Forensics Report

Prepared for

hdd.dd

application

Finding MD5 Hashes

Prepared by

Bashetty Arun Kumar

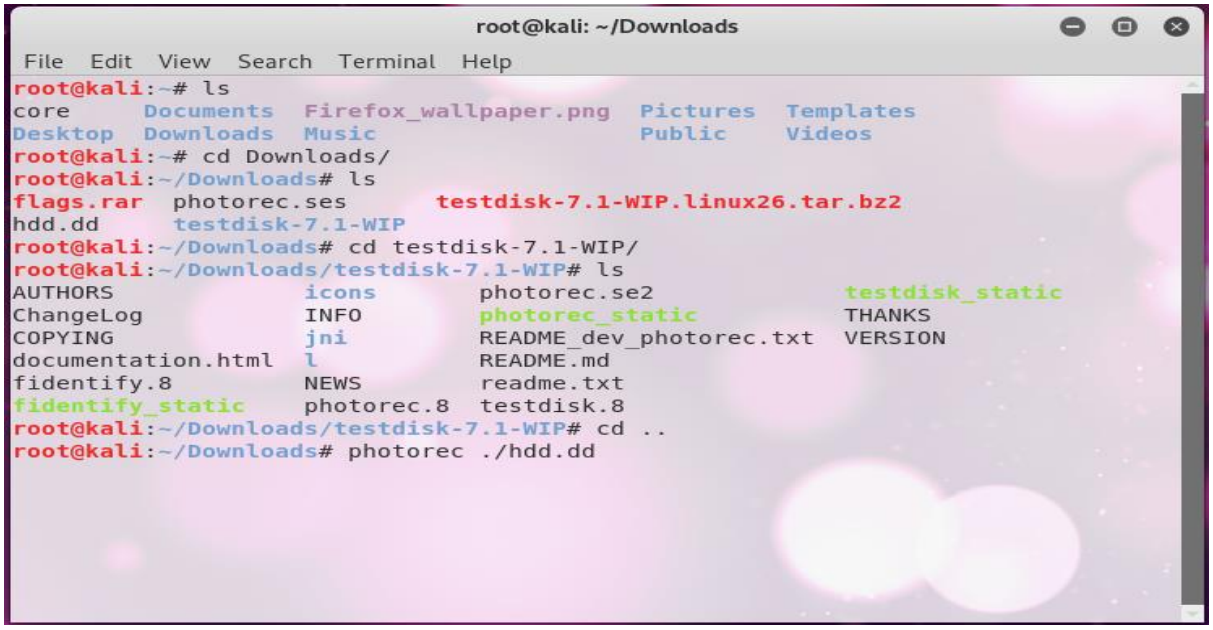
Master of Computer Security

27-December-2018

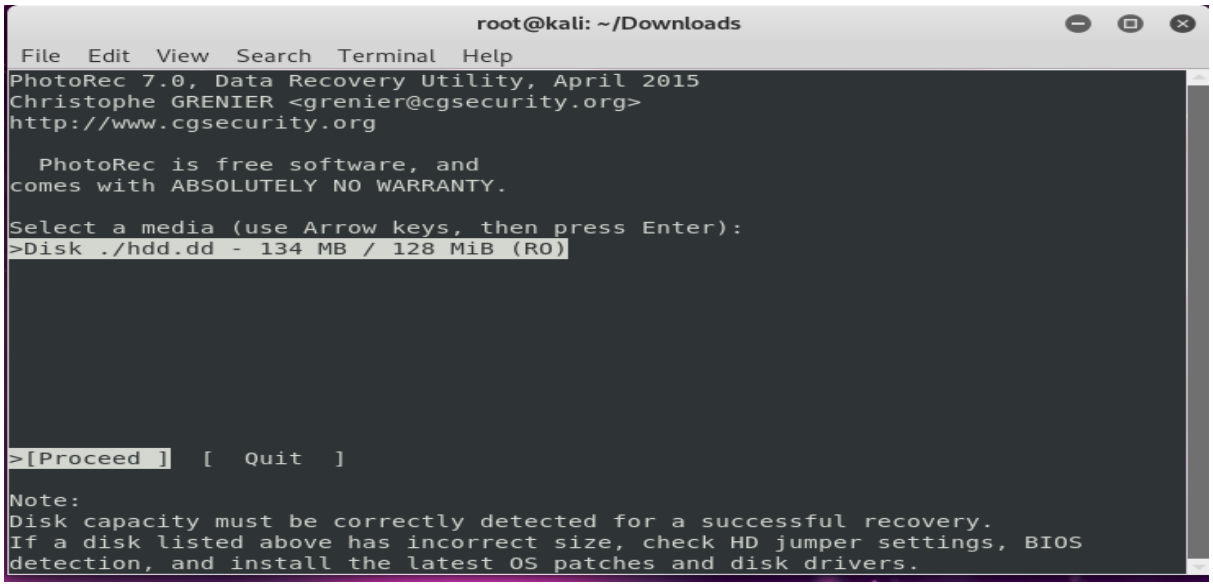
Steps to recover the .tar.gz deleted files from the NTFS partition:

Before doing below all steps, first you can download hdd.dd file from http://www.adeleda.com/epita/forensics/ I already Downloaded **hdd.dd** and you can see the file inside downloads.

