



TDX ARENA

Certification Report

Case: Imperial Memory

08/07/2024

Executive Summary

Jules, a cyber researcher, left his office on a way to a new job; and at his farewell party, I approached him and asked what the secret to his success was. Jules promised the next day the answer would be on my desktop. When logging into my desktop the next day, I discovered a file with a note from Jules to always keep this in your memory.

The objective of this investigation is to thoroughly examine the files Jules left on my desktop and unravel the mystery of his success. This task requires a detailed analysis of the documents, piecing together clues, and understanding the underlying principles that propelled Jules to his esteemed position. By meticulously reviewing the provided information, I hope to uncover valuable insights and strategies that contributed to his achievements, ultimately applying these lessons to my own professional growth.

Findings and Analysis

Present the findings relevant to the investigation in a structured and detailed manner. For each finding, explain its cybersecurity context and its significance to the investigation.

Finding	Finding Details	Description
Zip File	gift.7z	A compressed file utilizing 7-zip, a free and open-source file archiver software used to compress and decompress files.
This is how Jules packaged his test for me after I asked for the secret to his success. 7-zip is a program that allows a user to compress one or more files into smaller sizes. This program allowed Jules to compress several folders and files into (1) file, and then secure that file further requiring a password to obtain the data.		
Finding	Finding Details	Description
Hash	md5sum	A widely used cryptographic hash function that produces a 128-bit (16-byte) hash value from input

		data.
--	--	-------

This is how we were able to find the hash flag for the challenge. Like the description says, this is a widely used function that produces a hash of a file that is unique to the data within it. If data is altered the hash would be different.

Finding	Finding Details	Description
Strings	Command line tool.	This command-line tool scans files and prints sequences of printable characters, which can be useful for finding hidden text in executables or memory dumps.

The Emperor.vmem file held the password to extract the files from the gift.7z zip file. In order to get this information, a strings command had to be run on the file to find the data in a legible form.

Finding	Finding Details	Description
vmem	Virtual Memory	A file format that contains the state of a devices RAM at a specific point in time, useful for debugging, analysis, and forensic investigations.

Emperor.vmem was a file on our desktop when we launched our machine. This was likely put on our desktop by Jules along with the gift.7z zip file as it contained valuable information to obtain access to the document inside. Vmem files are incredibly useful in forensic investigations as they will have information on systems or machines at any given point in time.

Methodology

Tools and Technologies Used

List and describe the tools and technologies employed in the investigation, including a brief explanation of why they were used.

Zip File: A compressed file format used to store one or more files or folders in a smaller size. It uses compression algorithms to reduce file size, making it easier to transfer and store data.

Strings: A command-line tool used to extract readable text from binary files. It scans files and prints sequences of printable characters, which can be useful for finding hidden text in executables or memory dumps.

Volatility: An open-source memory forensics framework used for analyzing memory dumps. It helps investigators extract digital artifacts from volatile memory (RAM) to understand system activity, recover data, and investigate incidents.

Vmem: A file format used to store the contents of a device's virtual memory. It captures the state of the device's RAM at a specific point in time, useful for debugging, analysis, and forensic investigations.

Md5 Hash: A widely used cryptographic hash function that produces a 128-bit (16-byte) hash value from input data. It is commonly used for verifying data integrity by comparing hash values to ensure that data has not been altered.

