

# WRITEUP GUINEAN CTF

---

## GUINEE

**Enoncé** : 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}

**Solution** : Pour résoudre ce **chall**, mon meilleur ami était **Google**.

1- ccTLD = .gn

2- LOI L-2016-037-AN

3- GMT+0

**Flag:** GCSC2022{.gn\_LOI L-2016-037-AN\_GMT+0}

---

## MALI

**Énoncé** : 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 après le tiret (-), majuscule en début de mot, mot au singulier.

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?

Format du flag : GCSC2022{md5(Reponse1\_Reponse2\_Reponse3\_Reponse4\_Reponse5)}

**Solution** : Toujours avec l'aide de mon meilleur ami (**Google**), j'ai pu obtenir les différentes réponses sans trop de soucis.

1- Tout débutant en sécurité informatique devrait connaître le triangle **CIA** (Confidentiality-Integrity-Availability).

2- **Danois Harald à la dent bleue** (Ça vous parle ?) Et **Harald Bluetooth** ? Eh bien c'est la même personne ! (**roi des vikings**) donc on a **Bluetooth**. Et pour la version ? Lis bien wikipédia [ici](#) tu trouveras (**v5.2**). D'où : **Bluetooth v5.2**

- 3- **WPA2** est la version de la norme **IEEE 802.11i**

4- Confidentiality-Integrity-Availability\_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

5- **Faux** (Ne soyez pas aussi naïf).

**Flag** : GCSC2022{bcdcf079cae36b60dc8071a18ea491290}

**Note** : pour convertir le tout en **md5**, vous pouvez utiliser **md5sum** de linux (pour les liens) et **Google** pour les rapides. [ici](#)

---

## ZAMBIE

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.

**Solution** : Quelle chance ! La connexion n'est pas sécurisée bah let's go !

En ouvrant **connexion-non-sécurisée.pcap** avec **Wireshark**, j'aperçois déjà le **Three-way handshake**. Je constate également qu'une action a été menée avec la méthode POST.

18	59.669810	127.0.0.1	127.0.0.1	HTTP	678	POST /action_page.php HTTP/1.1 (application/x-www-form-urlencoded)
19	59.669820	127.0.0.1	127.0.0.1	TCP	66	34001 → 54216 [ACK] Seq=1 Ack=613 Win=65536 Len=0 TSval=25220...
20	59.671389	127.0.0.1	127.0.0.1	HTTP	1294	HTTP/1.1 200 OK (text/html)

En analysant bien la trame, j'obtiens ce trésor.

**HTML Form URL Encoded: application/x-www-form-urlencoded**

- Form item: "username" = "GCSC"
- Form item: "password" = "{Ut1l1\$3z\_70uJoURS\$\_H77P\$!}"

**Flag** : GCSC2022{Ut1l1\$3z\_70uJoURS\$\_H77P\\${!}}

## CONGO KINSHASA

Un de nos agents du service de contre-espionnage a mis la main sur un fichier crypté de la CyberBadCorp. Aide-le à accéder à son contenu.

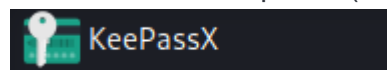
**Solution** : Avez-vous déjà entendu parler de KeePass ? Eh bien nous avons à faire à cela. Cependant, la base de donnée est hachée, il faut donc extraire le hash. Pour ce faire, j'ai utilisé **keepass2john**.

```
(ctf@kali)-[~/Téléchargements]
$ keepass2john secrets.kdbx > t.txt
```

