases/calllog.db. it is important to note that in order to access this type of documents we must have superuser access, when manipulating these databases, we must change the permissions after copying them to normal user because if we leave in superuser we will not be able to visualize them. The database that we took out for the list of calls now of visualizing it in SQLite gives us these calls:

	_id	number	ent: dial_nun	date	ratio_us:ypeatur:com ript:ione_account_adre:cou:ub_i:new	name
	Filter	Filter	F... F... F...	Filter	F... F... F... F... F... F... Filter	F... F... F... Filter
1	1	+61449857236	1	1726311533266	0 ... 5 0 C... ... +15555215554 0 -1 1	Lily Parker
2	2	+61449857236	1	1726311536819	0 ... 5 0 C... ... +15555215554 0 -1 1	Lily Parker
3	3	+61449857236	1	1726311539845	0 ... 5 0 C... ... +15555215554 0 -1 1	Lily Parker
4	4	+61449857236	1	1726311542954	0 ... 5 0 C... ... +15555215554 0 -1 1	Lily Parker
5	5	+61417692485	1	1726311562841	70 ... 2 0 C... ... +15555215554 0 -1 1	Sophie Bennett

Figure 23, call history

1. Date call to Lily Sat 14 Sep 2024 10:58:53 AM UTC, no answer
2. Date call to Lily Sat 14 Sep 2024 10:58:56 AM UTC, no answer
3. Date call to Lily Sat 14 Sep 2024 10:58:59 AM UTC, no answer
4. Date call to Lily Sat 14 Sep 2024 10:59:02 AM UTC, no answer
5. Date call to Sophia Sat 14 Sep 2024 10:59:22 AM UTC, duration 1:10

Command used for 'contact list': 'Find /mnt/e01 -name "\*contact\*"'. The most likely to be the one which we are looking for is

/mnt/e01/data/com.android.providers.contacts/databases/contacts2.db or  
/mnt/e01/data/com.google.android.gms/databases/icing\_contacts.db.

Opening these ones, we can see Alex had 4 contacts in his list. However, we also can see that Alex erased the first 3 contacts on his list

	_id	contact_id	lookup_key	icon_uri	display_name	given_names	imes_contacter	score	mai kna'ote nizi	phone_numbers	postal_address	phonetic_name
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	F... F... F... F...	Filter	Filter	Filter
1	4	4	2437i46a07...	NULL	Lily Parker	Lily	NULL	1	... ... ...	+61 449 857 236	NULL	NULL
2	5	5	2437i27eaf...	NULL	Sophie Bennett	Sophie	NULL	1	... ... ...	+61 417 692 485	NULL	NULL
3	6	6	2437i382bc...	NULL	Mum	Mum	NULL	1	... ... ...	+61 438 179 564	NULL	NULL
4	7	7	2437i4bd09...	NULL	Dad	Dad	NULL	1	... ... ...	+61 467 315 782	NULL	NULL

Figure 24, contact list

Icing\_contacts.db-wal backup of contacts in bless hex These files may contain older versions of data before the changes were committed to the database.

```

.....
.....F.....7.).....)....243
7i1607b7590e26fa7fLalo SalamancaLalo(046) 473
-4229<.....7.....)....2437i790569dc8e6d1d45
MikeMike(049) 845-3251?.....7.....)....2437i
3159db238d31485eGus FringGus(044) 675-7823...
....."..a@ks^3I.Ga&.....F....:....
.....

```

Figure 25, deleted contacts

Command used for “Messages”: ‘Find /mnt/e01 -name “\*sms\*”’. The most likely to be the one who we are looking for is /mnt/e01/user\_de/0/com.android.providers.telephony/databases/mmssms.db