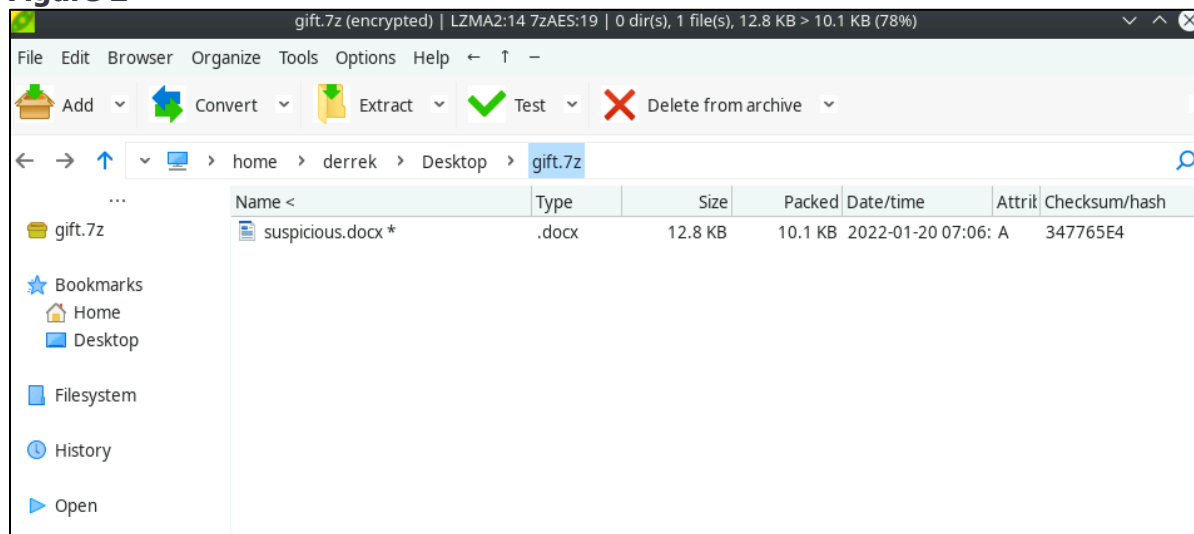
Investigation Process

1. When starting our machine, we see an Ubuntu desktop with (2) interesting files (Figure 1). Emperor.vmem, a virtual memory dump of what I can only assume is from Jules; and gift.7z, a zip file with a document called 'suspicious.docx' inside (Figure 2).

Figure 1

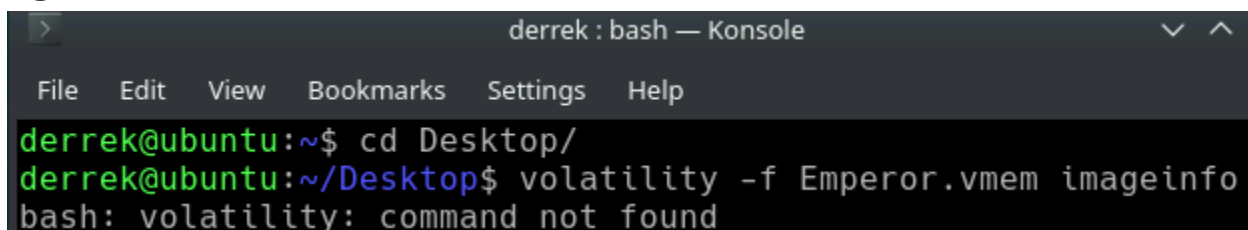


Figure 2



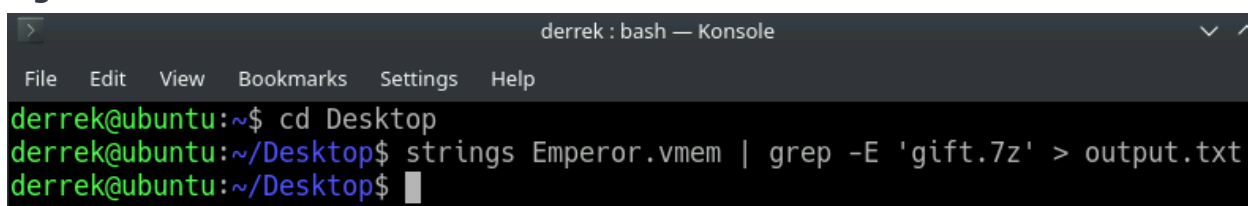
2. We are unable to extract the docx file from the zipped folder without a password, and my immediate thought is to check the Emperor.vmem file on the desktop to see if it has a password for the document extraction.
3. I attempted to utilize the volatility command, but was advised the command was not found (Figure 3)

