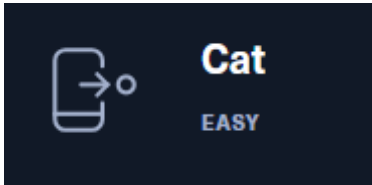


# Cat



By Youness LAGNAOUI

## Intro :

Ce challenge est un challenge de forensics mobile. L'objectif est d'extraire des données d'un dump de smartphone android

## Analyse du fichier

```
(kalilinux@kalilinux2022)-[~/HTB/Chall/Mobile/DEMO]
$ file cat.ab
cat.ab: Android Backup, version 5, Compressed, Not-Encrypted
```

Le fichier est un Android Backup.

Pour extraire la data de ce fichier on peut utiliser un outils appelé abe.jar (lien : <https://github.com/nelenkov/android-backup-extractor/releases>)

Avec la commande :

```
java -jar abe.jar unpack cat.ab extract.tar
```

cette commande permet de convertir le backup Android en archive .tar dézippable

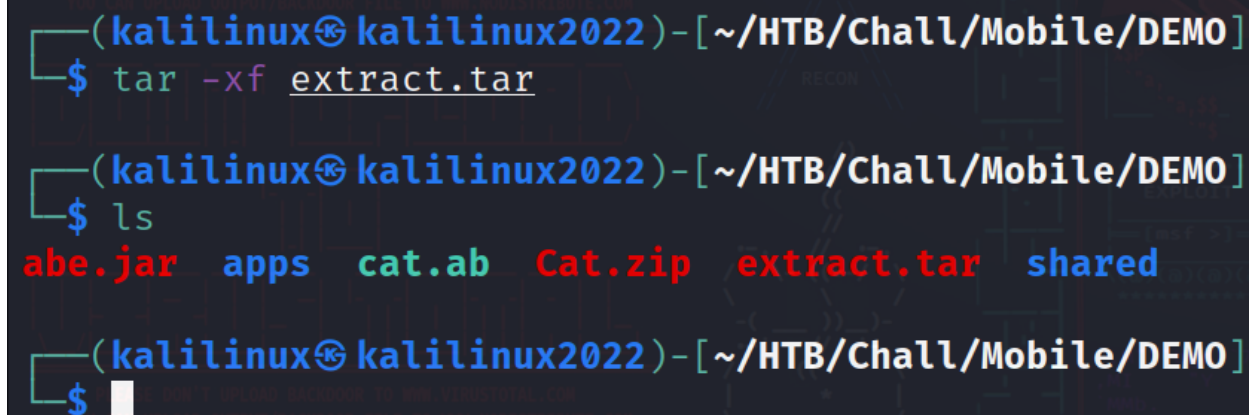
```
(kalilinux@kalilinux2022)-[~/HTB/Chall/Mobile/DEMO]
$ java -jar abe.jar unpack cat.ab extract.tar
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
0% 1% 2% 3% 4% 5% 6% 7% 8% 9% 10% 11% 12% 13% 14% 15% 16% 17% 18% 19% 20% 21% 22% 23% 24% 25% 26% 27% 28% 29% 30% 31% 32% 33%
34% 35% 36% 37% 38% 39% 40% 41% 42% 43% 44% 45% 46% 47% 48% 49% 50% 51% 52% 53% 54% 55% 56% 57% 58% 59% 60% 61% 62% 63% 64% 65%
66% 67% 68% 69% 70% 71% 72% 73% 74% 75% 76% 77% 78% 79% 80% 81% 82% 83% 84% 85% 86% 87% 88% 89% 90% 91% 92% 93% 94% 95% 96%
97% 98% 99% 100%
4853760 bytes written to extract.tar.

(kalilinux@kalilinux2022)-[~/HTB/Chall/Mobile/DEMO]
$ ls
abe.jar  cat.ab  Cat.zip  extract.tar

(kalilinux@kalilinux2022)-[~/HTB/Chall/Mobile/DEMO]
$
```

