FORENSICS: FOLLOW THE STREAM BY Monhal

EASY

Scenario:

During a Cyber Criminal investigation, a suspect hinted that the password for his computer is backed up on one of his flash drives.
You found a suspicious flash drive containing mostly useless text files. But you suspect there is something else hidden.

Objectuves:

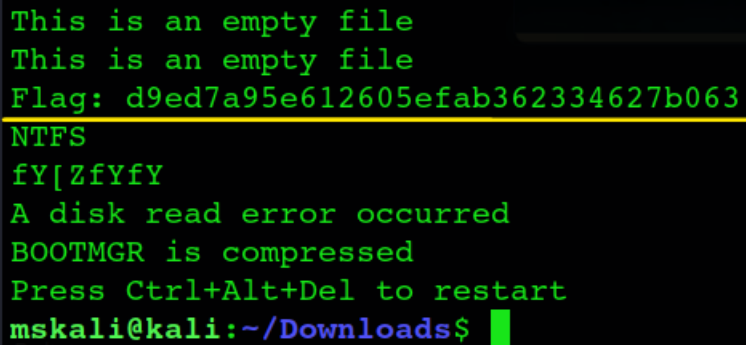- Investigate the drive image and find the password hidden within the files.

Used tools:

   Strings

After downloading the file and unzipping it in kali, the file is investigated using 'strings' command : strings -n 10 [filename]
The flag is displayd in the output.

Figure 1 - strings output


```
This is an empty file
This is an empty file
Flag: d9ed7a95e612605efab362334627b063
NTFS
fY[ZfYfY
A disk read error occurred
BOOTMGR is compressed
Press Ctrl+Alt+Del to restart
mskali@kali:~/Downloads$
```

CHALLENGE PWNED!