Figure 3



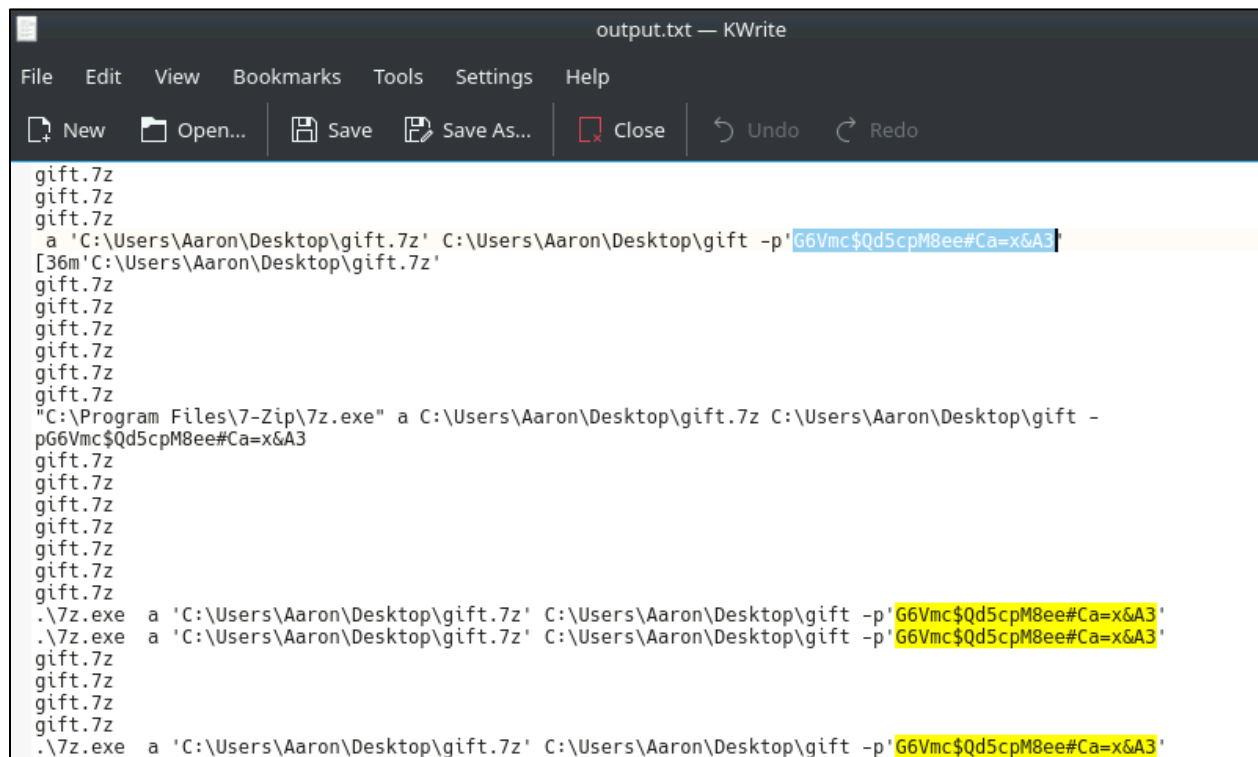
4. After volatility failed, I went to use strings as an attempt to find the information I needed in the file. I tried a few different words and phrases to find the password, but ultimately the best option to find the password ended up being the zip file name itself (Figure 4). I saved the output as a text document on my desktop for easier searching.

Figure 4



5. In the output file it was clear to find the password needed for the extraction indicated by "-p" after the filepath (Figure 5).

