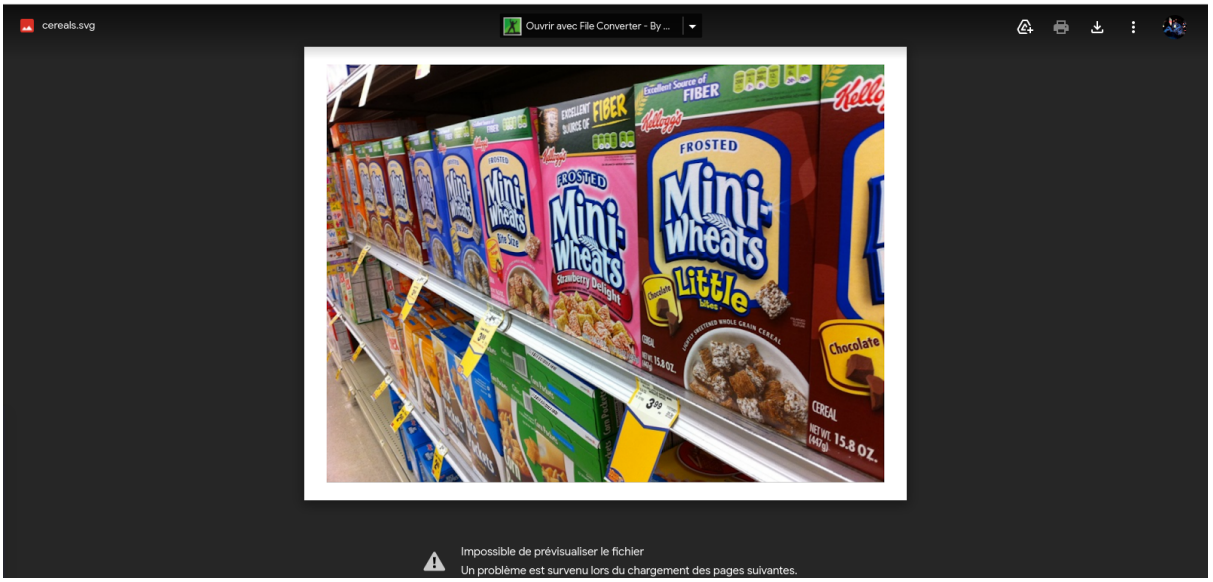
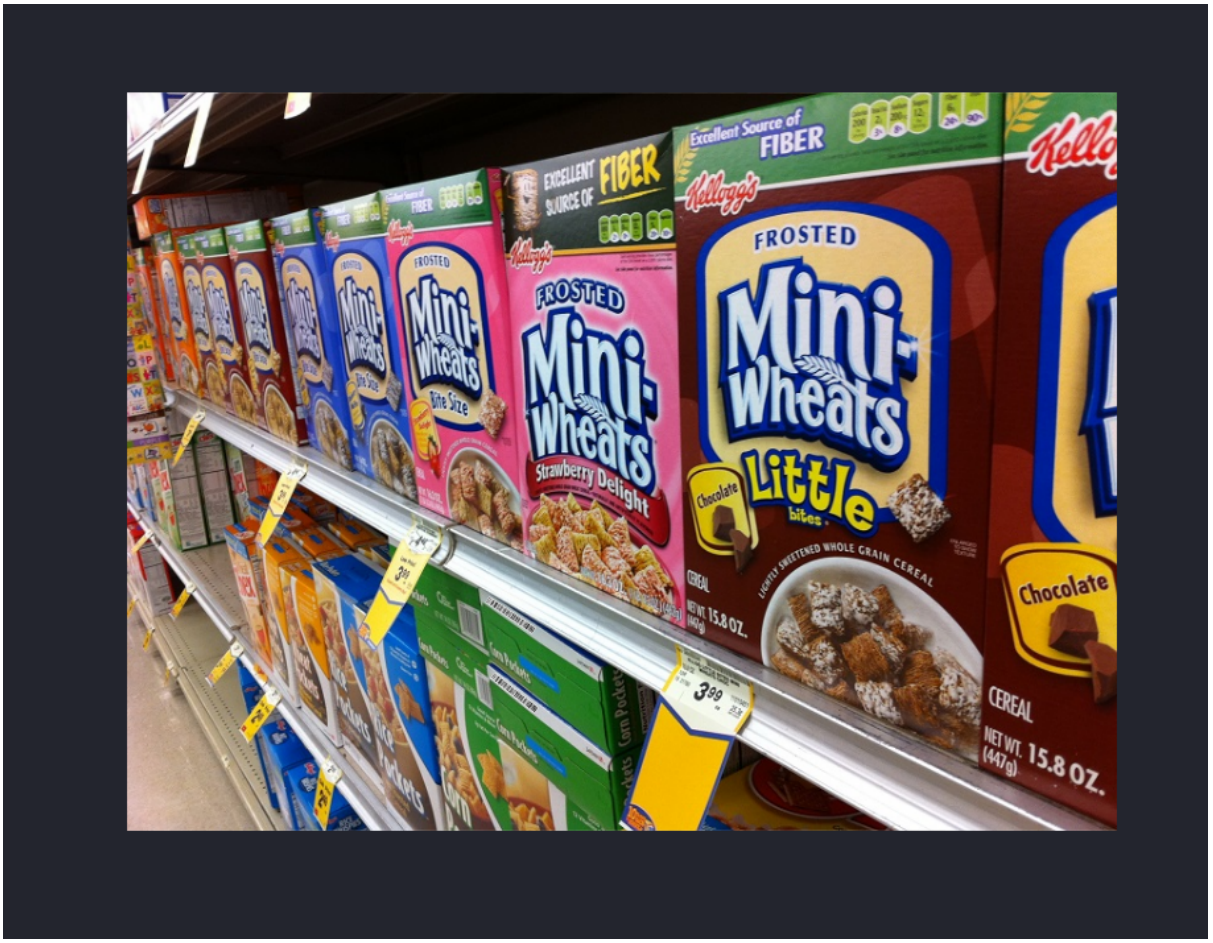
WRITE-UP MALHOMME POUR LA COMETITION
https://challenges.guinean-cybertaskforce.com/index.php?p=game

AFRIQUE DU SUD

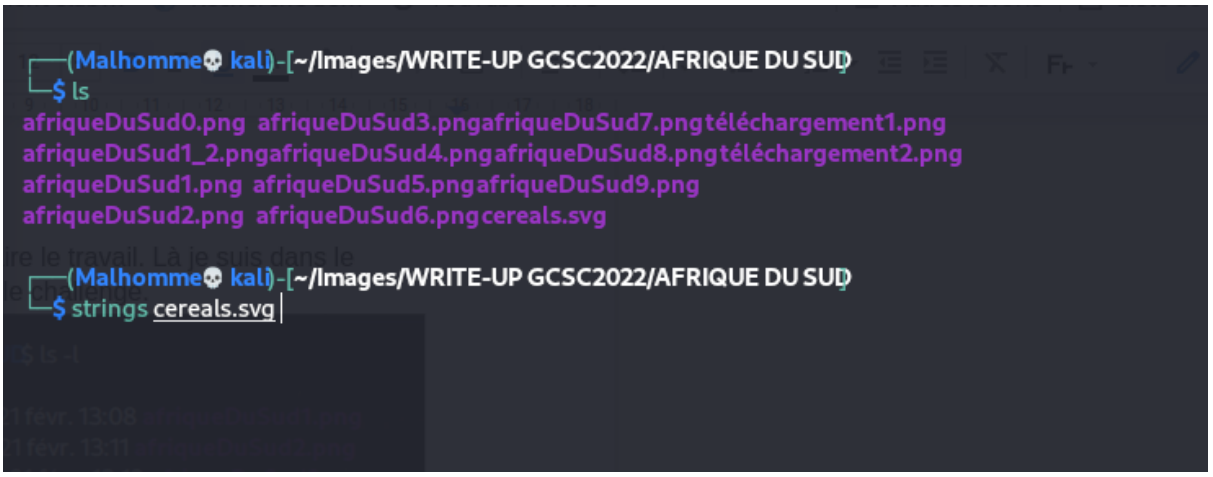
Lorsque que vous cliquez sur Link 1 vous obtenez la page qui est à l'image suivante. A ce niveau vous téléchargez le fichier image.



Après le téléchargement vous obtiendrez l’image suivante.



Je suis rentré dans mon terminal linux pour faire le travail. Là je suis dans le répertoire qui contient les fichiers concernant le challenge.



Après avoir effectué la fonction strings sur le fichier image au format svg, j'obtiens le résultat suivant.
A ce niveau je remarque deux liens à la fin de ma sortir qui peuvent être lisible par mon navigateur.

Donc voici les deux liens en gras qui m'intéressent, je les mets dans bar d'URL et je tape entre.

<image
width="12.062613"
height="1.5402763"
preserveAspectRatio="none"

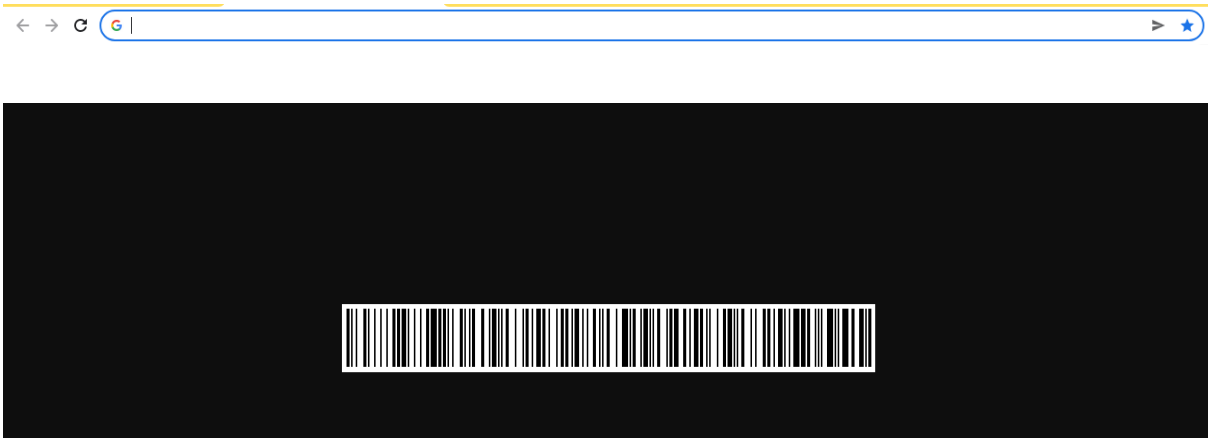
xlink:href="
ZCAYAAAA6hTwfAAAABHNCSVQICAgIfAhkiAAAAnxJREFUeJzt3EFuwjAUQM
Gm6v2v7K5YFMIyTCigp5Idk+D8Khg9seAYY4wvAAAI+X73AAAA8GwiFwCAHJ
ELAECOyAUAIEfkAgCQ8zM7cRzHn79vP8JwO37/owyz41fXPbv+s87P5Iodn51/9
7yr+XaPv+q53x+fvX73frPrHn2uq/I35929bnWfs/Pdv/7RdVfzzu7/6H1X/8fZOXb32
Wqe/34/7O7z3X30qfvi0c/j2bqz6161b67uo9Icn/bcVsdnr5/NO5vj6nO7ut5q3tX53f2
42xtn5919P8zWm12/O+eVzzPf5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
ByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAgByRCwB
AjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAgByRCwBAjsgFAC
BH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAgByRCwBAjsgFACBH5AIAk
CNyAQDIEbkAAOSIXAAAckQuAAA5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDI
EbkAAOSIXAAAckQuAAA5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAO
SIXAAAckQuAAA5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAc
kQuAAA5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA
5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOQcY4zx7iEAAOCZfJMLAE
COyAUAIEfkAgCQI3IBAMgRuQAA5IhcAAByfgFRxiK6XYCKsAAAAABJRU5Erk
Jggg==
id="image29"
x="150.91969"
y="70.401352"
transform="rotate(38.524062)" />

<image
width="12.062613"
height="1.5402763"
preserveAspectRatio="none"

xlink:href="
ZCAYAAAA6hTwfAAAABHNCSVQICAgIfAhkiAAAAnxJREFUeJzt3EFuwjAUQM
Gm6v2v7K5YFMIyTCigp5Idk+D8Khg9seAYY4wvAAAI+X73AAAA8GwiFwCAHJ
ELAECOyAUAIEfkAgCQ8zM7cRzHn79vP8JwO37/owyz41fXPbv+s87P5Iodn51/9
7yr+XaPv+q53x+fvX73frPrHn2uq/I35929bnWfs/Pdv/7RdVfzzu7/6H1X/8fZOXb32
Wqe/34/7O7z3X30qfvi0c/j2bqz6161b67uo9Icn/bcVsdnr5/NO5vj6nO7ut5q3tX53f2
42xtn5919P8zWm12/O+eVzzPf5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
ByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAgByRCwB
AjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAgByRCwBAjsgFAC
BH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAgByRCwBAjsgFACBH5AIAk
CNyAQDIEbkAAOSIXAAAckQuAAA5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDI
EbkAAOSIXAAAckQuAAA5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAO
SIXAAAckQuAAA5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAc
kQuAAA5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA
5IhcAgByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOQcY4zx7iEAAOCZfJMLAE

COyAUAlEfkAgCQl3lBAMgRuQAA5lhc
AAByfgFRxiK6XYCKsAAAAABJRU5ErkJggg== "
id="image29-2"
x="134.73402"
y="69.453888"
transform="rotate(33.907631)" />

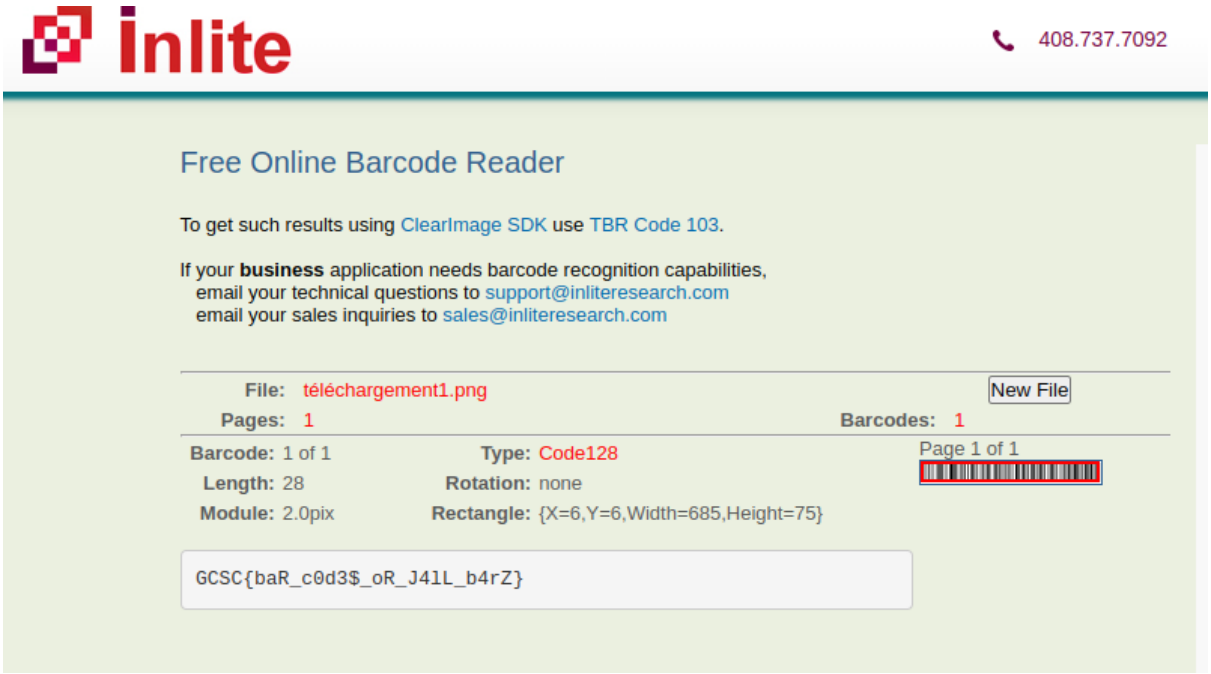
On obtient les deux résultats suivant respectivement selon chaque lien:



Je remarque que c’est du code bar.

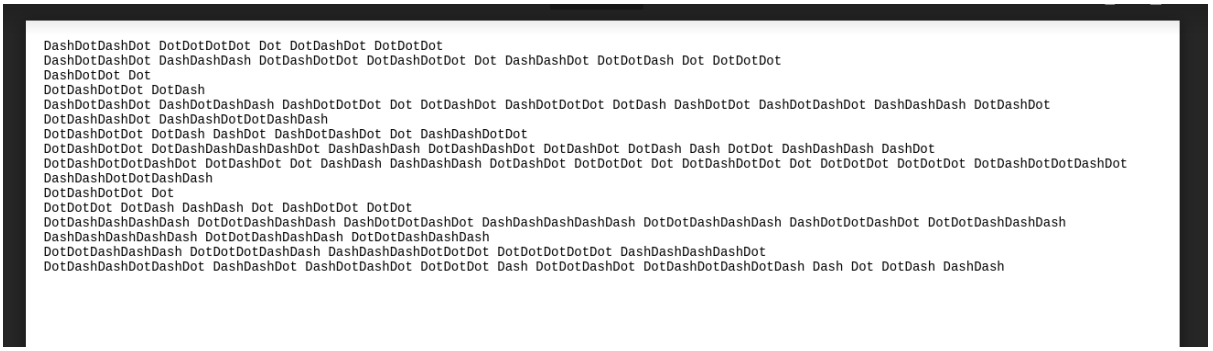
Je les télécharge puis j’utilise l'outil lecteur de code bar en ligne Free Online Barcode reader.

Et j'obtiens le flag. C’est facile n’est ce pas !

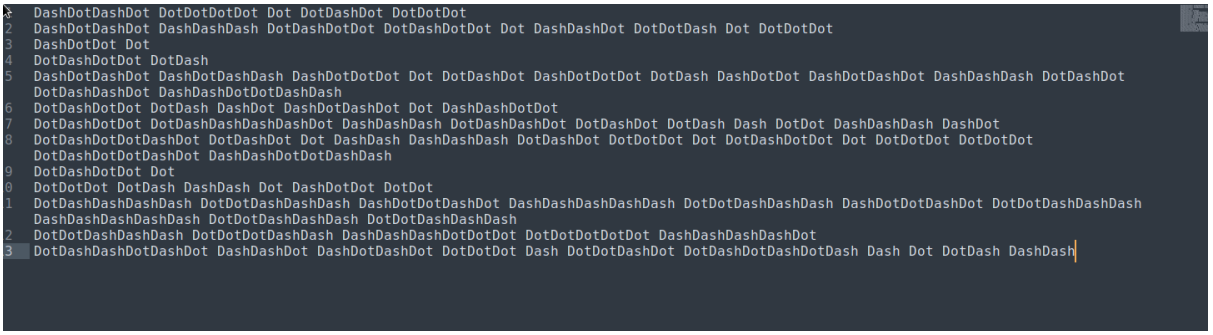


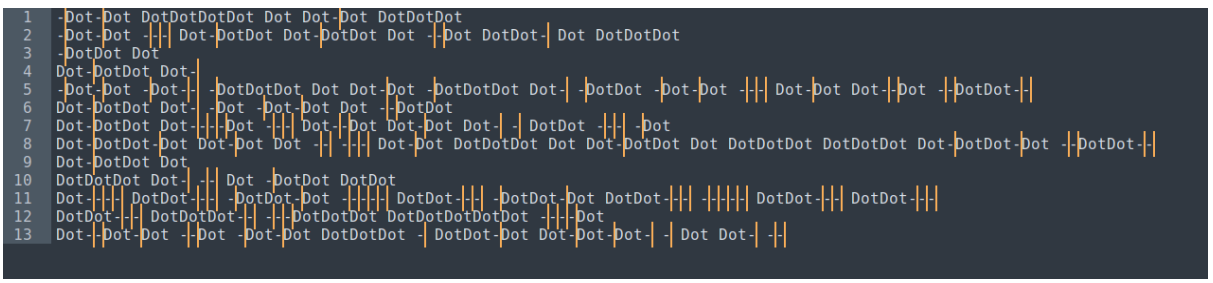
ALGERIE

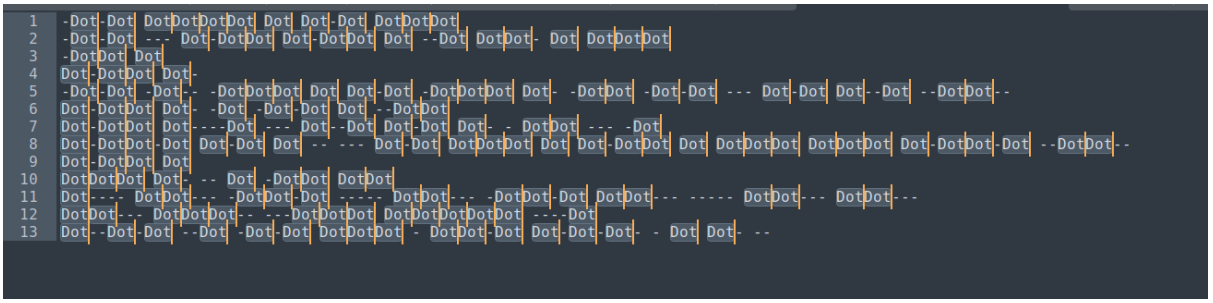
Lorsque je clique sur Link 1, j'obtiens le résultat sur l'image suivante.



