A close up of a sign

Description automatically generated

**COMP 5350**

**Digital Forensics**

**Hands-on Activity#** 1

Kate Moreland

kem0149

9/22/25

# Executive Summary

The following report shows the process of extracting active and deleted files from a disk image that was involved in the APT99 Central Bank heist. The files were recovered from two FAT16 partitions which led to the plans of the criminals.

|  |  |
| --- | --- |
| Q1. Specify the number and type of partitions on the disk image. | There are two FAT16 partitions on the disk image. |
| Q2. Specify the number of files, file names, and file size of each file on the partition. | The 3 files are email.log.odt, Bank.png, and Plan.zip. The size of email.log.odt is 19968 on partition 1. The size of Bank.png is 1907200 on partition 2. The size of Plan.zip is 1439 on partition 2. |
| Q3. Specify the starting and ending byte offset location of each file on the partition. | email.log.odt: Starting (1171456) Ending (1191424)  Bank.png: Starting(53743616) Ending(55650813)  Plan.zip: Starting(55652352) Ending(55653888) |
| Q4. For each FAT partition explain the contents of the File Allocation Table and Root Directory. | Partition 1:  The file allocation table shows that there is a buffer of 4 between the beginning of the Data Area and the location of the files. In the root directory it shows that there is one active file that is an email called email.log.odt.  Partition 2:  The file allocation table shows that there is also a buffer of 4 between the beginning of the Data Area and the location of the files. In the root directory, it shows that there is 1 active file called Bank.png and then there is one deleted file called Plan.zip. |
| Q5. Manually recover all files from each disk image. | dd if=captured\_image.dd of=email.log.odt bs=512 skip=2288 count=39  dd if=captured\_image.dd of=Bank.png bs=512 skip=104968 count=37215  dd if=captured\_image.dd of=Plan.zip bs=512 skip=108696 count=3 |
| Q6. Provide a thorough analysis of the recovered files: Determine the contents of these files to understand the objectives, the plan, and any other critical information about the hack. | The recovered files took us through the plan of the hackers. The first file was an email that was sent between the hackers about a change in the plans that is stored in a zip file. The password to the zip file, Phantom$123, is stated. The user says to delete the email but in the recovery process it is found to not be deleted. The second file is an image. The image is of the Bank that the hackers were targeting. The third file is a zip file that contains to .txt files. The plan.txt file is a list of the plan of how they are going to steal the money. The are able to take use of a buffer overflow error to enter the building. They were able to get access to internal network through a successful phishing attempt on a bank employee. They then access the financial system and then transfer money to offshore accounts. The address.txt file is a Base64 encoded message for the address of the bank. The address is Old Warehouse, Dock 9, New York, NY 10013, United States. |

# Table of Contents

[Executive Summary 2](#_Toc209465877)

[Table of Contents 5](#_Toc209465878)

[List of Figures 6](#_Toc209465879)

[List of Tables 8](#_Toc209465880)

[1 Detailed Analysis of Partition Allocation 9](#_Toc209465881)

[2 Detailed Analysis of Recovery Process 13](#_Toc209465882)

[2.1 Partition 1 File 1 13](#_Toc209465883)

[2.2 Partition 2 File 2 15](#_Toc209465884)

[2.3 Partition 2 File 3 16](#_Toc209465885)

[3 Description of Analysis Techniques Utilized 17](#_Toc209465886)

[4 Results and Discussion 18](#_Toc209465887)

[5 Conclusions and recommendations 18](#_Toc209465888)

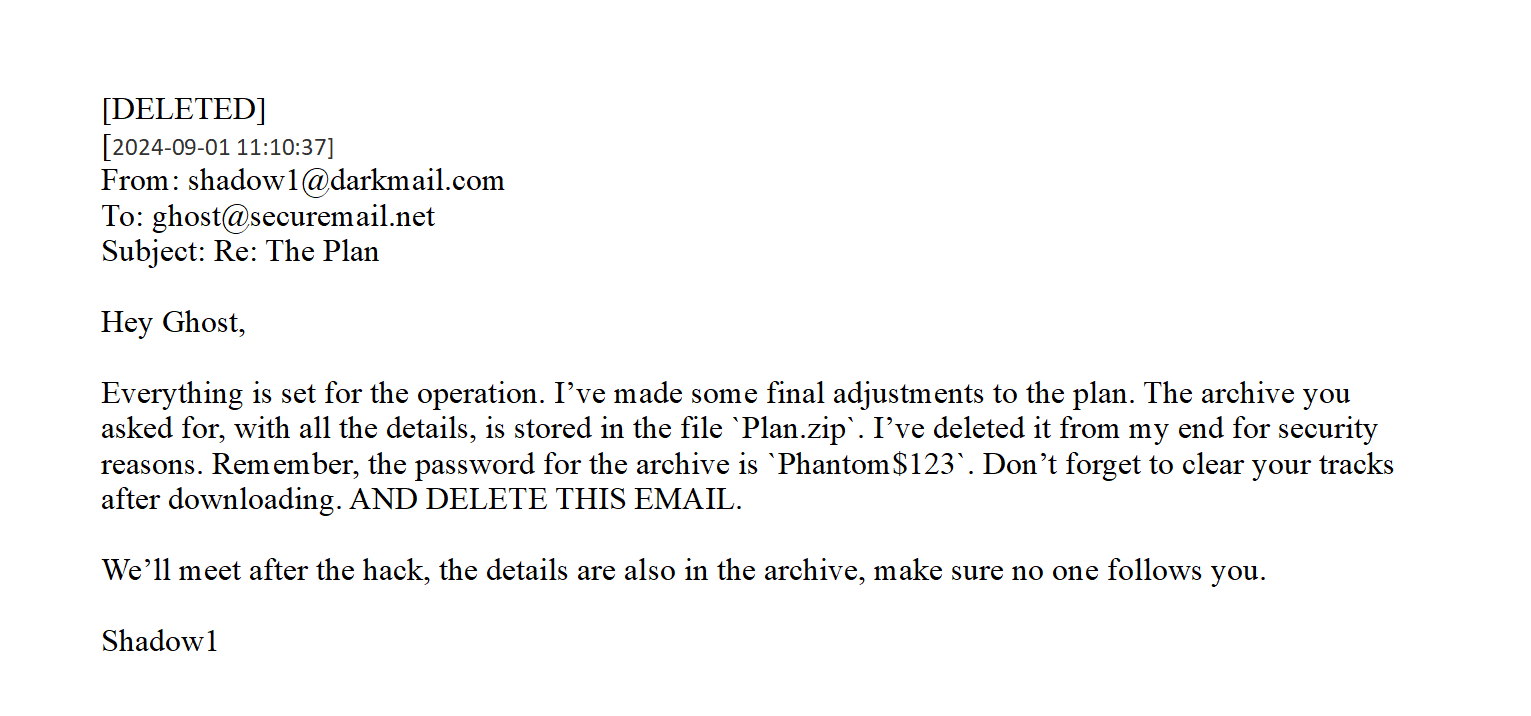
[6 Acknowledgements 18](#_Toc209465889)

[7 AI Use Statement 18](#_Toc209465890)

[8 References 19](#_Toc209465891)

# List of Figures

email.log.odt



Bank.png

A bank building with a sign

AI-generated content may be incorrect.

