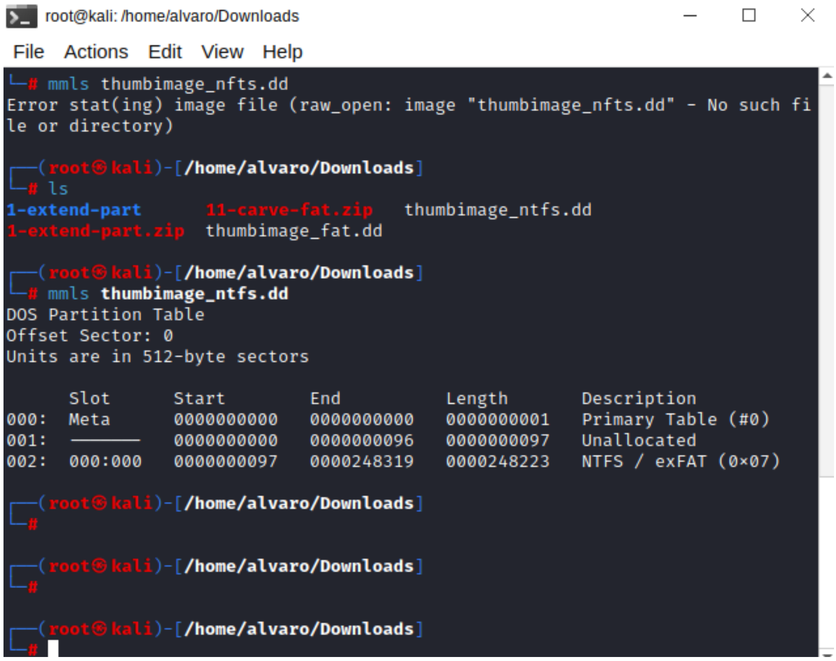
Dikerjakan oleh: Alvaro Austin (2106752180)

Tugas Individu

1. **Exercise 7.5.2**

A. Disk Analysis with *mmls*.

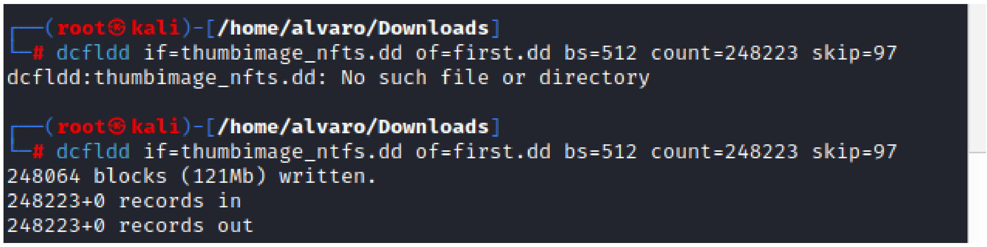

root@kali: /home/alvaro/Downloads
File Actions Edit View Help

```
└─# mmls thumbimage_nfts.dd
Error stat(ing) image file (raw_open: image "thumbimage_nfts.dd" - No such fi
le or directory)

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# ls
1-extend-part       11-carve-fat.zip  thumbimage_ntfs.dd
1-extend-part.zip  thumbimage_fat.dd

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# mmls thumbimage_ntfs.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000000096   0000000097   Unallocated
002:  000:000   0000000097   0000248319   0000248223   NTFS / exFAT (0x07)

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─#

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─#

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─#
```

First Partition	
Start LBA Address	97
Number of Sector in Partition	248223
Size Of Partition (MB)	127.090176
Type of partition	NTFS / exFAT (0x07)

B. Part B: Use dcfldd to Extract the First Partition Image from the Disk Image Provided

```
dcfldd if=thumbimage_ntfs.dd of=first.dd bs=512 count=248223
skip=97
```

