Description

All we know is the file with the flag is named `down-at-the-bottom.txt`... Disk image: [dds2-alpine.flag.img.gz]()

Hints

- The sleuthkit has some great tools for this challenge as well.
- Sleuthkit docs here are so helpful: [TSK Tool Overview]()
- This disk can also be booted with qemu!

Solución

```
┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ gzip -d dds*.gz

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ ls
dds2-alpine.flag.img  dd-sleuth-2.md

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ file dds2-alpine.flag.img
dds2-alpine.flag.img: DOS/MBR boot sector; partition 1 : ID=0x83, active,
start-CHS (0x0,32,33), end-CHS (0x10,81,1), startsector 2048, 260096 sectors

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ fsstat dds2-alpine.flag.img
Cannot determine file system type

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ mmls dds2-alpine.flag.img
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   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0000262143   0000260096   Linux (0x83)

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ fsstat dds2-alpine.flag.img -o 2048
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext3
Volume Name:
Volume ID: dc53a3bb0ae739a5164c89db56bbb12f

Last Written at: 2021-02-16 13:21:20 (EST)
Last Checked at: 2021-02-16 13:21:19 (EST)

Last Mounted at: 2021-02-16 13:21:19 (EST)
Unmounted properly
Last mounted on: /os/mnt

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype,
Read Only Compat Features: Sparse Super, Large File,

Journal ID: 00
Journal Inode: 8

METADATA INFORMATION
--------------------------------------------
Inode Range: 1 - 32513
Root Directory: 2
Free Inodes: 30605

CONTENT INFORMATION
--------------------------------------------
Block Range: 0 - 130047
Block Size: 1024
Reserved Blocks Before Block Groups: 1
Free Blocks: 45669

BLOCK GROUP INFORMATION
--------------------------------------------
Number of Block Groups: 16
Inodes per group: 2032
Blocks per group: 8192
```

```
Group: 0:
  Inode Range: 1 - 2032
  Block Range: 1 - 8192
  Layout:
    Super Block: 1 - 1
    Group Descriptor Table: 2 - 2
    Data bitmap: 259 - 259
    Inode bitmap: 260 - 260
    Inode Table: 261 - 514
    Data Blocks: 515 - 8192
  Free Inodes: 2020 (99%)
  Free Blocks: 514 (6%)
  Total Directories: 2

Group: 1:
  Inode Range: 2033 - 4064
  Block Range: 8193 - 16384
  Layout:
    Super Block: 8193 - 8193
    Group Descriptor Table: 8194 - 8194
    Data bitmap: 8451 - 8451
    Inode bitmap: 8452 - 8452
    Inode Table: 8453 - 8706
    Data Blocks: 8707 - 16384
  Free Inodes: 1837 (90%)
  Free Blocks: 818 (9%)
  Total Directories: 39

Group: 2:
  Inode Range: 4065 - 6096
  Block Range: 16385 - 24576
  Layout:
    Data bitmap: 16385 - 16385
    Inode bitmap: 16386 - 16386
    Inode Table: 16387 - 16640
    Data Blocks: 16387 - 16386, 16641 - 24576
  Free Inodes: 2023 (99%)
  Free Blocks: 1324 (16%)
  Total Directories: 1

Group: 3:
  Inode Range: 6097 - 8128
  Block Range: 24577 - 32768
  Layout:
    Super Block: 24577 - 24577
    Group Descriptor Table: 24578 - 24578
    Data bitmap: 24835 - 24835
    Inode bitmap: 24836 - 24836
    Inode Table: 24837 - 25090
    Data Blocks: 25091 - 32768
  Free Inodes: 2028 (99%)
  Free Blocks: 970 (11%)
  Total Directories: 3

Group: 4:
  Inode Range: 8129 - 10160
  Block Range: 32769 - 40960
  Layout:
    Data bitmap: 32769 - 32769
    Inode bitmap: 32770 - 32770
    Inode Table: 32771 - 33024
    Data Blocks: 32771 - 32770, 33025 - 40960
  Free Inodes: 1460 (71%)
  Free Blocks: 3026 (36%)
  Total Directories: 139

Group: 5:
  Inode Range: 10161 - 12192
  Block Range: 40961 - 49152
  Layout:
    Super Block: 40961 - 40961
    Group Descriptor Table: 40962 - 40962
    Data bitmap: 41219 - 41219
    Inode bitmap: 41220 - 41220
    Inode Table: 41221 - 41474
    Data Blocks: 41475 - 49152
  Free Inodes: 1399 (68%)
  Free Blocks: 1523 (18%)
  Total Directories: 78

Group: 6:
  Inode Range: 12193 - 14224
  Block Range: 49153 - 57344
  Layout:
    Data bitmap: 49153 - 49153
    Inode bitmap: 49154 - 49154
    Inode Table: 49155 - 49408
    Data Blocks: 49155 - 49154, 49409 - 57344
  Free Inodes: 1748 (86%)
  Free Blocks: 6774 (82%)
  Total Directories: 33
```

```
Group: 7:
  Inode Range: 14225 - 16256
  Block Range: 57345 - 65536
  Layout:
    Super Block: 57345 - 57345
    Group Descriptor Table: 57346 - 57346
    Data bitmap: 57603 - 57603
    Inode bitmap: 57604 - 57604
    Inode Table: 57605 - 57858
