L’KRIM MOHAMED-ANOUAR

KAROUGBE ESSOGNIM GILLES

OBJECTIF :

Script Python pour l'analyse d’une image disque, l’on va automatiser l’Extraction du MBR, de la table des partitions, les types de système de fichier utiliser sur chacune de ces partitions. Le script devra aussi détecter les erreurs et de les corrigées en menant une analyse approfondie.

PARTIE-1

Nous avons fait l’analyse de l’image « deviceImageCorrupted.raw » que nous avons utilisé dans le TP :

Grâce au script, nous pouvons afficher les différentes sections suivantes : MBR, secteur de démarrage et table de partition :

```
------------------------------------MBR-------------------------------------------------

33c08ed0bc007cfb5007501ffcbe1b7cbf1b065057b9e501f3a4cbbdbe07b104386e007c09751383c510e2f4cd188bf583c610497419382c74f6a0b507b4078bf0ac3c0
-----------------------------------------------------------------------------------

-------------------------------------------BOOT_SECTOR-----------------------------------------------

33c08ed0bc007cfb5007501ffcbe1b7cbf1b065057b9e501f3a4cbbdbe07b104386e007c09751383c510e2f4cd188bf583c610497419382c74f6a0b507b4078bf0ac3c0
-----------------------------------------------------------------------------------

-----------------------------------------Partition_Table-------------------------------------------

8001010083fe3f083f0000008a3402000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
-----------------------------------------------------------------------------------
```

Le nombre de partition :

```
1) Nombre de partitions est  1
```

Avant la correction de l'erreur :

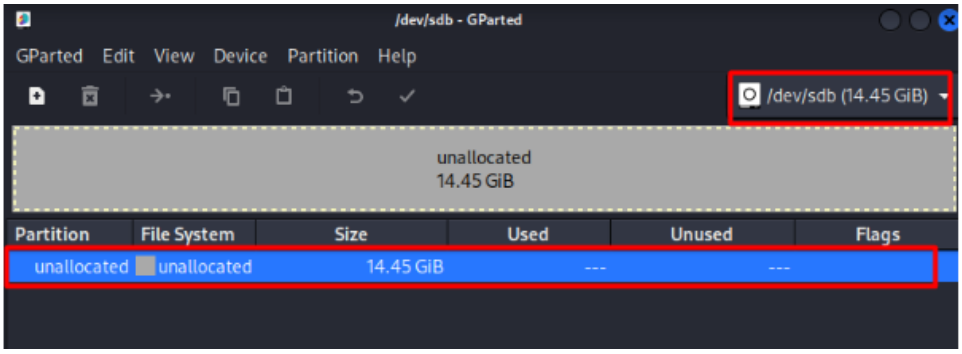
```
 *) --------------------Pour Partition 1 :----------------------------
1) Type de partition 1 est : EXT2_Unix
2) Le secteur qui démarre la première partition est : 63
==>et tant que le FS est EXT alors faut ajouter 2(secteur de padding) donc ==>  65
3) la taille de la première partition en kilo-octets, selon le MBR : 72261.0  ko
4) 60230000 (little endian) ===> 00002360 (big endian)
le nombre d'inodes est : 9056
5)  91460000 (little endian) ===> 00004691 (big endian)
 le nombre de blocks est : 18065
6)04000000 (little endian) ===>  00000004(big endian)
 la taille d'un block est : 16384
*) La taille du fichier est :  74027520 octets
la vrai taille d'un block apartir de cette formule  (taille_fichier-(1024+1024))/blocks : 4097
il y a un erreur au niveau de system de partition 1
courrigement :
le nombre exacte de s_log_block_size est : 2 ==> 00000002 (hex) (big endian) ===> (little endian) b'\x02\x00\x00\x00'
la nouvelle partie courigge extraite du fichier est : b'\x02\x00\x00\x00'
```