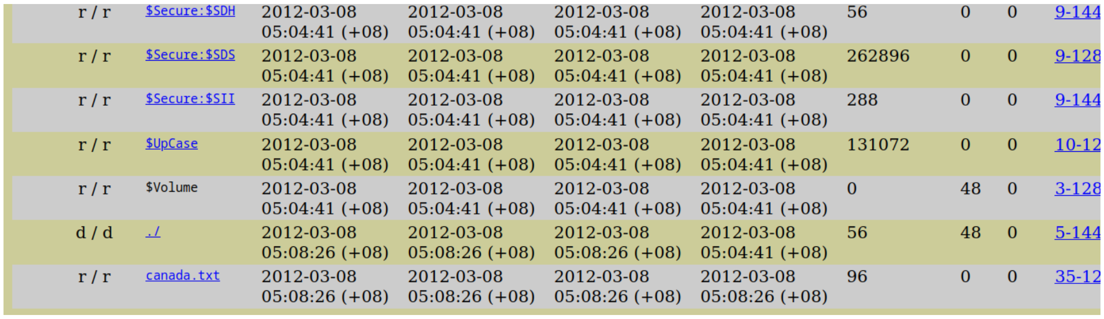


```
┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# dcfldd if=thumbimage_nfts.dd of=first.dd bs=512 count=248223 skip=97
dcfldd:thumbimage_nfts.dd: No such file or directory

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# dcfldd if=thumbimage_ntfs.dd of=first.dd bs=512 count=248223 skip=97
248064 blocks (121Mb) written.
248223+0 records in
248223+0 records out
```

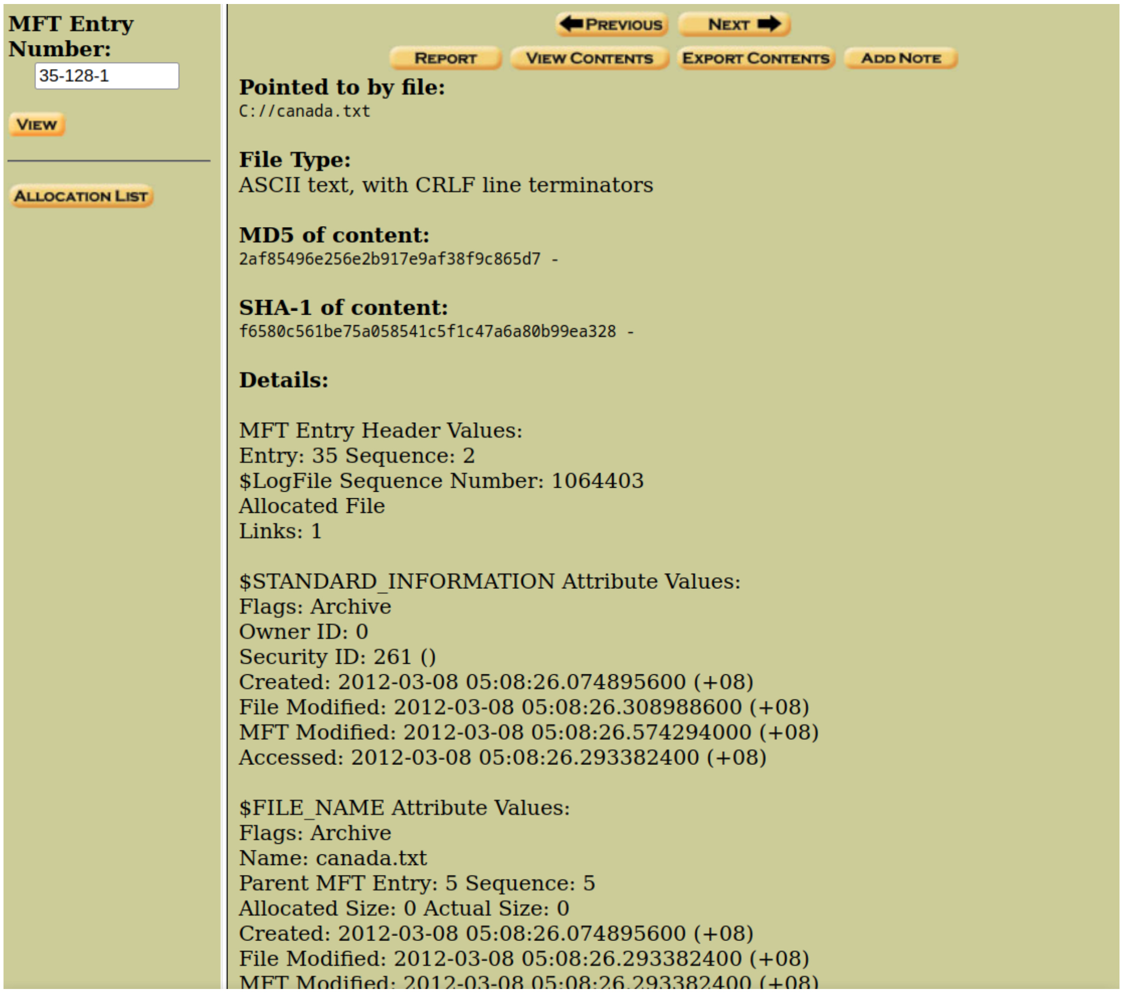
Dikerjakan oleh: Alvaro Austin (2106752180)