Le hash étant maintenant prêt, j'ai procédé à son déchiffrement via **john**.

```
(ctf@kali)-[~/Téléchargements/GUINEAN]
$ john -w=/usr/share/wordlists/rockyou.txt t.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 30 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
rellik000 (secrets)
1g 0:00:00:13 DONE (2022-02-20 11:15) 0.07656g/s 62174p/s 62174c/s 62174C/s rellik000
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Une fois le mot de passe (**rellik000**) obtenu, je me suis connecté à la base de donnée via **KeePassX**



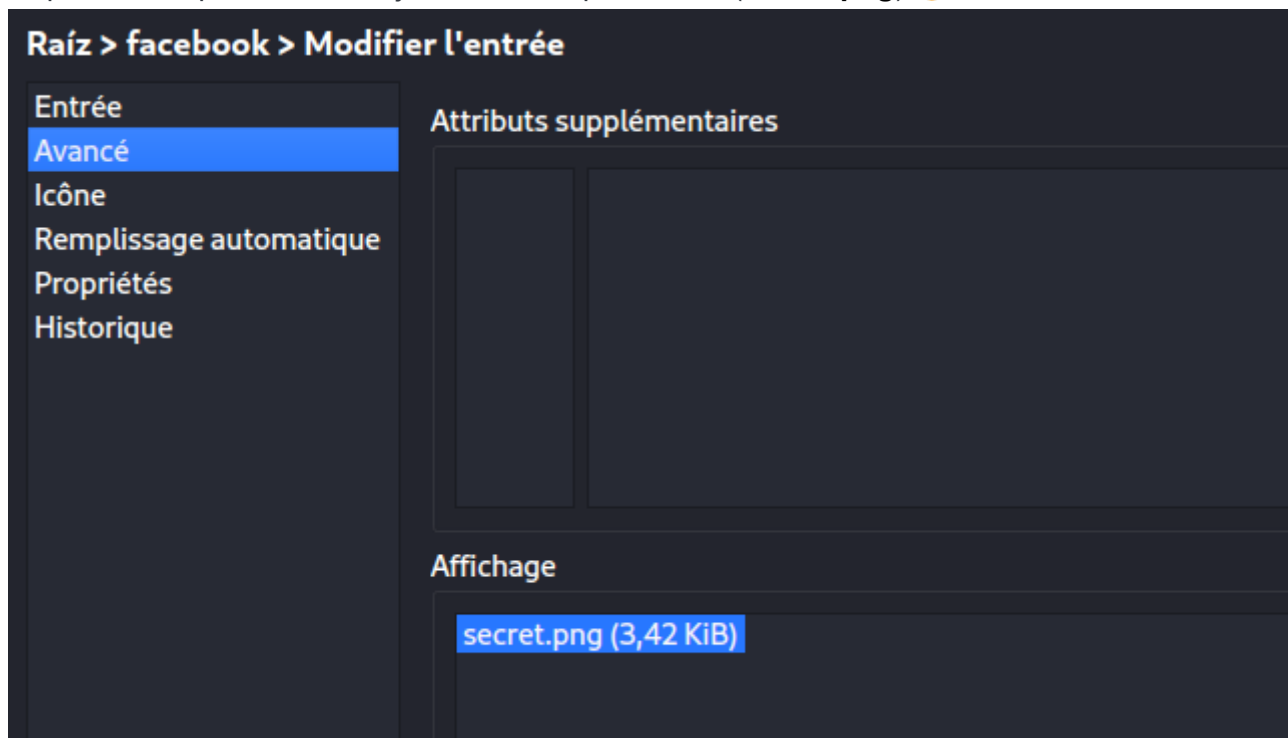
**Entrez la clé maître**

/home/ctf/Téléchargements/GUINEAN/secrets.kdbx

✓ Mot de passe : rellik000

Raiz	Titre	Nom d'utilisateur	URL
	facebook	test666	
	gmail	test666@gmail.com	
	twitter	test666	

Depuis le compte **facebook**, j'ai obtenu un petit trésor (**secret.png**) 🕶️.



GCSC{4uCU\_n\_7roUv3r4\_C3t\_MoT\_D3\_P45\$3}

---

## IRAN

Énoncé : En pause café avec tes collègues, ton Responsable d'opération surgit dans la salle avec un dossier d'une priorité très élevée. Il s'agit encore de ce même groupe qui vient de mettre SOTELGUI à l'arrêt.

Mène tes enquêtes et stoppe ces cybercriminels. Nous t'avons préparé des questions qui te faciliteront ton travail.

1- Quel groupe de hackers cible principalement les sociétés de télécommunications : Réponse attendue : Nom groupe - ID sur Att&ck

2.- Quel est le pays d'origine de ce fameux groupe ?

Réponse attendue : Pays en français

3- Le groupe utilise une technique spéciale pour exfiltrer les données. Quels sont le nom et l'ID de la technique. Réponse attendue : Nom - ID

4- Pour mitiger la technique précédente, un moyen est utilisé. Quel est le nom de cette mitigation ainsi que son ID ? Réponse attendue : Mitigation - ID

5- Quelle est la sous-technique la plus utilisée par le groupe de hackers pour cibler les victimes de l'entreprise ? Réponse attendue : Nom sous-technique - ID

6- Quel est l'interpréteur de commandes et scripts utilisé dans la sous-technique précédente pour lancer des commandes sur les machines des victimes ?

Réponse attendue : Nom interpréteur - ID

Format du flag: GCSC2022{md5(Réponse1/Réponse2/Réponse3/Réponse4/Réponse5/Réponse6)}

**Solution** : Heureusement, **Google** existe ! Comme le challenge porte le même nom que le pays en question, je me suis renseigné sur le groupe d'espion **iranien** qui s'intéresse aux **secteurs des télécommunications** et j'ai trouvé [ça](#). Puis, je me suis référé à ceux-ci : [ici](#) et [ici](#) (pour répondre aux questions). Au final, j'ai constitué ceci :

