**Forensics Report**

**Prepared for**

**hdd.dd**

**application**

**Finding MD5 Hashes**

Prepared by

**Bashetty Arun Kumar**

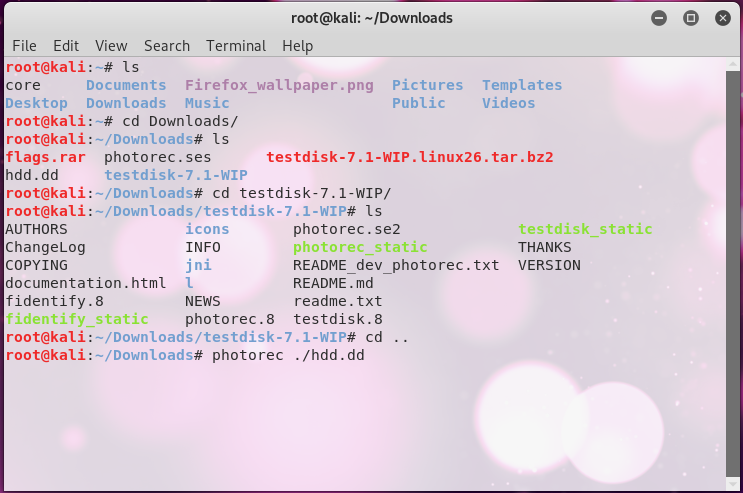
**Master of Computer Security**

**27-December-2018**

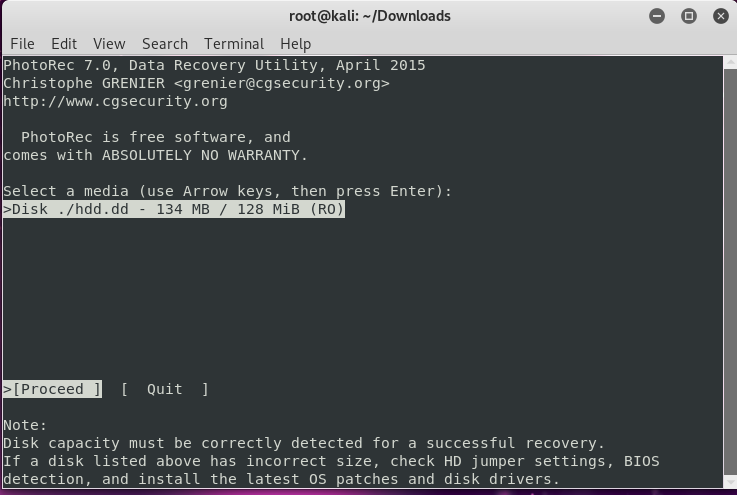
**Steps to recover the .tar.gz deleted files from the NTFS partition:**

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.

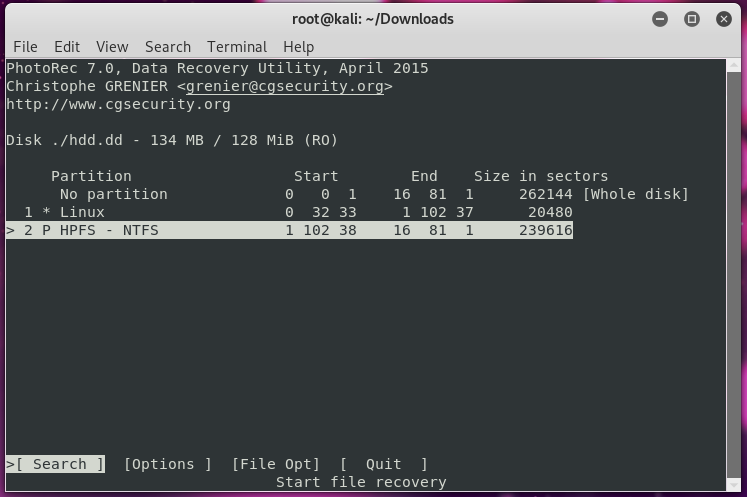
Now, first download the **Photorec** application from <https://www.cgsecurity.org/wiki/PhotoRec_FR> , this application is used to recover all files from hard disk.