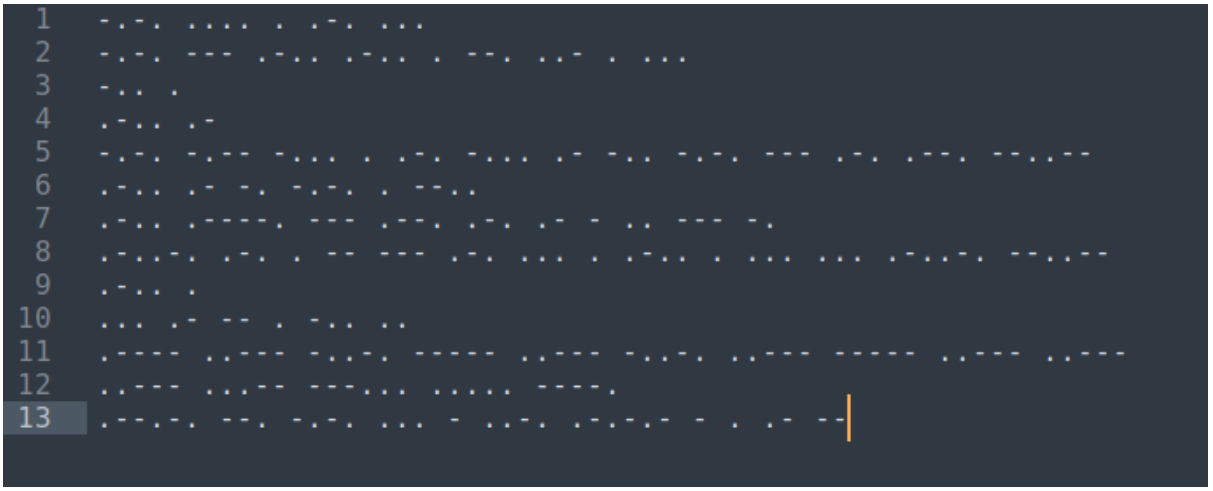
C’est du code Morse.
Dot = .
Dash = -
Donc j’ai converti tout le code en code morse.
J’ai utilisé sublime texte et vite remplacé ce qui est par ce qui convient.



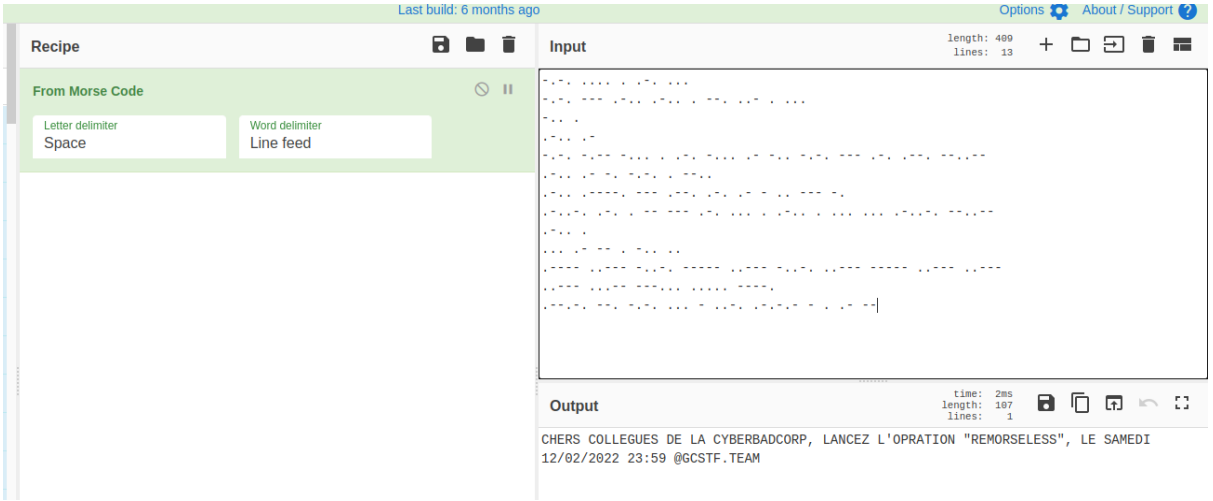




Après avoir remplacé chaque chose.
J'obtiens la ligne suivante. Et c’est ça du code morse.



J’utilise l’utilitaire cyberchef en ligne pour convertir le codage morse en compréhensible. pour obtenir le flag.



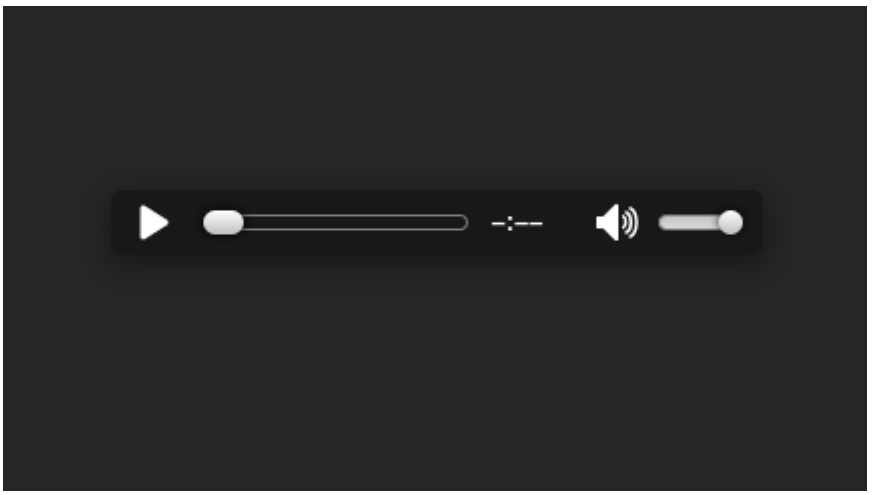
```
14
15
16  CHERS COLLEGUES DE LA CYBERBADCORP, LANCEZ L'OPRATION "REMORSELESS", LE SAMEDI 12/02/2022 23:59 @GCSTF.TEAM
17
18  Flag : GCSC2022{minuscule(nom_de_loperation)}
19
20
21
22
23
24  le final flag -             GCSC2022{remorseless}
```

Après cela je suis les instructions du contexte et j'obtiens mon flag.

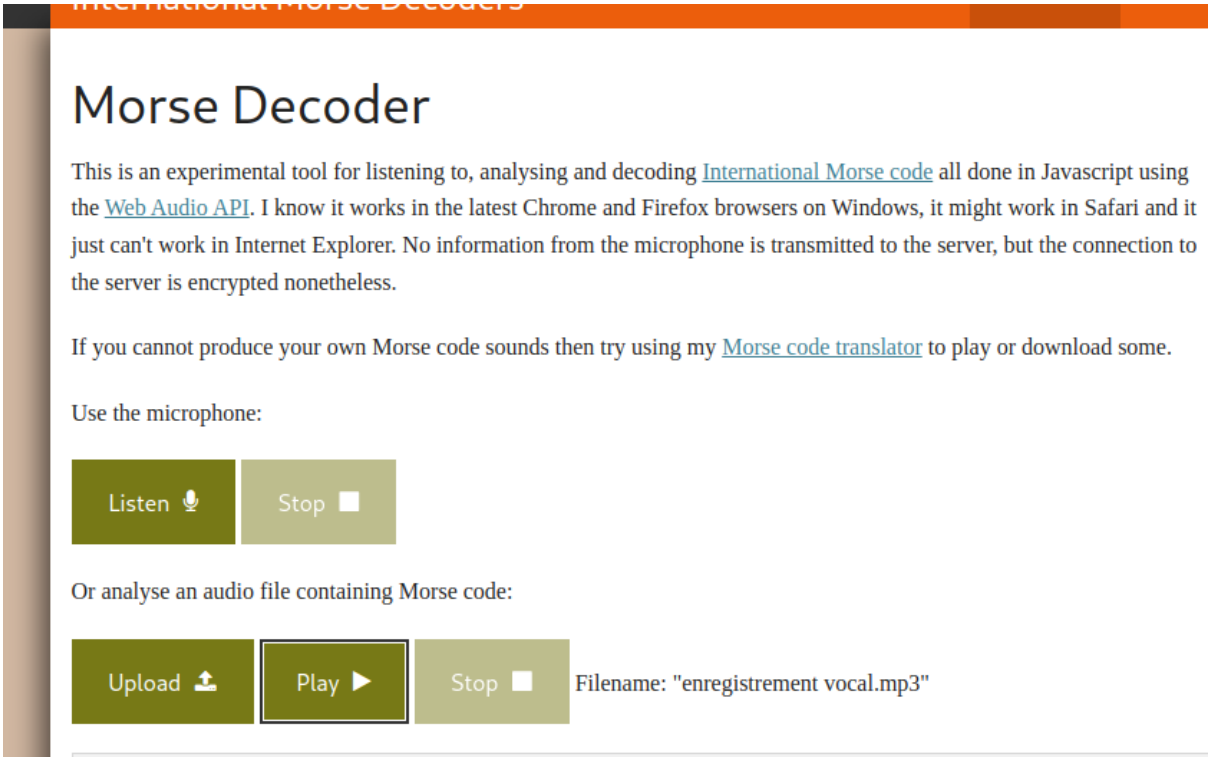
```
le final flag -             GCSC2022{remorseless}
```

ANGOLA

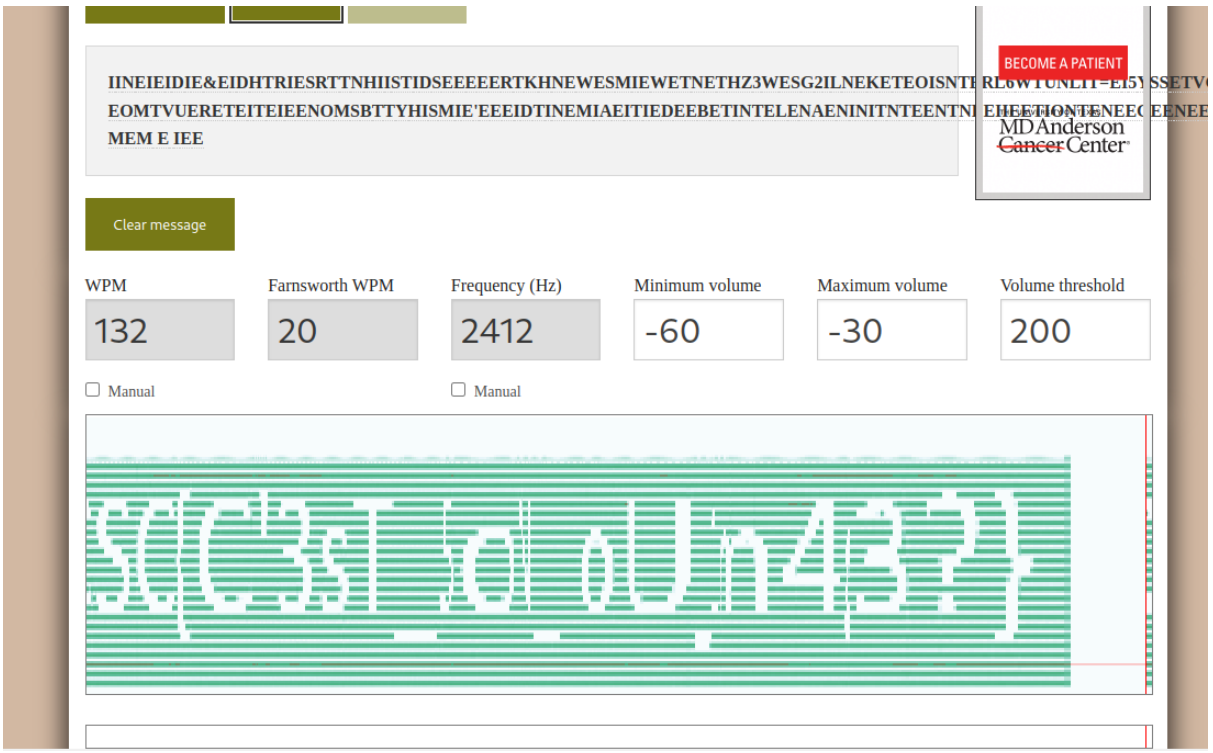
Je clique sur Link 1
J'obtiens l'audio suivante:

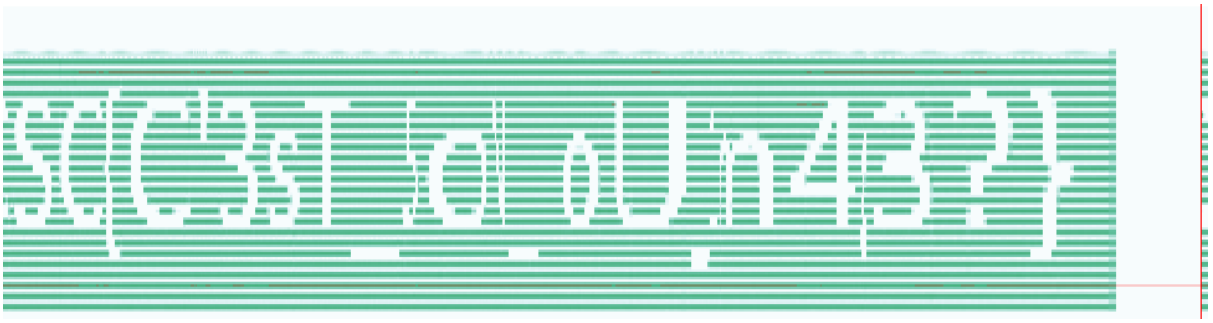


J'upload dans Morse Decoder audio online

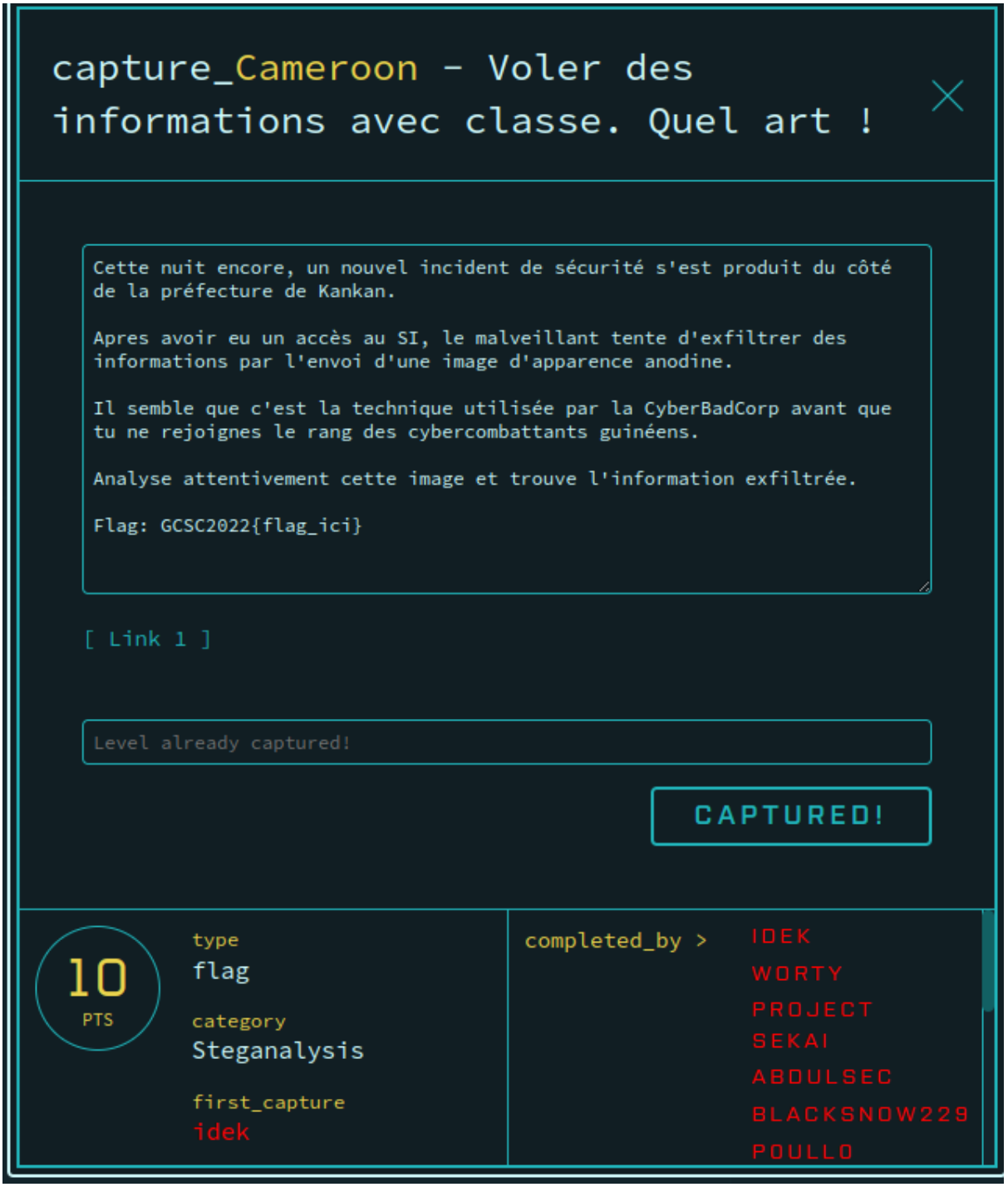


Je patiente un peu et à la fin de l'audio j'obtiens le flag suivant qui valide le challenge.