```
APT39 - G0087/Iran/Exfiltration Over C2 Channel - T1041/Network Intrusion Prevention  
- M1031/Spearphishing Attachment - T1566.001/Visual Basic - T1059.005
```

**Flag** : `GCSC2022{4a154dfdc0e789b56deaa0db6ecd72c4}`

## USA RSA

On te donne le cryptosystème utilisé : message, clé privée et clé publique.

**Solution** : Ils sont gentils les organisateurs ! Donner le message, la clé privée et publique, le job est déjà fait 😊😎 ! Plus qu'à déchiffrer le mystère... Pour cela, ne te casse pas la tête, utilise [ça](#) et hopppppp!

### Clé publique

```
-----BEGIN PUBLIC KEY-----  
MIGfMA0GCSqGSIb3DQEBAQUAA4GNAD  
CBiQKBgQC3Coz02BrFQ42/fNEfHyls569Z  
0oIFZVy+Y6ppnV5/LqUol/OUTSYBLSPI1Gi  
2HTikYu/Z9Rng59qkftbaxVXk/bz5  
NHiEAKaXdGWrW9QldGGJ1doQ8lQiMcZe  
bQ3xmhJ05Uo5SFs1Fwa7mpR55e+EinNc  
qT+1BqibAcLijX18IQIDAQAB  
-----END PUBLIC KEY-----
```

### Clé privée

```
WJBAJI3gdZ4pSHqeZITRK/Bt4lpwno8  
mXHp/i9QwNtA18PatsattkINGeiJlrYEmW  
5u4RXtctG14PzVzg1rvJPY5O8CQDe1  
r+rTlnEYXlvr7sHHaKK+ARPXzBi9DtRnA  
EcNFQPF872p2DWDLR9TS/vzNitPUMr  
kXz9EtsmPm+BEiyjOOkCQHgQWr+oUX  
Q/mhZ9mG2jZeJxhfmPSOf58SxG4KwFY  
vmX  
MPTO6kbiKZ4/CLPiNqgliR1zu0i3quKaS4  
8w4dWVz+4=  
-----END RSA PRIVATE KEY-----
```

### Message en texte clair

```
UxL8XXqLetXJ0h7RTifRCiKBv7zJw7siJ7ZE  
kw90+XcXqb9cezi9Ps3LFyZSjqUVIIWS0l+i  
2oqgkYTaSVH6NnPOOf1B/4ulEoZfXQ8S9o  
Sx32/2R39ZKjN5AppIMY63AvV4U9+yV7w  
C1suOp9A2LMRpRc2lvO90+FNTLhkfb7c=
```

### sortir

```
GCSC2022{RSA_cetait_facile_quand_mem  
e}
```

## RUSSIE

La CyberBadCorp s'est rendue compte de ton intrusion dans leur Système d'Information à la suite de ton succès dans le challenge France. Ils ont pris de nouvelles méthodes, que dis-je? de nouvelles mesures de sécurité. Rappelle-toi : la GCSC t'aidera à passer de l'autre côté de la force : devenir un hacker éthique.

**Solution** : Bon c'est vrai qu'avec un simple **curl**, on a pas grande chose. Cependant, (**Rappelle-toi : la GCSC t'aidera à passer de l'autre côté de la force : devenir un hacker éthique**) n'était pas une blague 😊😊 ! J'ai essayé une technique de contournement du **curl** avec l'option **-X** et j'ai obtenu ça :

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# curl -X GCSC http://challenges.guinean-cybertaskforce.com:8001
Qu'est ce que c'est ce methode??
```

