



DIGITAL FORENSICS AND INCIDENTS RESPONSE

- Yogitha satya sai Pantham

SUMMARY

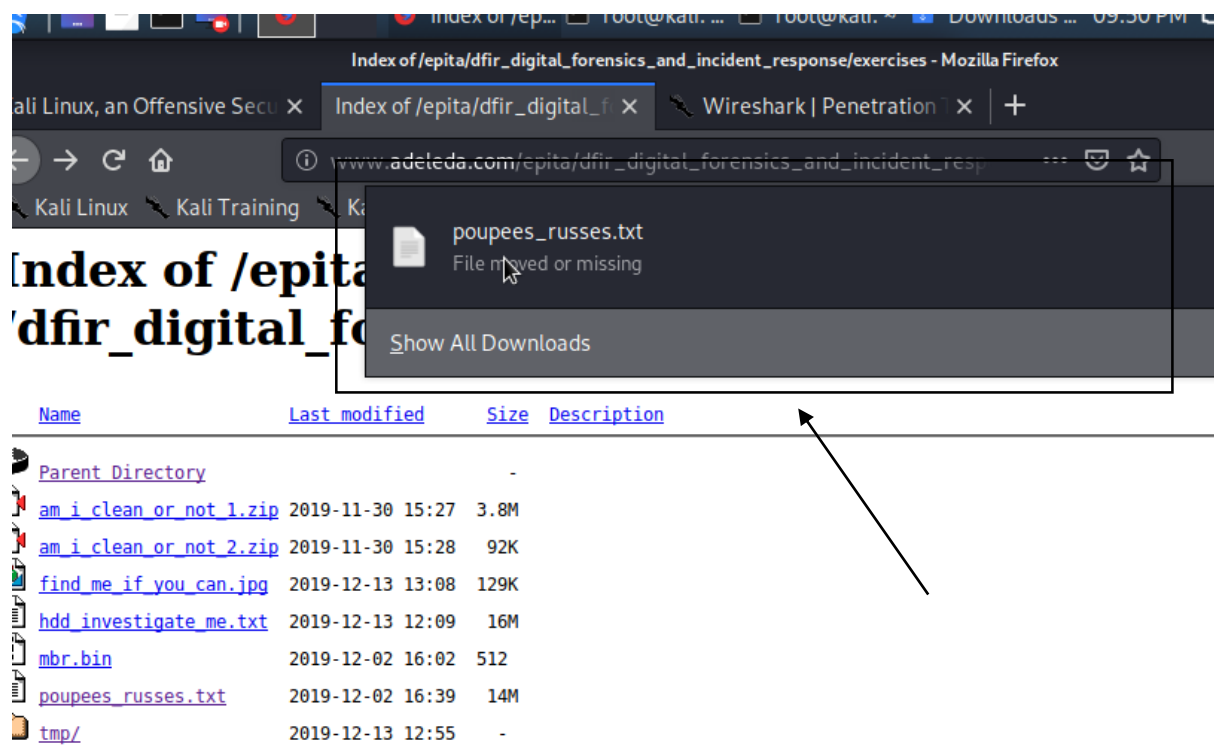
First, we have to download the poupees_russes.txt file from

http://www.adeleda.com/epita/dfir_digital_forensics_and_incident_response/exercises/poupees_russes.txt

It is an encrypted file and we need to decode this file.

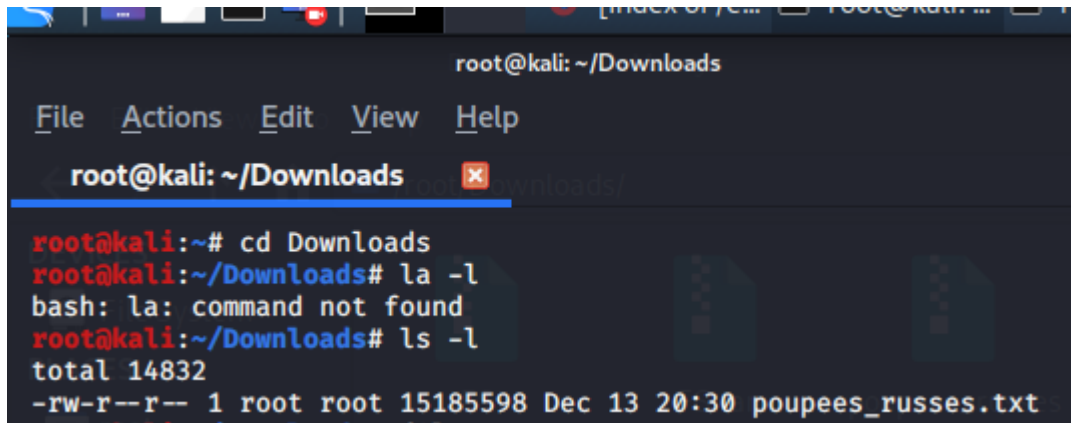
PROCESS

We have to download the required poupees_russes.txt file.



STEP-1:

We have to check whether it is downloaded or no.