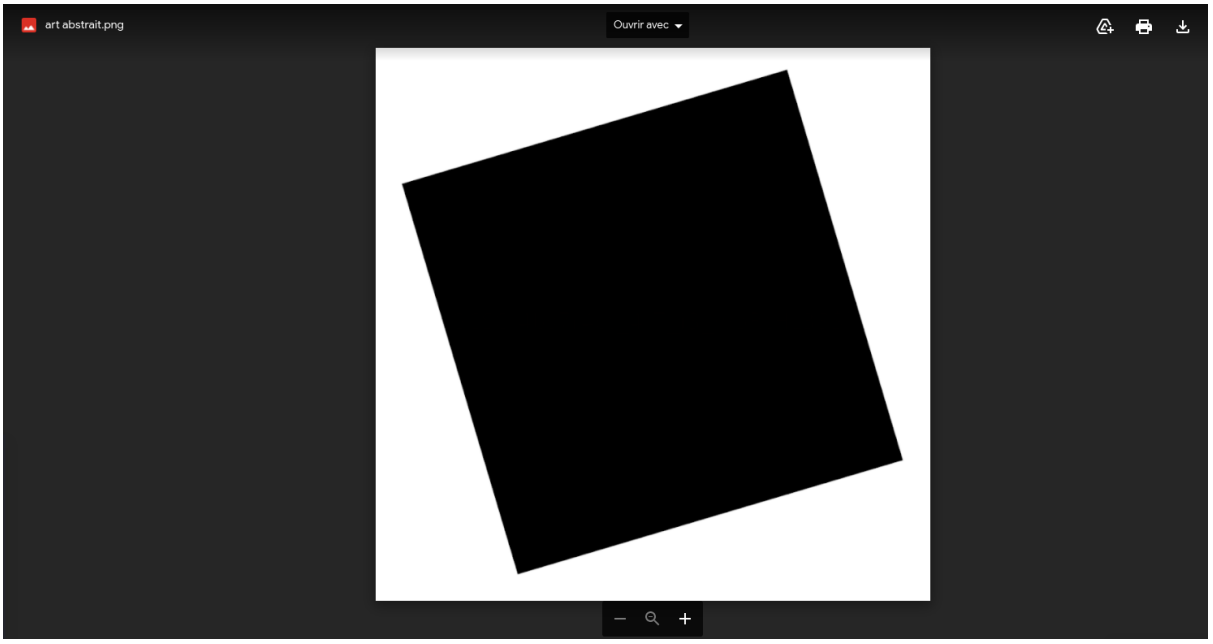

IINEIEIDIE&EIDHTRIESRTTNHIISTIDSEEEEERTKHNEWESMIEWETNETHZ3WESG2ILNEKETEOISNTE RL6WTUNLTI=E15Y SSETV
EOMTVUERETEITEIEENOMSBTTYHISMIE'EEEIDTINEMIAEITIEDEEBETINTELENAENINITNTEENTNI EHEETIONTENEEC EENEE
MEM E IEE
BECOME A PATIENT
MD Anderson Cancer Center
Clear message
WPM
132
Farnsworth WPM
20
Frequency (Hz)
2412
Minimum volume
-60
Maximum volume
-30
Volume threshold
200
Manual
Manual



CAMEROON

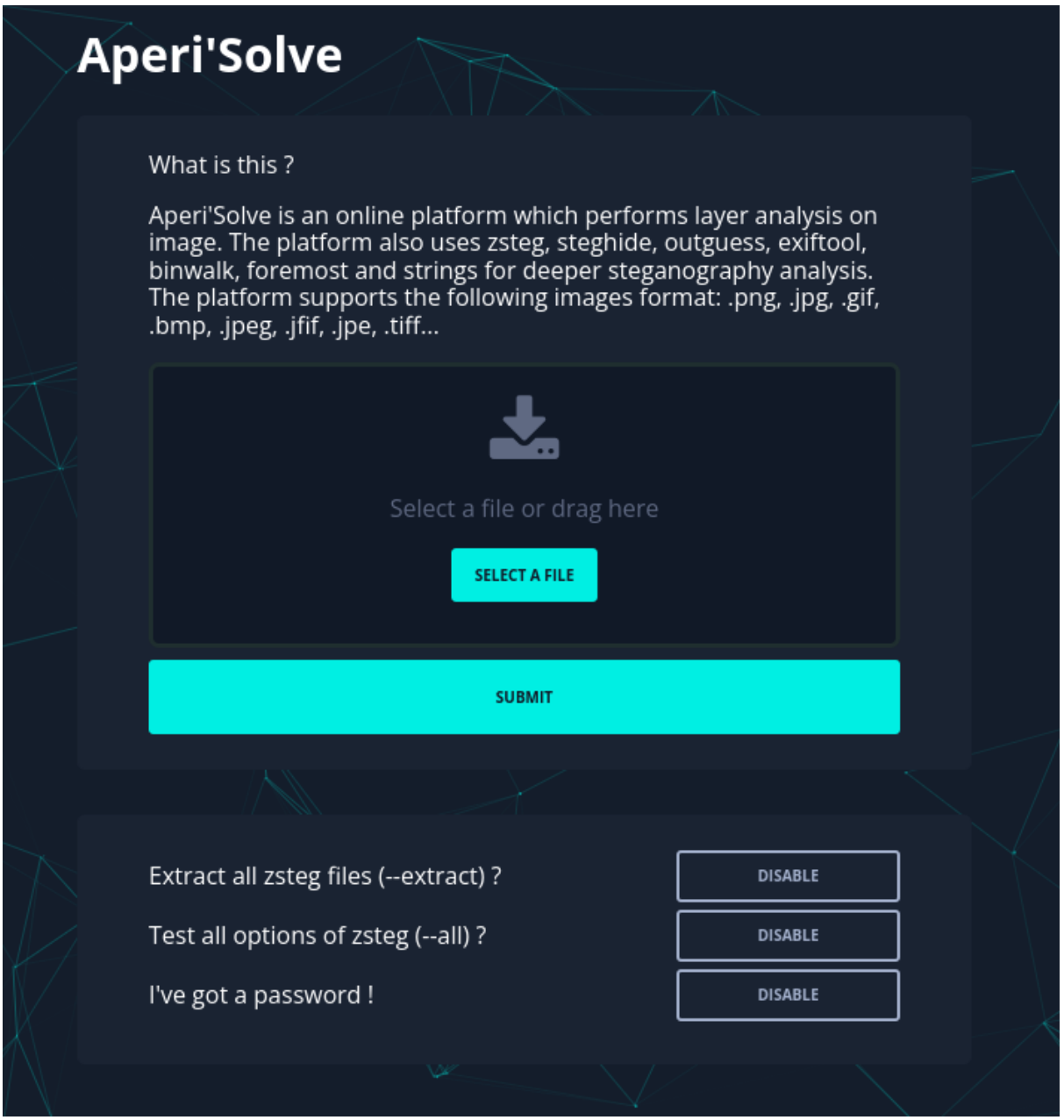


Je clique sur Link 1 et je télécharge l'image, puis je strings dans le terminal.




```
Malhomme@kali:~/Téléchargements/CAMEROON$ ls
'art abstrait.png'
Malhomme@kali:~/Téléchargements/CAMEROON$ strings 'art abstrait.png'
IHDR
sRGB
gAMA
    pHYs
IDATx^
,0tE
PDTTl
O&,"
0::1
0::1
0::1
0::1
0::1
0::1
0::1
0::1
0::1
WkjjJJJ
4'''33S6
ruuuQQ
kjjd
SWWWQQ
$'''//O68
>utt
    ggg
UUU%
<(33
W_}u
```

String me donne pas grand chose, alors j’ouvre avec Aperi’Solve


Aperi'Solve
What is this ?
Aperi'Solve is an online platform which performs layer analysis on image. The platform also uses zsteg, steghide, outguess, exiftool, binwalk, foremost and strings for deeper steganography analysis. The platform supports the following images format: .png, .jpg, .gif, .bmp, .jpeg, .jfif, .jpe, .tiff...
Select a file or drag here
SELECT A FILE
SUBMIT
Extract all zsteg files (--extract) ?
DISABLE
Test all options of zsteg (--all) ?
DISABLE
I've got a password !
DISABLE

Aperi'Solve

What is this ?

Aperi'Solve is an online platform which performs layer analysis on image. The platform also uses zsteg, steghide, outguess, exiftool, binwalk, foremost and strings for deeper steganography analysis. The platform supports the following images format: .png, .jpg, .gif, .bmp, .jpeg, .jfif, .jpe, .tiff...

art%20abstrait.png

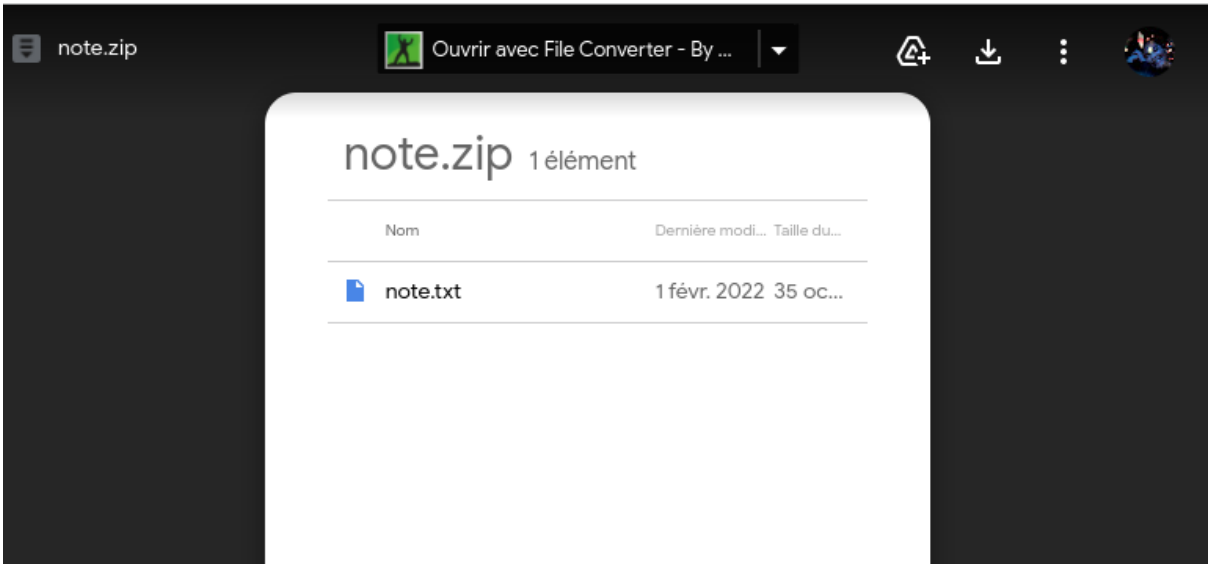
SUBMIT

Et j’obtiens le flag.


GCSC{4bs7r4ct_4rT_i$_woRtHL3$$}

CHAD

Je télécharge le note.zip puis je j'applique zip2john puis du hashcat avec la liste rockyou.txt et j'obtiens la clé qui me permet d'ouvrir le fichier note.txt.

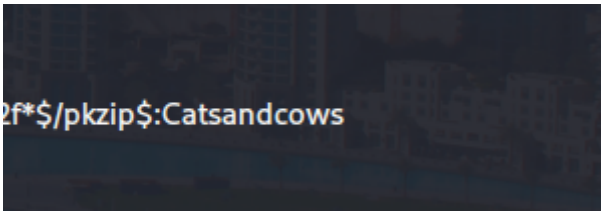


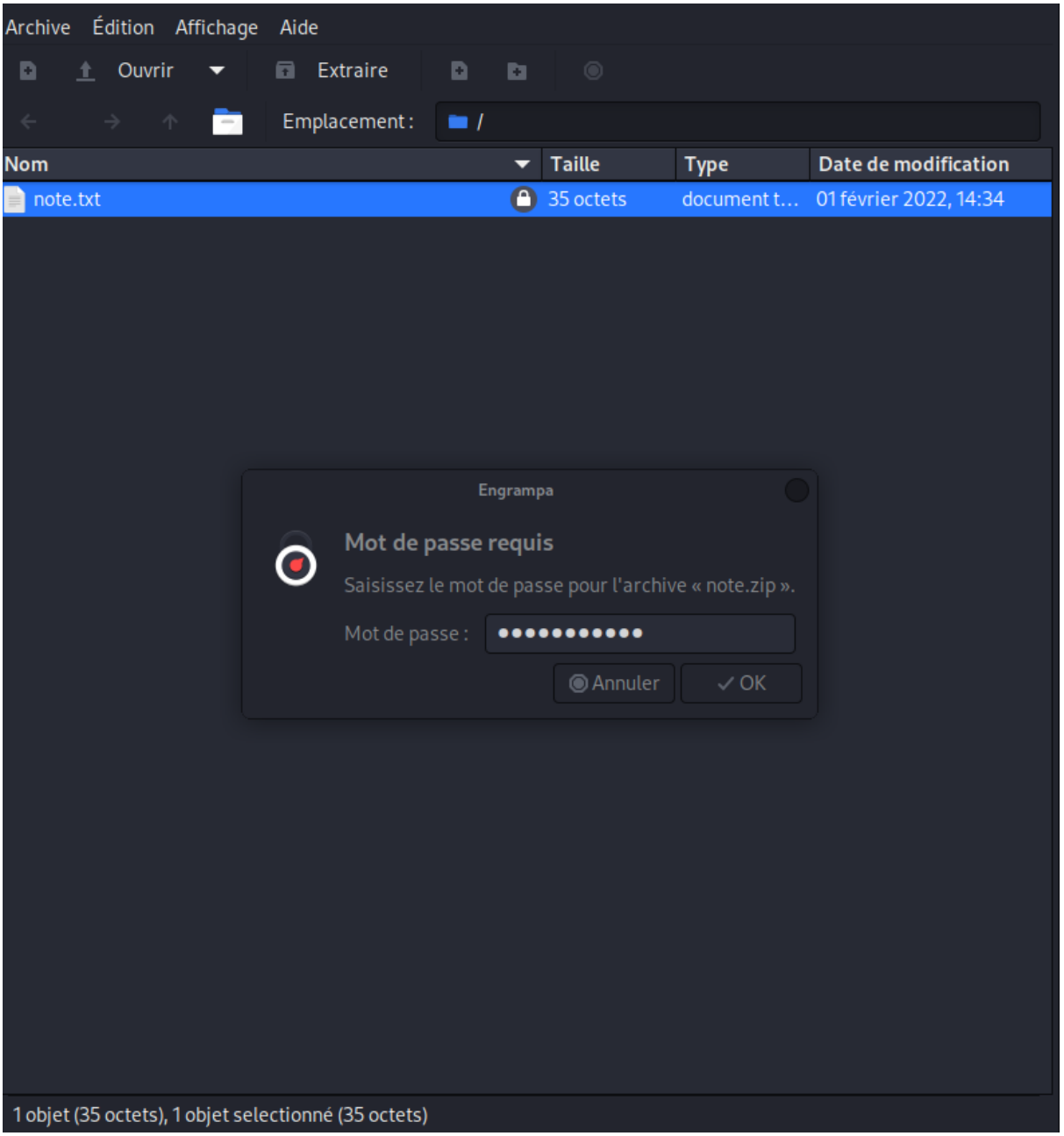

```
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAD$ ls
note.zip
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAD$ strings note.zip
ZtAT
note.txt
CZ]/
[~/PK
ZtAT
note.txt
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAD$ zip2john note.zip > crack.hash
ver 2.0 note.zip/note.txt PKZIP Encr: cmplen=47, decmplen=35, crc=D4124615 ts=745A cs=d412 type
=0
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAD$ ls
crack.hash  note.zip
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAD$ cat crack.hash
note.zip/note.txt:$pkzip$1*1*2*0*2f*23*d4124615*0*26*0*2f*d412*0ff07062b8da65181bef4b45fc92eb57
472f113ac911676100ab435a5d2f951791cd2aa52db3459b1524cce55b7e2f*$/pkzip$:note.txt:note.zip::note
.zip
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAD$ nano crack.hash
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAD$ cat crack.hash
$pkzip$1*1*2*0*2f*23*d4124615*0*26*0*2f*d412*0ff07062b8da65181bef4b45fc92eb57472f113ac911676100
ab435a5d2f951791cd2aa52db3459b1524cce55b7e2f*$/pkzip$:note.txt:note.zip::note.zip
```

```
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAL$ ls
ch3.png cha1.png cha2.png crack.hash flag.png note.zip zip.hash
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAL$ cat crack.hash
$pkzip$1*1*2*0*2f*23*d4124615*0*26*0*2f*d412*0ff07062b8da65181bef4b45fc92eb57472f113ac911676100
ab435a5d2f951791cd2aa52db3459b1524cce55b7e2f*$/pkzip$
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAL$ hashcat --help | grep -i "$pkzip$1*1*2*"
  3200 | bcrypt $2*$, Blowfish (Unix)                 | Operating System
  s |  !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
* https://hashcat.net/wiki/#howtos_videos_papers_articles_etc_in_the_wild
* https://hashcat.net/faq/
* https://hashcat.net/discord
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAL$ hashcat --help | grep -i "pkzip"
  17220 | PKZIP (Compressed Multi-File)               | Archive
  17200 | PKZIP (Compressed)                          | Archive
  17225 | PKZIP (Mixed Multi-File)                    | Archive
  17230 | PKZIP (Mixed Multi-File Checksum-Only)      | Archive
  17210 | PKZIP (Uncompressed)                        | Archive
  20500 | PKZIP Master Key                            | Archive
  20510 | PKZIP Master Key (6 byte optimization)      | Archive
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAL$
```

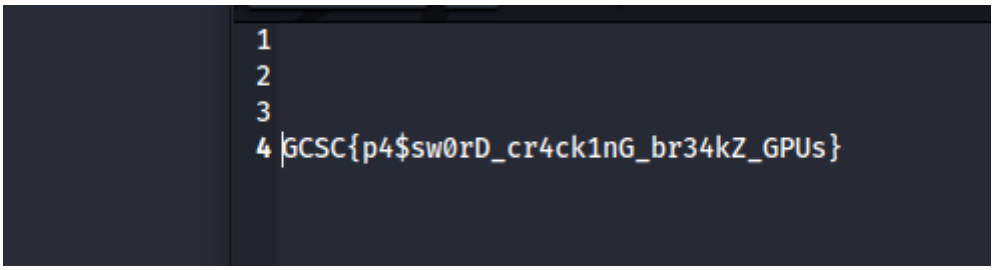
```
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHAL$ hashcat -a 0 -m 17210 crack.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting

/sys/class/hwmon/hwmon2/temp1_input: No such file or directory

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i7 CPU     M 620  @ 2.67GHz, 2112/4288 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Not-Iterated
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
```

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / dr          e right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make us         our parallelization power:
  https://hashcat.net/faq/morework

$pkzip$1*1*2*0*2f*23*d4124615*0*26*0*2f*d412*0ff07062b8da65181bef4b45fc92eb57472f113ac911676100ab435a5d2f951791cd2aa52db3459b1524cce55b7e2f*$/pkzip$:Catsandcows