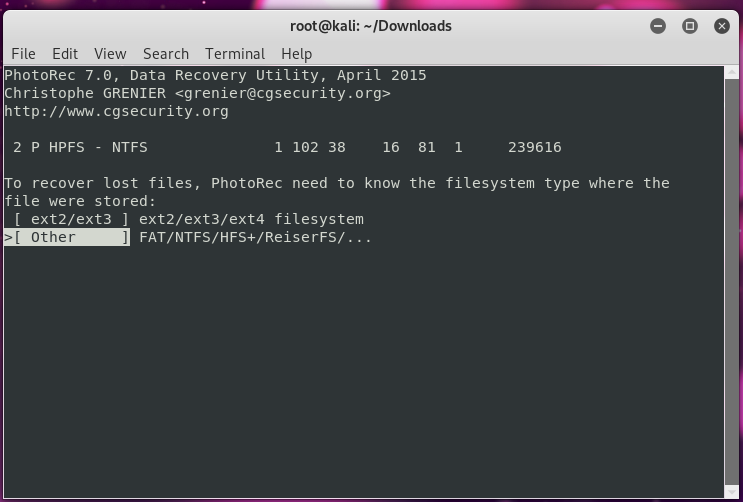


When you enter photorec ./hdd.dd, it will start hdd.dd application inside the photorec software and you can see the size of hard disk.

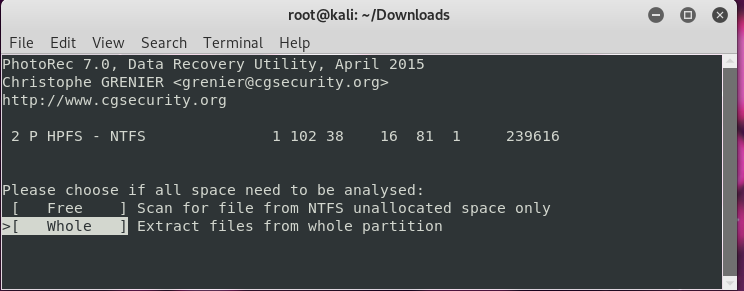


* Click on proceed and it will display 2 partitions, and you have to choose which partition we retrieve and after research we found HPFS-NTFS contain data. So, click proceed on 2nd partition.



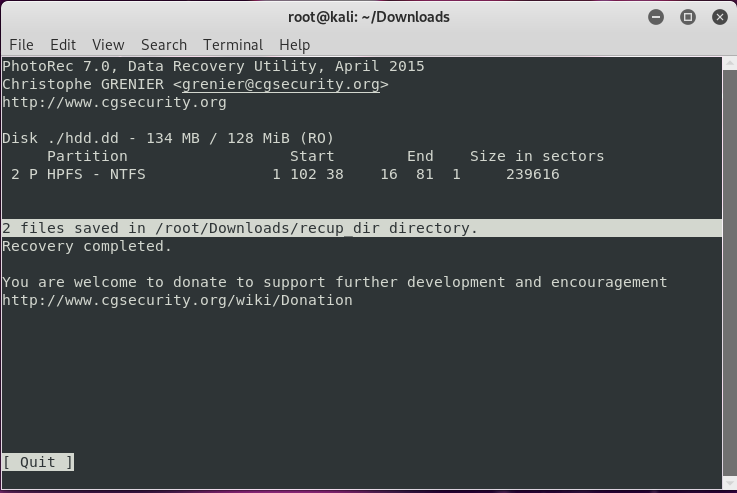


Now, it will ask to extract whole partition or just NTFS unallocated space only, click on whole option to get all recovered files,



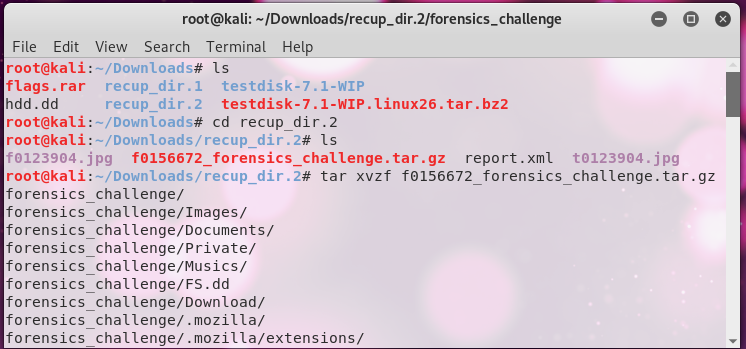
After clicking on proceed, it displays those recovered files stored inside /root/Downloads/recup\_dir directory.