C. Part C: Analyze File Properties

Saya akan menggunakan autopsy untuk melakukan analisis terhadap partition disk tersebut.



r / r	$Secure:$SDH	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	56	0	0	9-144
r / r	$Secure:$SDS	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	262896	0	0	9-128
r / r	$Secure:$SII	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	288	0	0	9-144
r / r	$UpCase	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	131072	0	0	10-12
r / r	$Volume	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	2012-03-08 05:04:41 (+08)	0	48	0	3-128
d / d	./	2012-03-08 05:08:26 (+08)	2012-03-08 05:08:26 (+08)	2012-03-08 05:08:26 (+08)	2012-03-08 05:04:41 (+08)	56	48	0	5-144
r / r	canada.txt	2012-03-08 05:08:26 (+08)	2012-03-08 05:08:26 (+08)	2012-03-08 05:08:26 (+08)	2012-03-08 05:08:26 (+08)	96	0	0	35-12



MFT Entry Number: 35-128-1

Pointed to by file:
C://canada.txt

File Type:
ASCII text, with CRLF line terminators

MD5 of content:
2af85496e256e2b917e9af38f9c865d7 -

SHA-1 of content:
f6580c561be75a058541c5f1c47a6a80b99ea328 -

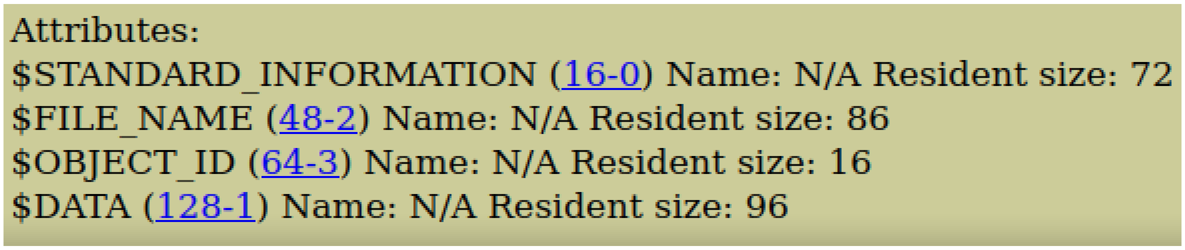
Details:

MFT Entry Header Values:
Entry: 35 Sequence: 2
$LogFile Sequence Number: 1064403
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 261 ()
Created: 2012-03-08 05:08:26.074895600 (+08)
File Modified: 2012-03-08 05:08:26.308988600 (+08)
MFT Modified: 2012-03-08 05:08:26.574294000 (+08)
Accessed: 2012-03-08 05:08:26.293382400 (+08)