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 17210 (PKZIP (Uncompressed))
Hash.Target......: $pkzip$1*1*2*0*2f*23*d4124615*0*26*0*2f*d412*0ff070...pkzip$
Time.Started.....: Mon Feb 21 17:40:18 2022 (7 secs)
Time.Estimated...: Mon Feb 21 17:40:25 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1746.2 kH/s (0.40ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 11296768/14344385 (78.75%)
Rejected.........: 0/11296768 (0.00%)
Restore.Point....: 11294720/14344385 (78.74%)
```



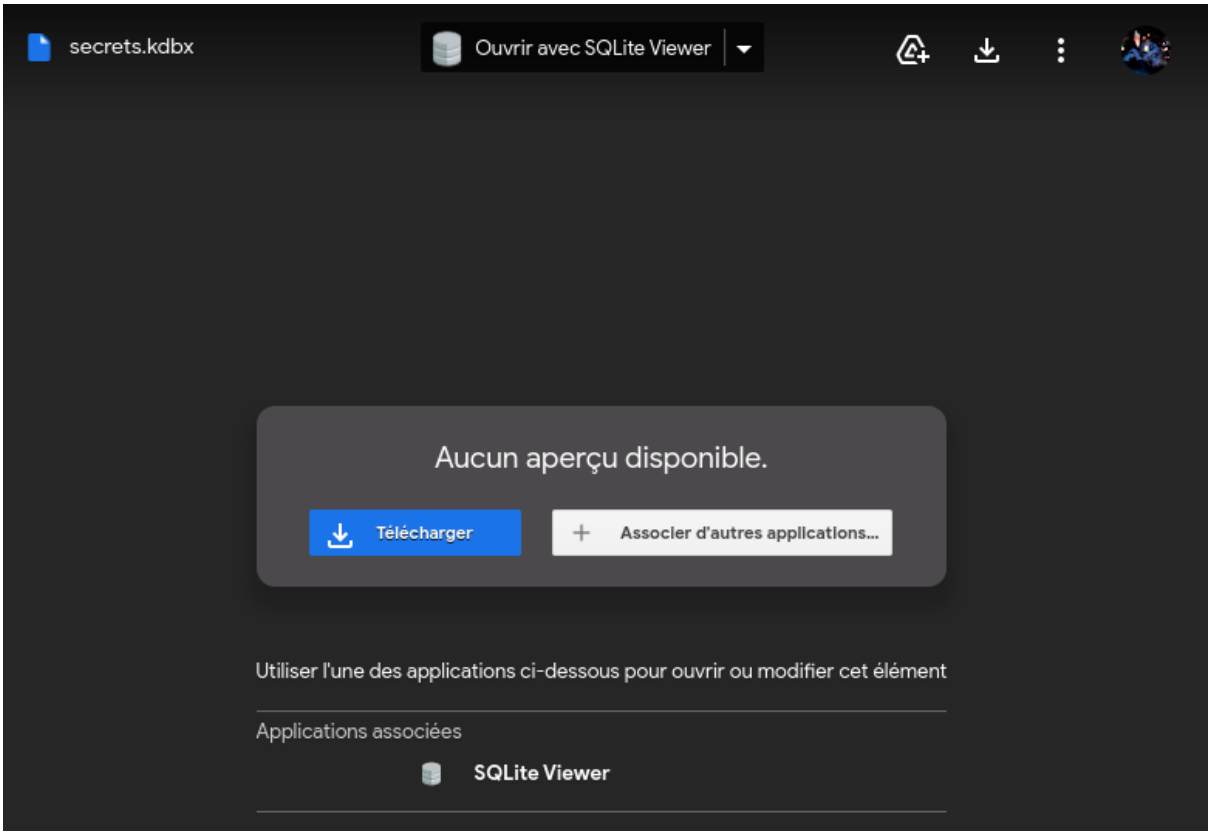


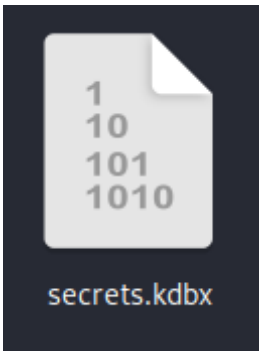
Et j'obtiens le flag pour valider.

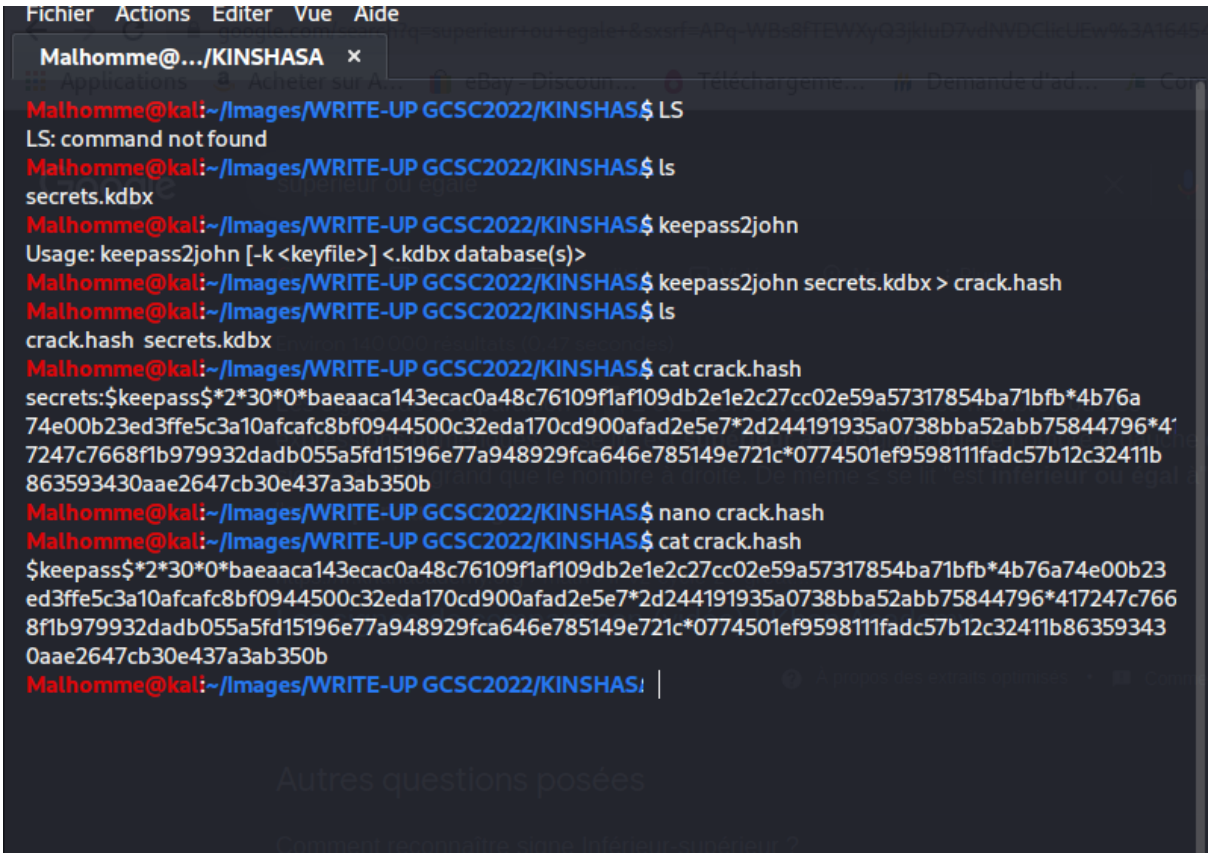


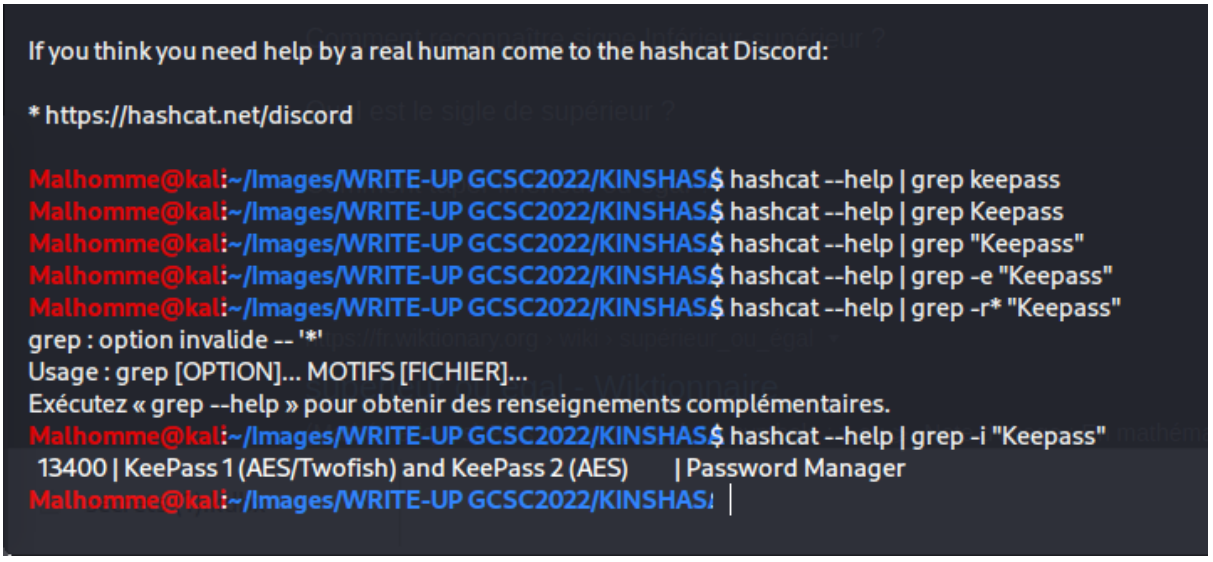
CONGO-KINSHASA

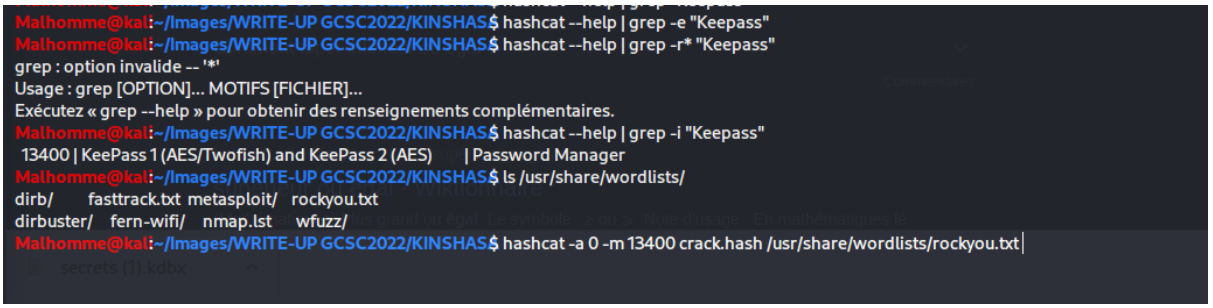
Je télécharge le fichier secret.kdbx et j'y applique du keepass2john puis du hashcat pour obtenir le mot de passe situé dans le fichier rockyou.txt


secrets.kdbx
Ouvrir avec SQLite Viewer
Aucun aperçu disponible.
Télécharger
Associer d'autres applications...
Utiliser l'une des applications ci-dessous pour ouvrir ou modifier cet élément
Applications associées
SQLite Viewer


1
10
101
1010
secrets.kdbx


Fichier Actions Editer Vue Aide
Malhomme@.../KINSHASA
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ LS
LS: command not found
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ ls
secrets.kdbx
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ keepass2john
Usage: keepass2john [-k <keyfile>] <.kdbx database(s)>
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ keepass2john secrets.kdbx > crack.hash
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ ls
crack.hash secrets.kdbx
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ cat crack.hash
secrets:$keepass$*2*30*0*baeaaca143ecac0a48c76109f1af109db2e1e2c27cc02e59a57317854ba71bfb*4b76a
74e00b23ed3ffe5c3a10afcafc8bf0944500c32eda170cd900afad2e5e7*2d244191935a0738bba52abb75844796*4
7247c7668f1b979932dadb055a5fd15196e77a948929fca646e785149e721c*0774501ef9598111fadc57b12c32411b
863593430aae2647cb30e437a3ab350b
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ nano crack.hash
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ cat crack.hash
$keepass$*2*30*0*baeaaca143ecac0a48c76109f1af109db2e1e2c27cc02e59a57317854ba71bfb*4b76a74e00b23
ed3ffe5c3a10afcafc8bf0944500c32eda170cd900afad2e5e7*2d244191935a0738bba52abb75844796*417247c766
8f1b979932dadb055a5fd15196e77a948929fca646e785149e721c*0774501ef9598111fadc57b12c32411b86359343
0aae2647cb30e437a3ab350b
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$

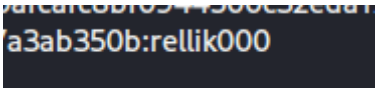

If you think you need help by a real human come to the hashcat Discord:
* https://hashcat.net/discord
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep keepass
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep Keepass
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep "Keepass"
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -e "Keepass"
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -r* "Keepass"
grep : option invalide -- '*'
Usage : grep [OPTION]... MOTIFS [FICHIER]...
Exécutez « grep --help » pour obtenir des renseignements complémentaires.
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -i "Keepass"
13400 | KeePass 1 (AES/Twofish) and KeePass 2 (AES) | Password Manager
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$


Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -e "Keepass"
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -r* "Keepass"
grep : option invalide -- '*'
Usage : grep [OPTION]... MOTIFS [FICHIER]...
Exécutez « grep --help » pour obtenir des renseignements complémentaires.
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -i "Keepass"
13400 | KeePass 1 (AES/Twofish) and KeePass 2 (AES) | Password Manager
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ ls /usr/share/wordlists/
dirb/ fasttrack.txt metasploit/ rockyou.txt
dirbuster/ fern-wifi/ nmap.lst wfuzz/
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat -a 0 -m 13400 crack.hash /usr/share/wordlists/rockyou.txt

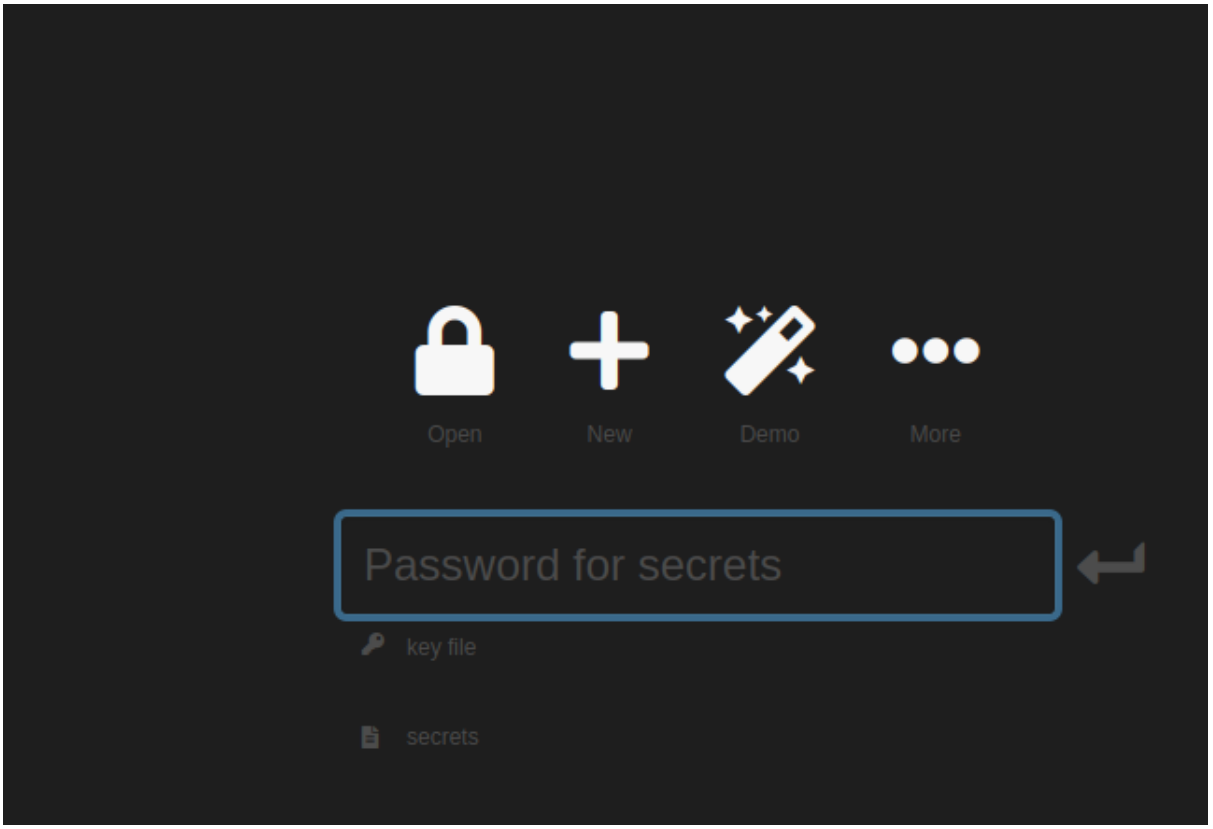
```
dirbuster/  fern-wifi/  nmap.lst  wfuzz/
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat -a 0 -m 13400 crack.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting

/sys/class/hwmon/hwmon2/temp1_input: No such file or directory

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i7 CPU     M 620  @ 2.67GHz, 2112/4288 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 3 secs

$keepass$*2*30*0*baeaaca143ecac0a48c76109f1af109db2e1e2c27cc02e59a57317854ba71bfb*4b76a74e00b23ed3ffe5c3a10afcafc8bf0944500c32eda170cd900afad2e5e7*2d244191935a0738bba52abb75844796*417247c7668f1b97
9932dadb055a5fd15196e77a948929fca646e785149e721c*0774501ef9598111fadc57b12c32411b863593430aae2647cb30e437a3ab350b:rellik000
```

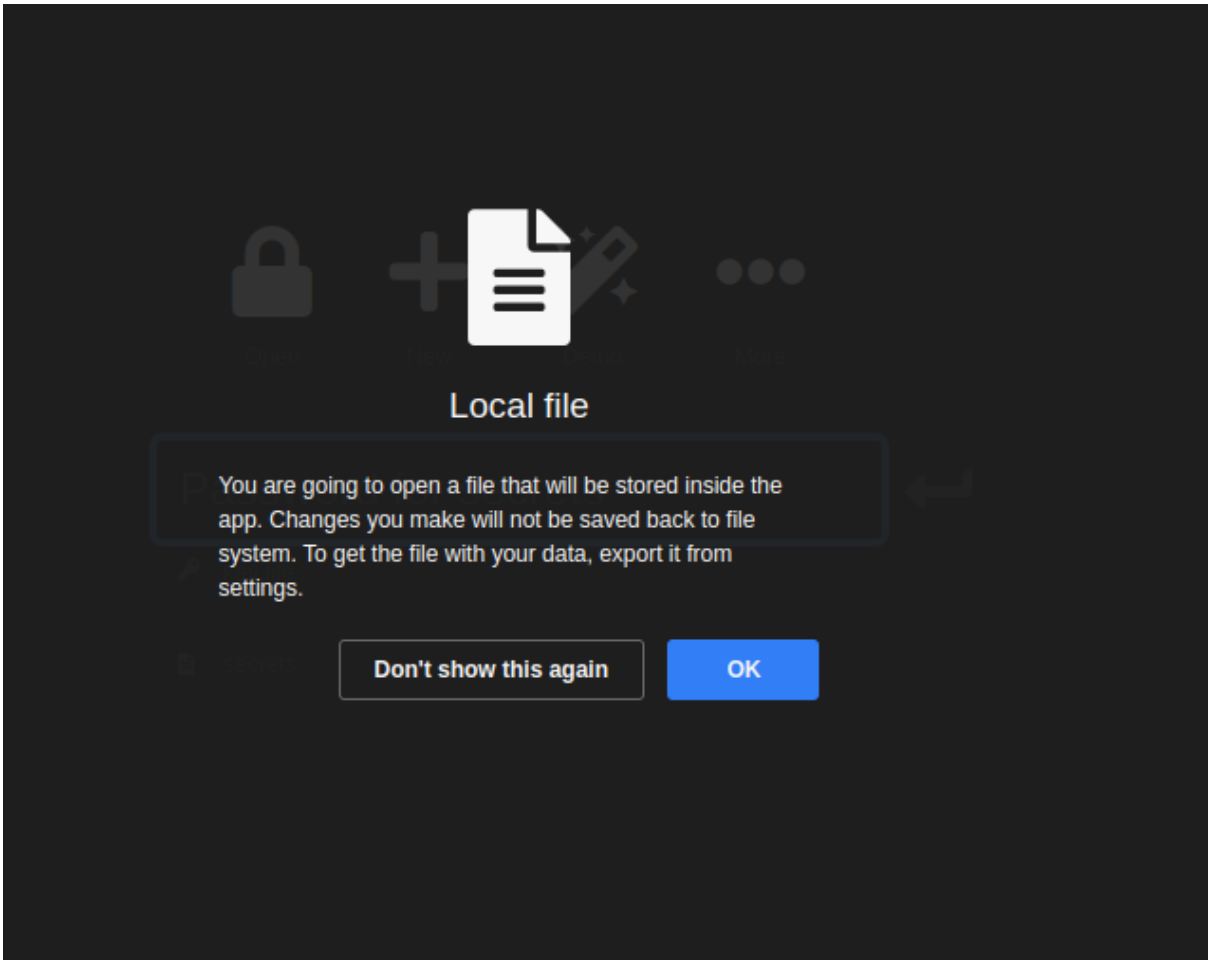
```
$keepass$*2*30*0*baeaaca143ecac0a48c76109f1af109db2e1e2c27cc02e59a57317854ba71bfb*4b76a74e00b23ed3ffe5c3a10afcafc8bf0944500c32eda170cd900afad2e5e7*2d244191935a0738bba52abb75844796*417247c7668f1b97
9932dadb055a5fd15196e77a948929fca646e785149e721c*0774501ef9598111fadc57b12c32411b863593430aae2647cb30e437a3ab350b:rellik000