Plan.zip

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# List of Tables

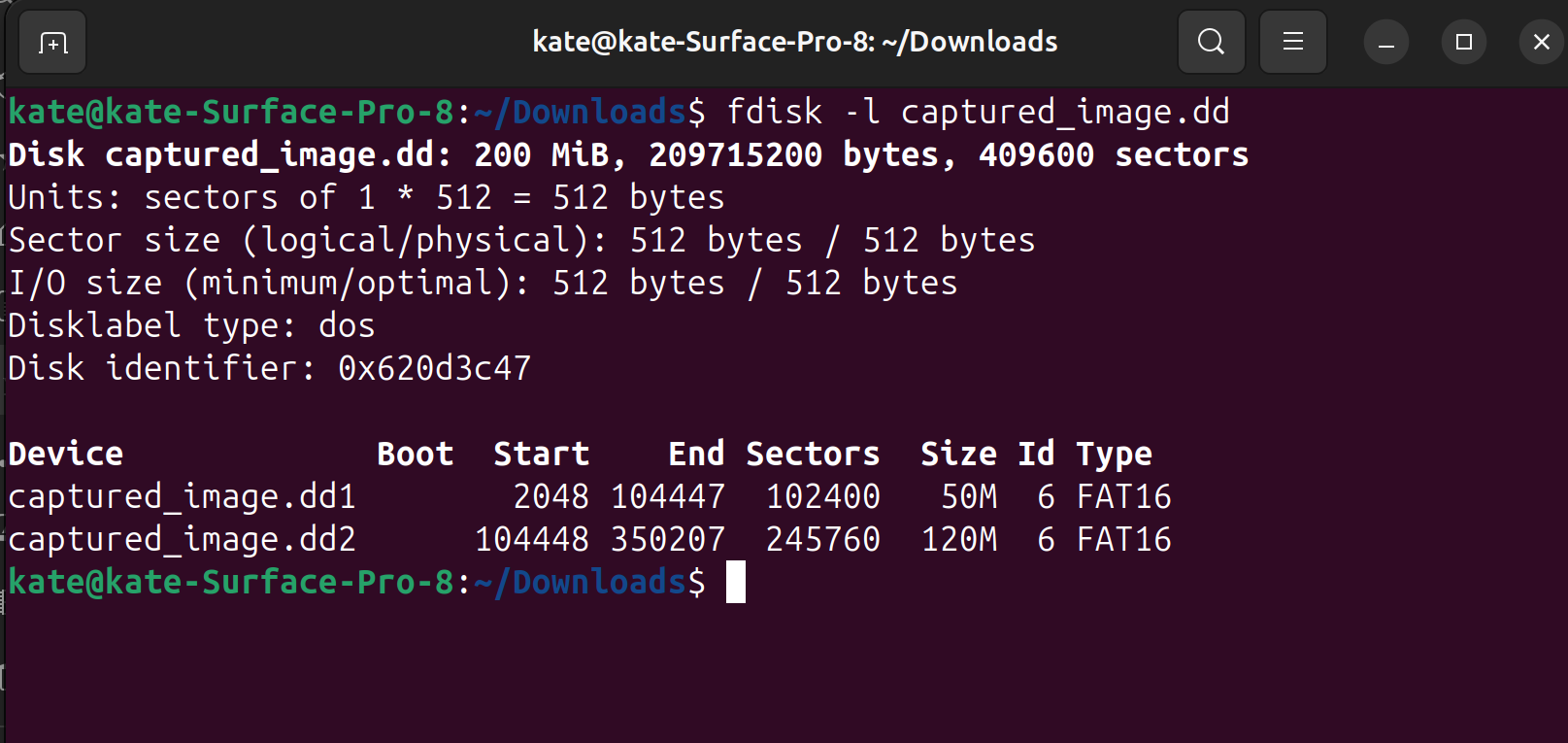
|  |  |  |
| --- | --- | --- |
| File Name | Starting Offset | Ending Offset |
| Email.log.odt | 1171456 | 1191424 |
| Bank.png | 53743616 | 55650813 |
| Plan.zip | 55652352 | 55653888 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Disk Information | Reserved Area | 1st FAT area | 2nd FAT area | Root Discovery | Data Area |
| 0-2048 | 2048-2052 | 2052-2152 | 2152-2252 | 2252-2284 | 2284-104447 |
| 0-2048 | 104448-104452 | 104452-104692 | 104692-104932 | 104932-104964 | 104964-350207 |

|  |  |  |
| --- | --- | --- |
| File | Confirmation Command | Recovery Command |
| email.log.odt | hexdump -C -s $((2288\*512)) -n $((39\*512)) captured\_image.dd | dd if=captured\_image.dd of=email.log.odt bs=512 skip=2288 count=39 |
| Bank.png | hexdump -C -s $((104968\*512)) -n $((3725\*512)) captured\_image.dd | dd if=captured\_image.dd of=Bank.png bs=512 skip=104968 count=37215 |
| Plan.zip | hexdump -C -s $((108696\*512)) -n $((3\*512)) captured\_image.dd | dd if=captured\_image.dd of=Plan.zip bs=512 skip=108696 count=3 |