i	ead	address	arsc	date	date_sent	otoc	eatatu	ype	ath	ibje	body	
F...	F...	Filter	F...	Filter	Filter	F...	F...	F...	F...	F...	Filter	
1	1	3	+61449857236	4	1726318296614	1726318296000	0	1	-1	1	0	Hey, can we talk tonight? We really need to sort this out.
2	2	3	+61449857236	...	1726318315571	0	...	1	-1	2	...	Not tonight, Lily. I'm dealing with a lot right now.
3	3	3	+61449857236	4	1726318328913	1726318329000	0	1	-1	1	0	Alex, this is important. I can't keep going on like this, wondering where we stand.
4	4	3	+61449857236	...	1726318345012	0	...	1	-1	2	...	I know, I know. But I just can't tonight. Tomorrow?
5	5	3	+61449857236	4	1726318358407	1726318358000	0	1	-1	1	0	Tomorrow might be too late, Alex. If you don't end this with her, I will.
6	6	3	+61449857236	...	1726318370594	0	...	1	-1	2	...	Lily, please don't do anything rash. I'll figure it out, I promise.
7	7	3	+61449857236	4	1726318383723	1726318384000	0	1	-1	1	0	You better. I'm done waiting.
8	8	4	+61417692485	5	1726318414246	1726318414000	0	1	-1	1	0	Alex, I'm outside your dorm. Can we talk?
9	9	4	+61417692485	...	1726318436692	0	...	1	-1	2	...	Sophia, now's not a good time. I'm swamped.
10	10	4	+61417692485	5	1726318448139	1726318448000	0	1	-1	1	0	It'll only take a minute. Please, I really need to see you.
11	11	4	+61417692485	...	1726318462131	0	...	1	-1	2	...	Fine, come up. But I don't have long.
12	12	4	+61417692485	5	1726318476579	1726318476000	0	1	-1	1	0	Thank you. I just... I need to know where we stand. I can't keep feeling like this.
13	13	4	+61417692485	...	1726318495175	0	...	1	-1	2	...	We'll talk when you get here.
14	14	4	+61417692485	5	1726318507084	1726318507000	0	1	-1	1	0	Okay, I'm on my way.
15	15	5	+61458230941	...	1726318530873	1726318531000	0	1	-1	1	0	You're overdue on the payment. We agreed you'd have it by tonight.
16	16	5	+61458230941	...	1726318551689	0	...	1	-1	2	...	I'm working on it. I just need a bit more time.
17	17	5	+61458230941	...	1726318563835	1726318564000	0	1	-1	1	0	Time's up, Alex. You don't want to see what happens if you keep stalling.
18	18	5	+61458230941	...	1726318574996	0	...	1	-1	2	...	I'll have it by tomorrow. Please, just one more day.
19	19	5	+61458230941	...	1726318588633	1726318588000	0	1	-1	1	0	Fine. One day. But after that, we're done talking.
20	20	5	+61458230941	...	1726318602541	0	...	1	-1	2	...	Thank you. I won't let you down.
21	21	4	+61417692485	5	1726318688949	1726318689000	0	1	-1	1	0	I'm just outside. I can't take this anymore, Alex. You promised you'd choose me.
22	22	4	+61417692485	...	1726318705775	0	...	1	-1	2	...	Sophia, please, I need time. We'll talk, but not like this.
23	23	4	+61417692485	5	1726318716247	1726318716000	0	1	-1	1	0	No, I need to know now. It's either me or her.
24	24	4	+61417692485	...	1726318729430	0	...	1	-1	2	...	Come up, we'll talk. But you need to calm down.
25	25	4	+61417692485	5	1726318740656	1726318740000	0	1	-1	1	0	I'm calm, but I don't think you understand what this means for me. You can't just toss me aside.
26	26	4	+61417692485	...	1726318761732	0	...	1	-1	2	...	I'm not tossing you aside. Let's talk when you get here.

Figure 26, Alex's sms list

As we can see in the database above there were some interactions that Alex had with messages on his mobile phone, we can identify one conversation with Lily that starts Sat 14 Sep 2024 12:51:36 PM UTC and ends Sat 14 Sep 2024 12:53:03 PM UTC, two with Sophia, which starts Sat 14 Sep 2024 12:53:34 PM UTC and ends Sat 14 Sep 2024 12:55:07 PM UTC; the second one starts Sat 14 Sep 2024 12:58:08 PM UTC and ends Sat 14 Sep 2024 12:58:08 PM UTC and ends Sat 14 Sep 2024 12:59:21 PM UTC and one with an unknown number, which is not in the contact list and does not refer to any name, however, we can see the registered phone number

which is +61458230941, the conversation starts Sat 14 Sep 2024 12:55:30 PM UTC and ends Sat 14 Sep 2024 12:56:42 PM UTC. This number is not even the ones which Alex deleted.