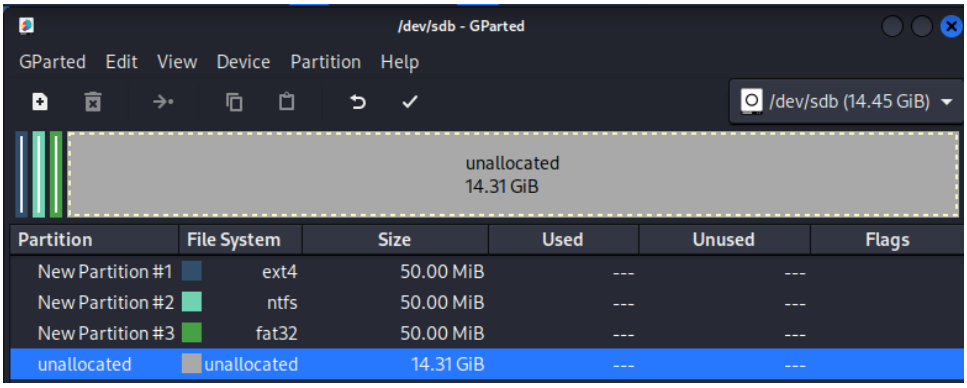
Lors de la prochaine exécution, l'erreur sera corrigée et aucune nouvelle erreur ne sera détectée :

```
*) --------------------Pour Partition 1 :----------------------------
1) Type de partition 1 est : EXT2_Unix
2) Le secteur qui démarre la première partition est : 63
==>et tant que le FS est EXT alors faut ajouter 2(secteur de padding) donc ==>  65
3) la taille de la première partition en kilo-octets, selon le MBR : 72261.0  ko
4) 60230000 (little endian) ===> 00002360 (big endian)
le nombre d'inodes est : 9056
5)  91460000 (little endian) ===> 00004691 (big endian)
 le nombre de blocks est : 18065
6)02000000 (little endian) ===>  00000002(big endian)
 la taille d'un block est : 4096
*) La taille du fichier est :  74027520 octets
la vrai taille d'un block apartir de cette formule  (taille_fichier-(1024+1024))/blocks : 4097
il n y a pas un erreur au niveau de partition 1
```