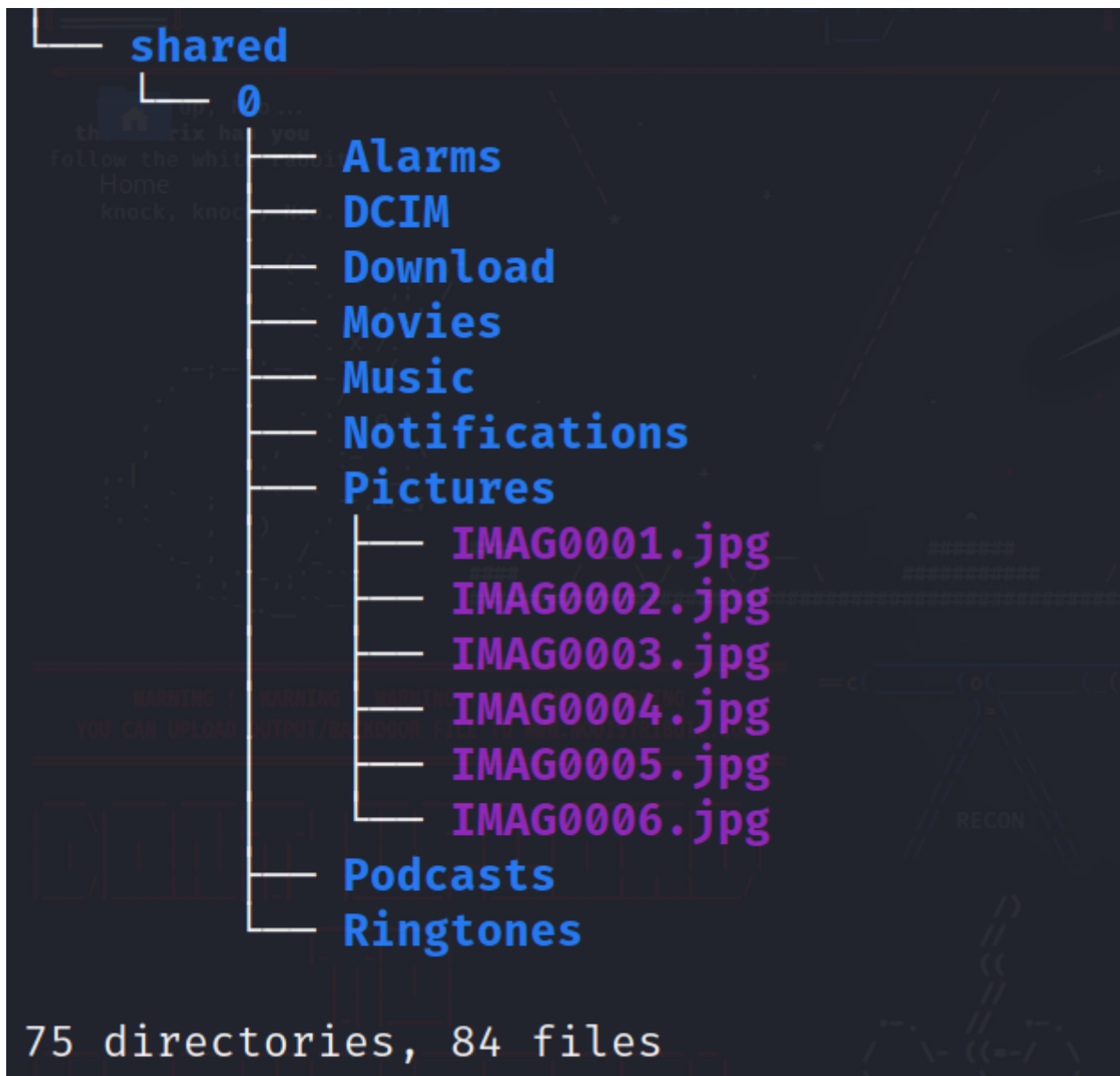
Maintenant que le backup est stocké dans un tar on peut dézipper le tar avec la commande :

```
tar -xf extract.tar
```

A terminal window with a dark background and light blue text. The prompt is '(kalilinux@kalilinux2022)-[~/HTB/Chall/Mobile/DEMO]'. The first command is '\$ tar -xf extract.tar'. The second command is '\$ ls', followed by the output: 'abe.jar apps cat.ab Cat.zip extract.tar shared'. The third command is '\$' followed by a cursor.

```
(kalilinux@kalilinux2022)-[~/HTB/Chall/Mobile/DEMO]  
$ tar -xf extract.tar  
  
(kalilinux@kalilinux2022)-[~/HTB/Chall/Mobile/DEMO]  
$ ls  
abe.jar  apps  cat.ab  Cat.zip  extract.tar  shared  
  
(kalilinux@kalilinux2022)-[~/HTB/Chall/Mobile/DEMO]  
$
```