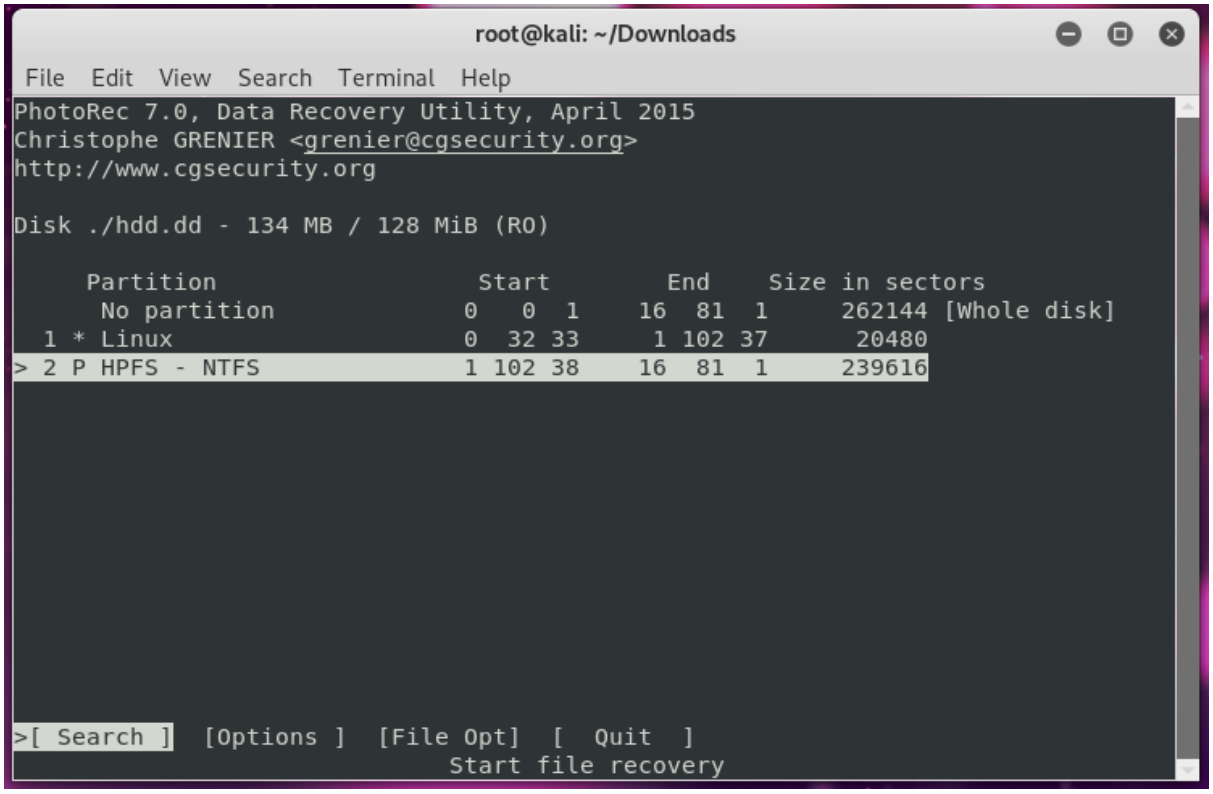
Now, first download the **Photorec** application from https://www.cgsecurity.org/wiki/PhotoRec_FR , this application is used to recover all files from hard disk.

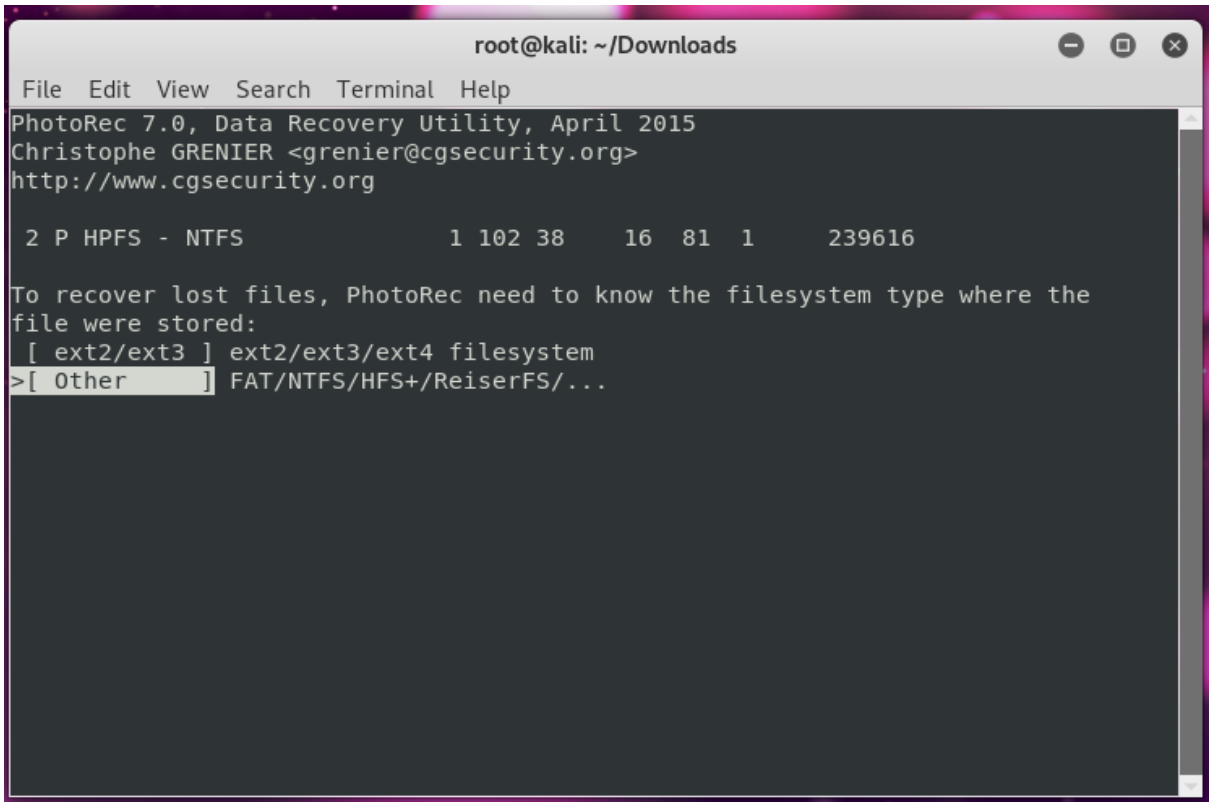


When you enter photorec ./hdd.dd, it will start hdd.dd application inside the photorec software and you can see the size of hard disk.