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13400 (KeePass 1 (AES/Twofish) and KeePass 2 (AES))
Hash.Target......: $keepass$*2*30*0*baeaaca143ecac0a48c76109f1af109db2...ab350b
Time.Started.....: Mon Feb 21 15:56:41 2022 (5 secs)
Time.Estimated...: Mon Feb 21 15:56:46 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  140.4 kH/s (8.98ms) @ Accel:512 Loops:30 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 813056/14344385 (5.67%)
Rejected.........: 0/813056 (0.00%)
Restore.Point....: 811008/14344385 (5.65%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-30
Candidate.Engine.: Device Generator
Candidates.#1....: reynaline -> red616
Hardware.Mon.#1..: Util: 95%

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / dr          e right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make us          our parallelization power:
  https://hashcat.net/faq/morework

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => Started: Mon Feb 21 15:55:01 2022
Stopped: Mon Feb 21 15:56:49 2022
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$
```

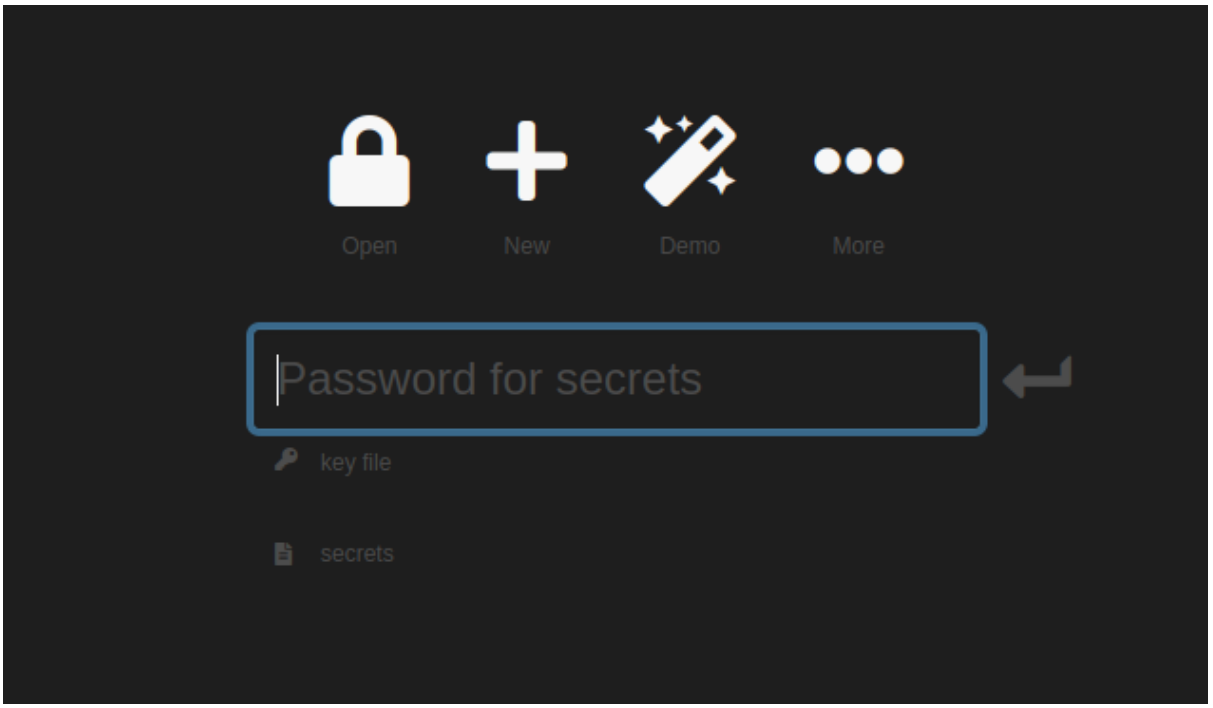
Et voici le mot de passe.

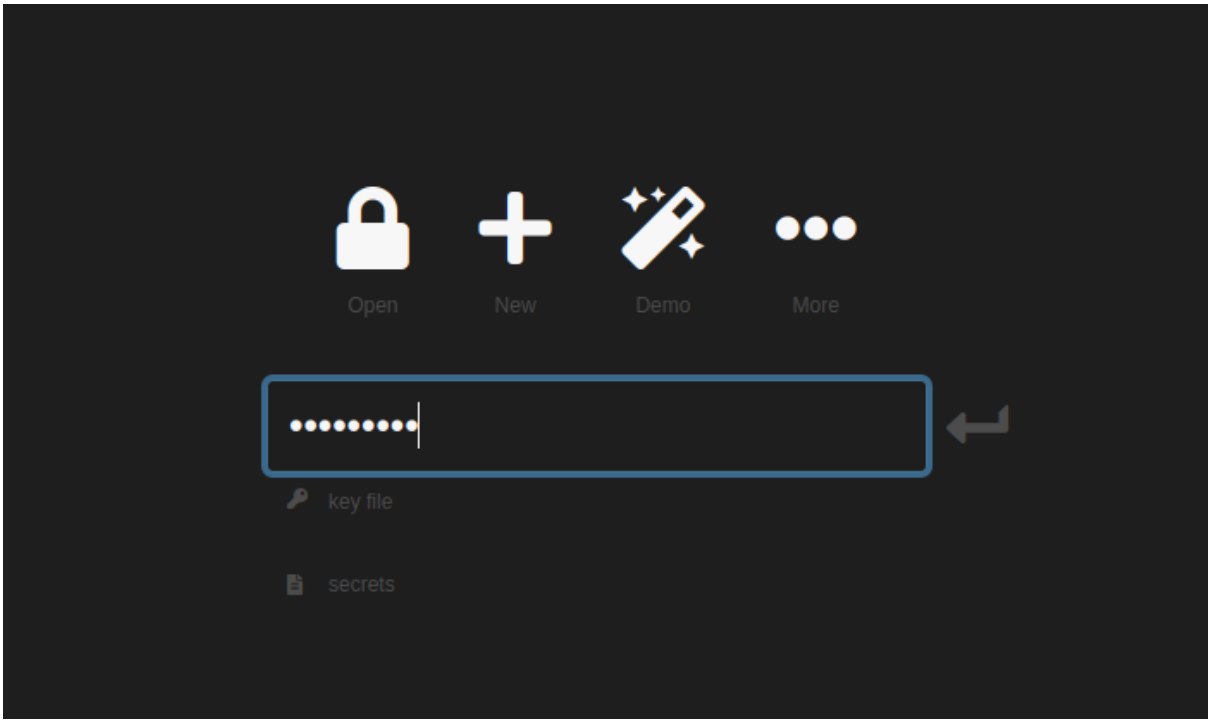


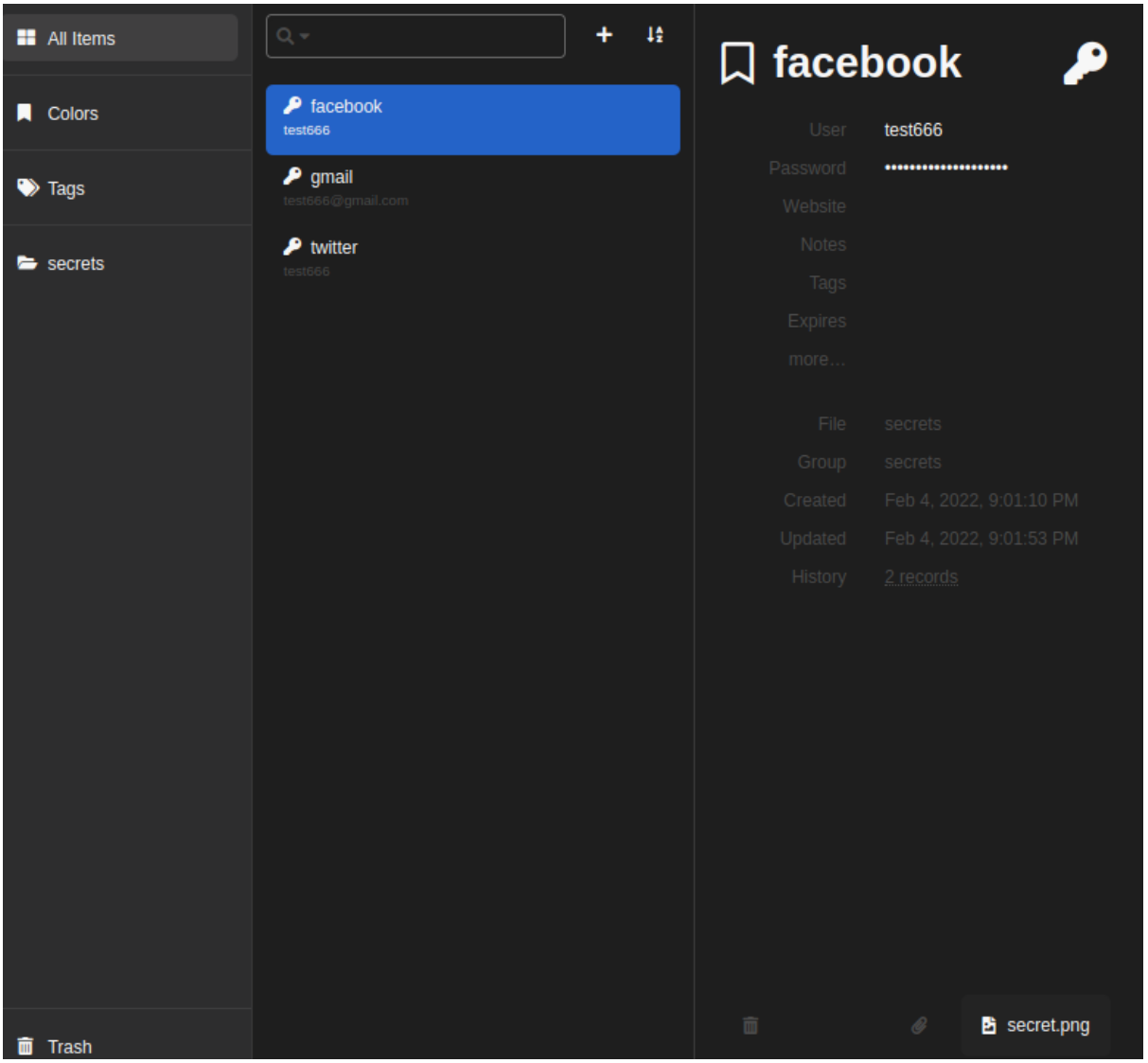
J’utilise app.keeweb.info pour uploader le fichier secret.kdbx et j’y applique le mot de passe trouver dans la liste. Et j’obtiens le flag situé dans le fichier image dans l’angle droit bas.

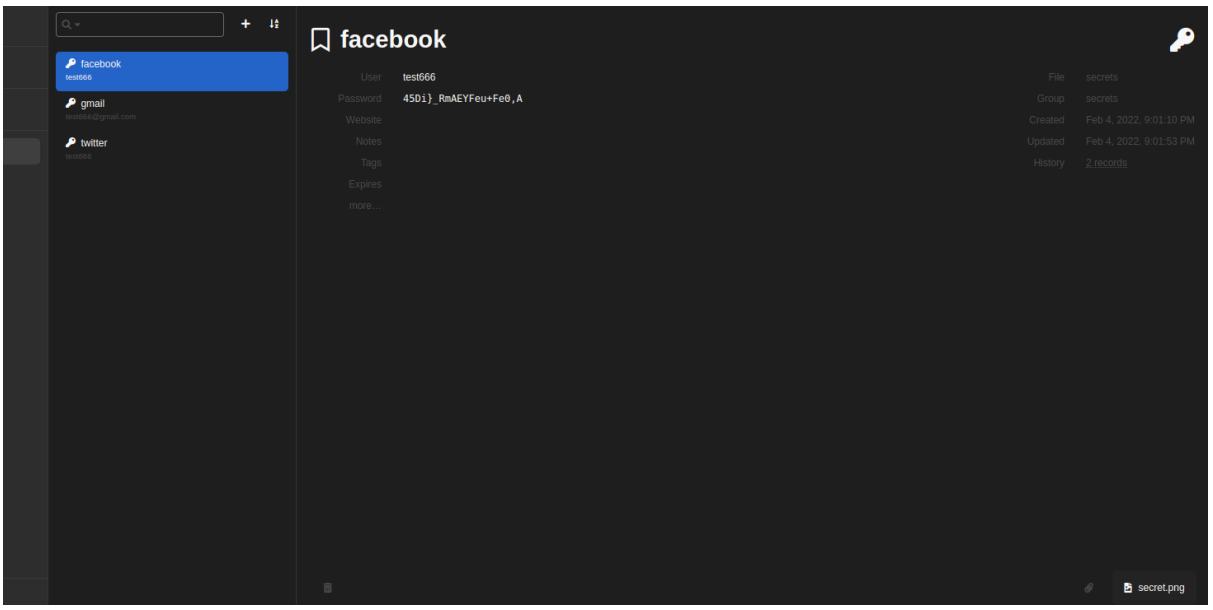

Open
New
Demo
More
Password for secrets
key file
secrets

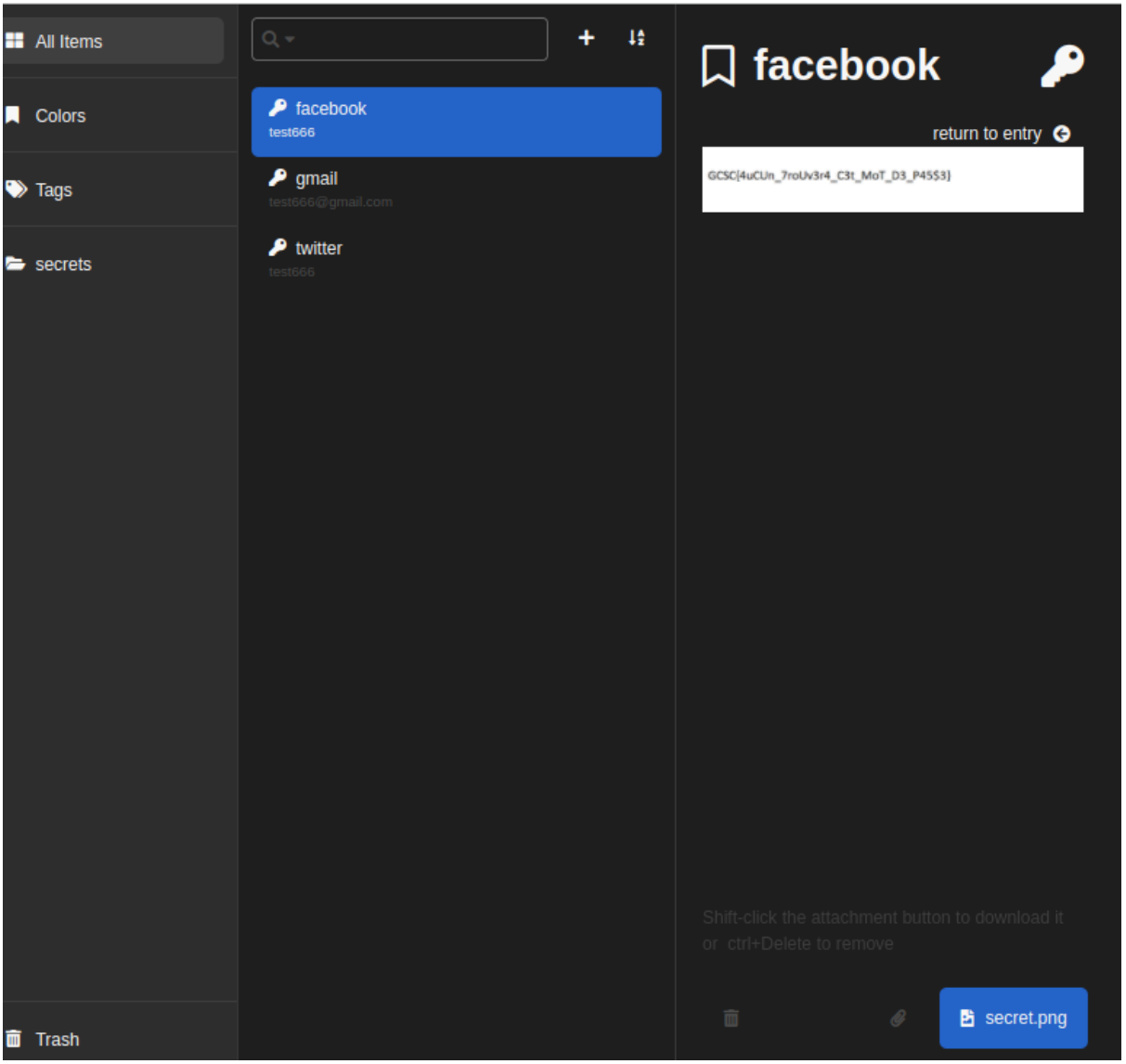

Local file
You are going to open a file that will be stored inside the app. Changes you make will not be saved back to file system. To get the file with your data, export it from settings.
Don't show this again
OK


Open
New
Demo
More
Password for secrets
key file
secrets


Open
New
Demo
More
key file
secrets


All Items
Colors
Tags
secrets
Trash
facebook
test666
gmail
test666@gmail.com
twitter
test666
facebook
User test666
Password ••••••••••••••••••••
Website
Notes
Tags
Expires
more…
File secrets
Group secrets
Created Feb 4, 2022, 9:01:10 PM
Updated Feb 4, 2022, 9:01:53 PM
History 2 records
secret.png


facebook
test666
gmail
twitter
facebook
User test666
Password 45Di}_RmAEYFeu+Fe0,A
Website
Notes
Tags
Expires
more…
File secrets
Group secrets
Created Feb 4, 2022, 9:01:10 PM
Updated Feb 4, 2022, 9:01:53 PM
History 2 records
secret.png



Et voici le flag pour valider.

GCSC{4uCUn_7roUv3r4_C3t_MoT_D3_P45$3}

GUINEA

J'utilise google et trouve le flag.

En tant que Agent de terrain, tu dois connaître au bout des doigts les empreintes numériques de notre pays.

Les malveillants que tu seras amené à traquer pourraient les utiliser en remplacement de son nom officiel "Guinée".

1. Quel est le ccTLD de la Guinée ?
2. Quel est la codification de la loi relative à la Cybersécurité et la Protection des Données à Caractère Personnel en Guinée?
3. Quel est le fuseau horaire de la Guinée?

- Le format attendu est :
Réponse1: tout en minuscule
Réponse2: tout en majuscule
Réponse3: tout en majuscule et n'oublie pas le petit +

Flag: GCSC2022{Reponse1_Reponse2_Reponse3}

REPONSE 1: .gn

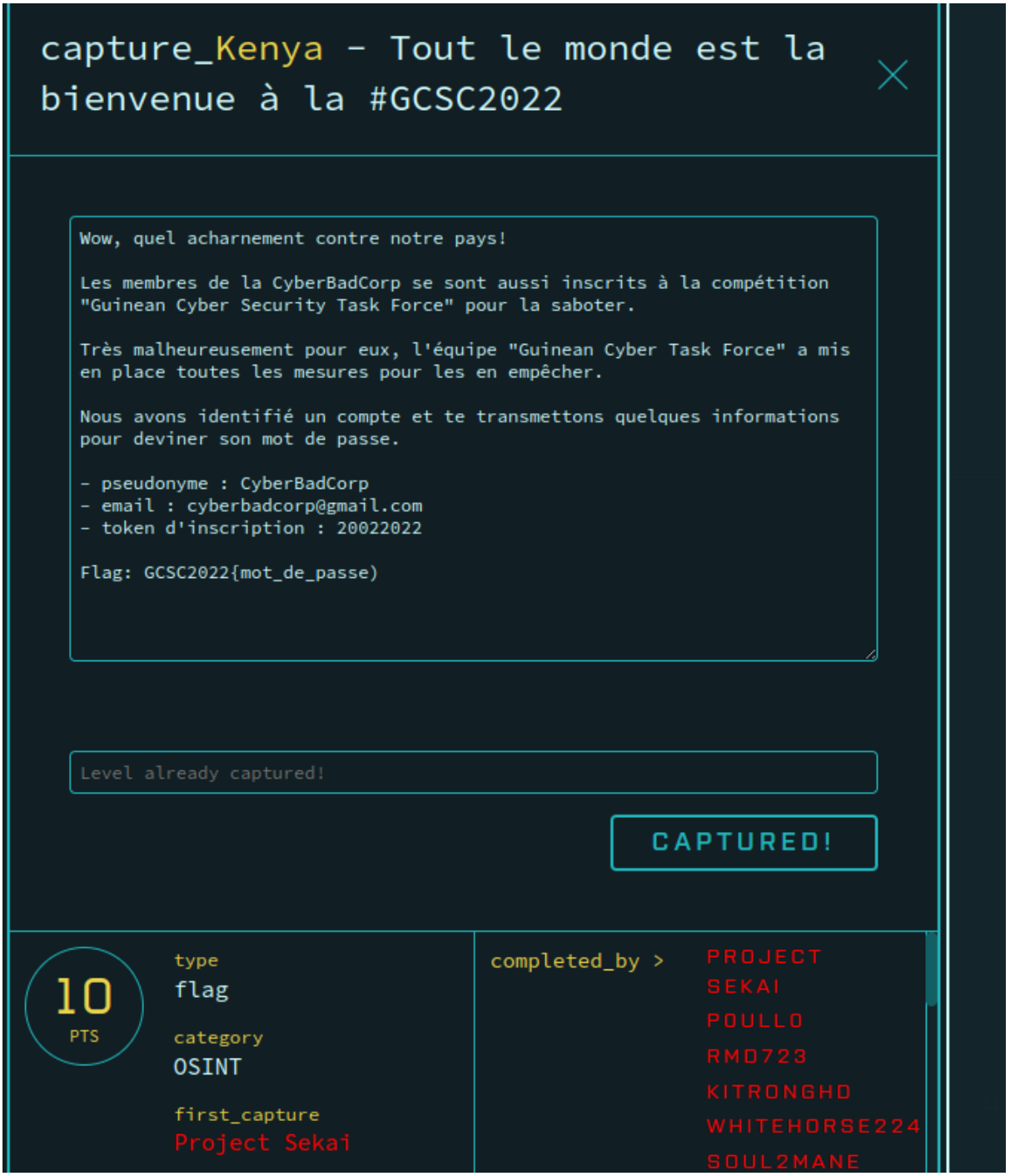
REPONSE 2: L/2016/037/AN ||| L-2016-037-AN

REPONSE 3: GMT+0

.gn_L/2016/037/AN_GMT+0

le flag ::::::: GCSC2022{.gn_L-2016-037-AN_GMT+0}

KENYA



Je regarde mon mot de passe de connexion et je construit le flag puis je remplace le parenthèse de la fin par un accolade.