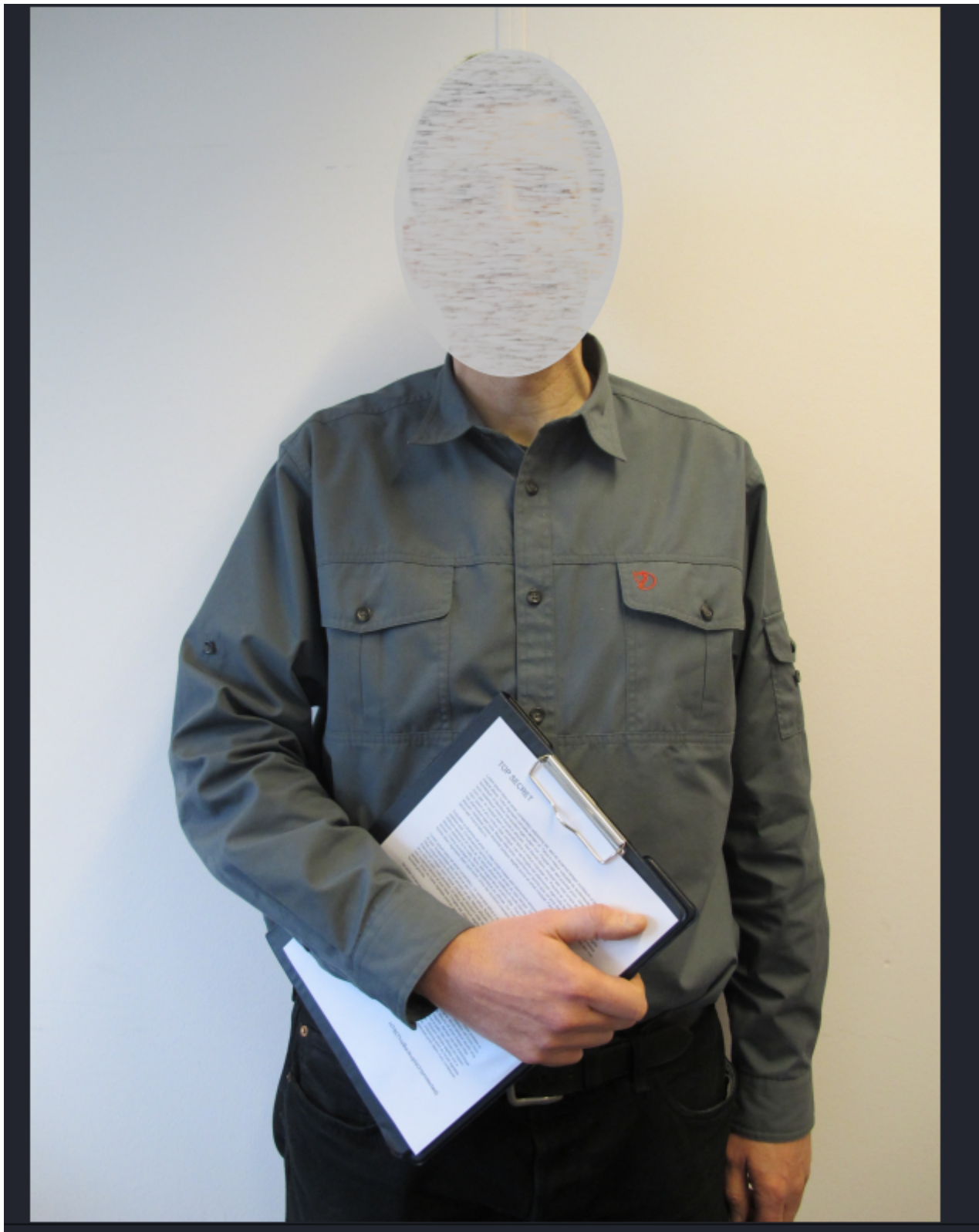
2 dossiers ont pop : apps et shared, utilisons la commande tree pour voir comment sont constituer les dossier au sein du dump :



Il y a plein de fichier mais on peut observer que dans le dossier shared/0/Pictures il y a des photo allons voir ça :