# 1 Detailed Analysis of Partition Allocation

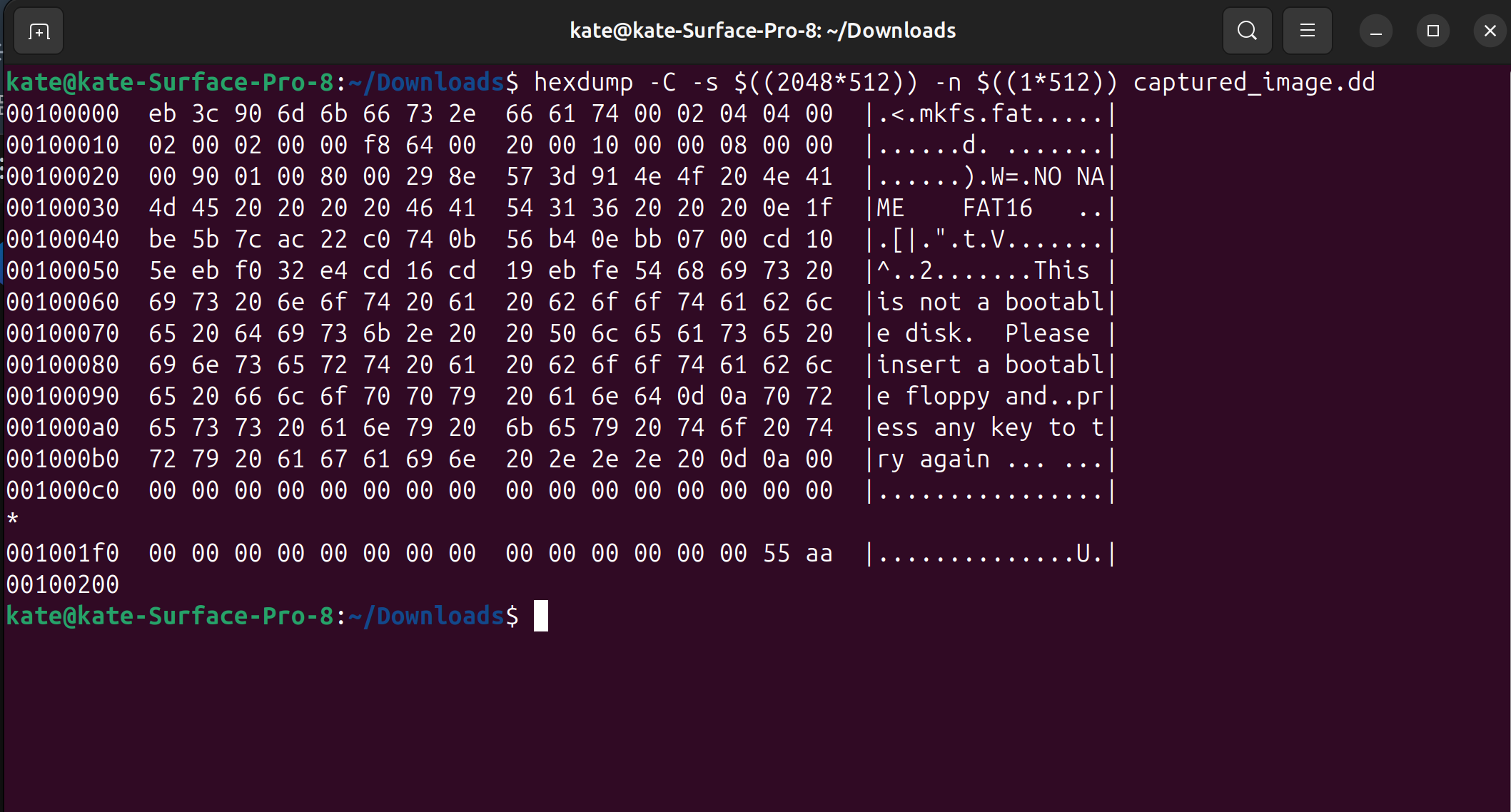
There are two partitions in the image. They are both type FAT16. You can see that the sectors before partition are 2048 because that is when the first partition starts. Below is an image of the partitions with descriptions of where the partitions start and end.





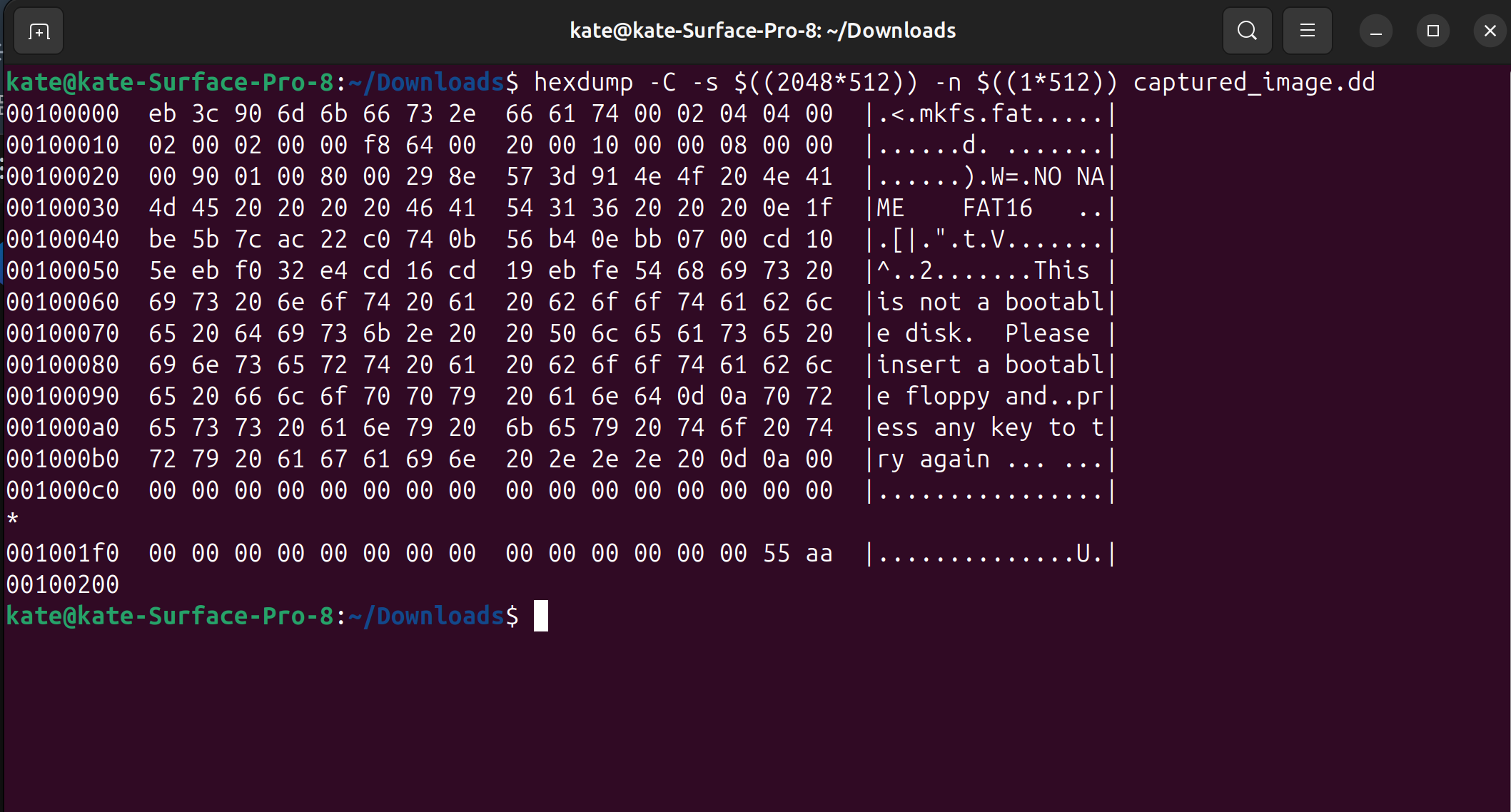
**Partition 1:**

I was able to see the disk information by typing in the following command “hexdump -C –s $((2048\*512)) -n (512\*1)) captured\_image.dd”. I found the bytes/sec by looking at the location 000Bh for 2 bytes which is 0002 then do big endian and it is 512(0x0200).