**By Guessing**, il fallait juste mettre **flag** à la fin. Quel miracle 😊!

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# curl -X GCSC http://challenges.guinean-cybertaskforce.com:8001/flag
GCSC{p0s7_Et_g3t_ne_$ont_p4$_sp3c13lle5}
```

**Flag** : GCSC2022{p0s7\_Et\_g3t\_ne\_\$ont\_p4\$\_sp3c13lle5}

---

## CAMEROUN

Cette nuit encore, un nouvel incident de sécurité s'est produit du côté de la préfecture de Kankan. Après avoir eu un accès au SI, le malveillant tente d'exfiltrer des informations par l'envoi d'une image d'apparence anodine. Il semble que c'est la technique utilisée par la CyberBadCorp avant que tu ne rejoignes le rang des cybercombattants guinéens. Analyse attentivement cette image et trouve l'information exfiltrée.

**Solution** : Rien d'aussi simple ! Connais-tu Aperisolve ? Si non, regarde [là](#), il te suffira d'uploader l'image en question et on obtient ce trésor 😊.



GCSC{4bs7r4ct\_4rT\_i\$\_woRtHL3\$\$}

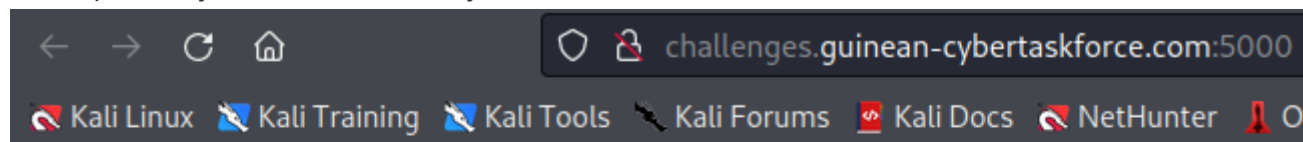
---

## CANADA

**Énoncé** : Houhou! On te présente ce formulaire du site web en cours de construction. Interagit avec le serveur de la CyberBadCorp et trouve-lui un usage non sollicité.

**Solution** : Bon..... Je crois ce **chall** m'a vraiment surpris dans le sens où c'était le contraire à tout ce que je m'y attendais. 😞

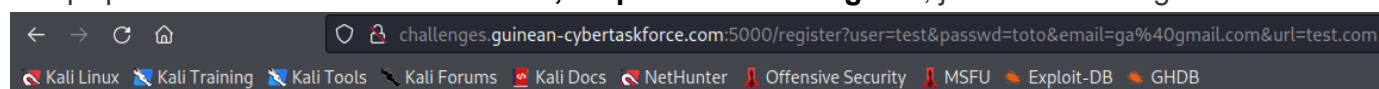
En cliquant déjà sur le lien donné, je me suis retrouvé là :



Please, register a new user to continue

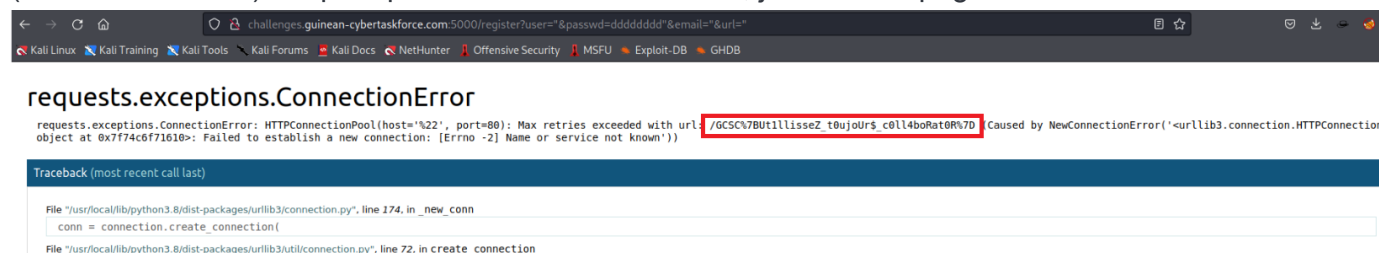
user
password
email
test.com
Submit Query