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



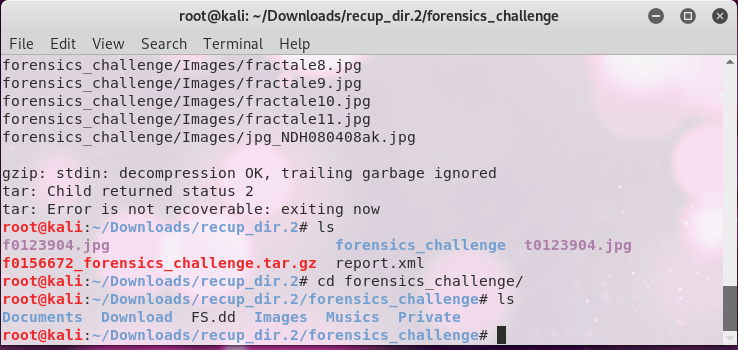
Inside download you can check the .tar.gz file, but you must extract to see inside the files

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



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.



**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:**

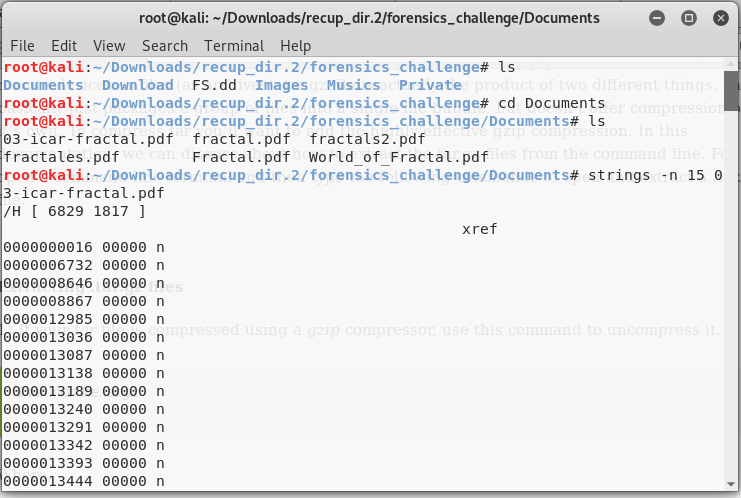
This command we already know that converting the string to base64 decoded.

**Wireshark:**

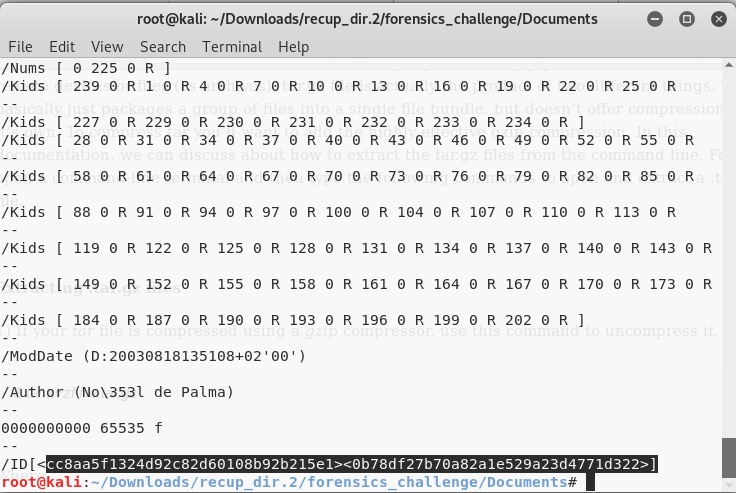
Wireshark is open source, it is used for network troubleshooting, analysis, software and communications protocol development, and education

**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.



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

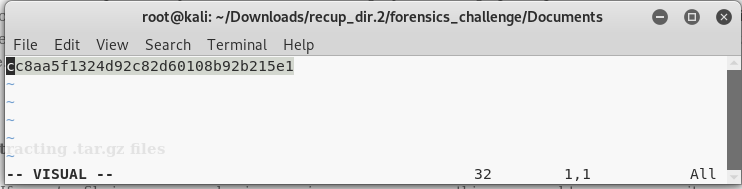


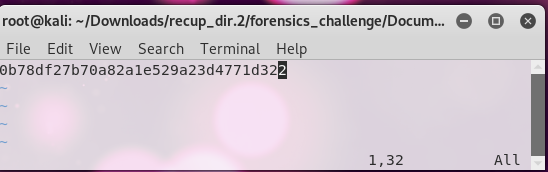
**Note:**

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.