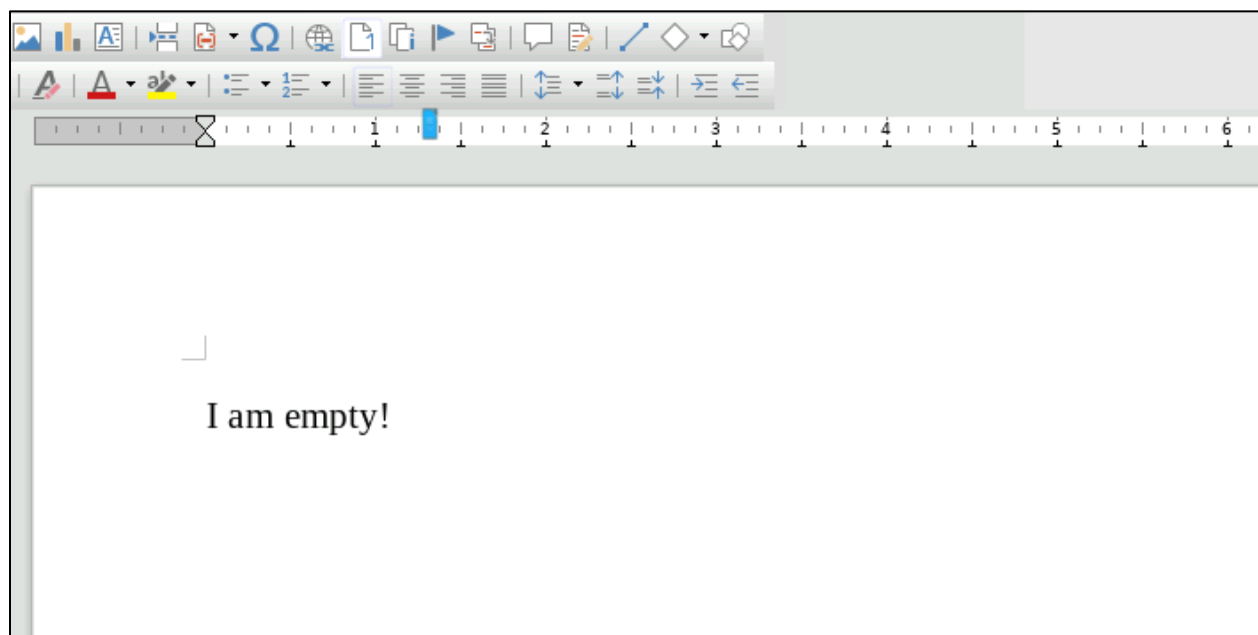
Figure 5



```
output.txt — KWrite
File Edit View Bookmarks Tools Settings Help
New Open... Save Save As... Close Undo Redo
gift.7z
gift.7z
gift.7z
a 'C:\Users\Aaron\Desktop\gift.7z' C:\Users\Aaron\Desktop\gift -p'G6Vmc$Qd5cpM8ee#Ca=x&A3'
[36m'C:\Users\Aaron\Desktop\gift.7z'
gift.7z
gift.7z
gift.7z
gift.7z
gift.7z
gift.7z
gift.7z
"C:\Program Files\7-Zip\7z.exe" a C:\Users\Aaron\Desktop\gift.7z C:\Users\Aaron\Desktop\gift -
pG6Vmc$Qd5cpM8ee#Ca=x&A3
gift.7z
gift.7z
gift.7z
gift.7z
gift.7z
gift.7z
gift.7z
.\7z.exe a 'C:\Users\Aaron\Desktop\gift.7z' C:\Users\Aaron\Desktop\gift -p'G6Vmc$Qd5cpM8ee#Ca=x&A3'
.\7z.exe a 'C:\Users\Aaron\Desktop\gift.7z' C:\Users\Aaron\Desktop\gift -p'G6Vmc$Qd5cpM8ee#Ca=x&A3'
gift.7z
gift.7z
gift.7z
.\7z.exe a 'C:\Users\Aaron\Desktop\gift.7z' C:\Users\Aaron\Desktop\gift -p'G6Vmc$Qd5cpM8ee#Ca=x&A3'
```