Ce qui plutôt normal ! En entrant un **user**, un **password** et un **gmail**, j'ai eu ce message.



S'il vous plait, votre mot de passe doit etre de 8 caractères ou plus

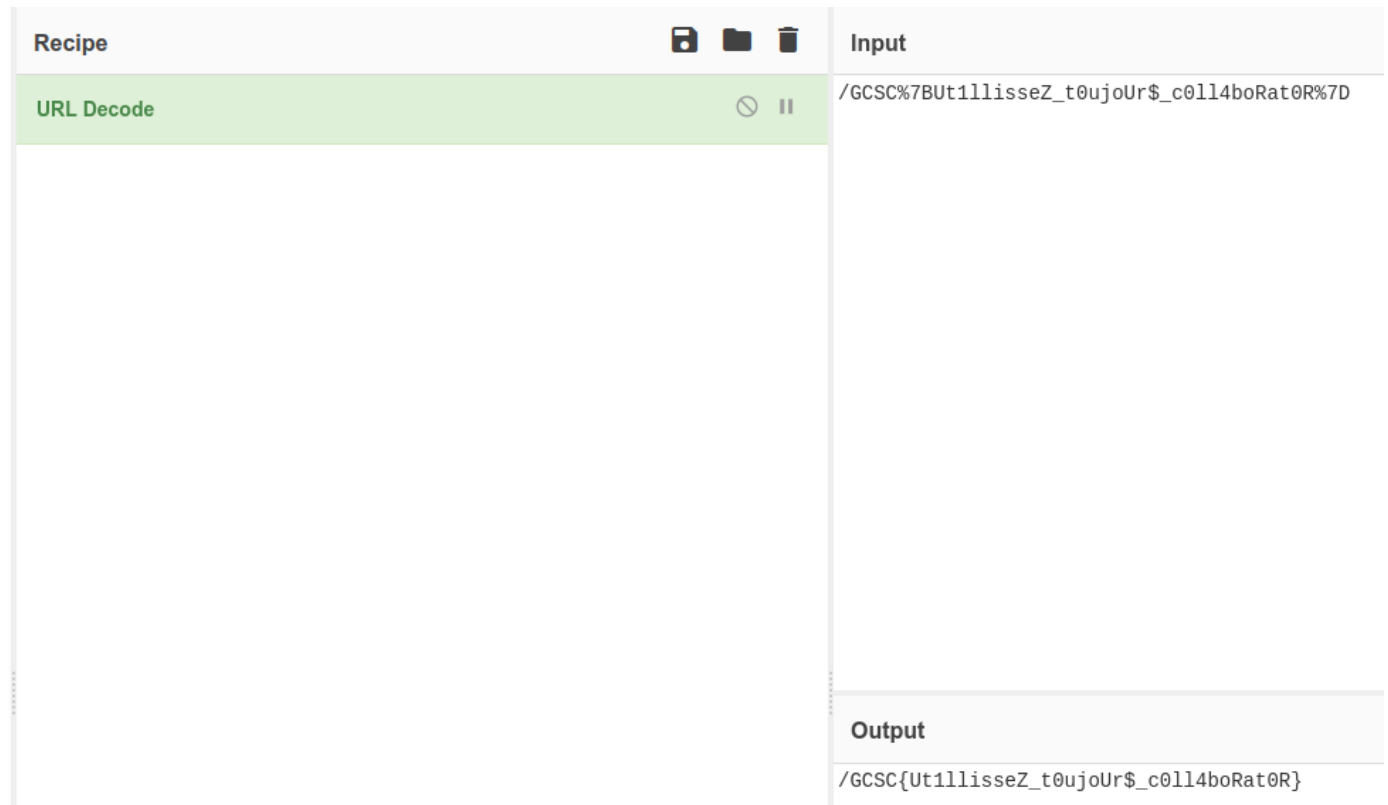
Ce qui était une fois de plus normal. Cependant, en mettant un **password** de plus de 8 caractères (comme demandé) et après plusieurs minutes d'attente, j'ai eu cette page :



Et là, j'étais agréablement surpris 🤩 puisque le flag en face de moi. On voit par miracle `url :`  
`/GCSC%7BUt1llisseZ_t0ujoUr$c0ll4boRat0R%7D` (haha 😁).



Je crois que là, le travail était déjà fait, il suffisait juste d'utiliser [CyberChef](#)



The screenshot shows the CyberChef interface. On the left, under the 'Recipe' tab, the 'URL Decode' recipe is selected and active. The main workspace is empty. On the right, the 'Input' tab shows the string: `/GCSC%7Bt1llisseZ_t0ujoUr$_c0ll4boRat0R%7D`. Below the input, the 'Output' tab shows the decoded result: `/GCSC{Ut1llisseZ_t0ujoUr$_c0ll4boRat0R}`.

Et Boom !!! On a : `GCSC2022{Ut1llisseZ_t0ujoUr$_c0ll4boRat0R}`

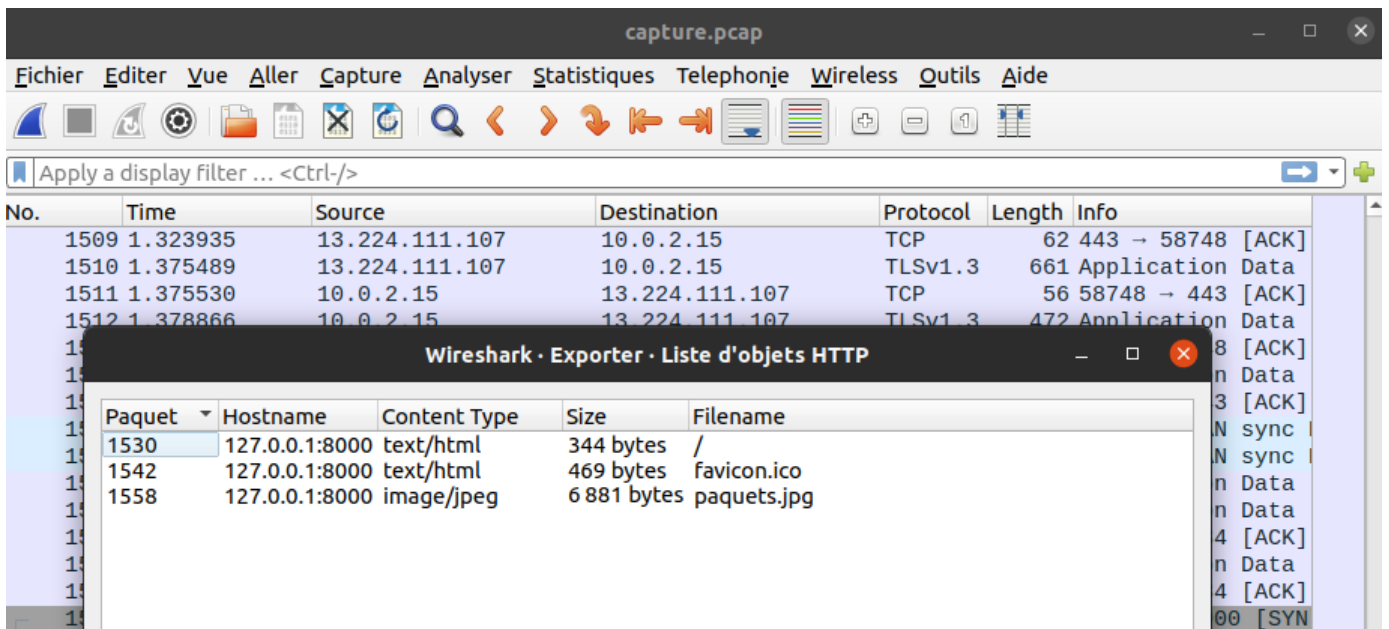
---

## SOMALIE

Énoncé : Il y a un risque d'identification lorsqu'on utilise une carte SIM enregistrée en son nom pour surfer sur Internet. Les membres de la CyberBadCorp en sont conscients. Alors, ils font souvent recours aux cybercafés. Or, l'ANSSI-Guinée a récemment exigé aux cybercafés opérant sur toute l'étendue du territoire Guinéen de mettre en place des mesures garantissant l'authentification, la traçabilité, l'imputabilité/la non-répudiation