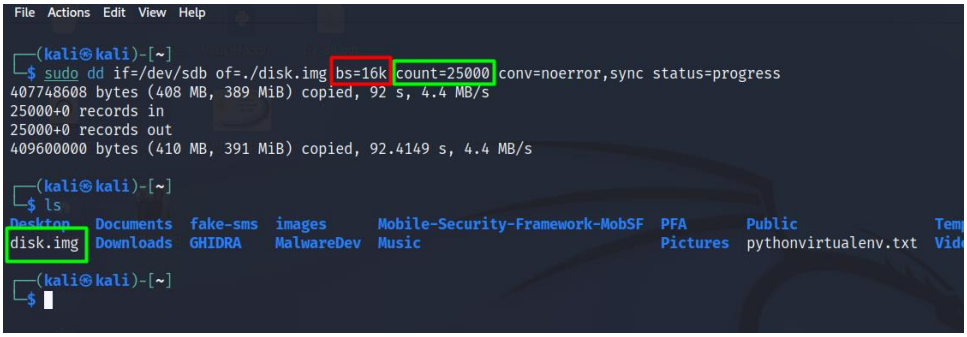
PARTIE-2

1. PARTIONNEMENT DU DISQUE PHYSIQUE

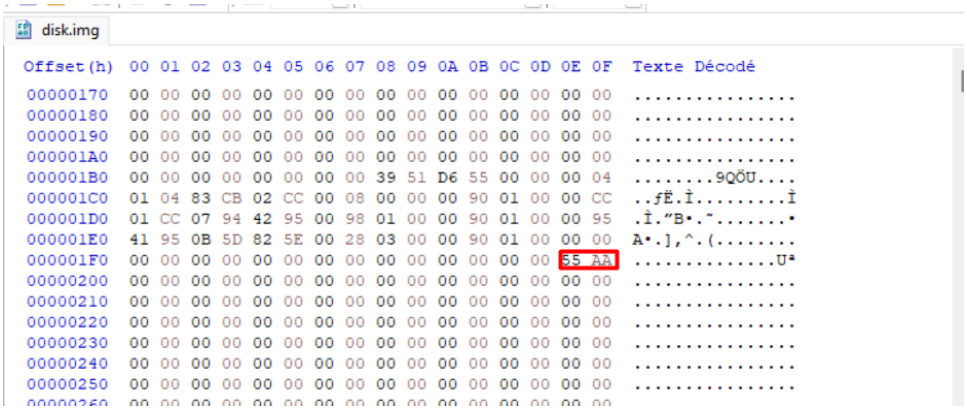




2. CREATION DE L'IMAGE



3. ANALYSE MANUELLE(HxD) DE L'IMAGE



4. ANALYSE AUTOMATISER DE L'IMAGE

```
PS C:\Users\hhss\Documents\Forensics\PROJET> python -u "c:\Users\hhss\Documents\Forensics\PROJET\
main.py"
-------------------------------------MBR-------------------------------------------------

fab800108ed0bc00b0b800008ed88ec0fbbe007cbf0006b90002f3a4ea21060000bebe073804750b83c61081fefe0775f
3eb16b402b001bb007cb2808a74018b4c02cd13ea007c0000ebfe000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000003951d65500000004010483cb02cc0008000009001000cc01cc0794429500980100009001000095419 50b5d82
5e00280300009001000000000000000000000000000000000055aa
-----------------------------------------------------------------------------------------
```

```
-----------------------------------------BOOT_SECTOR-----------------------------------------
----

fab800108ed0bc00b0b800008ed88ec0fbbe007cbf0006b90002f3a4ea21060000bebe073804750b83c61081fefe0775f
3eb16b402b001bb007cb2808a74018b4c02cd13ea007c0000ebfe000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000003951d6550000
-----------------------------------------------------------------------------------------
```

```
-----------------------------------------Partition_Table-------------------------------------
-------

0004010483cb02cc0008000009001000cc01cc0794429500980100009001000095419 50b5d825e00280300009001000
0000000000000000000000000000000000
-----------------------------------------------------------------------------------------

[['00', '040104', '83', 'cb02cc', '00080000', '00900100'], ['00', 'cc01cc', '07', '944295', '0098
0100', '00900100'], ['00', '954195', '0b', '5d825e', '00280300', '00900100'], ['00', '000000', '0
0', '000000', '00000000', '00000000']]
(3, ('EXT2_Unix', 'NTFS', 'FAT32', ''))
```

```
  ---------------------------------------TP1-------------------------------------------------

  Nombre de partitions: 3

   *) --------------------Pour Partition 1 :----------------------------
  Q1-Secteur sur lequel commence la partition: 32768
  Q2-Secteur sur lequel fini la partition:
  Q3-Système de fichier de la partition EXT2_Unix
  Q4-Taille de la partition en kilooctets : 525440.0 ko
```

```
   *) --------------------Pour Partition 2 :----------------------------
  Q1-Secteur sur lequel commence la partition: 1083648
  Q2-Secteur sur lequel fini la partition:
  Q3-Système de fichier de la partition NTFS
  Q4-Taille de la partition en kilooctets : 525440.0 ko

   *) --------------------Pour Partition 3 :----------------------------
  Q1-Secteur sur lequel commence la partition: 3179008
  Q2-Secteur sur lequel fini la partition:
  Q3-Système de fichier de la partition FAT32
  Q4-Taille de la partition en kilooctets : 525440.0 ko
```

```
---------------------------------------TP2-------------------------------------------------

4) 3e00ae47 (little endian) ===> 47ae003e (big endian)
le nombre d'inodes est : 1202585662
5)  14000014 (little endian) ===> 14000014 (big endian)
 le nombre de blocks est : 335544340
6)00000000 (little endian) ===>  00000000(big endian)
 la taille d'un block est : 1024
PS C:\Users\hhss\Documents\Forensics\PROJET>
PS C:\Users\hhss\Documents\Forensics\PROJET>
```