    Data Blocks: 57859 - 65536
  Free Inodes: 2007 (98%)
  Free Blocks: 7664 (93%)
  Total Directories: 21

Group: 8:
  Inode Range: 16257 - 18288
  Block Range: 65537 - 73728
  Layout:
    Data bitmap: 65537 - 65537
    Inode bitmap: 65538 - 65538
    Inode Table: 65539 - 65792
    Data Blocks: 65539 - 65538, 65793 - 73728
  Free Inodes: 2028 (99%)
  Free Blocks: 7936 (96%)
  Total Directories: 4

Group: 9:
  Inode Range: 18289 - 20320
  Block Range: 73729 - 81920
  Layout:
    Super Block: 73729 - 73729
    Group Descriptor Table: 73730 - 73730
    Data bitmap: 73987 - 73987
    Inode bitmap: 73988 - 73988
    Inode Table: 73989 - 74242
    Data Blocks: 74243 - 81920
  Free Inodes: 1951 (96%)
  Free Blocks: 7678 (93%)
  Total Directories: 4

Group: 10:
  Inode Range: 20321 - 22352
  Block Range: 81921 - 90112
  Layout:
    Data bitmap: 81921 - 81921
    Inode bitmap: 81922 - 81922
    Inode Table: 81923 - 82176
    Data Blocks: 81923 - 81922, 82177 - 90112
  Free Inodes: 1945 (95%)
  Free Blocks: 3 (0%)
  Total Directories: 1

Group: 11:
  Inode Range: 22353 - 24384
  Block Range: 90113 - 98304
  Layout:
    Data bitmap: 90113 - 90113
    Inode bitmap: 90114 - 90114
    Inode Table: 90115 - 90368
    Data Blocks: 90115 - 90114, 90369 - 98304
  Free Inodes: 2032 (100%)
  Free Blocks: 607 (7%)
  Total Directories: 0

Group: 12:
  Inode Range: 24385 - 26416
  Block Range: 98305 - 106496
  Layout:
    Data bitmap: 98305 - 98305
    Inode bitmap: 98306 - 98306
    Inode Table: 98307 - 98560
    Data Blocks: 98307 - 98306, 98561 - 106496
  Free Inodes: 2032 (100%)
  Free Blocks: 1232 (15%)
  Total Directories: 0

Group: 13:
  Inode Range: 26417 - 28448
  Block Range: 106497 - 114688
  Layout:
    Data bitmap: 106497 - 106497
    Inode bitmap: 106498 - 106498
    Inode Table: 106499 - 106752
    Data Blocks: 106499 - 106498, 106753 - 114688
  Free Inodes: 2031 (99%)
  Free Blocks: 1959 (23%)
  Total Directories: 1

Group: 14:
  Inode Range: 28449 - 30480
  Block Range: 114689 - 122880
  Layout:
    Data bitmap: 114689 - 114689
    Inode bitmap: 114690 - 114690
    Inode Table: 114691 - 114944
    Data Blocks: 114691 - 114690, 114945 - 122880
  Free Inodes: 2032 (100%)
  Free Blocks: 1721 (21%)
  Total Directories: 0

Group: 15:
  Inode Range: 30481 - 32512
  Block Range: 122881 - 130047
  Layout:
    Data bitmap: 122881 - 122881
    Inode bitmap: 122882 - 122882
    Inode Table: 122883 - 123136
    Data Blocks: 122883 - 122882, 123137 - 130047
  Free Inodes: 2032 (100%)
  Free Blocks: 1920 (26%)
  Total Directories: 0

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ fsstat dds2-alpine.flag.img -o 2048 | head
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext3
Volume Name:
Volume ID: dc53a3bb0ae739a5164c89db56bbb12f

Last Written at: 2021-02-16 13:21:20 (EST)
Last Checked at: 2021-02-16 13:21:19 (EST)

Last Mounted at: 2021-02-16 13:21:19 (EST)

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ fls -r  dds2-alpine.flag.img -o 2048 | grep down-at
+ r/r 18291:    down-at-the-bottom.txt

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ fls -r  dds2-alpine.flag.img -o 2048 | grep down
++ d/d 2177:    if-down.d
++ d/d 2178:    if-post-down.d
++ d/d 2180:    if-pre-down.d
++ d/d 2204:    shutdown
+ r/r 18291:    down-at-the-bottom.txt
+ l/l 18311:    ifdown
+ r/r 18344:    openrc-shutdown
+++++ r/r 12472:        down.sh

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$ icat ./dds2-alpine.flag.img -o 2048 18291
   _     _     _     _     _     _     _     _     _     _     _     _     _
  / \   / \   / \   / \   / \   / \   / \   / \   / \   / \   / \   / \   /
\
 ( p ) ( i ) ( c ) ( o ) ( C ) ( T ) ( F ) ( { ) ( f ) ( 0 ) ( r ) ( 3 ) ( n
)
  \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/
\_/
   _     _     _     _     _     _     _     _     _     _     _     _     _
  / \   / \   / \   / \   / \   / \   / \   / \   / \   / \   / \   / \   /
\
 ( s ) ( 1 ) ( c ) ( 4 ) ( t ) ( 0 ) ( r ) ( _ ) ( n ) ( 0 ) ( v ) ( 1 ) ( c
)
  \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/
\_/
   _     _     _     _     _     _     _     _     _     _     _
  / \   / \   / \   / \   / \   / \   / \   / \   / \   / \   / \
 ( 3 ) ( _ ) ( f ) ( 5 ) ( 5 ) ( 6 ) ( 5 ) ( e ) ( 7 ) ( b ) ( } )
  \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/   \_/

┌──(kali㉿kali)-
[~/…/parciales/parcial_02/parte_04_forensic_02/disk_disk_sleuth_02]
└─$
```

Bandera

```
flag: picoCTF{f0r3ns1c4t0r_n0v1c3_f5565e7b}
```

Notas Adicionales

Referencias

-