15. What Internet searches has the owner of the phone made?

Using the command: 'Find /mnt/e01 -name "\*\*History\*\*"', we can see that there are 2 documents that can give us access to Alex's web history, the one we are most interested in is 'History', when we open it we can see that it manages to block some numbers that may be related to the deleted contact list in the screenshots above, the searches were as follows:

- California Community Colleges Chancellor's Office
- nearest campus security office - Google Search
- Android Archive or delete messages, calls, or voicemails - Android - Google Voice Help
- How to delete messages permanently on Android - Google Search
- Block or unblock a phone number - Phone app Help
- emergency loan options for students - Google Search
- Phones in Phones With Plans - Walmart.com
- how to delete messages permanently on android
- how to block calls from a specific number
- emergency loan options for students
- cheap burner phones near me

16. Is there other evidence on the phone that might indicate the role of the owner in Alex's death?

There is a particular file 'bigTopDataDB.1204881091-wal' that when verified in a text editor we can see that there are fractions of emails where Alex maintained communications with various people, this may also be key to the investigation, however, they are only fractions and the conversations are not complete:

#thread-f:1810175122003025626 msg-f:1810175122003025626 [cm363478@gmail.com](mailto:cm363478@gmail.com)

From: Oliver Marshall

Final Warning

Alex, This is your final warning. I've spoken to the bank, and if you don't start showing some responsibility, I'm pulling the plug on your account. I'm done funding your reckless ...

#thread-a:r-7537124641970367694 msg-a:r-6039400458804423887 [sr8640171@gmail.com](mailto:sr8640171@gmail.com)

To: ht317117@gmail.

I'm Sorry

Lily, I'm sorry for everything. I know I've hurt you, and I hate that I've let things get this far. I don't want to lose you, but I don't know how to fix this mess. I've been under a lot of pressure, and I've made some decisions. You deserve better than what I've given you. I want to talk tomorrow and figure out a way forward. Please, don't give up on me just yet....

#thread-a:r-7237313750365217425 msg-a:r5220043711744680689 [sr8640171@gmail.com#](mailto:sr8640171@gmail.com#)

To: vb9945311@gmail.com

We Need to Talk

Sophia, We need to talk. Things have gotten too complicated, and I don't know how to handle it all. I've made mistakes, and I need to set things right. I care about you, but I can't keep leading you on. We need to be honest with each other about where this is going. I don't want to hurt you, but I'm not sure what else to do. Let's talk tonight and figure out what happens next .....

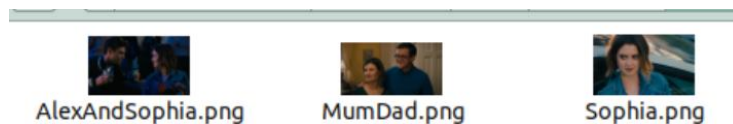
#thread-f:1810175188739464079 msg-f:1810175188739464079 saul46811@gmail.com

From:Saul Reynolds

Urgent: Academic Integrity

Alex, I've been informed that there are serious allegations against you regarding the sale of exam answers. This is a direct violation of the university's academic integrity policy. I need to ....

In addition, we found in the download folder some photos that link Alex and Sophia, there is also a photo of their parents, along with these documents there is one called 'recording.aes', this document may be fundamental to the investigation, when we open it, we see that it is encrypted, for this reason it is essential to see the contents of it. To decrypt it, we will need the initial vector and the key that is somewhere on the evidence. Unfortunately, by this time I could not find the key. However, I truly believe that Alex knew something was about to happen, that's why he took all the precautions to distribute the keys in different ways.