de l'usage des appareils de leurs parcs informatiques. Plus concrètement, il s'agit d'identifier les utilisateurs, de journaliser les actions et superviser l'ensemble des flux entrants et sortants de chaque poste. En charge de l'analyse des captures réseaux bimensuels de certains cybercafés de la capitale, tu décides de commencer ta journée par celle-ci. Y a t'il quelque chose dans ces paquets qui mettraient en péril la sécurité nationale?

**Solution :** Pour ce chall, la question **(y a t'il quelque chose dans ces paquets qui mettraient en péril la sécurité nationale ?)** m'a toute de suite donné une piste. Je me suis dit que si l'on surfe sur Internet on laisse forcément des traces et ma première réflexion était de voir si je pouvais obtenir quelques pistes. De ce fait, je me suis dit qu'il y a forcément des fichiers cachés quelque part dans **capture.pcap** que j'ai ouvert avec mon **wireshark**. Puis, je suis allé dans **fichier ==> Exporter Objects ==> HTTP** et boom🕶️🕶️ !





J'ai trois fichiers, mais le plus intrigant était le **paquets.jpg**. En ouvrant **paquets.jpg**, j'ai trouvé ceci :

GCSC{ToU7\_3sT\_d4N\$\_l3\$\_p4Qu3t5}

## ALGERIE

**Énoncé** : La CyberBadCorp vient de recruter un stagiaire débutant pour développer son malware. Ce dernier ayant appris la cryptographie sur le tas, il pense bien dissimuler les informations sur la prochaine attaque. Retrouve le nom de l'opération dans le fichier ou lien joint et préviens tes collègues.

**Solution** : Bon en regardant ce texte, je me suis dit qu'il se cachait quelque derrière.

DashDotDashDot DotDotDotDot Dot DotDashDot DotDotDot  