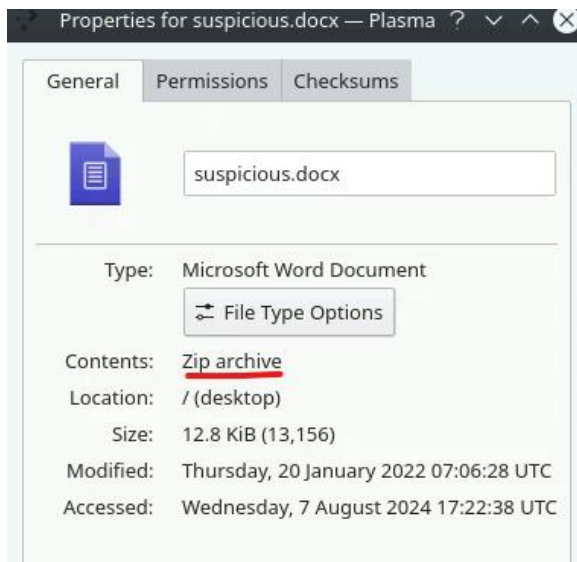
6. Using the password obtained I was able to extract the file to my desktop. When I opened the file, I was met with a disappointing message (Figure 6).

Figure 6



7. This then made me curious, so I clicked in to see the properties of the 'suspicious.docx' file, and found it hiding its true form as another zip archive (Figure 7).

Figure 7



8. Using the peazip tool (Figure 8), I was then able to extract another set of documents from this zip file (Figure 9).

Figure 8

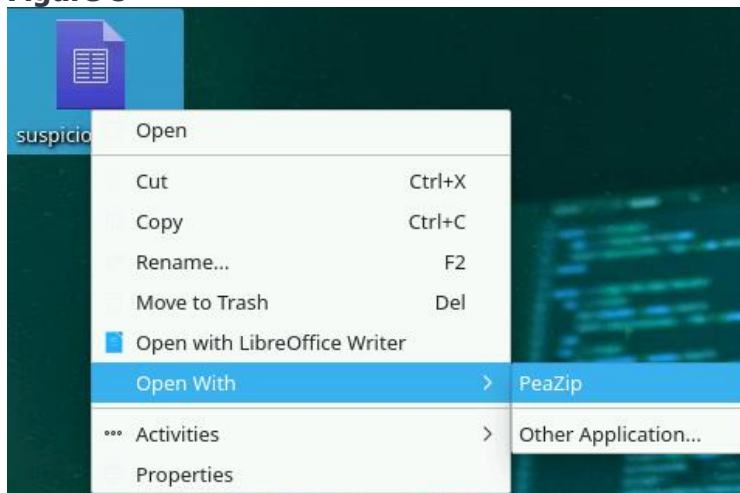
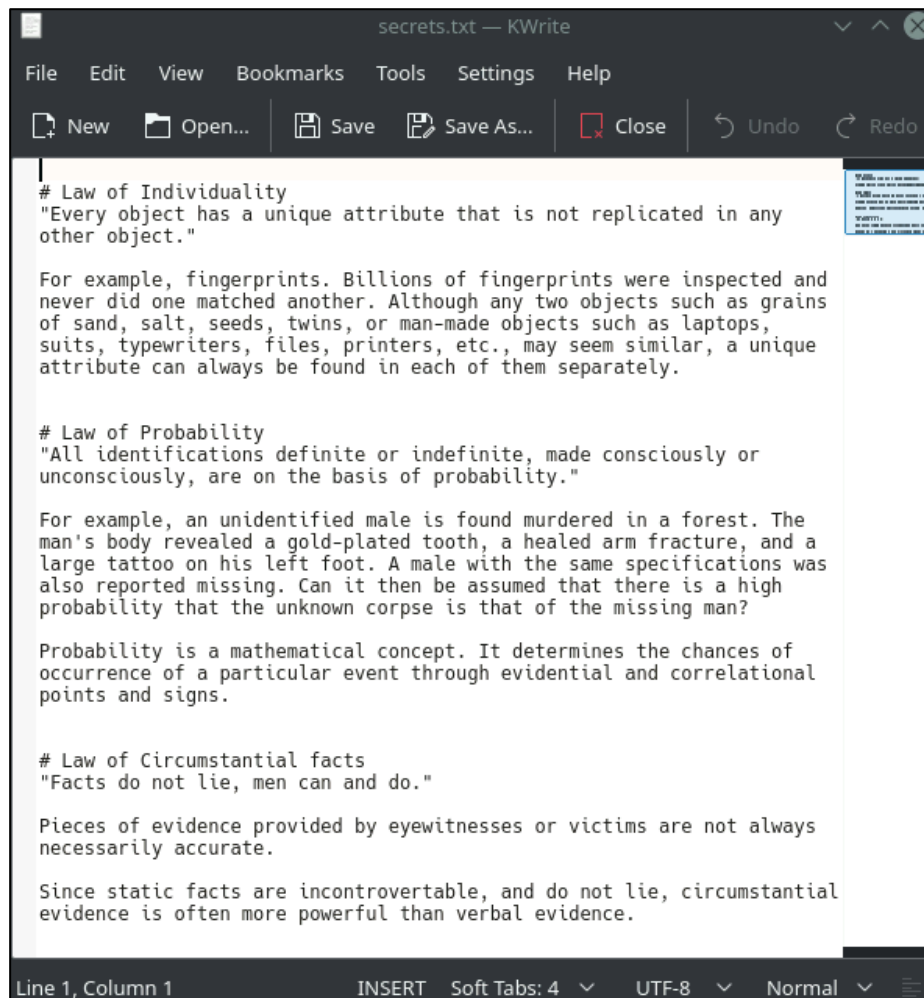