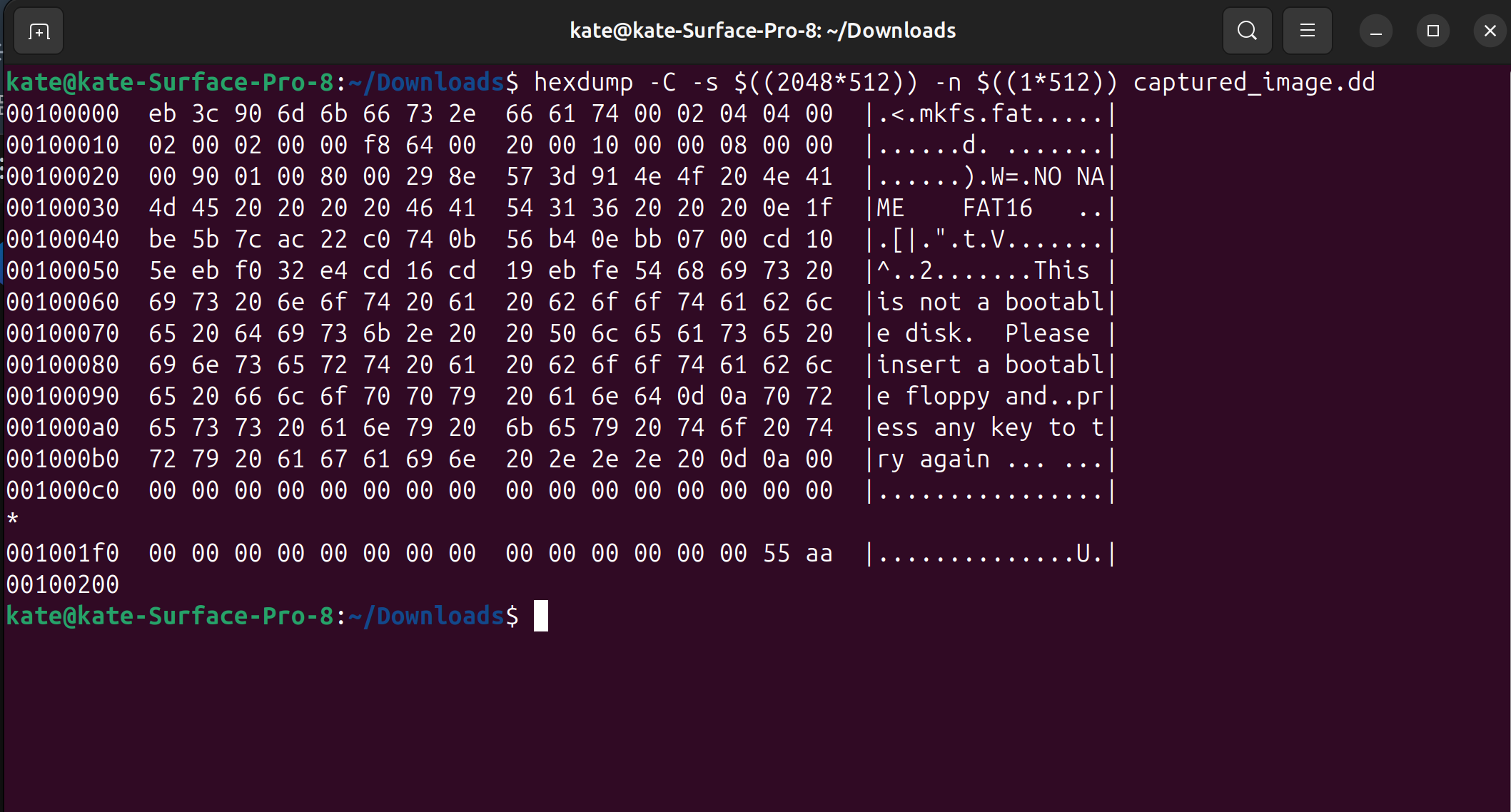


I found the number of sec/cluster by looking at the location 000Dh for 1 byte which is 04. In decimal it is the same so the answer is 4.



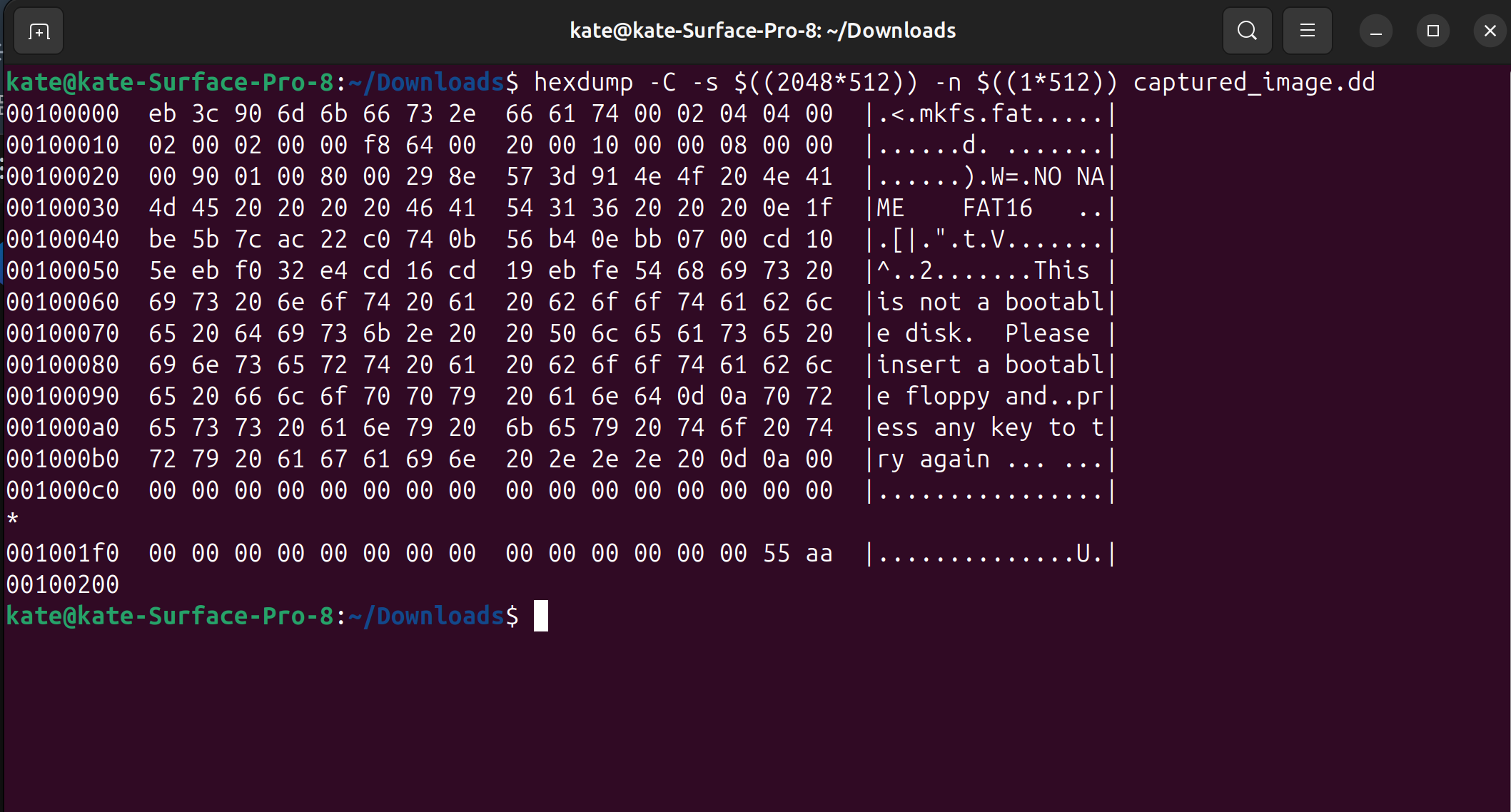


I found the reserved sectors by looking at location 000Eh for 2 bytes. It is 0400 and when you do bid endian you get 4 (0004).