$FILE_NAME Attribute Values:
Flags: Archive
Name: canada.txt
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 0 Actual Size: 0
Created: 2012-03-08 05:08:26.074895600 (+08)
File Modified: 2012-03-08 05:08:26.293382400 (+08)
MFT Modified: 2012-03-08 05:08:26.293382400 (+08)

Q2. The entry number of the MFT entry which points to the file “canada.txt”:
Entry: 35, Sequence: 2



```
Attributes:
$STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
$FILE_NAME (48-2) Name: N/A Resident size: 86
$OBJECT_ID (64-3) Name: N/A Resident size: 16
$DATA (128-1) Name: N/A Resident size: 96
```

Q3. How many attributes are contained in this entry? **4 attributes**

Q4. How many bytes are used by the second attribute? **86**

Q5. The attribute type for the second attribute: **48-2**

Q6. The size of content in the second attribute (in decimal bytes): **86**

Q7. One of attributes in this MFT entry is $FILE_NAME. What is the length of the file name? **10**

Q8. The attribute type for the last attribute: **128-1**

Q9. Is the last attribute a resident one? (Yes/No): **Yes**

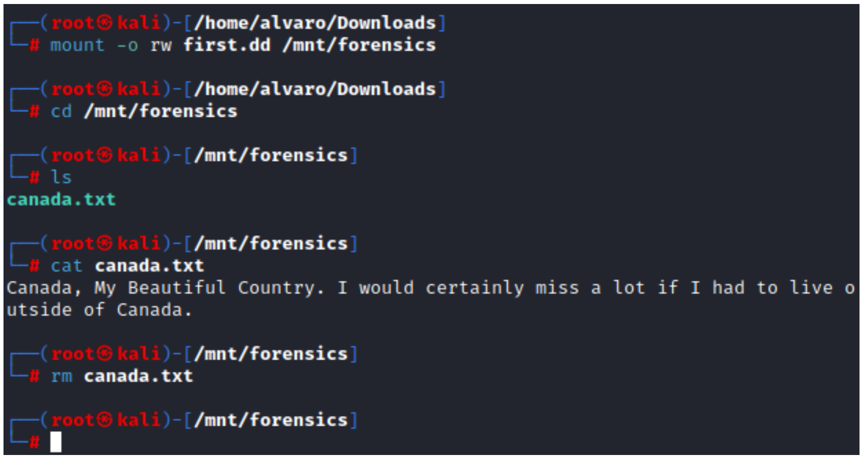
2. Exercise 8.2.2

A. File System Layer Analysis

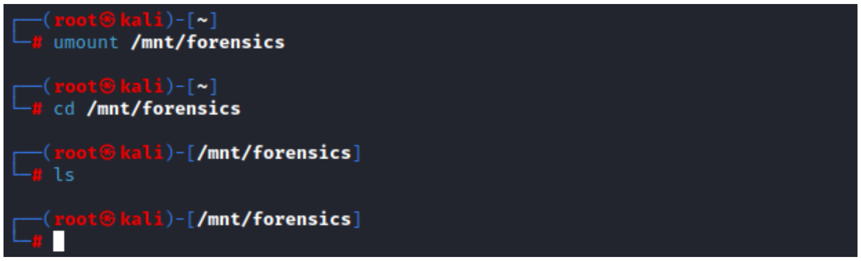
Q1. What is the cluster size (in bytes)? **4096 Bytes**

Q2. What is the MFT entry size (in bytes)? **1024 Bytes**

B. Mounting and Unmounting File Systems



```
┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# mount -o rw first.dd /mnt/forensics

┌──(root㉿kali)-[/home/alvaro/Downloads]
└─# cd /mnt/forensics

┌──(root㉿kali)-[/mnt/forensics]
└─# ls
canada.txt

┌──(root㉿kali)-[/mnt/forensics]
└─# cat canada.txt
Canada, My Beautiful Country. I would certainly miss a lot if I had to live o
utside of Canada.

┌──(root㉿kali)-[/mnt/forensics]
└─# rm canada.txt

┌──(root㉿kali)-[/mnt/forensics]
└─#
```