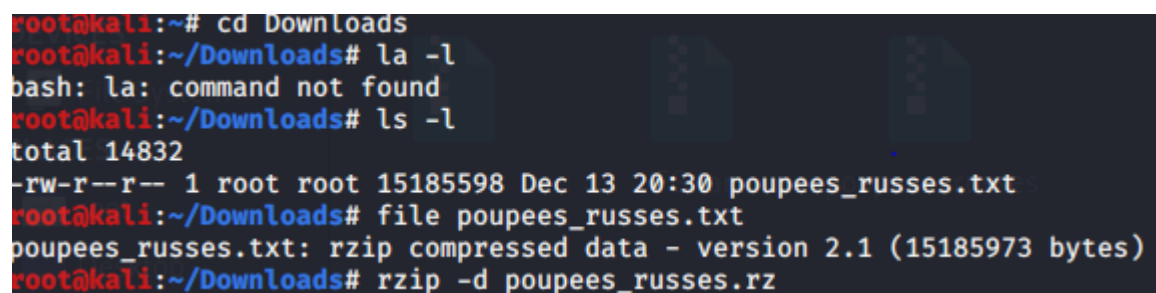
A terminal window titled 'root@kali: ~/Downloads' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the following commands and output:

```
root@kali:~# cd Downloads
root@kali:~/Downloads# la -l
bash: la: command not found
root@kali:~/Downloads# ls -l
total 14832
-rw-r--r-- 1 root root 15185598 Dec 13 20:30 poupees_russes.txt
```

We can see that the file is in Downloads block.

STEP-2:

Now, change the poupees_russes.txt file into poupees_russes.rz file and then we can see it as an zip file by using the below command.

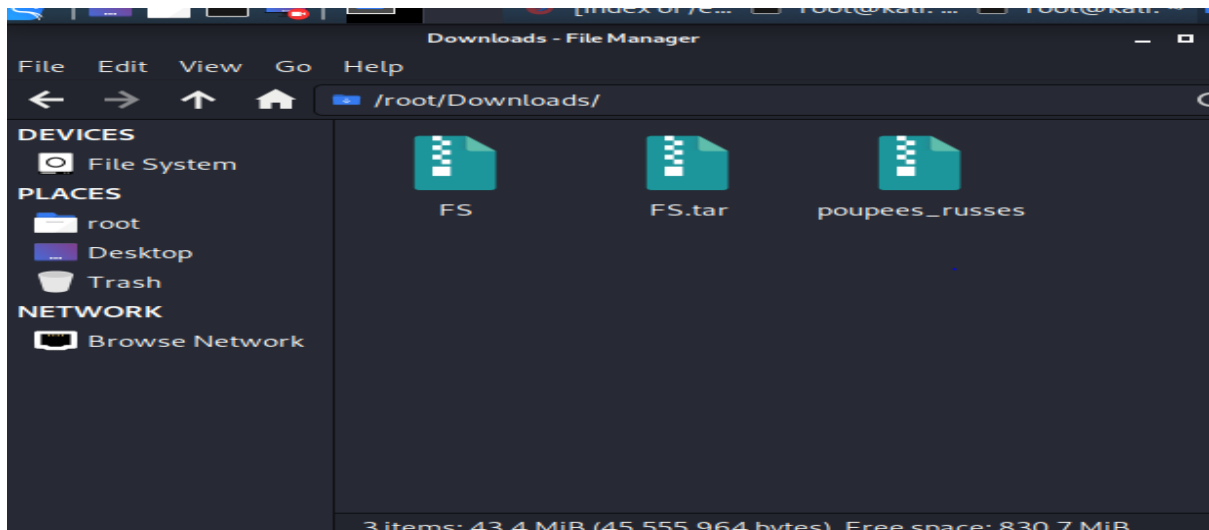
A terminal window titled 'root@kali: ~/Downloads' showing the following commands and output:

```
root@kali:~# cd Downloads
root@kali:~/Downloads# la -l
bash: la: command not found
root@kali:~/Downloads# ls -l
total 14832
-rw-r--r-- 1 root root 15185598 Dec 13 20:30 poupees_russes.txt
root@kali:~/Downloads# file poupees_russes.txt
poupees_russes.txt: rzip compressed data - version 2.1 (15185973 bytes)
root@kali:~/Downloads# rzip -d poupees_russes.rz
```

STEP-3:

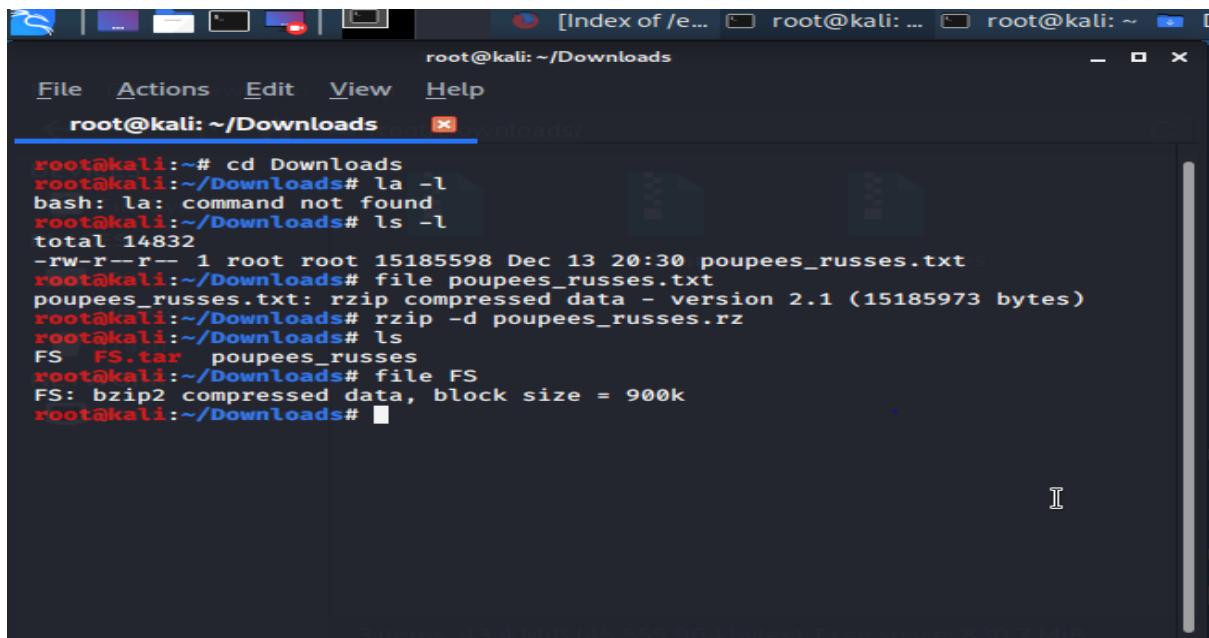
- 1) Extract the poupees_russes.rz file and we can see a new FS.rar file

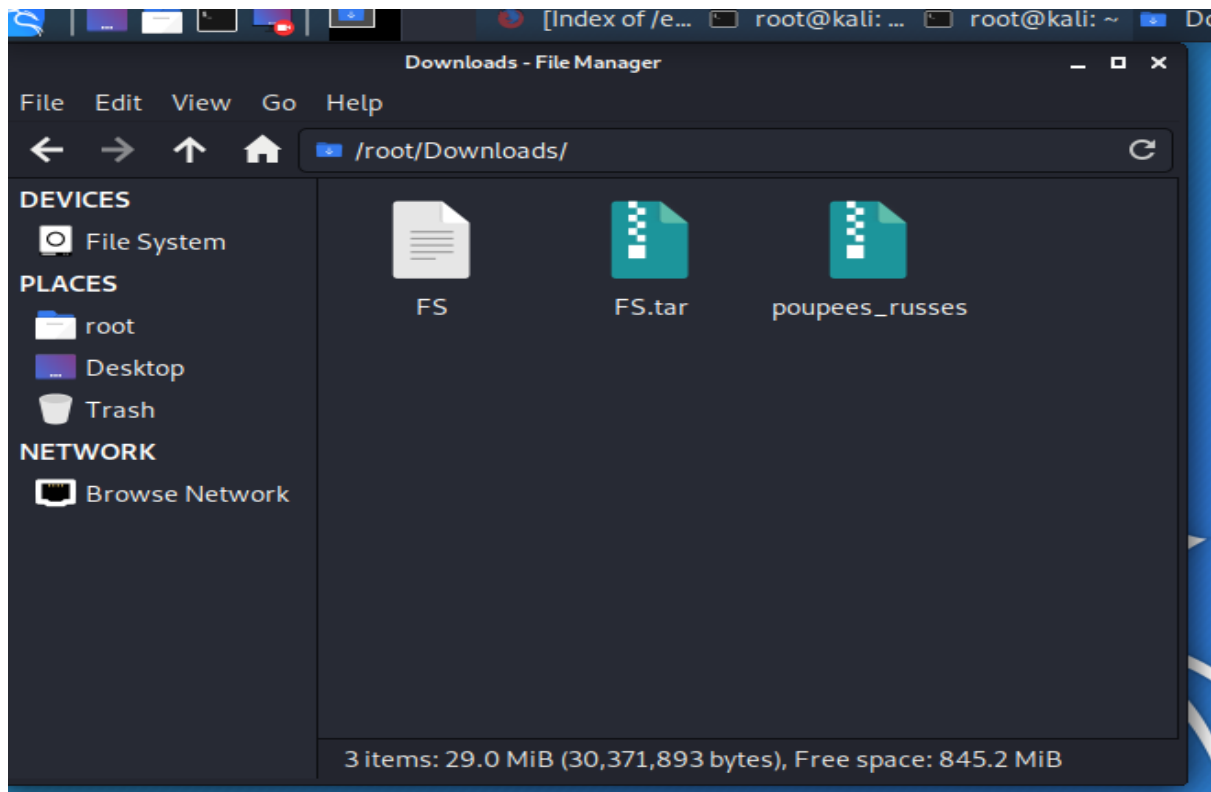
- 2) Then, again extract the FS.rar file and then we can find FS as a new file as shown below.



STEP-4:

In the below picture we can see that the file FS has the compressed data.





THANK YOU