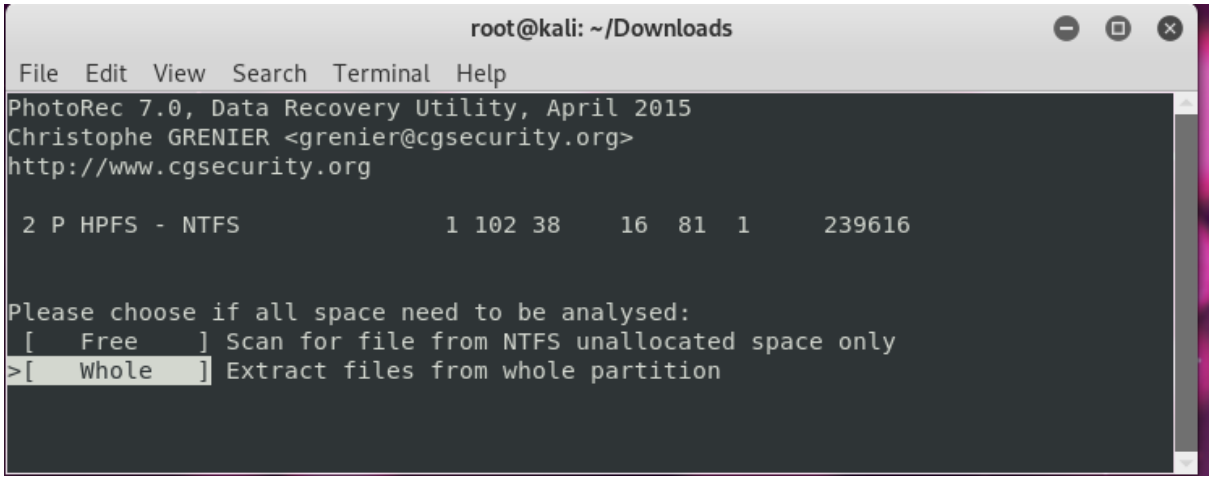


- Click on proceed and it will display 2 partitions, and you have to choose which partition we retrieve and after research we found HPFS-NTFS contain data. So, click proceed on 2nd partition.



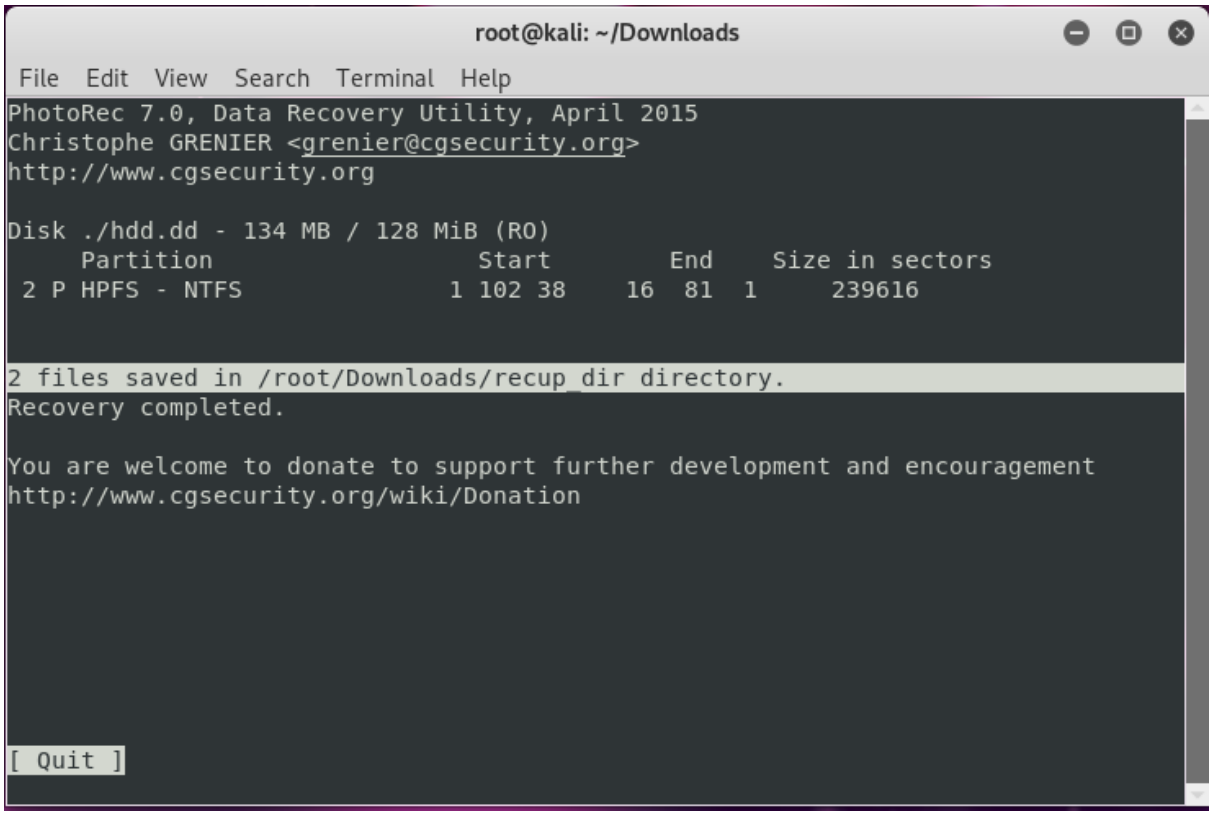


Now, it will ask to extract whole partition or just NTFS unallocated space only, click on whole option to get all recovered files,



After clicking on proceed, it displays those recovered files stored inside /root/Downloads/recup_dir directory.

Click on q , it will close the photorec application and get back to the normal terminal.