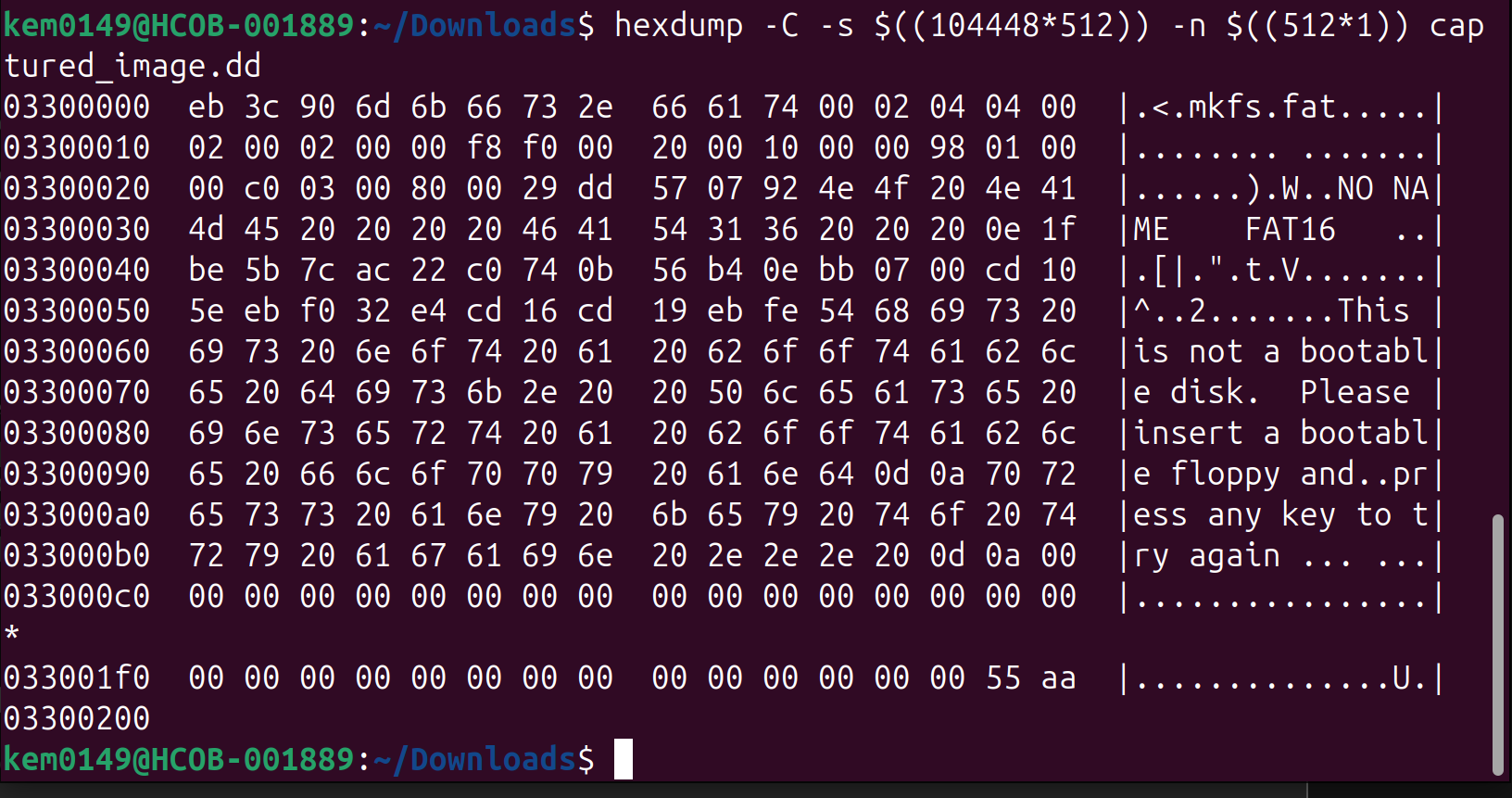
I found the sec/fat by looking at location 0016h for 2 bytes. It is 6400 and when you do big endian you get 100 (0064).