```
Wow, quel acharnement contre notre pays!

Les membres de la CyberBadCorp se sont aussi inscrits à la compétition "Guinean Cyber Security Task Force" pour la saboter.

Très malheureusement pour eux, l'équipe "Guinean Cyber Task Force" a mis en place toutes les mesures pour les en empêcher.

Nous avons identifié un compte et te transmettons quelques informations pour deviner son mot de passe.

- pseudonyme : CyberBadCorp
- email : cyberbadcorp@gmail.com
- token d'inscription : 20022022


Flag: GCSC2022{GCSC2022_CyberBadCorp20022022cyberbadcorp@gmail.com20022022}

      |------La difference c'est la parenthèse )
```

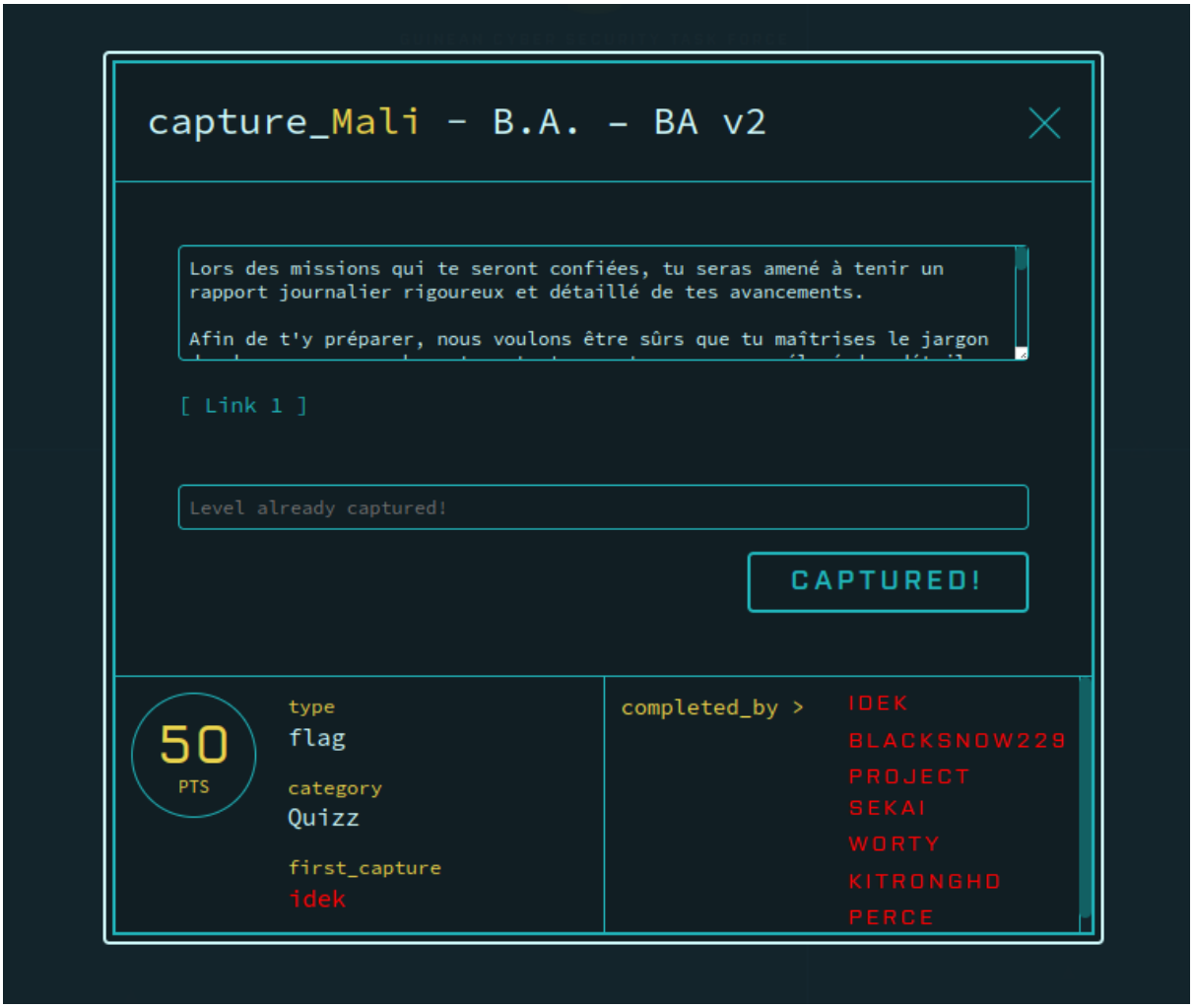
```
Flag: GCSC2022{GCSC2022_CyberBadCorp20022022cyberbadcorp@gmail.com20022022}
```

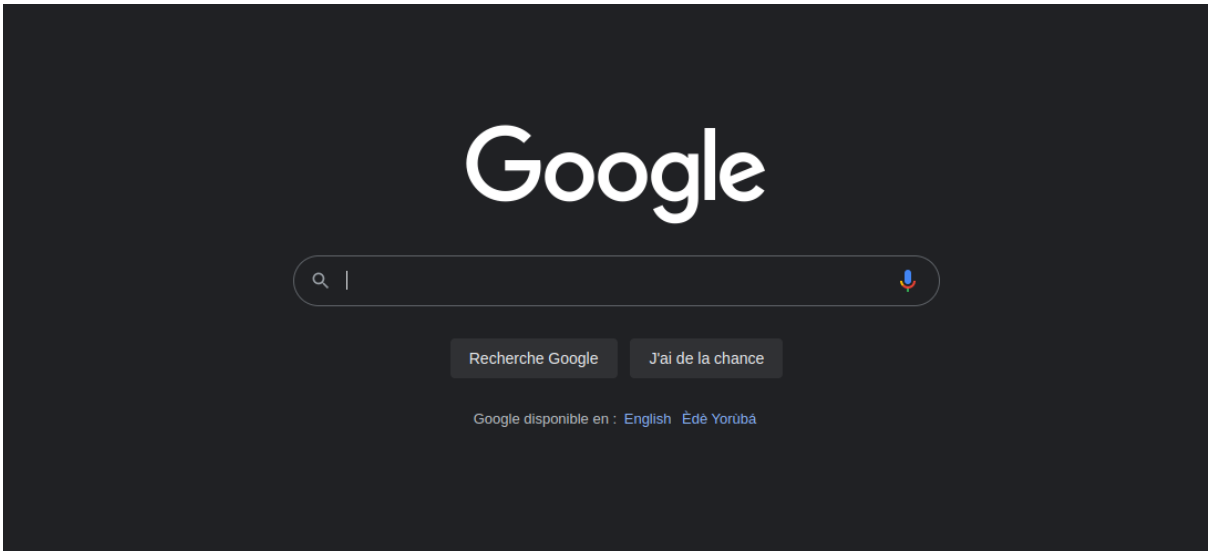
MADAGASCAR


```
1
2  N'oublie pas d'accéder au serveur Discord!
3  Flag : GCSC2022{lien_serveur_discord}
4
5
6  https://discord.gg/3gvtd8N6
7
8
9
10
11 Flag: GCSC2022{https://discord.gg/3gvtd8N6}
12
13
```

```
10
11  Flag: GCSC2022{https://discord.gg/3gvtd8N6}
12
13
```

MALI






```
Lors des missions qui te seront confiées, tu seras amené à tenir un rapport journalier rigoureux et détaillé de tes avancements.

Afin de t'y préparer, nous voulons être sûrs que tu maîtrises le jargon des hommes en capuches et surtout, que tu as un sens élevé des détails (recherches)!

Applique-toi.

1- Quels sont les trois éléments qui composent la triade CIA ?
-Réponse attendue : Cite-les dans cet ordre en Anglais, séparé par des tirets (-), première lettre de mot en majuscule et sans espace

2- On s'intéresse à la norme de télécommunication fonctionnant sur la fréquence 2.4 GHz dont le nom est inspiré du roi des Viking. Donne-le nom suivi de sa dernière version.
- Réponse attendue sous la forme: LoRaWAN v1.1

3- Parmi les technologies suivantes, laquelle est la plus appropriée pour sécuriser son accès Wifi : WEP, WPA, WPS, WPA2? La réponse est sa norme IEEE.
- Réponse attendue sous la forme: IEEE 802.11X

4- Que signifie chacun des sigles suivants: AV, FW, IDS, IPS, SIMS, SOC et VPN?
- Réponse attendue : définition séparée par des tirets (-), un espace avant et apres le tiret (-), majuscule en début de mot, mot au signulier.

5- J'utilise un laptop MacBook pour mes activités quotidiennes. J'utilise Linux pour naviguer sur des sites douteux. J'utilise le réseau social LinkedIn. Dans ce cas, je ne peux pas du tout subir de piratage. Vrai ou Faux?



_Confidentality-Integrity-Avaibility
_Bluetooth v5.2
_IEEE 802.11i
_Antivirus - Firewall - Intrusion Detection System - Intrusion Prevention System - Security Information Management System - Security Operation Center - Virtual Private Network
_Faux


flag : GCSC2022{md5(Confidentality-Integrity-Avaibility_Bluetooth v5.2_IEEE 802.11i_Antivirus - Firewall - Intrusion Detection System - Intrusion Prevention System - Security Information Management System - Security Operation Center - Virtual Private Network_Faux)}
```

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Confidentality-Integrity-Avaibility_Bluetooth v5.2_IEEE 802.11i_Antivirus - Firewall - Intrusion Detection System - Intrusion Prevention System - Security Information Management System - Security Operation Center - Virtual Private Network_Faux

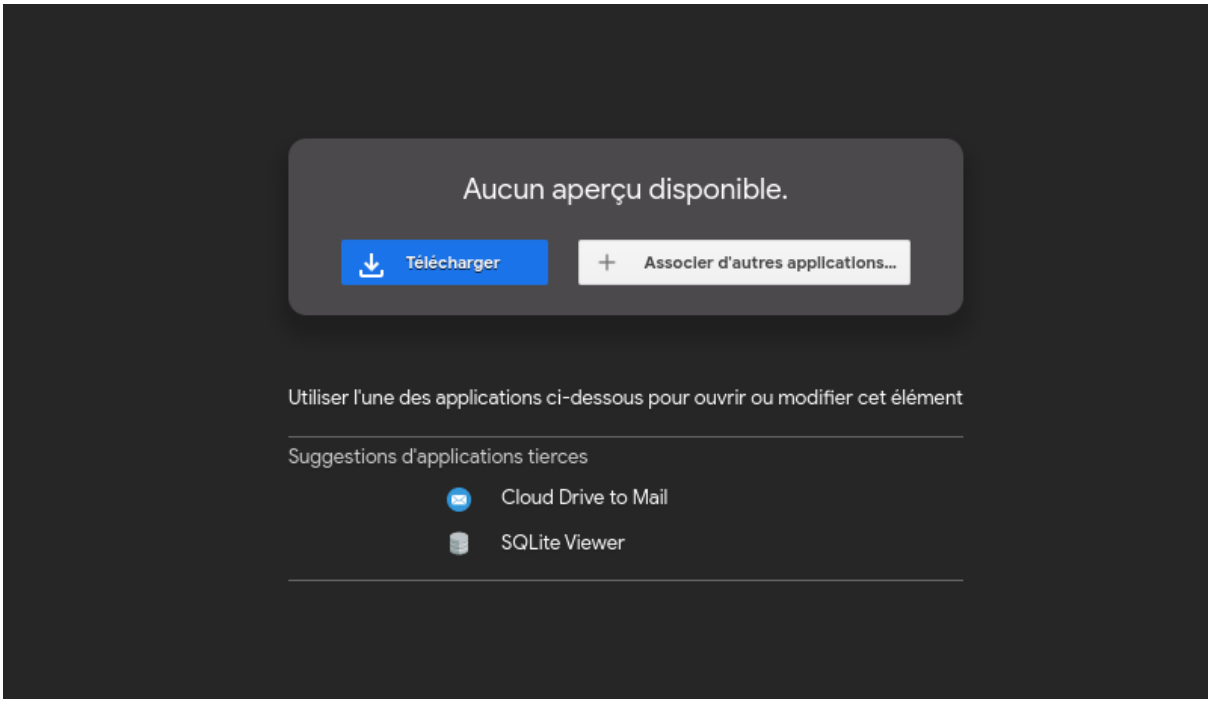
Generate →

Your String	Confidentality-Integrity-Avaibility_Bluetooth v5.2_IEEE 802.11i_Antivirus - Firewall - Intrusion Detection System - Intrusion Prevention System - Security Information Management System - Security Operation Center - Virtual Private Network_Faux
MD5 Hash	bcdf079cae36b60dc8071a18ea491290 Copy
SHA1 Hash	b255611d27f0e46ab7172d6e5a140cb64d50b726 Copy

```
flag : GCSC2022{md5(Confidentality-Integrity-Avaibility_Bluetooth v5.2_IEEE 802.11i_Antivirus - Firewall - Intrusion Detection System - Intrusion Prevention System - Security Information Management System - Security Operation Center - Virtual Private Network_Faux)}


flag : GCSC2022{bcdf079cae36b60dc8071a18ea491290}
```

NIGERIA


capture_Nigeria - Mots de passe d'une application étrange
Tu as vite retrouvé la base de données reliée à cette application.
Maintenant, trouve leurs mots de passe.
Flag: GCSC2022{Password1_Password2_Password3)
[Link 1]
Level already captured!
CAPTURED!
30
PTS
type
flag
category
Miscellaneous
first_capture
idek
completed_by >
IDEK
OFSH1LL
RMD723
PROJECT SEKAI
BLACKSNOW229
LEOX



SQLite Viewer with Google Drive Memo

FileName: BD application mobile.db Save to Computer

TYPE PHONE NUMBER Search For Owner Full Name, Full Address, Relatives & More!

Powered By BeenVerified

Example: (123) 456-7890 ( ) - Search

Drop a file here to load sqlite file or click on this box to open file dialog.

users (3 rows)

```
SELECT * FROM 'users' LIMIT 0,30
```

Execute (Ctrl+Enter)

username	password
John	ODI3MDQ0MGMwZTk0MTExZDExZmFmMzg1MTI1Nzc4ZTc=
Marie	NDFkNTM4YTcxYjJhYTYwMDRkNTM0MjM3NzEwNDFjOWMK
Luc	NGVmY2RhYzg1YzZjNDk0YjNjZWY4NzgxY2M2Mzk4MDUK

Decode from Base64 format

Simply enter your data then push the decode button.

ODI3MDQ0MGMwZTk0MTExZDExZmFmMzg1MTI1Nzc4ZTc=

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on th

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character

DECODE Decodes your data into the area below.

8270440c0e94111d11faf385125778e7

NDFkNTM4YTcxYjJhYTYwMDRkNTM0MjM3NzEwNDFjOWMK

For encoded binaries (like images, documents, etc.) use the file upload form a lit

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only t

DECODE Decodes your data into the area below.

41d538a71b2aa6004d53423771041c9c

Decode from Base64 format

Simply enter your data then push the decode button.

NGVmY2RhYzg1YzZjNDk0YjNjZWY4NzgxY2M2Mzk4MDUK

For encoded binaries (like images, documents, etc.) use the file upload form a little furt

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UT

DECODE Decodes your data into the area below.

4efcdac85c6c494b3cef8781cc639805

8270440c0e94111d11faf385125778e7 : **p1ntap**

Trouvé en 0.41s

41d538a71b2aa6004d53423771041c9c : **fd1972**

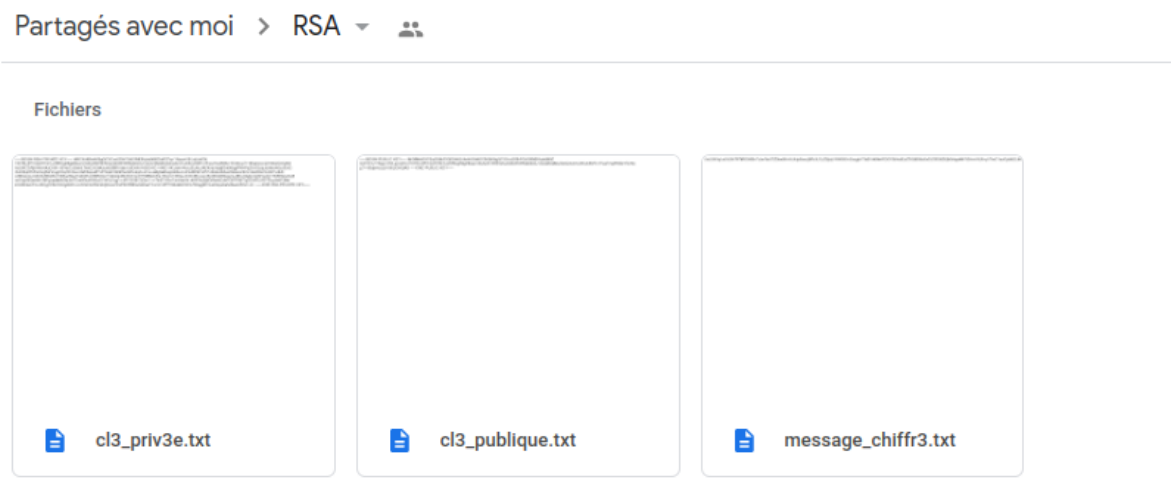
Trouvé en 0.269s

4efcdac85c6c494b3cef8781cc639805 : **AdDiCtIoN**

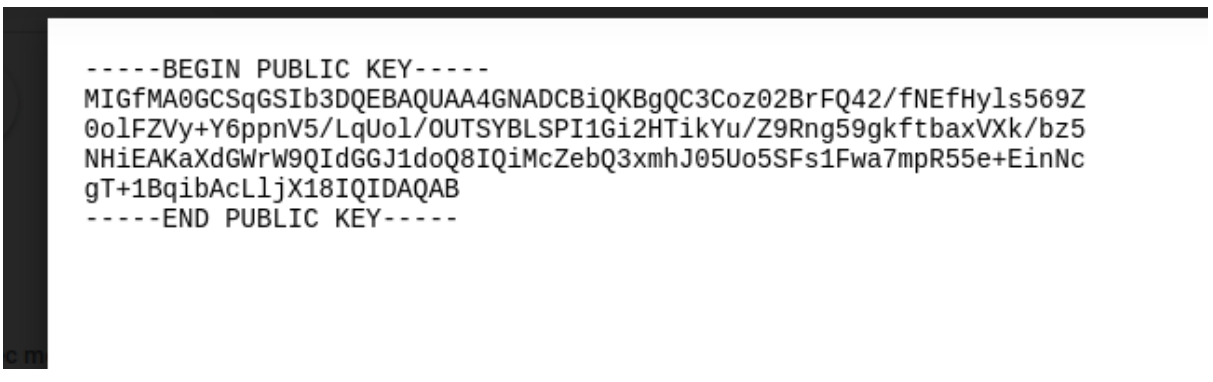
Trouvé en 0.453s