Figure 9



9. The directories that exported were either empty or had some .xml files with non-significant information in them. The more important document from the export was the file called 'secrets.txt'. Within this file was a list of a few inspirational quotes and examples that are ultimately the secrets to Jules' success (Figure 10).

Figure 10



10. At this point, I was at a loss. The secrets.txt document was the answer to the question I asked at the retirement party, but there is no flag to complete the challenge. After some time of frustration, and looking through all the other .xml files that were exported with it, I had an epiphany. My dad brain kicked in and I realized by asking for the secret to his success and him sending the secret text file, the file itself had to be the answer to the challenge. I ran an md5sum on the file and had my answer (Figure 11). I attribute this solution to dumb luck and a love for puns.

Figure 11

```
derrek@ubuntu:~/Desktop$ md5sum secrets.txt
0f235385d25ade312a2d151a2cc43865  secrets.txt
derrek@ubuntu:~/Desktop$ █
```

Recommendations

1. **Utilize Comprehensive File Analysis Tools:** When dealing with unknown or complex files, always use a combination of tools to ensure thorough analysis. Tools like Volatility for memory dumps and strings for extracting readable text can complement each other and provide a more complete picture.
2. **Practice Data Handling and Security:** Regularly practice and reinforce the use of secure file handling and encryption techniques. Always verify the integrity of files using cryptographic hashes like MD5, and secure sensitive data using strong encryption methods.
3. **Encourage Continuous Learning and Knowledge Sharing:** Foster a culture of continuous learning and knowledge sharing within the team. Encourage team members to share their insights, challenges, and solutions encountered during investigations.
4. **Improve Documentation and Reporting Skills:** Maintain detailed and clear documentation of the investigation process. This includes recording each step taken, the tools used, and the findings at each stage.