*Figure 277, Alex photos*

### **Additional Questions**

17. Conduct a timeline analysis of the pieces of evidence.

We can see that there is a record of events since February 2024 when we are presented with the first documents that show that Alex's life was not organised and things were not going as he expected, because of this, he had to do things he did not like at the university, selling exams was a help for his economic situation. From this event, Alex is involved in a series of events that were sinking him more and more, probably he could not get out of many debts that were increasing since he had a record of all debts. In August we can see that he started to have new devices such as a computer or a mobile phone, as we can see in the internet capture, he was still selling exams to people who did not trust him. In addition, it is here where he deleted a fundamental file from his computer, which at the time of the analysis we can see that it was his last will and testament, making it known that he was in danger. The last communication he had was on 14/09/24 with an unknown number but linked to the biggest debt he had and the message was a threat for non-payment.

Description	Date	Hour (If provided)
Alex's journal 1	28/2/24	
Alex's dad dissapointing email	3/10/24	
University warning	15/3/24	
Expenses march file	31/3/24	
Internship Offer	1/4/24	
Alex's journal 2	4/5/24	
Alex's mom letter	4/5/24	
Lily Parker debt (300)	10/4/24	
Credit card 1 debt (1200)	15/4/24	
Credit card 2 debt (800)	20/4/24	
Friends debt (150)	25/4/24	
Private loan debt (5000)	30/4/24	13:04:14
Windows instal date	27/8/24	13:05:43
last login on windows	27/8/24	13:15:35
Privatenotes.txt deleted from documents	27/8/24	13:15:35
Rubish.zip deleted from documents	27/8/24	07:57:11 - 08:08:45
Cheat chat (Dormking, PartyDude, AlexM21, BookWorm)	1/9/24	08:09:28 - 08:12:26
Private Chat with Sophia alias ArtLover99	1/9/24	08:20:53 - 08:23:51
Private Chat with Lily	1/9/24	08:16:09 - 08:46:20
Private chat between DormKing and PartyDude	1/9/24	8:42:54
sslkeyfile transferred from FTP protocol	1/9/24	10:58:53 - 10:59:02
calls to Lilly	14/9/24	10:59:22
call to sophia, duration 1:10	14/9/24	
Messages (SMS) with Lily	14/9/24	
Messages (SMS) with Sophia	14/9/24	
Message (SMS) with +61458230941	14/9/24	

18. Provide a brief final analysis of the evidence and your conclusions.

When analyzing all the pieces of evidence we can have some people involved in the case, the most direct culprits are Lily and Sophia as they had a more frequent communication with Alex, however, this does not mean that they are the culprits in question, there are more people involved such as the colleagues who needed the answers to the exams or the unknown number that gave him an ultimatum for Alex to pay his debt, debt which we can see in his computer that reached 5000 dollars, This theory gains strength because Alex knew that something bad could happen to him because he had a document on his computer that stated his will and justified his actions to his parents, Lily, and Sophia. There are also blocked contacts and from Alex's internet searches we know that he was trying to eliminate all traces of these people and knew that his life was in danger. Finally, the series of factors that came together, such as debts, the discovery of his fraud

at university, his affairs, which could be true, but it cannot be ruled out that Lily had discovered his relationship with Sophia and tried to try on Alex's life, and the pressure he was under from his father, are all critical factors.

## Task 2

- **Introduction**

The main objective of this report is to make known the processes that disk forensics and file carving have, in addition to their advantages and disadvantages, recommendations, and guidelines with the case of Alex Marshall. This technique is critical in digital forensics since it allows focusing on the extraction of documents that may have been intentionally deleted or hidden, it is also useful for recovering data bit by bit, and sometimes it is essential for cases of criminal investigation, fraud, or security breaches.

Obtaining digital evidence like this makes it extremely important in the case of Alex Marshall since we can investigate possible facts based on recovered files or even files saved within their operating system, with the help of file carving tools, we can draw small hypotheses of what happened or what background the victim had, in this case when analyzing this type of evidence we see some letters where they show that he began to have financial problems at the beginning of the year, this added to the pressure from his parents and the investigations of the university for accusations of selling exams makes Alex be in an uncomfortable position.

- **Evidence Acquisition**

The acquisition of this type of digital evidence, especially when dealing with large devices, is essential and fundamental for a concrete and fruitful analysis. For this reason, there are methods or tools that help us facilitate this process.

As a first point, imaging the disk is an exact copy at the bit level, that is, an identical copy of the disk must be made in order to have and ensure that the data is and will be properly transferred in the same original position, ensuring that at the time of the copy, it is not disorganized or there are data leaks.