Forensics Report

Inside download you can check the .tar.gz file, but you must extract to see inside the files

Use **tar xvzf** filename go get all files,

```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge
File  Edit  View  Search  Terminal  Help
root@kali:~/Downloads# ls
flags.rar  recup_dir.1  testdisk-7.1-WIP
hdd.dd     recup_dir.2  testdisk-7.1-WIP.linux26.tar.bz2
root@kali:~/Downloads# cd recup_dir.2
root@kali:~/Downloads/recup_dir.2# ls
f0123904.jpg  f0156672_forensics_challenge.tar.gz  report.xml  t0123904.jpg
root@kali:~/Downloads/recup_dir.2# tar xvzf f0156672_forensics_challenge.tar.gz
forensics_challenge/
forensics_challenge/Images/
forensics_challenge/Documents/
forensics_challenge/Private/
forensics_challenge/Musics/
forensics_challenge/FS.dd
forensics_challenge/Download/
forensics_challenge/.mozilla/
forensics_challenge/.mozilla/extensions/
```

Here, below screes shot, we can see one new directory displays "forensics_challenge", change the directory to forensics_challenge and use ls command to check inside the directory files and it will show all files

Next, you can open every directory and check the MD5 hashes.

```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge
File  Edit  View  Search  Terminal  Help
forensics_challenge/Images/fractale8.jpg
forensics_challenge/Images/fractale9.jpg
forensics_challenge/Images/fractale10.jpg
forensics_challenge/Images/fractale11.jpg
forensics_challenge/Images/jpg_NDH080408ak.jpg

gzip: stdin: decompression OK, trailing garbage ignored
tar: Child returned status 2
tar: Error is not recoverable: exiting now
root@kali:~/Downloads/recup_dir.2# ls
f0123904.jpg                        forensics_challenge  t0123904.jpg
f0156672_forensics_challenge.tar.gz  report.xml
root@kali:~/Downloads/recup_dir.2# cd forensics_challenge/
root@kali:~/Downloads/recup_dir.2/forensics_challenge# ls
Documents  Download  FS.dd  Images  Musics  Private
root@kali:~/Downloads/recup_dir.2/forensics_challenge#
```

Steps to find the many hidden MD5 hashes within directories:

Useful **commands** to get hashes from retrieve the directory,

Strings:

Strings command is useful to return each string of printable characters inside the files. Its main uses are to determine the contents of and extract text from binary files.

Exiftool:

Exiftool command is used to read and write meta information on a variety of file type.

This command will give images all clear information.

Gpicview:

This command is useful to show the image from terminal.

This application is Extremely lightweight and fast with low memory usage.

Base64 -d:

This command we already know that converting the string to base64 decoded.

Wireshark:

Wireshark is open source, it is used for network troubleshooting, analysis, software and communications protocol development, and education

Forensics Report

MD5 Hashes 1 & 2:

First change the directory to Documents by using cd(Change Directory)command. You can find .pdf files inside the Documents directory.

```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge/Documents
File  Edit  View  Search  Terminal  Help
root@kali:~/Downloads/recup_dir.2/forensics_challenge# ls
Documents  Download  FS.dd  Images  Musics  Private
root@kali:~/Downloads/recup_dir.2/forensics_challenge# cd Documents
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Documents# ls
03-icar-fractal.pdf  fractal.pdf  fractals2.pdf
fractales.pdf        Fractal.pdf  World_of_Fractal.pdf
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Documents# strings -n 15 0
3-icar-fractal.pdf
/H [ 6829 1817 ]
                                                xref
0000000016 00000 n
0000006732 00000 n
0000008646 00000 n
0000008867 00000 n
0000012985 00000 n
0000013036 00000 n
0000013087 00000 n
0000013138 00000 n
0000013189 00000 n
0000013240 00000 n
0000013291 00000 n
0000013342 00000 n
0000013393 00000 n
0000013444 00000 n
```

Use strings commands with 1st pdf file and you can see two MD5 Hashes.

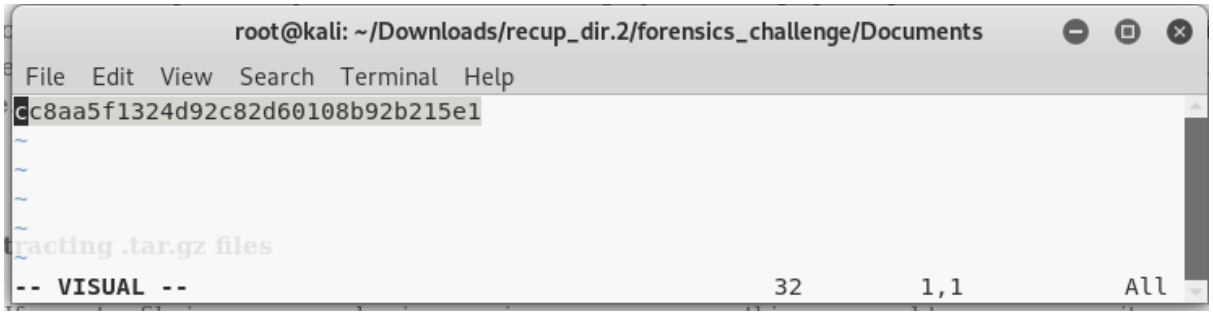
```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge/Documents
File  Edit  View  Search  Terminal  Help
/Nums [ 0 225 0 R ]
/Kids [ 239 0 R 1 0 R 4 0 R 7 0 R 10 0 R 13 0 R 16 0 R 19 0 R 22 0 R 25 0 R
--
/Kids [ 227 0 R 229 0 R 230 0 R 231 0 R 232 0 R 233 0 R 234 0 R ]
/Kids [ 28 0 R 31 0 R 34 0 R 37 0 R 40 0 R 43 0 R 46 0 R 49 0 R 52 0 R 55 0 R
--
/Kids [ 58 0 R 61 0 R 64 0 R 67 0 R 70 0 R 73 0 R 76 0 R 79 0 R 82 0 R 85 0 R
--
/Kids [ 88 0 R 91 0 R 94 0 R 97 0 R 100 0 R 104 0 R 107 0 R 110 0 R 113 0 R
--
/Kids [ 119 0 R 122 0 R 125 0 R 128 0 R 131 0 R 134 0 R 137 0 R 140 0 R 143 0 R
--
/Kids [ 149 0 R 152 0 R 155 0 R 158 0 R 161 0 R 164 0 R 167 0 R 170 0 R 173 0 R
--
/Kids [ 184 0 R 187 0 R 190 0 R 193 0 R 196 0 R 199 0 R 202 0 R ]
--
/ModDate (D:20030818135108+02'00')
--
/Author (No\353l de Palma)
--
0000000000 65535 f
--
/ID[<cc8aa5f1324d92c82d60108b92b215e1><0b78df27b70a82a1e529a23d4771d322>]
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Documents#
```