```
ODI3MDQ0MGMwZTk0MTExZDExZmFmMzg1MTI1Nzc4ZTc=      8270440c0e94111d11faf385125778e7    p1ntap
NDFkNTM4YTcxYjJhYTYwMDRkNTM0MjM3NzEwNDFjOWMK      41d538a71b2aa6004d53423771041c9c    fd1972
NGVmY2RhYzg1YzZjNDk0YjNjZWY4NzgxY2M2Mzk4MDUK      4efcdac85c6c494b3cef8781cc639805    AdDiCtIoN

le flag :::::::   GCSC2022{p1ntap_fd1972_AdDiCtIoN}
```

UNITED STATE

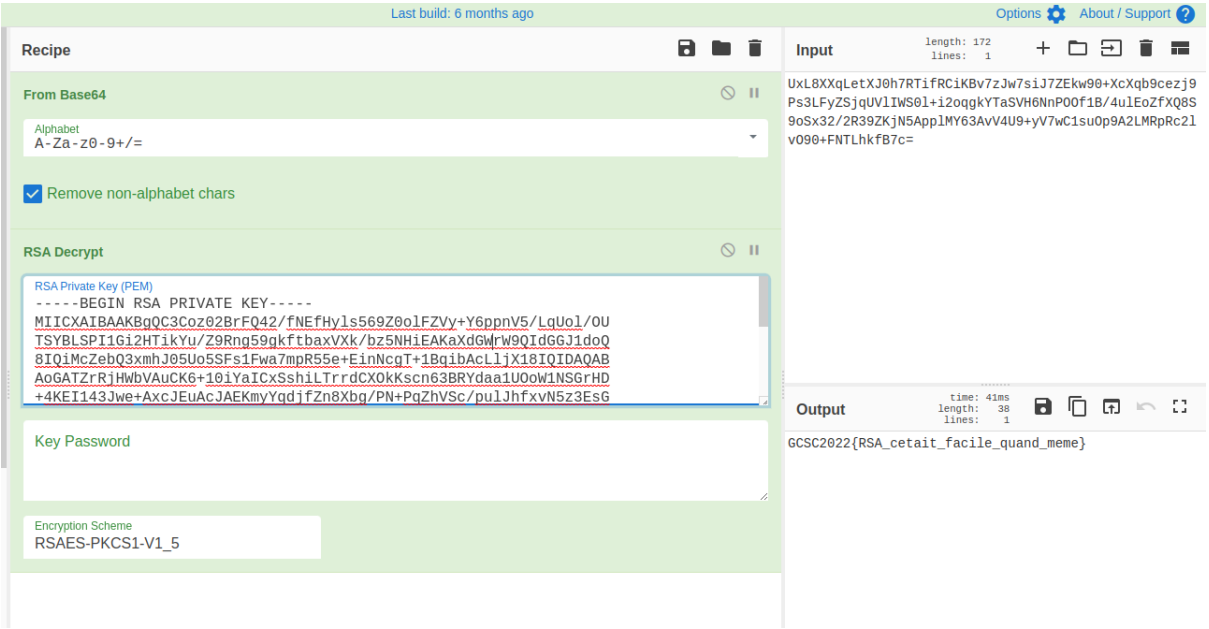


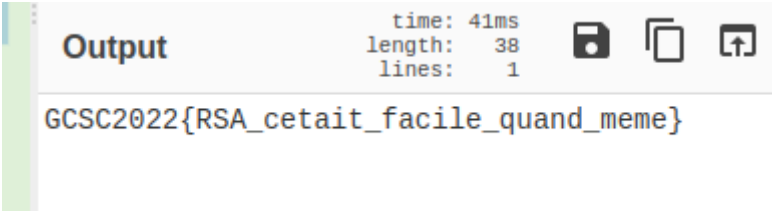
```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC3Coz02BrFQ42/fNEfHyls569Z0olFZVy+Y6ppnV5/LqUol/OU
TSYBLSPI1Gi2HTikYu/Z9Rng59gkftbaxVXk/bz5NHiEAKaXdGWrW9QIdGGJ1doQ
8IQiMcZebQ3xmhJ05Uo5SFs1Fwa7mpR55e+EinNcgT+1BqibAcLljX18IQIDAQAB
AoGATZrRjHWbVAuCK6+10iYaICxSshiLTrrdCXOkKscn63BRYdaa1UOoW1NSGrHD
+4KEI143Jwe+AxcJEuAcJAEKmyYqdjfZn8Xbg/PN+PqZhVSc/pulJhfxvN5z3EsG
tAJh8qXFhPuOcgfioFk/ygOXqCEr2wrJGrEfuiyx6TUPOqkCQQDhoGZLdqph+41e
eMg0aRcqjm6SvvLbhhdEIhFU/57+6tdsUbEwzh5dwVdInVn9sXI8cOi+Bi7vUk5i
wNKZpzsvAkEAz66QWJTXlEg4NquFabGEUANRSGo+VjlQOpDfaTc4VpcH7N9MeOKq
WqnCVWQyufVAml6LzaccfIzd5GIdNQaprwJBAJl3gbz4pSHqeZj1rK/Bf4lpwho8
mXHp/i9QwNtA18PqtsattklNGeiJlrYEmW5u4RXtctG14PzVzg1rvJPY5O8CQDe1
r+rTInEYXlvr7sHHaKK+ARPXzBj9DtRnAEcNFQPFR872p2DWDLR9TS/yzNitPUMr
kXz9EtsmPm+BEiyjOOkCQHgQWr+oUXQ/mhZ9mG2jZeJxhfmPSOf58SxG4KwFYvmX
MPTO6kbiKZ4/CLPiNqgliR1zu0i3quKaS48w4dWVz+4=
-----END RSA PRIVATE KEY-----
```



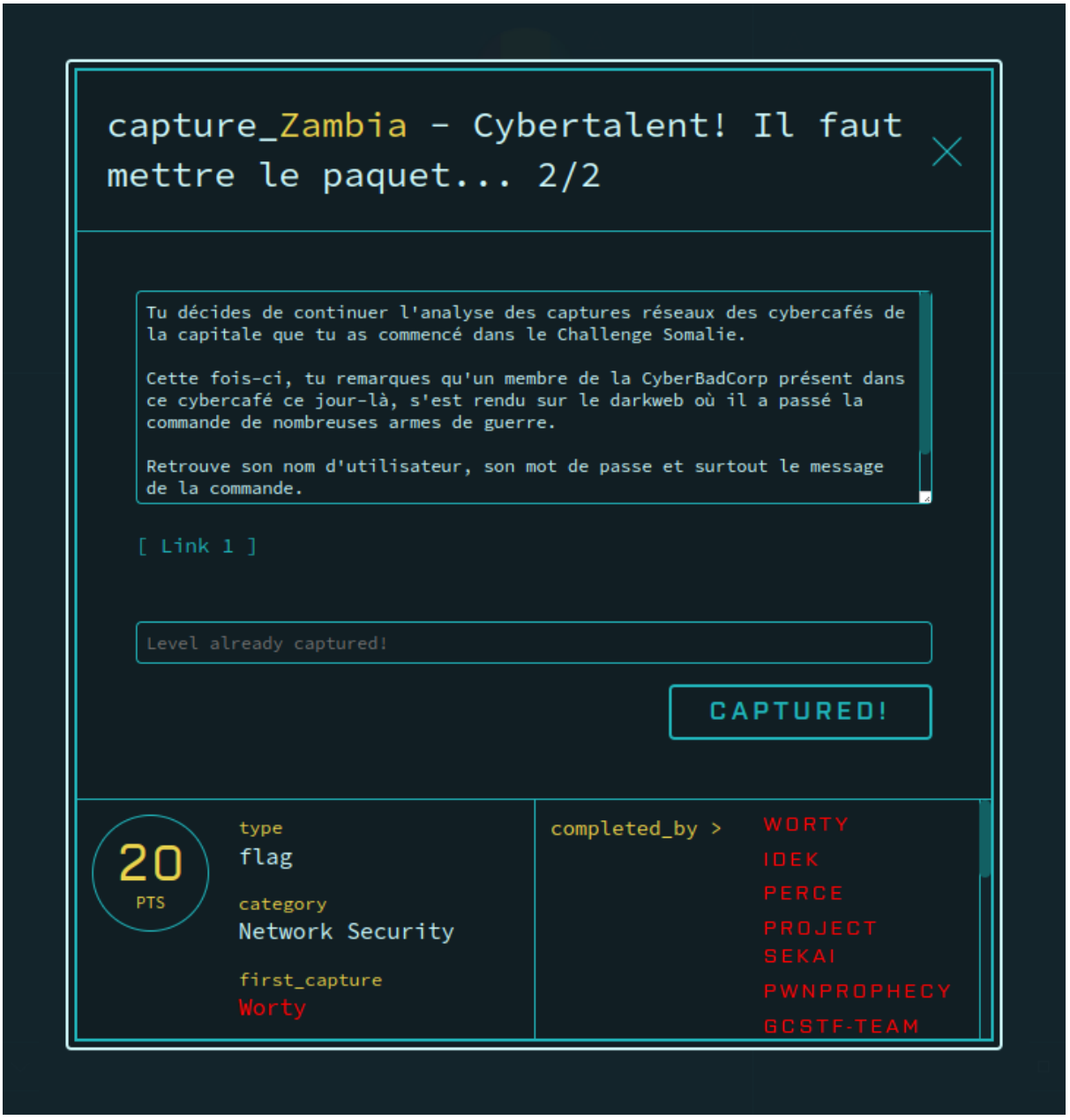
```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3Coz02BrFQ42/fNEfHyls569Z
0olFZVy+Y6ppnV5/LqUol/OUTSYBLSPI1Gi2HTikYu/Z9Rng59gkftbaxVXk/bz5
NHiEAKaXdGWrW9QIdGGJ1doQ8IQiMcZebQ3xmhJ05Uo5SFs1Fwa7mpR55e+EinNc
gT+1BqibAcLljX18IQIDAQAB
-----END PUBLIC KEY-----
```

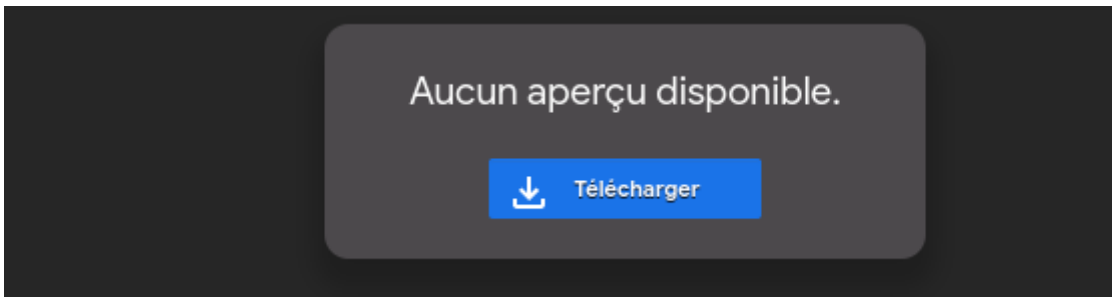
J’utilise cyberchef online pour décoder le texte.



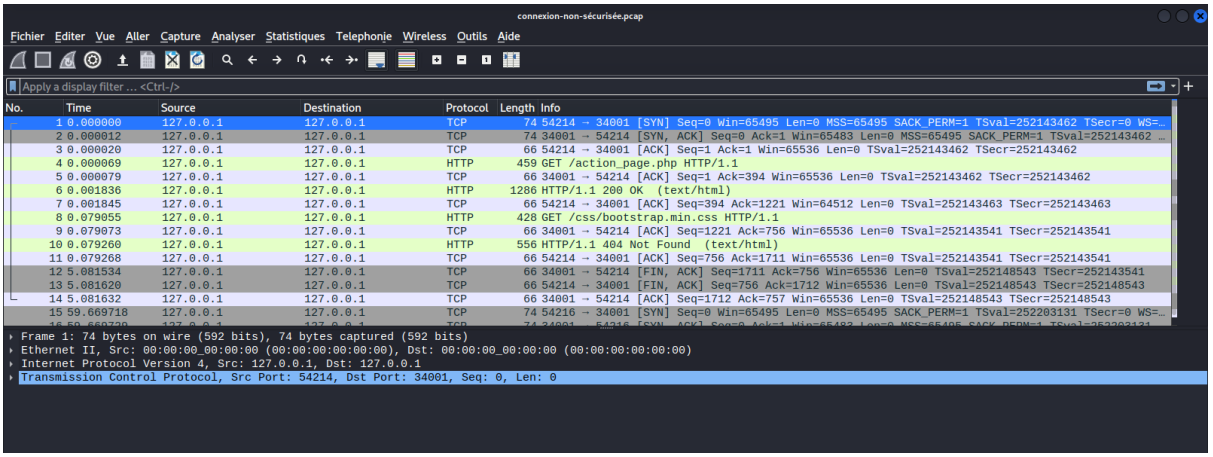


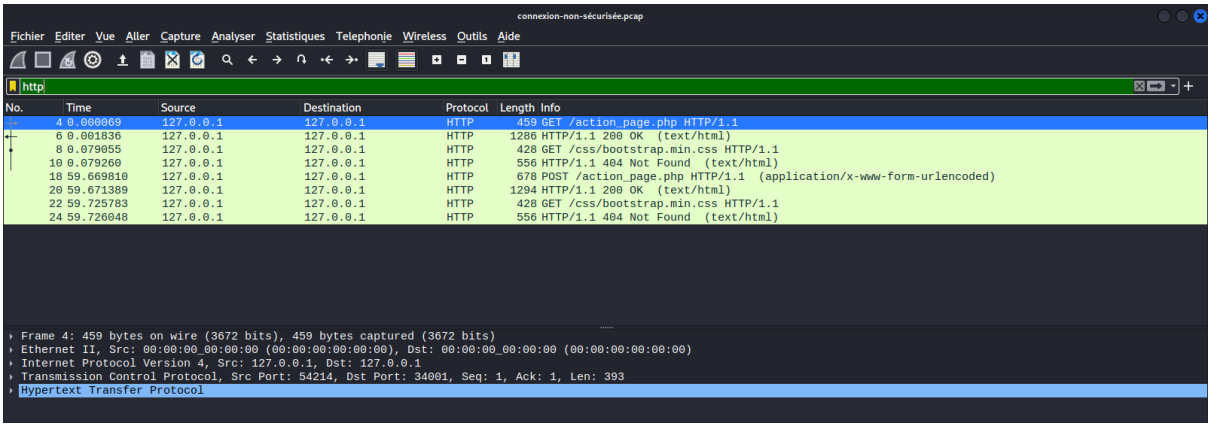
ZAMBIA

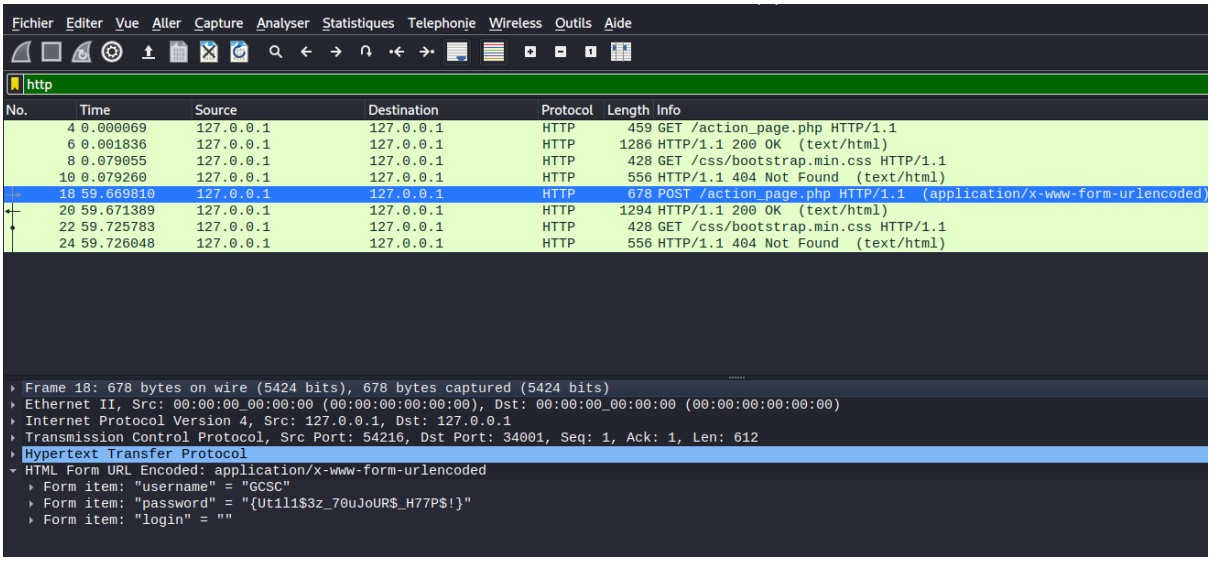

capture_Zambia - Cybertalent! Il faut mettre le paquet... 2/2
Tu décides de continuer l'analyse des captures réseaux des cybercafés de la capitale que tu as commencé dans le Challenge Somalie.