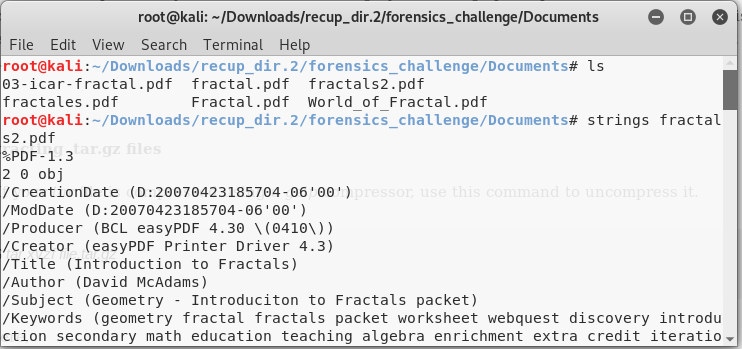




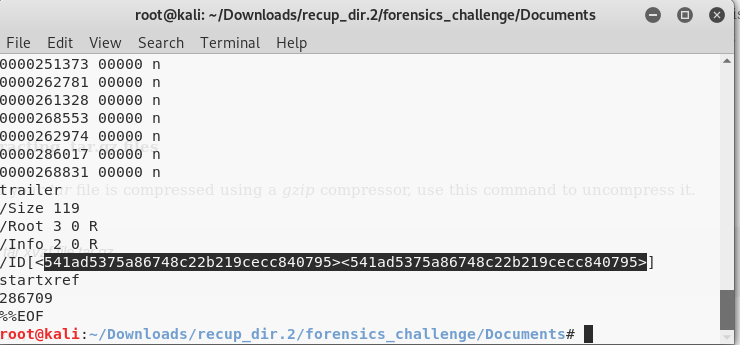
**MD5 Hashes 3 & 4:**

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.



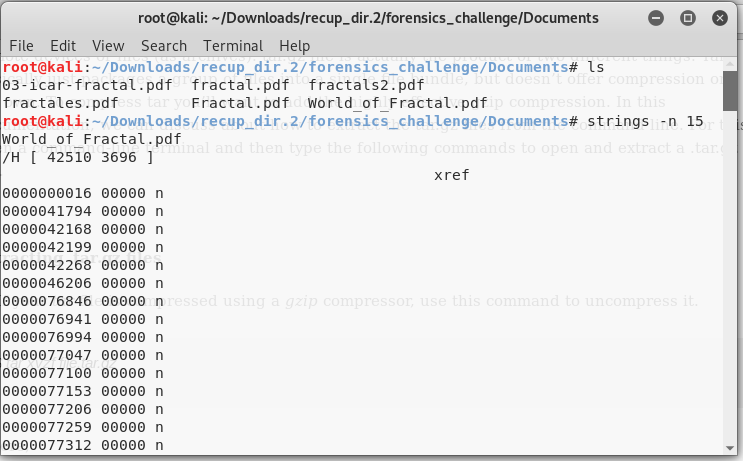
Here , you can see the 2 more hashes with 32 bits.



**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.



**MD5 Hash 7:**

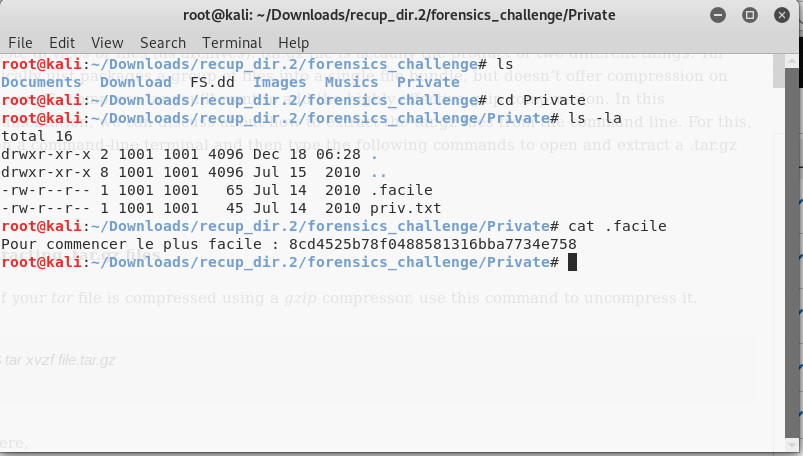
This one you can find easily without using any stress