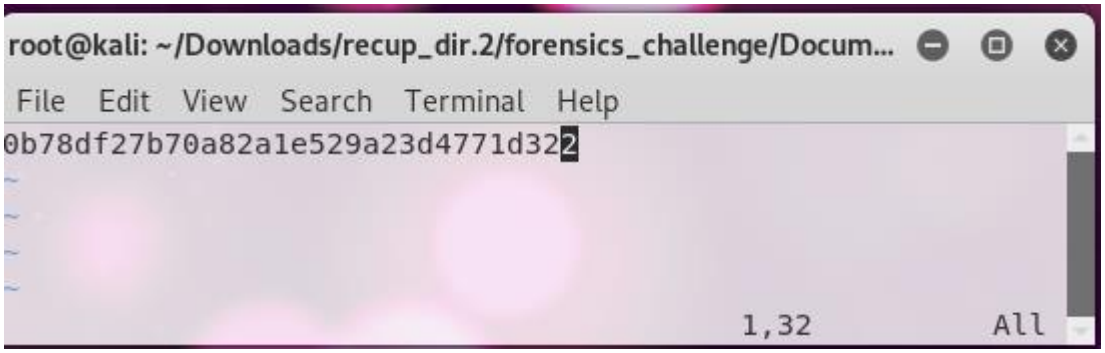
Note:

If you do not know, the display code is MD5 hash or not you can by below screenshot and steps.

=>First open a terminal, using vi command and paste the MD5 and normally MD5 has contain 32 bits.

=>Below Screenshot, you can see the pasted MD5 hash is 32 bits.





MD5 Hashes 3 & 4:

Now, you can check the next pdf file using same strings command.

Using strings **-n 15**, will display the only strings with 15 characters inside the file.

```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge/Documents
File  Edit  View  Search  Terminal  Help
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Documents# ls
03-icar-fractal.pdf  fractal.pdf  fractals2.pdf
fractales.pdf        Fractal.pdf  World_of_Fractal.pdf
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Documents# strings fractal
s2.pdf
%PDF-1.3
2 0 obj
/CreationDate (D:20070423185704-06'00')
/ModDate (D:20070423185704-06'00')
/Producer (BCL easyPDF 4.30 \(0410\))
/Creator (easyPDF Printer Driver 4.3)
/Title (Introduction to Fractals)
/Author (David McAdams)
/Subject (Geometry - Introduciton to Fractals packet)
/Keywords (geometry fractal fractals packet worksheet webquest discovery introdu
ction secondary math education teaching algebra enrichment extra credit iteratio
```

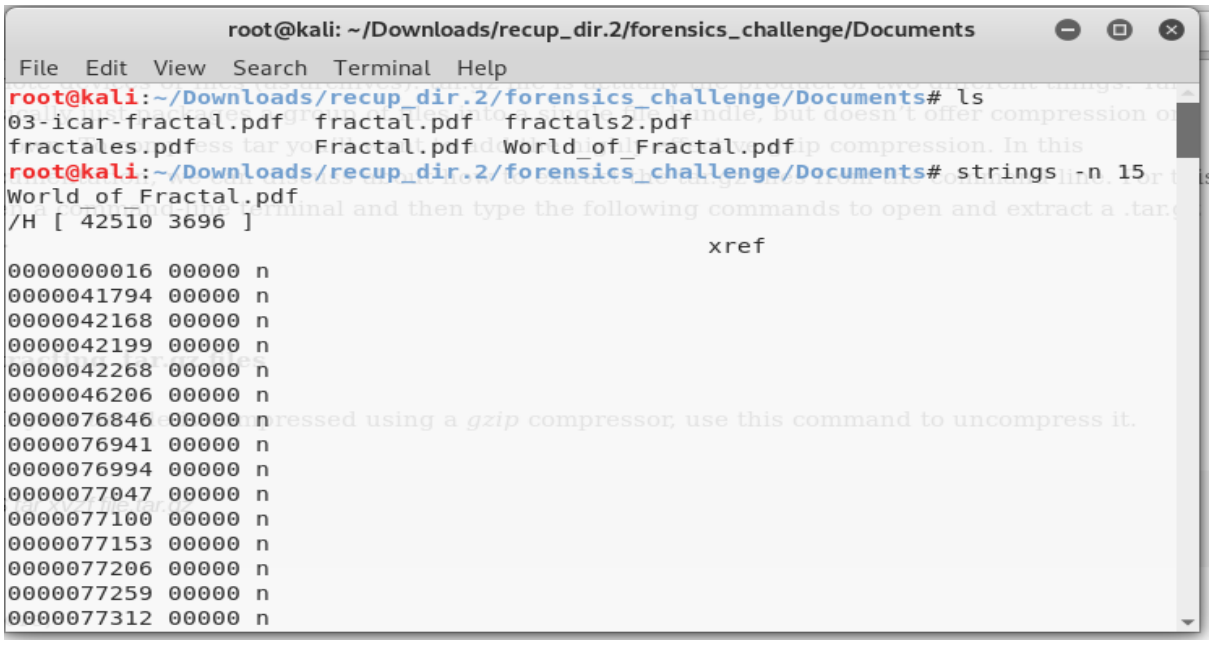
Here , you can see the 2 more hashes with 32 bits.

```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge/Documents
File  Edit  View  Search  Terminal  Help
0000251373 00000 n
0000262781 00000 n
0000261328 00000 n
0000268553 00000 n
0000262974 00000 n
0000286017 00000 n
0000268831 00000 n
trailer
/Size 119
/Root 3 0 R
/Info 2 0 R
/ID[<541ad5375a86748c22b219cecc840795><541ad5375a86748c22b219cecc840795>]
startxref
286709
%%EOF
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Documents#
```

MD5 Hashes 5 & 6:

=> Open the One more file inside the Documents using strings command.