Cette fois-ci, tu remarques qu'un membre de la CyberBadCorp présent dans ce cybercafé ce jour-là, s'est rendu sur le darkweb où il a passé la commande de nombreuses armes de guerre.
Retrouve son nom d'utilisateur, son mot de passe et surtout le message de la commande.
[Link 1]
Level already captured!
CAPTURED!
20
PTS
type
flag
category
Network Security
first_capture
Worty
completed_by >
WORTY
IDEK
PERCE
PROJECT SEKAI
PWNPROPHECY
GCSTF-TEAM



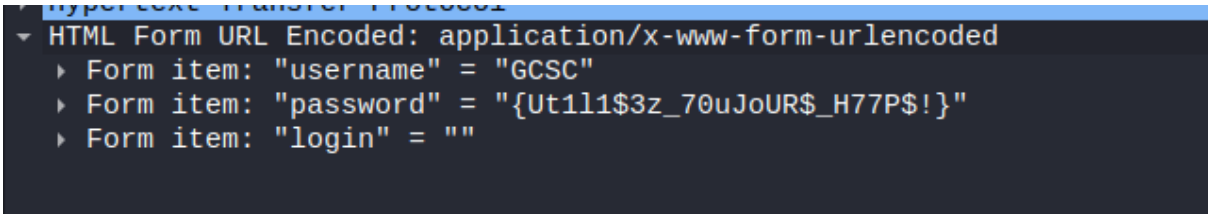
Après avoir téléchargé le fichier, j'ai ouvert avec Ettercap.
Et puis filtrer les paquets http et tcp.







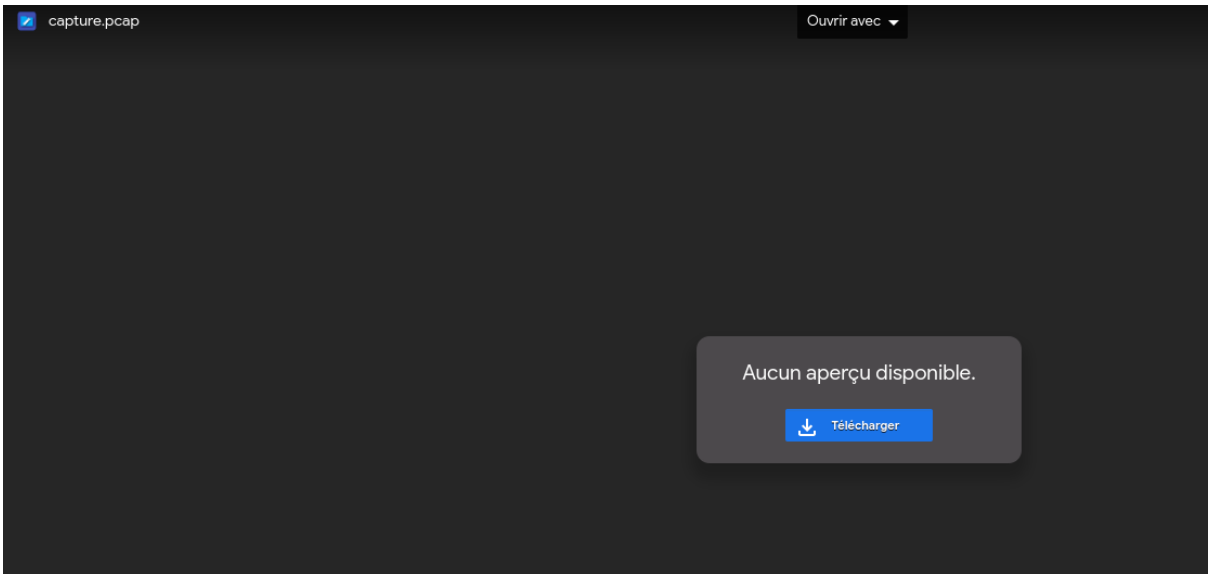
Puis dans une protocole Http, j'ai où la méthode POST est utilisée j'ai trouvé le flag.



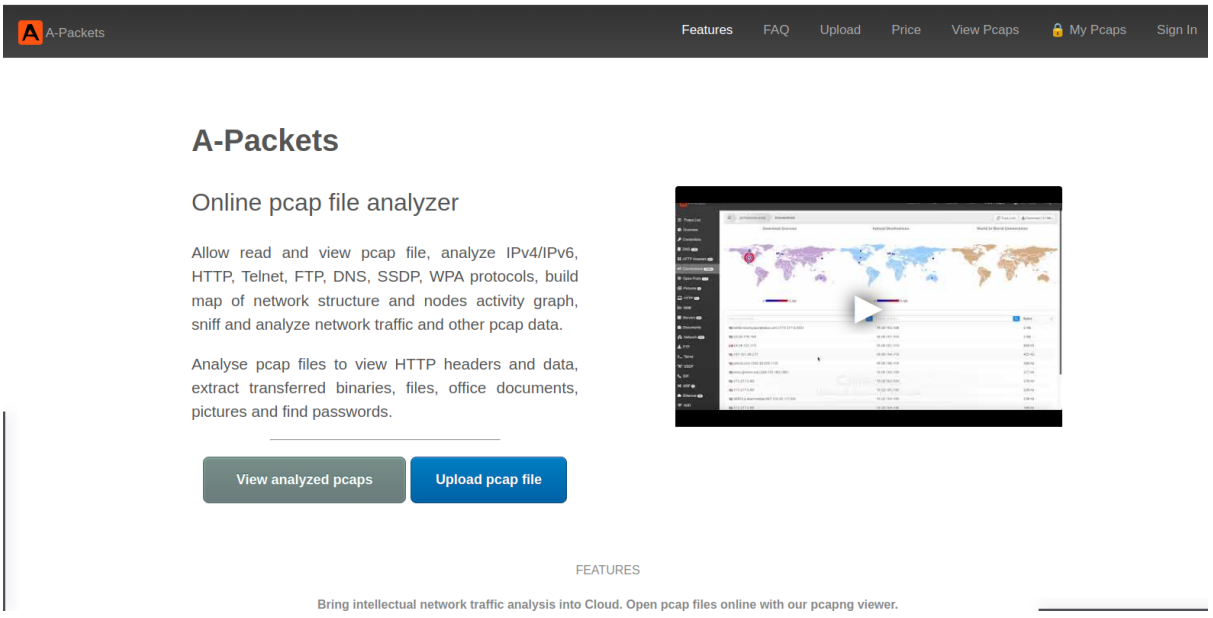
SOMALI

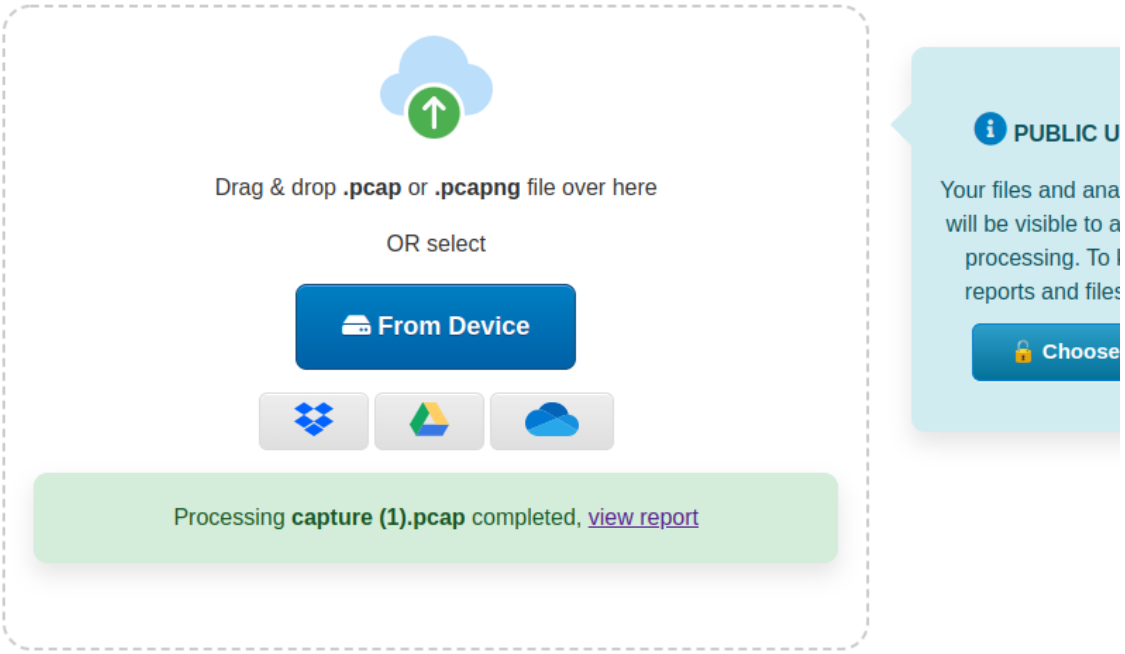
Je clique sur Link 1.

Puis je télécharge le fichier capture pcap.



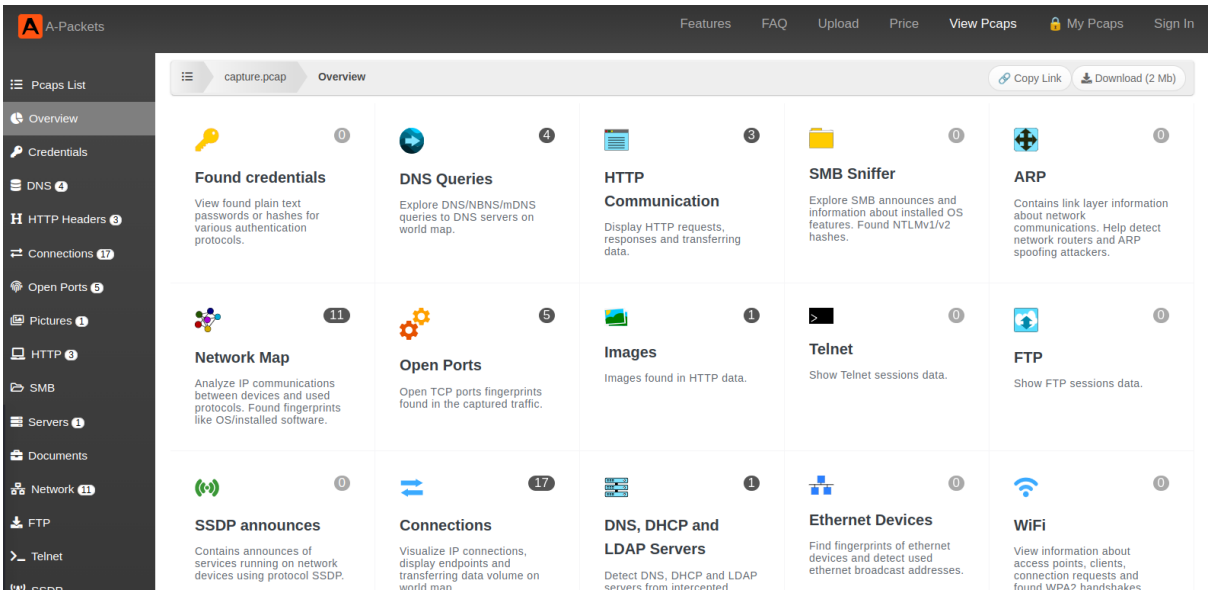
Après je l'ouvre avec l'utilitaire online A-Packets





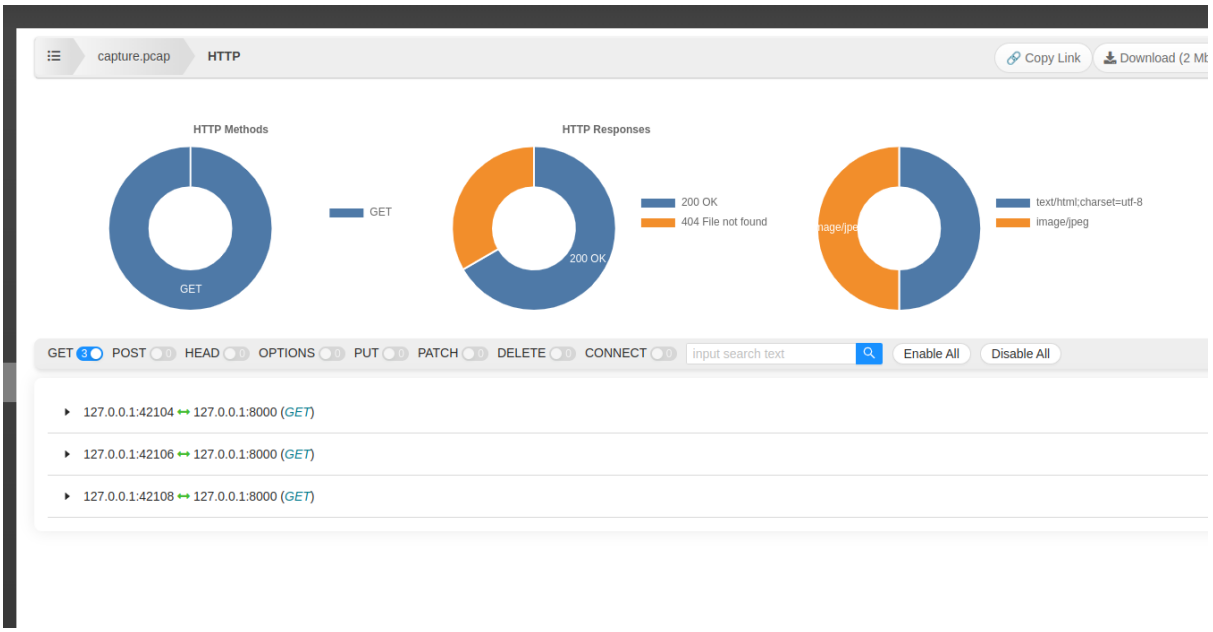
e pcap file on Windows

J'upload le fichier et A-Packet se charge de faire l'analyse puis je clique sur view report.
Pour voir le rapport.



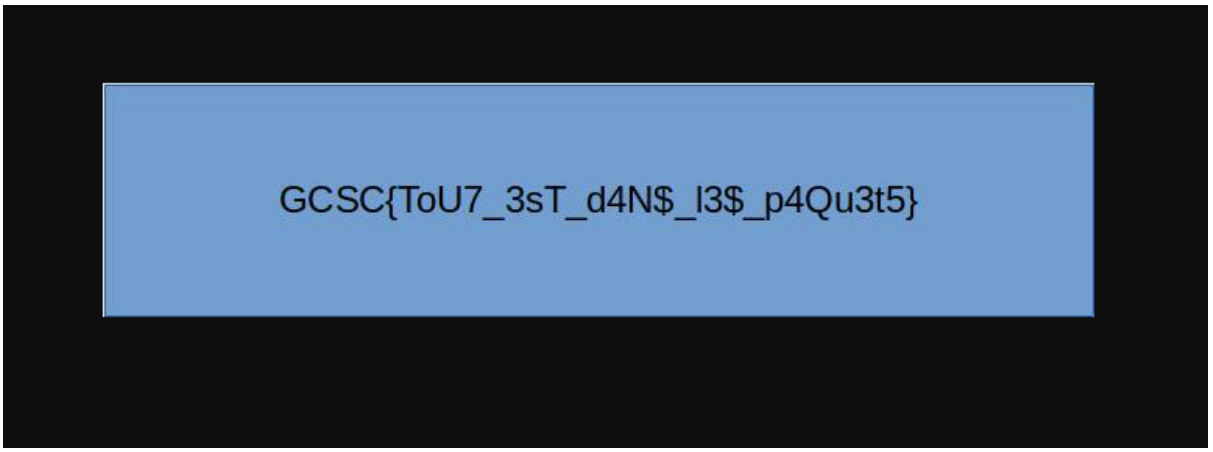
Je vois tous les services et protocoles utilisés et qui sont stockés dans le fichier pcap sur mon board.

Comme c'est le trafic qui me concerne. Je regarde dans HTTP Communication pour voir les échanges.



Ici le trouves les échanges entre différentes adresses IP.

Je visualise le tout. Et je vois que dans la dernière communication entre les ip, il y un fichier image qui est joint. Je l'ouvre pour voir.



Et c'est le flag.

CANADA

Je clique sur Link 1.
Link 2 c’est de la Fouine. Pour vous dire, ne stressez pas.

Please, register a new user to continue

Kante

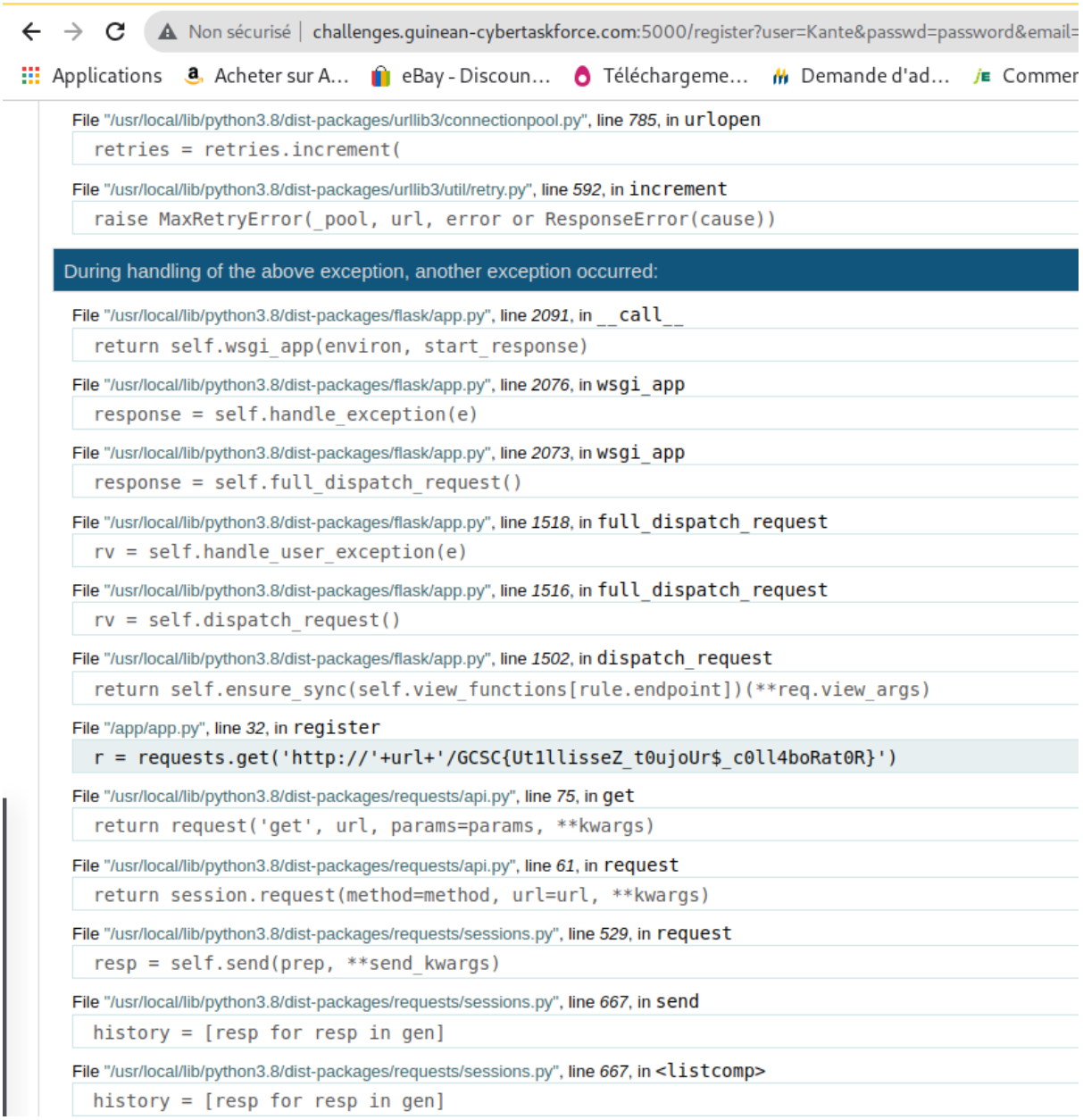
password

kante@gmail.com

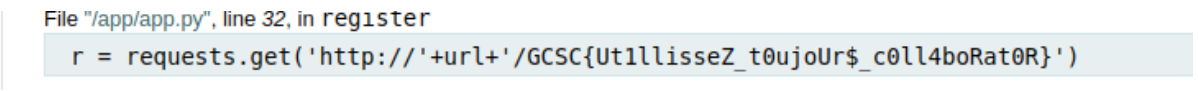
test.com

Envoyer

J’ai une page où je remplir le formulaire.
Essayons juste de remplir ce formulaire. Et j’ai eu la réponse.



voici le flag parmis toute la sortie.



Trouvez. J’ai trop bien aimé cette compétition.
Merci à GCSC2022.