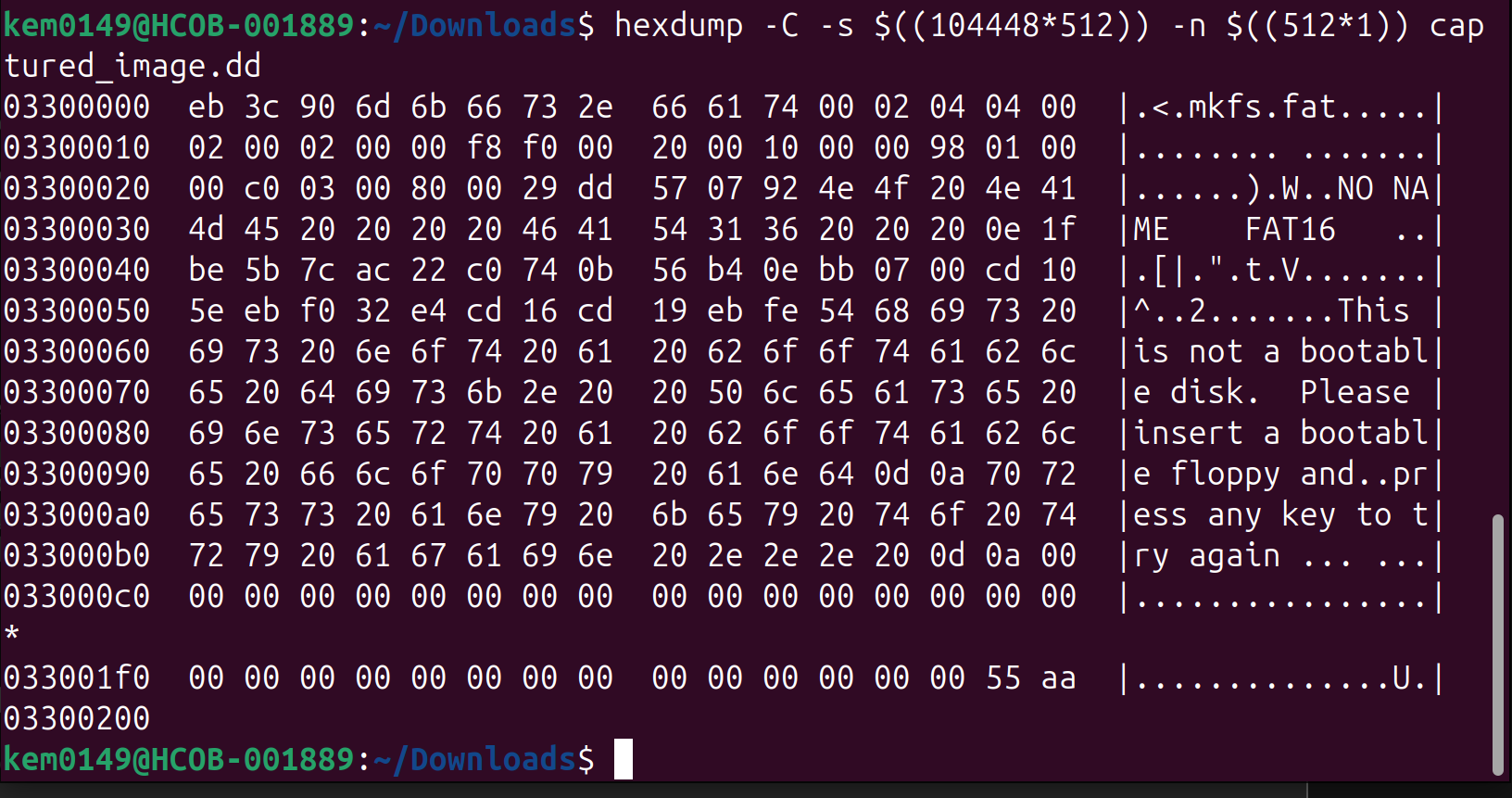
**Partition 2:**

Now to analyze the 2nd partition’s map. To find this type hexdump –C –s $((104448\*512)) -n $((512\*1)) captured\_image.dd. The bytes/sector are the same 0200 (512) located at 000Bh.