=> Open the World_of_Fractal.pdf file.



In below screenshot, we can find 2 hashes.

Forensics Report

MD5 Hash 7:

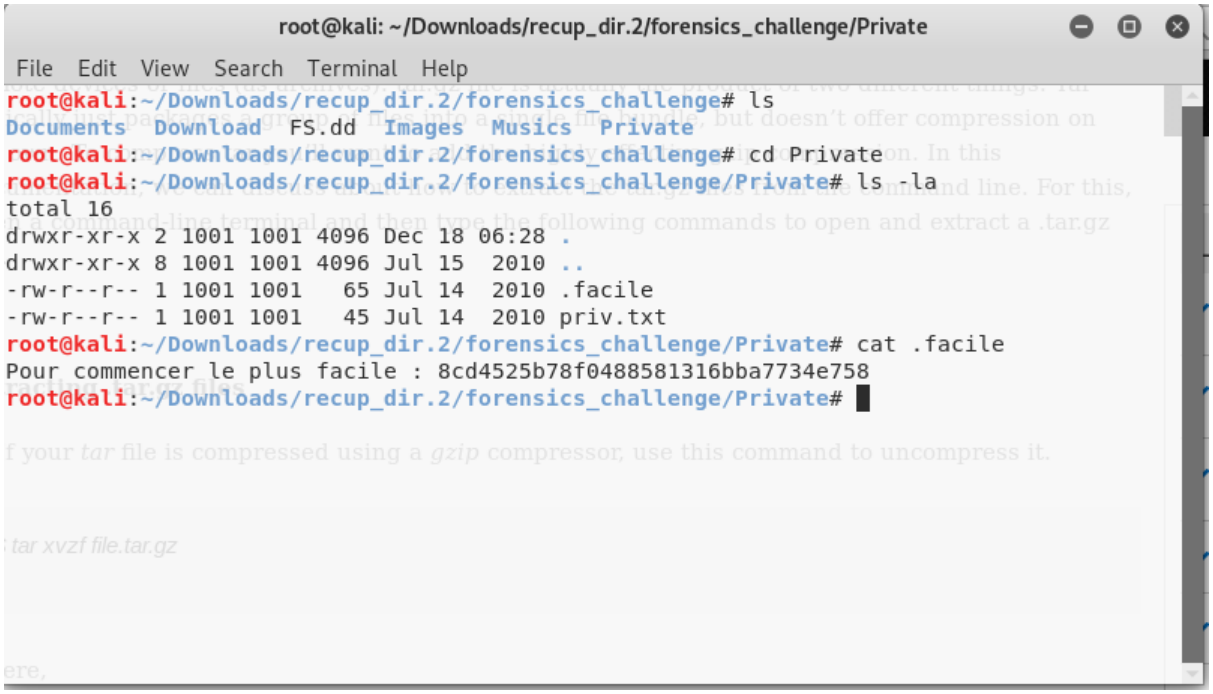
This one you can find easily without using any stress

=>Open the Private directory using the cd command

=>you can check the files inside the directory using ls -ls, it shows long listing data.

=>you can check the data inside the file using cat command

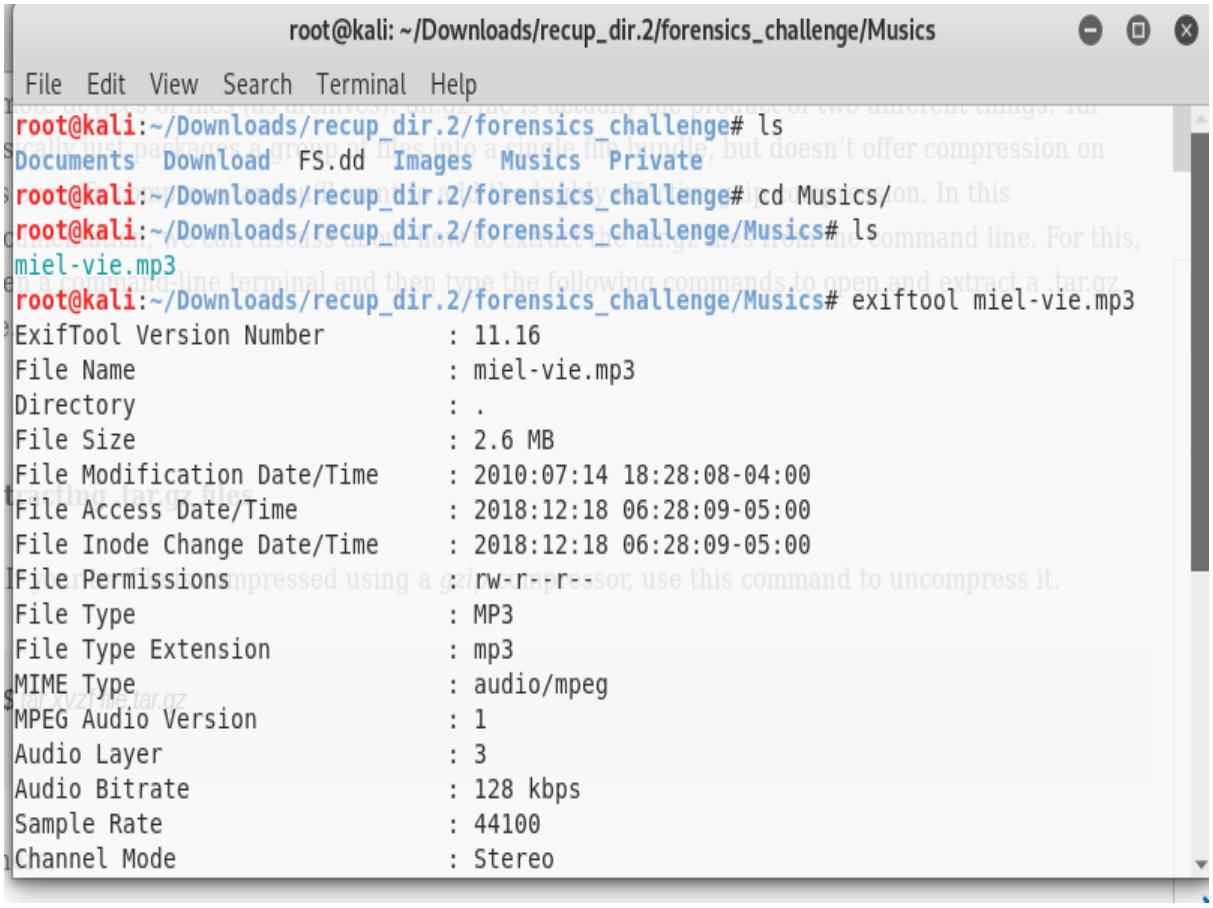
=>Inside **.facile** folder we found the hash.