=>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

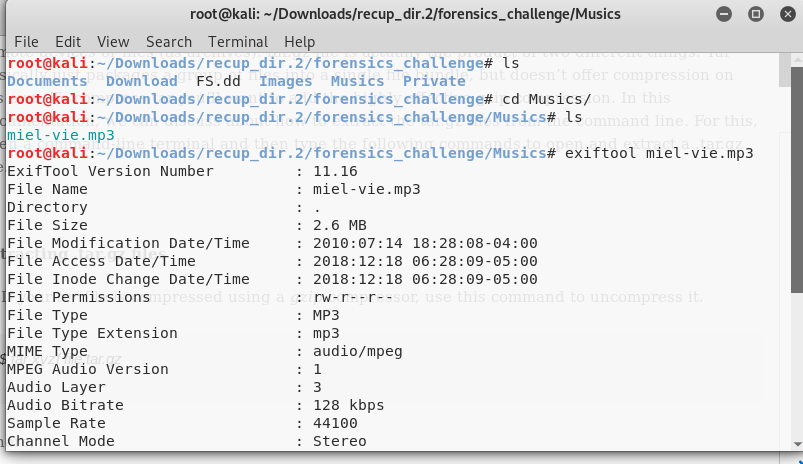
=>Inside **.facile** folder we found the hash.



**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.

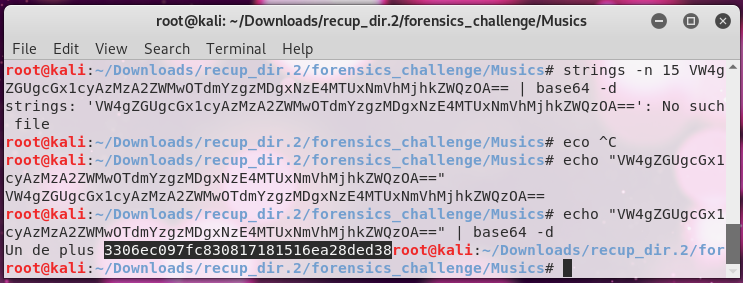


Below screenshot we can see Year look like MD5 has, after checking I found it is half MD5,

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



* 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.