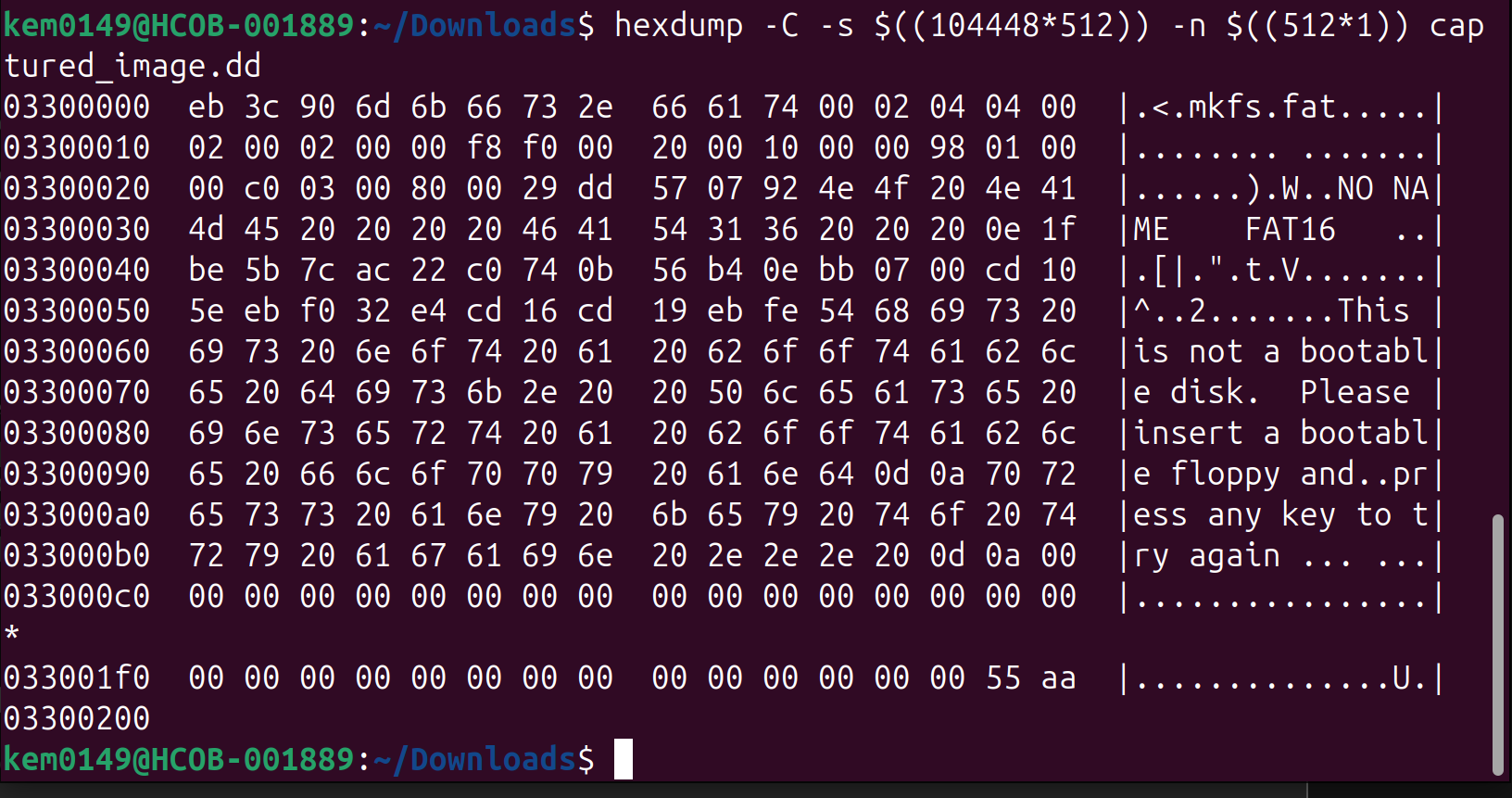


The sec/cluster are also the same at 4. This is located at 000Dh



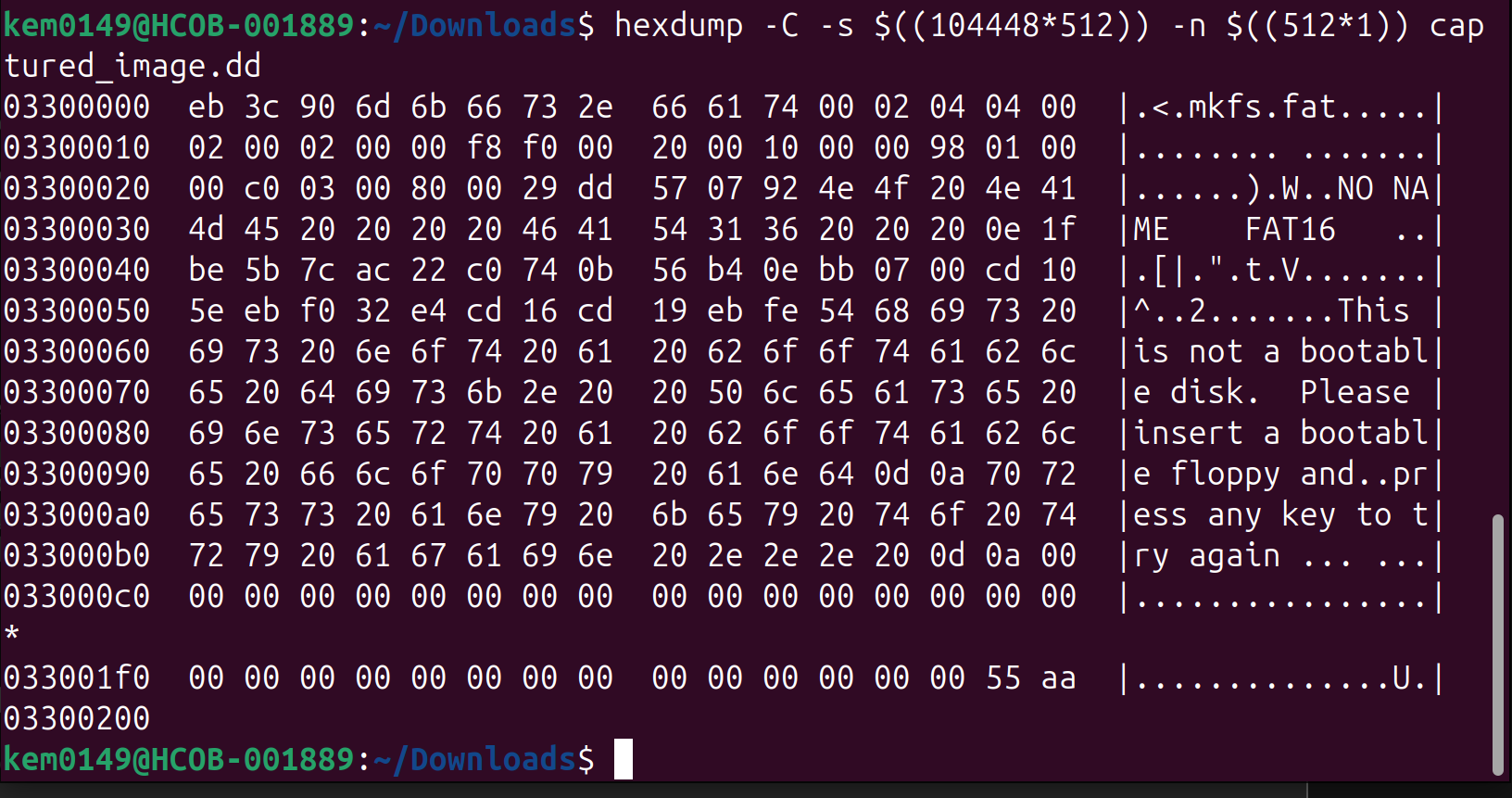


The reserved sectors are also the same at 4 as well. This is found at 000Eh.





The sec/FAT are different in this partition. This information is located at 0016h and is 2 bytes long. It is f0 00 and then with big endian it is 00 f0 (240).



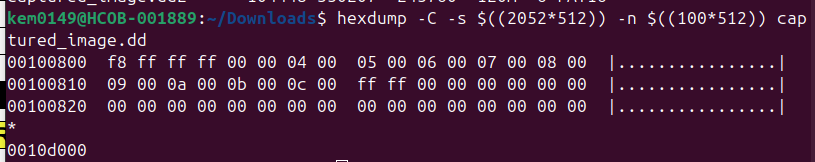


# 2 Detailed Analysis of Recovery Process

After the disk information is analyzed, look at the file allocation table and the root directory. The file allocation table will show how many buffers you have between the beginning of the data area and the start of the file location. Then look at the root directory. This will say how many files are on the partition, the size of the file, and the status of the file.

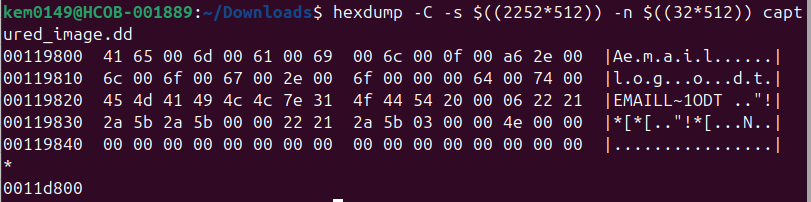
## 2.1 Partition 1 File 1

First take a look at the partition 1 file allocation table. This will indicate the size of the buffer. This is crucial because if it is ignored file carving will be done incorrectly. The size of the buffer is found by the number of clusters that are found before the files start. As is shown here, there is 1 cluster and then you multiply by 4 because there are 4 sectors per cluster.



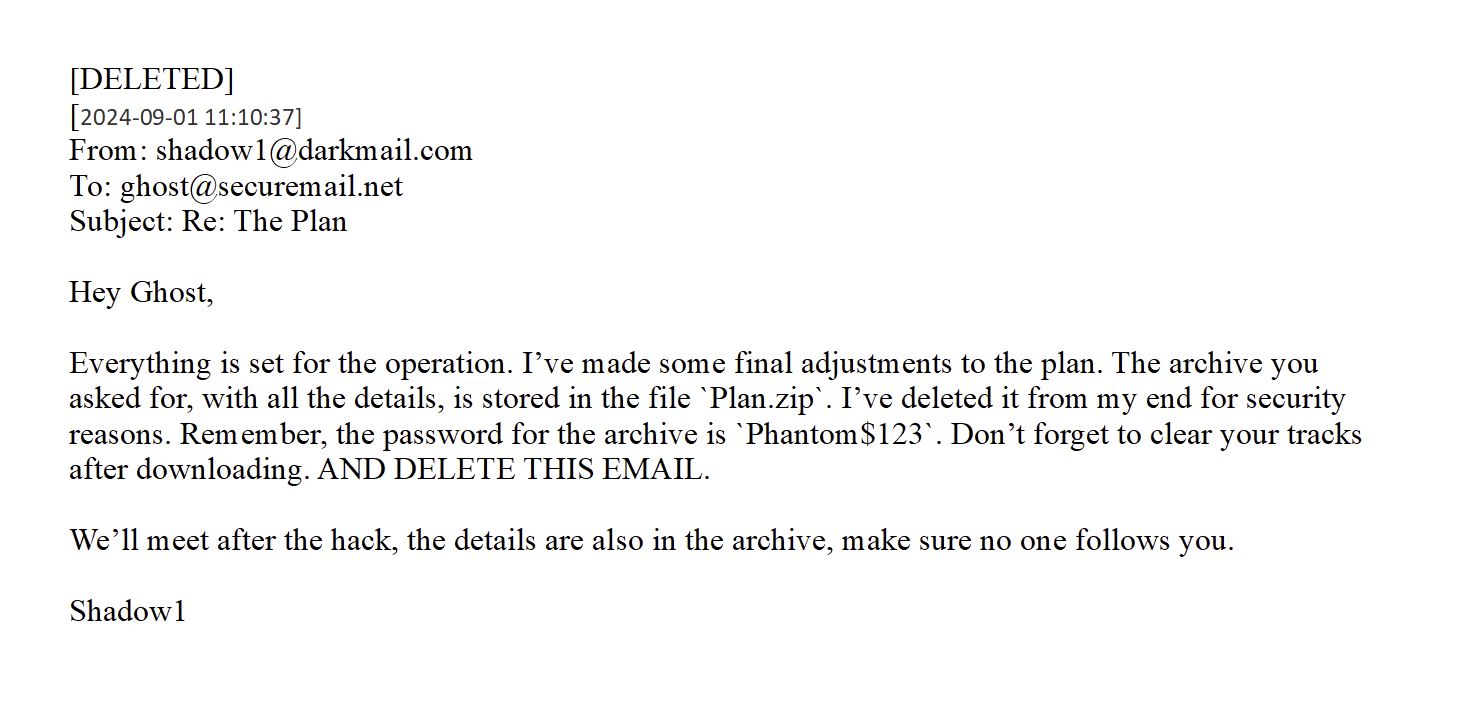


Next is to see what files are on the partition by looking in the root directory. This shows how many files are in the data area and the size of those files. Below it shows that there is one file called email.log.odt. The file status is shown here as 41 which means that it is active. To locate the file size look at the last 4 bytes and perform the big endian operation on them. The last 4 in this case is 00 4e 00 00 so after the big endian it is 00 00 4e 00 (19968). That indicates the file size. To calculate the number of sectors divide it by 4 and you will get 39. To find the sectors to skip add up all of the sectors to get here (2048+4+100+100+32+4) = 2288.