Write blockers can also be considered, which help ensure the integrity of the copied data; this technique helps us prevent the loss of data from the copied image. Finally, to keep track of this entire process, a chain of custody must be maintained, in order to have traceability from the beginning of the process to its end, the people involved and the tools used for effective data collection.

Returning to our case, the acquisition process and the time since Alex's death is essential because the more time passes, the more likely it is that someone will try to modify or destroy evidence where Alex's name is involved with the alleged murderer. For this reason, one of the advantages of the acquisition is to maintain efficient traceability, so we can know through whose hands Alex's order passed, also with the proper technique we are sure that the copy was made in a complete and integrated way, bit by bit, with which we can ensure that it is full and we could work in a better way within it, there are even indications that Alex himself wanted to eliminate some documents, this technique is further discussed later in the analysis, however, it is important to mention that the copy is safe and has maintained a well thought out chain of custody for this type of case where the integrity of the evidence is paramount.

- **Forensic Analysis**

After having a secure and complete copy of the disk, the parts of it must be analyzed, for this various data analysis techniques are used. In Linux, the system must be mounted in special folders where we can work with the system. One of the problems with this type of disk is that they come fragmented, this can violate the total integrity of the disk since corrupting one would not fit.

When mounting the complete system, the partitions of the same disk must be analyzed to see from which bit the data is what we want to analyze and thus be able to mount it in a way that benefits us for the analysis. Linux provides us with various tools to be able to execute this type of action, commands such as 'img\_stat' to see the type of image we are working with, or 'mmls' to see the disk partitions and know from where to mount the system in Linux are useful tools to identify these first steps.

To successfully mount the disk image, 'mount' is used. To do this, you must have privileged access or superuser 'sudo'. With this tool, the entire system is basically mounted from the bit indicated, in this case, it is in the 'Basic Data' partition.

Once the system is mounted, you can proceed to the digital forensic analysis. There are several methods to investigate the data. It is always important to examine the disk records to know which platform or operating system we are working on. A useful tool is 'rip.pl'. This helps us to verify the information within all the data and shows us the path where we can investigate. Due to its options, this tool can filter everything, then throws out the specific data if it is given a unique record. This is how we can see the Windows version of the disk the name of the computer, or even the name of the registered users. In the case of Alex, it is important to verify that this system was Alex's own, this tool gives us through grep which is a search filter the option to verify the accesses and the users, so we can say that it is Alex's computer.

The system being mounted within Linux, can be broken down into folders, this allows us to see and analyze the documents and applications that this system manages, making this tool more visible and dynamic for a forensic investigation.

All this analysis is an important part of the investigation of each case; therefore, the general context must always be analyzed, Alex had important documents to analyze within it such as letters, account statements, job offers, and warnings from the university, this allows you to investigate the victim's life more thoroughly and you can have more clues about his death. By delving into a system that the victim had daily, hypotheses can be verified or people involved in his life can be found. With this, the continuity of the case can be easier since the interactions that he had during his life are known.

- **Forensic Tools**

The forensic tools available on the market are vast, and each investigator can have a different method, with this it means that there is no strict and unique process to be able to find out certain specific information. There are several tools that facilitate the obtaining of data, but the reflection that the investigator has with the use of the same tools, the correlation that he gives to the specific case, the knowledge of the previous facts, and the conclusions that this type of data can help us to obtain always prevail.

In Alex's case, data recovery tools from the recycle bin were used, and copies of the disk were created so as not to work on top of the mounted system since the integrity of the same could be

altered. To recover documents, a common password cracking tool for zip files is 'fcrackzip'. This tool uses a brute force attack to discover the credentials and thus see the files that this document was hiding.

Another tool that we can use, more visible, is direct navigation within the mounted system, so we can see the personal documents folder that Alex had where key documents were recovered, such as his own journals, where he explains that he is deep in debt and has resorted to selling exam answers at the university, emails from his parents where they express that his grades do not reflect the human being that he is, an internship offer, his monthly expenses, and the debts he had at that time.