MD5 Hash 8:

Change the directory to Musics, inside **musics** folder I found one .mp3 file.

Using **exiftool**, open the file and we can clearly show the mp3 file data like it displays file format, size of the file, date of creation, date of modification, File permissions, File Type, Audio Layer etc.



Below screenshot we can see Year look like MD5 has, after checking I found it is half MD5,

We can see the comment code end with "==@, it means its base64 code,

```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge/Musics
File  Edit  View  Search  Terminal  Help
File Type                       : MP3
File Type Extension             : mp3
MIME Type                       : audio/mpeg
MPEG Audio Version              : 1
Audio Layer                     : 3
Audio Bitrate                   : 128 kbps
Sample Rate                     : 44100
Channel Mode                    : Stereo
MS Stereo                       : Off
Intensity Stereo                : Off
Copyright Flag                  : False
Original Media                  : True
Emphasis                        : None
ID3 Size                        : 128
Title                           : miel-vie
Artist                          : ???
Album                           : VW4gZGUgcGx1cyAzMzA2ZWMwOTdmYz
Year                            :
Comment                         : gzMDgxNzE4MTUxNmVhMjhkZWQzOA==
Genre                           : None
Duration                        : 0:02:51 (approx)
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Musics#
```

- ⇨ Using strings command, I concatenated both codes and decoded by using base64 -d option,
- ⇨ But, after getting wrong output, I Found strings is not correct for Concatenating.
- ⇨ After I used echo "code"=> it works, and two codes are combined and now it will be one code.
- ⇨ Using base64 -d, I coded code and I found MD5 code and it is super cool.

```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge/Musics
File  Edit  View  Search  Terminal  Help
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Musics# strings -n 15 VW4g
ZGUgcGx1cyAzMzA2ZWMwOTdmYzgzMDgxNzE4MTUxNmVhMjhkZWQzOA== | base64 -d
strings: 'VW4gZGUgcGx1cyAzMzA2ZWMwOTdmYzgzMDgxNzE4MTUxNmVhMjhkZWQzOA==': No such
 file
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Musics# eco ^C
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Musics# echo "VW4gZGUgcGx1
cyAzMzA2ZWMwOTdmYzgzMDgxNzE4MTUxNmVhMjhkZWQzOA=="
VW4gZGUgcGx1cyAzMzA2ZWMwOTdmYzgzMDgxNzE4MTUxNmVhMjhkZWQzOA==
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Musics# echo "VW4gZGUgcGx1
cyAzMzA2ZWMwOTdmYzgzMDgxNzE4MTUxNmVhMjhkZWQzOA==" | base64 -d
Un de plus 3306ec097fc830817181516ea28ded38root@kali:~/Downloads/recup_dir.2/for
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Musics#
```

MD5 Hash 9:

Change the directory to Images and use ls command to display inside the files,

Inside the Images directory you can see there are 17 files and you have to check and each and every folder inside by using exiftool or strings command to display hashes,

I tried all files and I found the MD5 hash inside the farctale5.jpg

```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge/Images
File  Edit  View  Search  Terminal  Help
root@kali:~/Downloads/recup_dir.2/forensics_challenge# ls
Documents  Download  FS.dd  Images  Musics  Private
root@kali:~/Downloads/recup_dir.2/forensics_challenge# cd Images
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Images# ls
fractale10.jpg  fractale2.png  fractale5.jpg  fractale8.jpg  jpg_NDH080408ak.jpg
fractale11.jpg  fractale3.jpg  fractale6.jpg  fractale9.jpg
fractale1.jpg   fractale4.jpg  fractale7.jpg  fractale.jpg
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Images# exiftool fractale5.jpg
ExifTool Version Number         : 11.16
File Name                       : fractale5.jpg
Directory                       : .
File Size                       : 398 kB
File Modification Date/Time     : 2010:07:14 17:15:38-04:00
File Access Date/Time           : 2018:12:18 06:28:09-05:00
File Inode Change Date/Time     : 2018:12:18 06:28:09-05:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
```

You can see the MD5 hash beside the comment,

```
root@kali: ~/Downloads/recup_dir.2/forensics_challenge/Images
File  Edit  View  Search  Terminal  Help
File Modification Date/Time     : 2010:07:14 17:15:38-04:00
File Access Date/Time           : 2018:12:18 06:28:09-05:00
File Inode Change Date/Time     : 2018:12:18 06:28:09-05:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Image Width                     : 664
Image Height                    : 498
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Comment                         : 1dcd64e16d97507052d67a6d0557ee8d
Image Size                      : 664x498
Megapixels                      : 0.331
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Images# vi
root@kali:~/Downloads/recup_dir.2/forensics_challenge/Images#
```