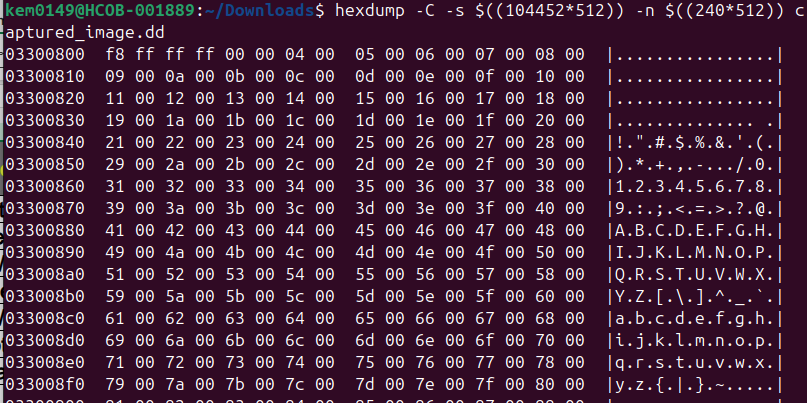


Now it is time to carve the file. Type in the following commands: dd if=capture\_image.dd of=email.log.odt bs=512 skip=2288 count=39. Below is the image of the file:



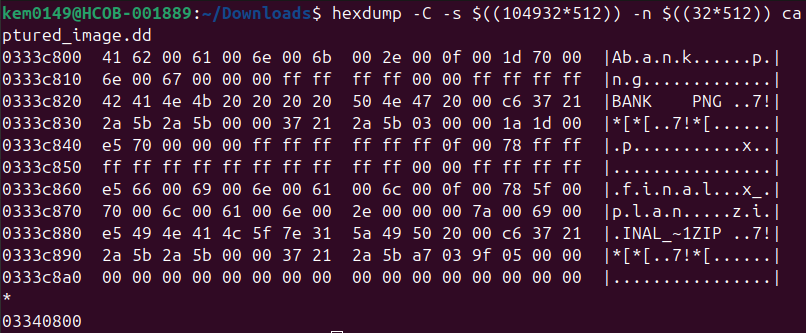
## 2.2 Partition 2 File 2

Since this is a new partition, we have to look at the partition 2 allocation table. The size of the buffer is the number of clusters before the start of the file contents. The buffer is the same as partition 1. There is 1 sector so there means that there are 4 sectors.





Now that the buffer is known move onto the root directory to determine the files, status, and size. There are 2 files in the partition. For this section focus on the first file. The first file is called bank.png. It is an active file because of the status 41. Take a look at the last 4 bytes before the next file to discover the size. The last 4 bytes are 00 1a 1d 00 and then with big endian it is 00 1d 1a 00 (1907200). To find it in sectors divide it by the number of bytes per sector (512) so it is 1907200/512 = 3725. To find when the file starts add up all of the past bytes. Partition 2 starts at 104448 so it should be 104448+4+240+240+32+4=104968.



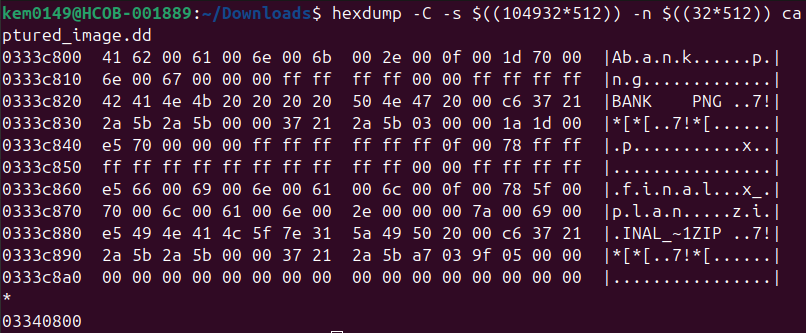


Now to carve the file we need to run the following command: dd if=capture\_image.dd of=Bank.png bs=512 skip =104968 count=3725. The result of that command is the image below:



## 2.3 Partition 2 File 3

The data area buffer was for this partition was discovered earlier as 4 so more onto the root directory. The file starts with e5 so that indicates that the file was deleted. To find the size of the file we need to look at the last 4 bytes of the file. The bytes are 9f 05 00 00 and then with big endian it is 00 00 05 9f (1439). That is the file size in bytes but in order to carve it has to be in sectors. To find that do divide the number by the # of bytes/sec and round up so it should be 1439/512 = 3. To find the where the file is located in the disk add up all of the past information so it should be 104448+4+240+240+32+4+3725=108696.





To carve the file type the following command: dd if=capture\_image.dd of=Plan.zip bs=512 skip=108696 count=3. A zip file is recovered that has a password that is found in the email from earlier.

# 3 Description of Analysis Techniques Utilized

During the hands-on-activity, the use of fdisk, hexdump, and dd were greatly utilized. Fdisk allowed to analyze the disk to discover the number of partitions on the disk, were each started, and how long they were. Hexdump allowed to analyze each part of the partitions to discover the sizing of the partitions and where the files were located. Finally, dd was utilized to carve out the files onto the device to discover the files.

# 4 Results and Discussion

The result of the data recovery was 3 files. This showed the process that the criminals used to rob the bank. The final zip file was password protected but it was discovered in the email. This zip file contained the step-by-step plans of the criminals as well as the address of the bank that was encoded in Base64.

# 5 Conclusions and recommendations

This hands-on assignment challenged the students on their knowledge of recovering files specifically from FAT16 partitions. The basic understanding of the structure was key to recovering the files correctly and navigating the disk image. The excel sheet was very useful in keeping track of sectors concisely. I feel like my skills in this area greatly increased throughout this assignment as well as my confidence in the material.

# 6 Acknowledgements

The lecture notes from Dr. K were used to aid in this assignment, specifically 04 – FAT16-FAT32 Storage Scenarios.

# 7 AI Use Statement

As part of this assignment, you are required to explain how Artificial Intelligence (AI) tools were used in your work. For this you need to describe:

* **Purpose of Use** – Formatting of Report.
* **Extent of Use** – I used AI to check my grammar of my report.
* **My Contribution** – I did not use AI during the part of the assignment when recovering the files.
* **Reflections** – I found that AI caught my errors in my wording and made it flow much better.

**By writing this reflection, I acknowledge that AI is a support tool, not a substitute for my own effort, and I take full responsibility for the final submission.**

# 8 References

[1] "Decimal to hex converter [Internet]. RapidTables; c2025 [cited 2025 Sep 22]. Available from: <https://www.rapidtables.com/convert/number/decimal-to-hex.html?x=0>".