Within an investigation as delicate as this, this type of information is important since we can know the actions he had in the past, the possible involvement with people who may have lent him money, and even his intrapersonal relationships with friends, family, or romantic relationships.

It is important to mention that there are also tools such as 'find', 'grep' or 'hex editor' that help us to filter or edit very important documents, especially the latter, as it serves to see the distribution of data hexadecimally, this makes us to see files that at first glance may be encrypted but simply are with extra bit that we can remove and see the main content of each file, this technique helped us to see the will of Alex and makes us see that he had a feeling that something bad could happen to him.

Each tool used has advantages and disadvantages, limitations in its use, and due to the amount of information being used, sometimes phantom information is investigated, and a lot of time is spent trying to find out something that is not relevant to the investigation, constant research and training by experts in new technologies is essential to obtain the best results.

- **Conclusions**

Disk forensics and file carving are indispensable in digital investigations, providing critical evidence that can be pivotal in legal proceedings. The field is continuously evolving, with advancements in tools and techniques enhancing the efficiency and accuracy of forensic analysis.

The evidence from Alex's computer gives us a brief introduction to the victim's life, the investigation into the data or documents that Alex had in his possession, makes us have some small nuances that already begin to involve people and what Alex's life was like, this makes us suppose and draw hypotheses about what could have happened and why, having a background for future evidence is essential for the investigation.

This field of forensic investigation is essential since by handling the information we can reach conclusions for each case, the carving file tools are improving every day, and the interpretation, training, and self-study of them is the responsibility of the person in charge of the investigation, therefore, investigators must be aware of the improvements of the same, updating their knowledge day by day and delving into the investigation. In any case, taking ownership of the case is a good technique to be able to better discover essential data.

Future directions include the development of more sophisticated algorithms for fragmented file recovery, increased automation, and the integration of AI to handle large datasets more effectively.

## Bibliography

- Bajpai P. (2014). *Windows registry forensics using 'RegRipper' command-line on Linux*. Infosec Resources. <https://www.infosecinstitute.com/resources/digital-forensics/registry-forensics-regripper-command-line-linux/>
- File Info Base. (2024). **VMEM file extension - How do I open it?** File Info Base. <https://fileinfobase.com/extension/vmem>
- GeeksforGeeks. (n.d.). *unzip command in Linux*. GeeksforGeeks. <https://www.geeksforgeeks.org/unzip-command-in-linux/>
- GeeksforGeeks. (n.d.). *mkdir command in Linux with examples*. GeeksforGeeks. <https://www.geeksforgeeks.org/mkdir-command-in-linux-with-examples>
- GeeksforGeeks. (n.d.). *cat command in Linux with examples*. GeeksforGeeks. <https://www.geeksforgeeks.org/cat-command-in-linux-with-examples/>
- GeeksforGeeks. (n.d.). *mount command in Linux with examples*. GeeksforGeeks. <https://www.geeksforgeeks.org/mount-command-in-linux-with-examples/>
- How-To Geek. (2023, September 11). *How to use the find command in Linux*. Retrieved October 8, 2024, from <https://www.howtogeek.com/771399/how-to-use-the-find-command-in-linux/>
- Kali Linux. (n.d.). *fcrackzip*. Kali Tools. Retrieved October 8, 2024, from <https://www.kali.org/tools/fcrackzip/#:~:text=fcrackzip%20is%20a%20fast%20password%20cracker%20partly%20written>

Mehrnoush. (2022, July 26). *Windows Recycle Bin forensics*. Medium.

<https://medium.com/@mehrnoush/windows-recyclebin-forensics-a0855b957a31>

SleuthKit. (n.d.). *img\_stat command*. SleuthKit.

[https://sleuthkit.org/sleuthkit/man/img\\_stat.html#toc2](https://sleuthkit.org/sleuthkit/man/img_stat.html#toc2)

TheLinuxCode. (2023). *How to use the md5sum command*. TheLinuxCode.

<https://thelinuxcode.com/use-md5sum-command/>

Volatility Foundation. (2024). **Volatility: An advanced memory forensics framework**. GitHub.

<https://github.com/volatilityfoundation/volatility>

Wireshark Foundation. (n.d.). *About Wireshark*. Wireshark. <https://www.wireshark.org/about.html>