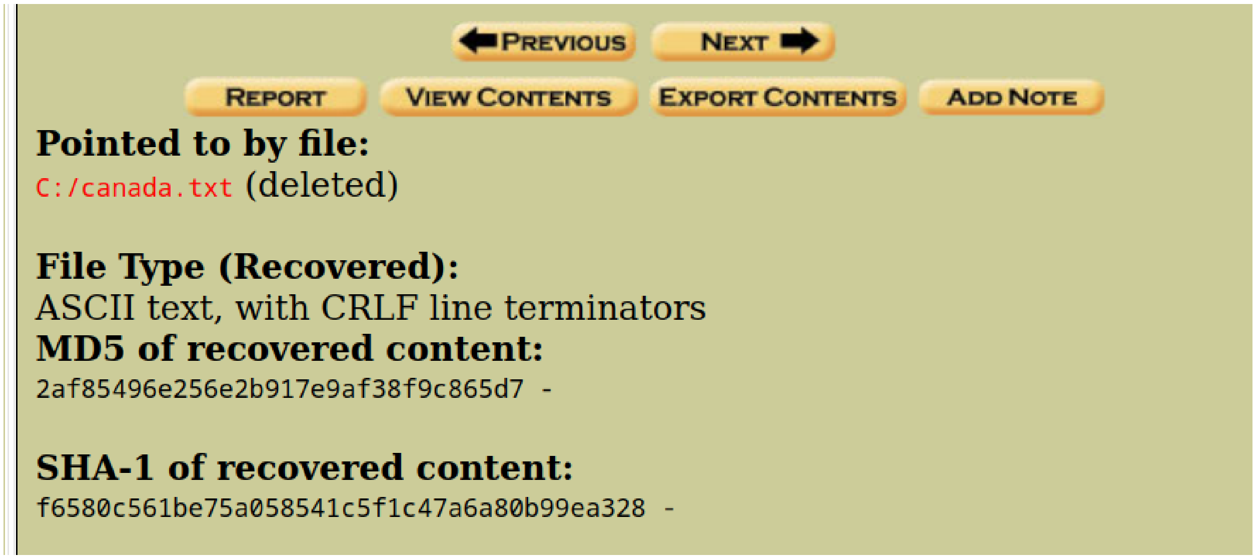


```
┌──(root㉿kali)-[~]
└─# umount /mnt/forensics

┌──(root㉿kali)-[~]
└─# cd /mnt/forensics

┌──(root㉿kali)-[/mnt/forensics]
└─# ls

┌──(root㉿kali)-[/mnt/forensics]
└─#
```

Q3. After the file canada.txt has been deleted, you can discover that its MFT entry has been marked as deleted, particularly with its byte offset 22-23 replaced with 0x0000.

- Scan the MFT one entry each time and locate the entry pointing to the deleted “canada.txt” file. Particularly, we look for the one with the value of 0x0000 from the byte offset 22–23 of each MFT entry. For simplify, you should be able to locate it by checking the first 50 entries in the NTFS image provided here.

- Analyze the identified MFT entry and extract its $DATA attribute. Parse the $DATA attribute and obtain the following information, including whether resident or non-resident attribute: **resident**, file size: **96 Bytes**
- If it is a resident attribute, it contains the file contents. Then, read and save the contents of the $DATA attribute as recovered file.