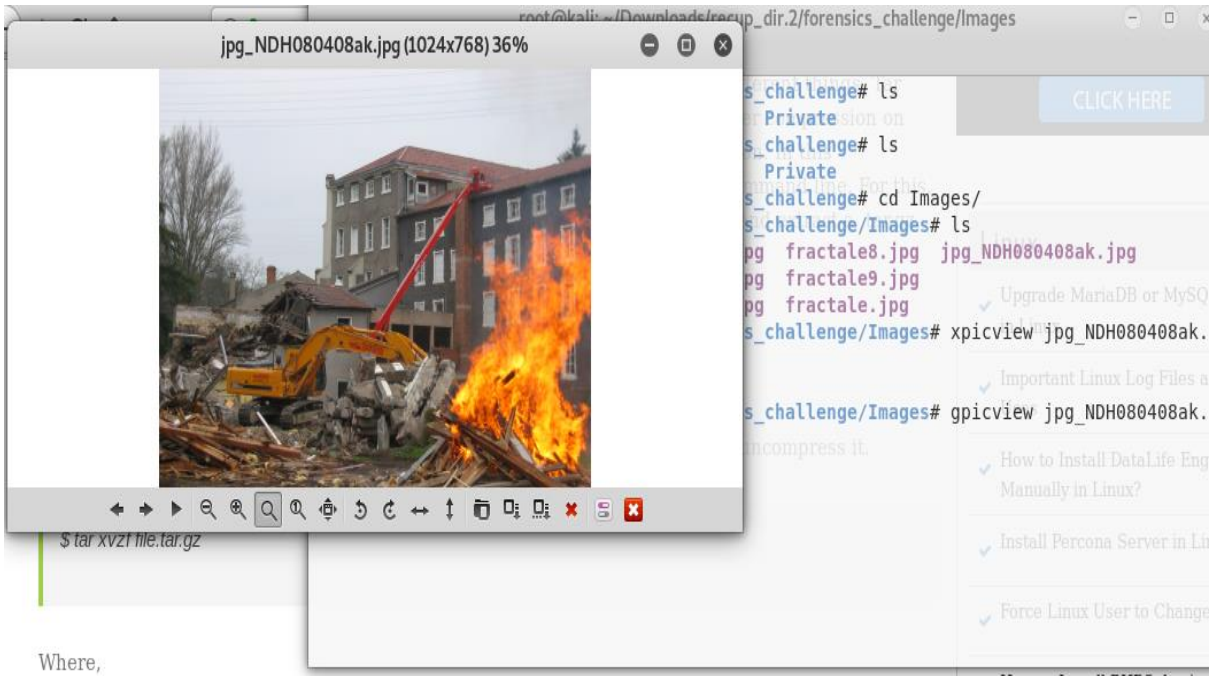
MD5 Hash 10:

Finding this MD5 is very interesting and it is super cool.

Inside the Images directory you can see the all files, one file is showing too different and open the image from kernel using gpicview command, you can see the something wired image.

First, we can check use the internet and check, how can check the MD5 hash inside the image.

This step is very interesting,

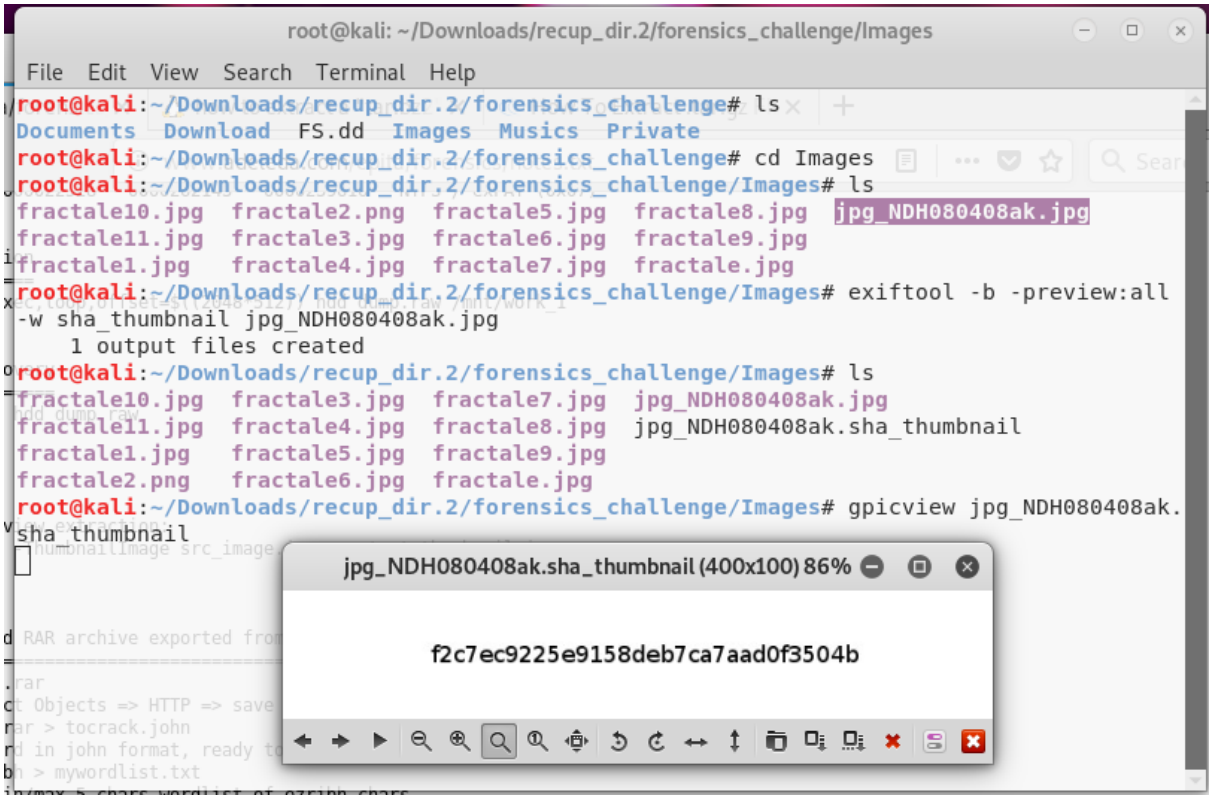


Forensics Report

Use exiftool -b -preview:all -w sha_thumbnail filename, we can see that one more file is created inside the Images directory,

Again, use the gpicview command to view the image,

You can use command like "**gpicview filename**", it will show the MD5 password.



This is the end of the report