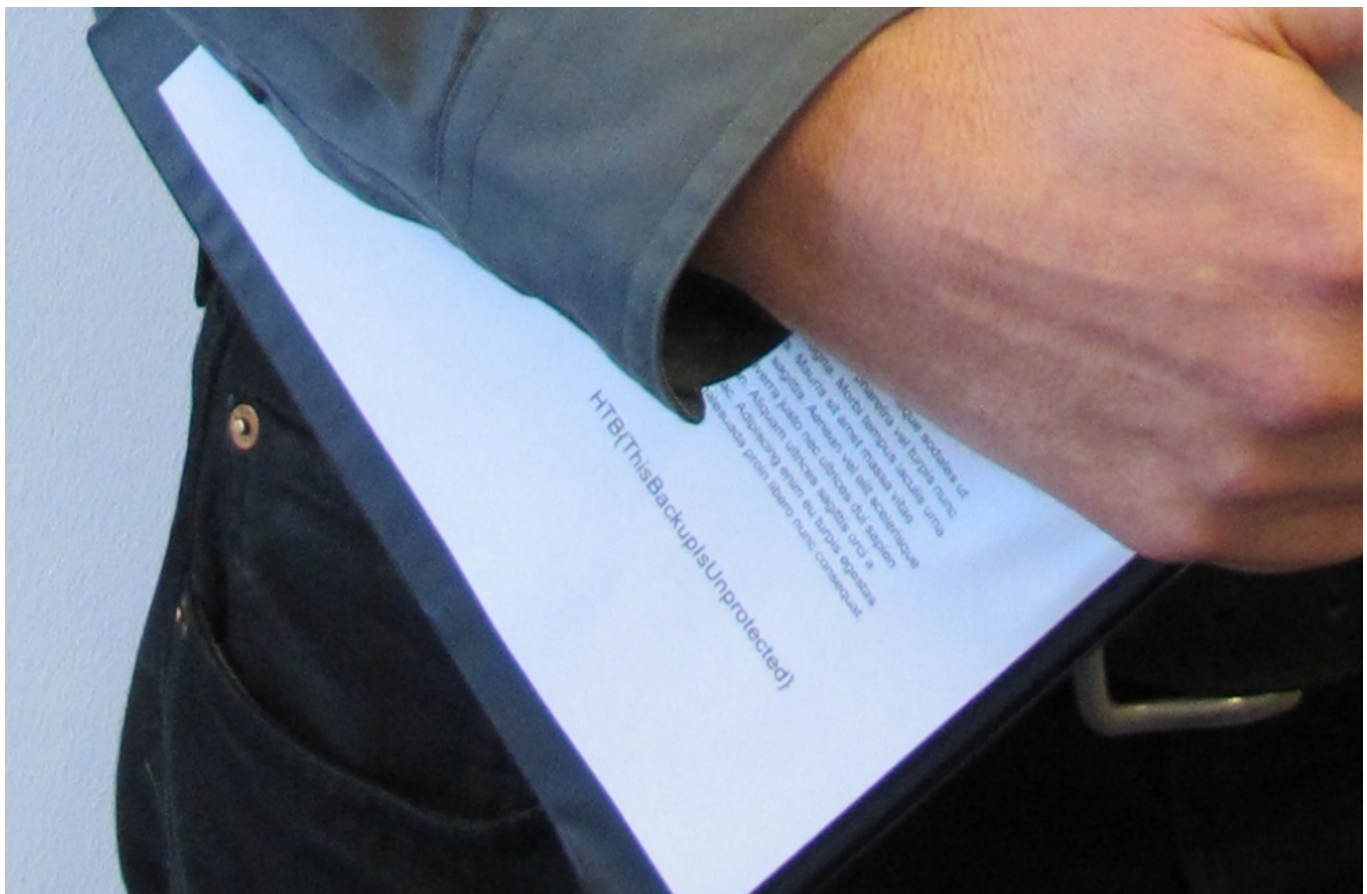


La plus part sont des images de chats tout mimi sauf une image :



Alors là j'ai passé un temps iiiiiincroyablement long avant de voir le flag.... j'ai regardé dans quasiment tous les fichiers du dump mais j'ai rien trouvé mais en fait si on zoom sur la photo on voit ça :





Le flag en tout petit évidemment, c'est du forensic ou un rendez vous chez l'ophtalmo ?

Bref voilà le flag :

```
HTB{ThisBackupIsUnprotected}
```