Pointed to by file:
C:/canada.txt (deleted)

File Type (Recovered):
ASCII text, with CRLF line terminators

MD5 of recovered content:
2af85496e256e2b917e9af38f9c865d7 -

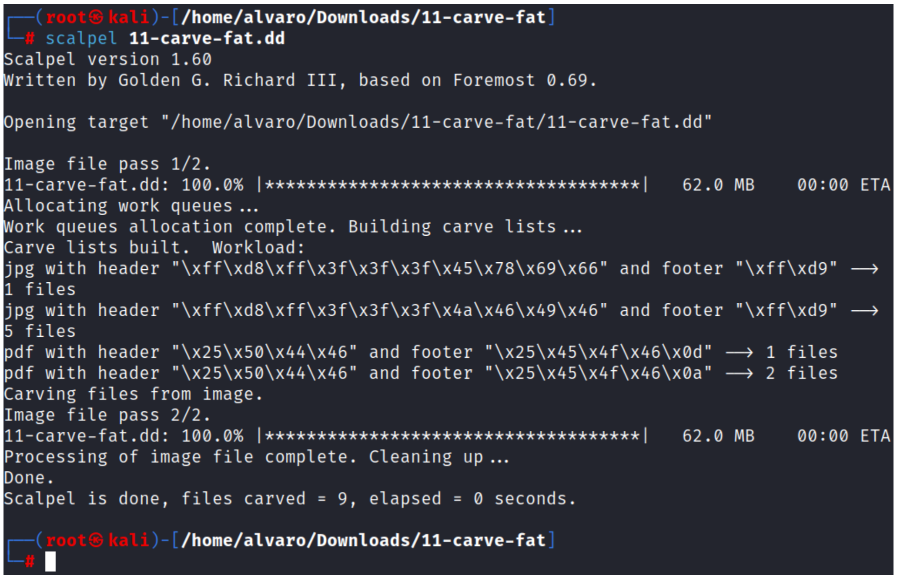
SHA-1 of recovered content:
f6580c561be75a058541c5f1c47a6a80b99ea328 -

3. Exercise 9.3.2 (File Carving)

Part A—Evidence Hashing

Q1. What is the MD5 hash value of the raw partition image used in the exercise?
0069813C892A462F88DC6D376624F7D9

Part B—Data Carving with Scalpel



```
┌──(root㉿kali)-[/home/alvaro/Downloads/11-carve-fat]
└─# scalpel 11-carve-fat.dd
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/home/alvaro/Downloads/11-carve-fat/11-carve-fat.dd"

Image file pass 1/2.
11-carve-fat.dd: 100.0% |*************************************|   62.0 MB    00:00 ETA
Allocating work queues ...
Work queues allocation complete. Building carve lists ...
Carve lists built.  Workload:
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66" and footer "\xff\xd9" ⟶
1 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer "\xff\xd9" ⟶
5 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0d" ⟶ 1 files
pdf with header "\x25\x50\x44\x46" and footer "\x25\x45\x4f\x46\x0a" ⟶ 2 files
Carving files from image.
Image file pass 2/2.
11-carve-fat.dd: 100.0% |*************************************|   62.0 MB    00:00 ETA
Processing of image file complete. Cleaning up ...
Done.
Scalpel is done, files carved = 9, elapsed = 0 seconds.

┌──(root㉿kali)-[/home/alvaro/Downloads/11-carve-fat]
└─# ▌
```

Q2. How many PDF files are recovered by Scalpel? **3 PDF Files**

Dikerjakan oleh: Alvaro Austin (2106752180)

Q3. How many JPG files are recovered by Scalpel? **6 JPG Files**
Q4. Is a file with a MD5 hash of “c0de7a481fddfa03b764fa4663dc6826” one of recovered JPG files? **No** (Yes/No)
Q5. Is a file with a MD5 hash of “80dc29617978b0741fa2ad3e452a6f9d” one of recovered PDF files? **No** (Yes/No)
Q6. There is a PDF file in the image (“11-carve-fat.dd”) called “lin_1.2.pdf” whose md5 hash value is “e026ec863410725ba1f5765a1874800d” in hex. What is the size of the file “lin_1.2.pdf”? **1399508 Bytes**