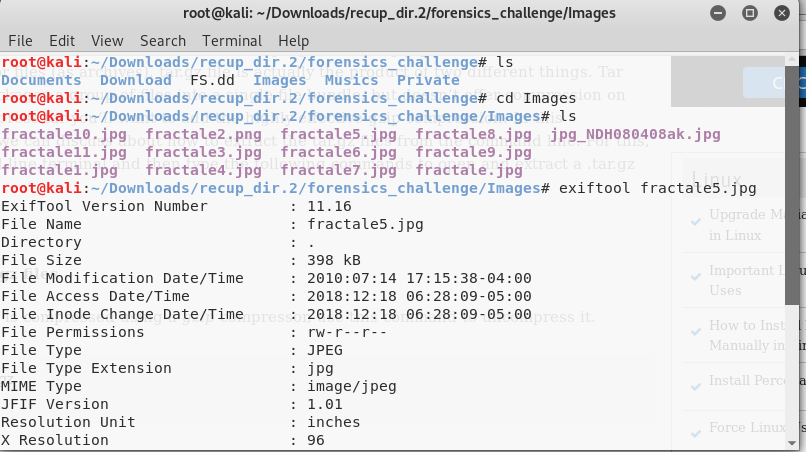


**MD5 Hash 9:**

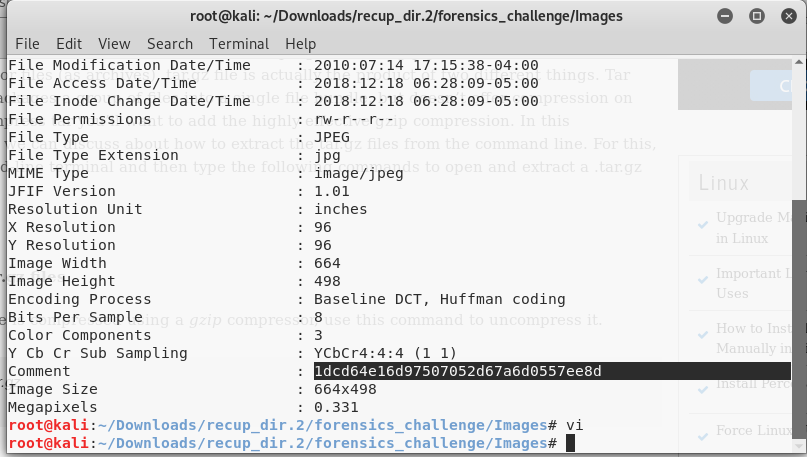
Change the directory to Images and use ls command to display inside the files,

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



You can see the MD5 hash beside the comment,



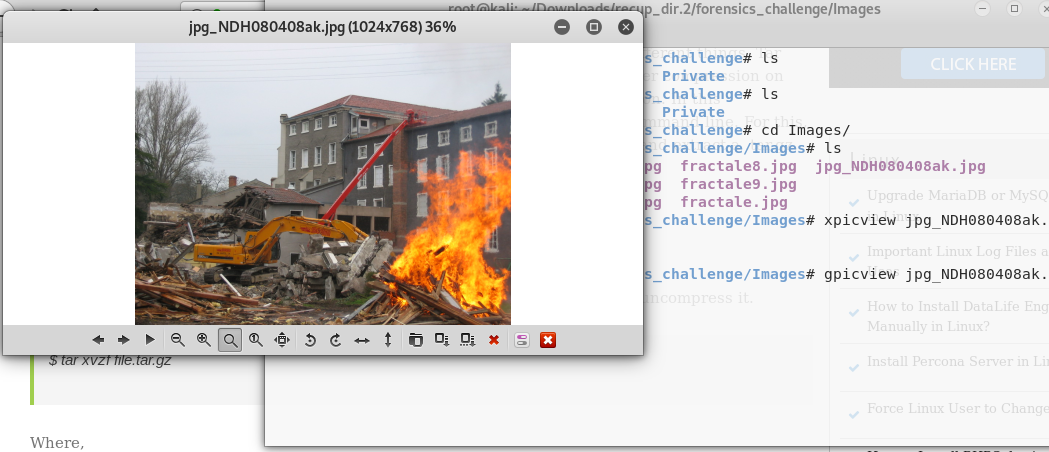
**MD5 Hash 10:**

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.

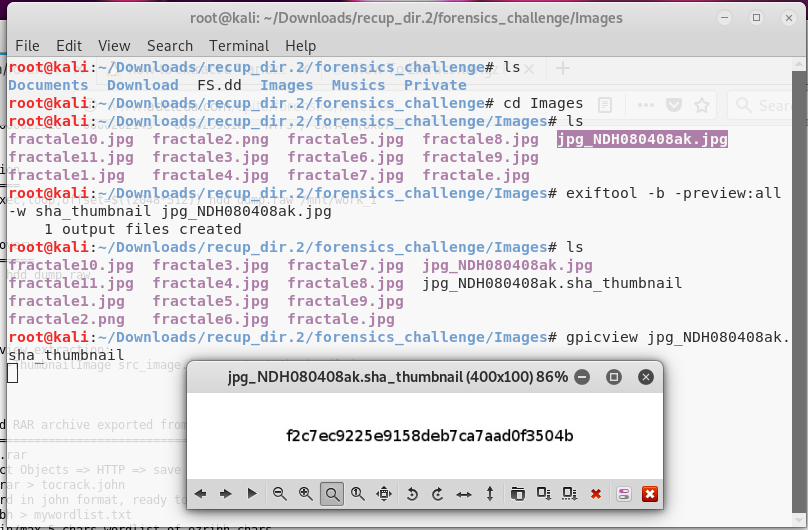
This step is very interesting,



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***