 DashDotDashDot DashDashDash DotDashDotDot DotDashDotDot Dot DashDashDot DotDotDash Dot DotDotDot  
 DashDotDot Dot  
 DotDashDotDot DotDash  
 DashDotDashDot DashDotDashDash DashDotDotDot Dot DotDashDot DashDotDotDot DotDash DashDotDot DashDotDashDot DashDashDash DotDashDot DotDashDashDot DashDashDotDotDashDash  
 DotDashDotDot DotDash DashDot DashDotDashDot Dot DashDashDotDot  
 DotDashDotDot DotDashDashDashDot DashDashDash DotDashDot DotDash Dash DotDot DashDashDash DashDot  
 DotDashDotDotDashDot DotDashDot Dot DashDash DashDashDash DotDashDot DotDotDot Dot DotDashDotDot Dot DotDotDot DotDotDot DotDashDotDotDashDot DashDashDotDotDashDash  
 DotDashDotDot Dot  
 DotDotDot DotDash DashDash Dot DashDotDot DotDot  
 DotDashDashDashDash DotDotDashDashDash DashDotDotDashDot DashDashDashDashDash DotDotDashDashDash DashDotDotDashDot DotDotDashDashDash DashDashDashDashDash DotDotDashDashDash  
 DotDotDashDashDash  
 DotDotDashDashDash DotDotDotDashDash DashDashDashDotDotDot DotDotDotDotDot DashDashDashDashDot  
 DotDashDashDotDashDot DashDashDot DashDotDashDot DotDotDot Dash DotDotDashDot DotDashDotDashDash Dash Dot DotDash DashDash

J'ai donc essayé de le mettre en morse depuis mon **via** avec les commandes (**:%s/Dash/-/g** et **%s/Dot/./g**).

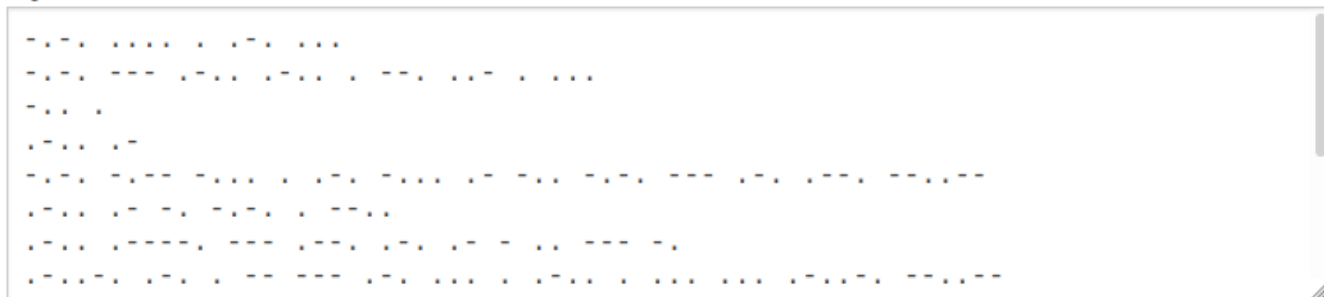


Une fois l'écriture en morse obtenue, il ne restait plus à savoir ce que cela pouvait donner. Pour cela,

j'ai utilisé **Cyberchef** .

### Translate a Message

Input:



Output:

```
CHERSCOLLEGUESDELACYBERBADCORP, LANCEZL ' OPRATION"REMORSELESS", LESAMED12/02  
/202223:59@GCSTF . TEAM
```

Flag : GCSC2022{remorselles}

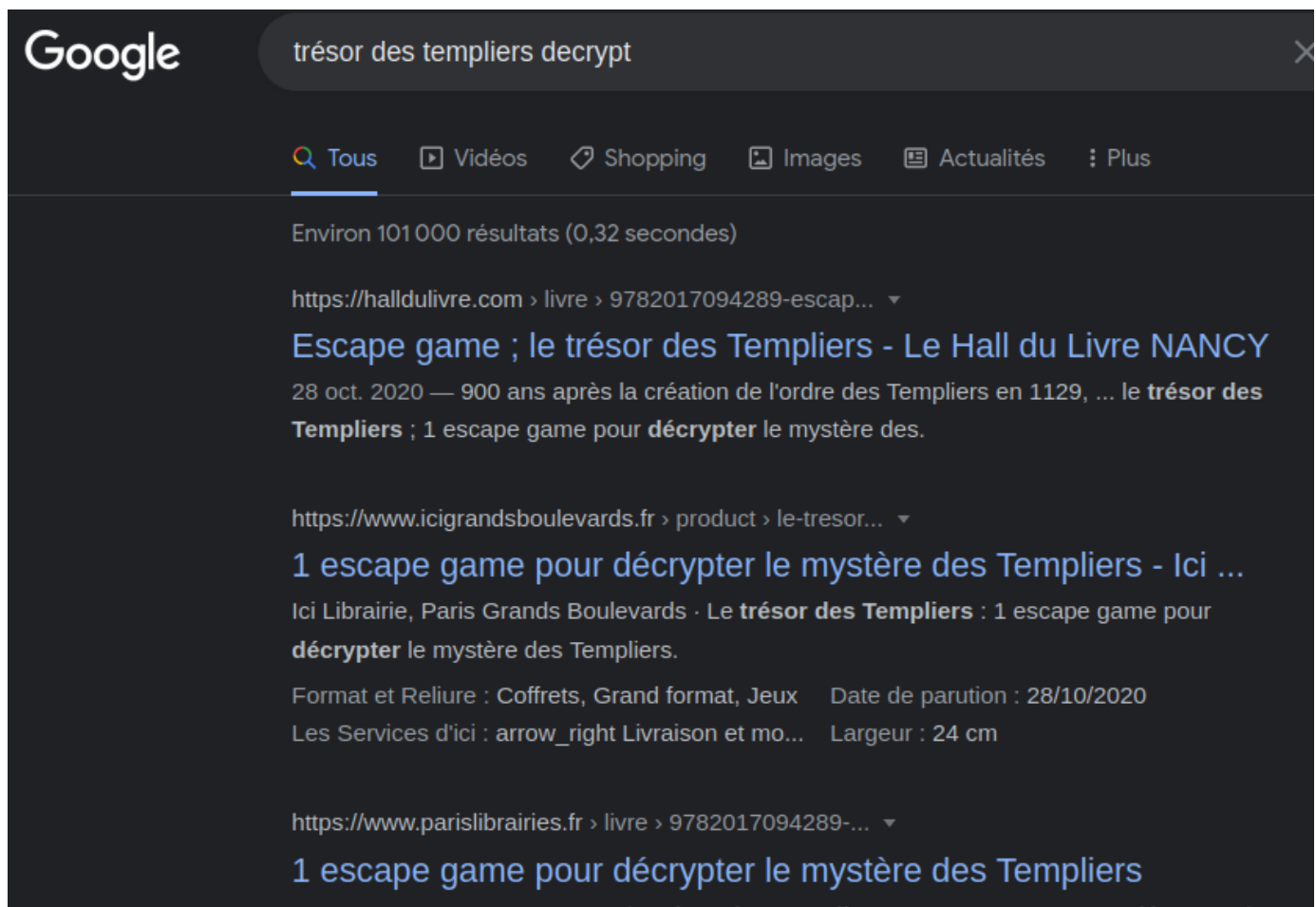
## LIBYE

<https://www.dcode.fr/chiffre-templiers>

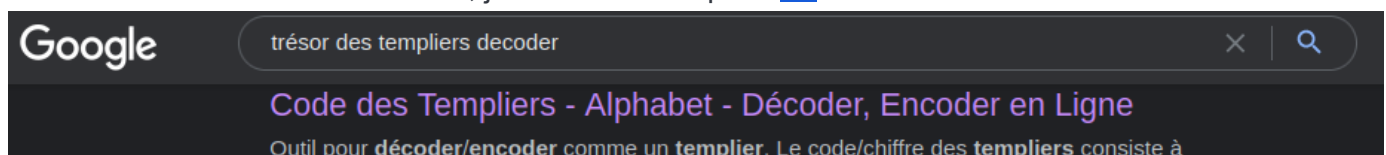
**Énoncé** : Ouh! Ce sont des génies ces petits malins. Que voulait dire ce membre fuité de la CyberBadCorp aux nouvelles recrues ?



**Solution** : Bon c'est vrai qu'avec cette image, j'étais un peu perdu au début car ni **Aperisolve** ni **Exiftool** donnait quelque chose de concret. Mais comme on dit souvent, **les détails comptent** ! En relisant l'énoncé, je me suis aperçu que le **chall** portait le nom (**C'était quoi le trésor des Templiers ?**) et pour avoir quelques idées et pistes, j'ai cherché sur **Google** **Trésor des templiers** malheureusement, je n'ai rien trouvé. Toujours dans ma recherche, j'ai retapé **Trésor des templiers decrypt** et là, je suis tombé sur des sites liés à **l'escape game** (dommage ! 😞 😞 )



C'était un peu la déception jusqu'à ce que je retape à nouveau **Trésor des templiers decoder.** Et boom !! J'étais l'un de ces heureux, j'avais enfin une piste [ici](#).



Il ne restait plus qu'à saisir le mystère comme sur l'image



Flag : `GCSC2022{secret_of_templairs}`

CHAD

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# fcrackzip -u -D -p '/usr/share/wordlists/rockyou.txt' note.zip
```

```
PASSWORD FOUND!!!!: pw = Catsandcows
```

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# unzip note.zip
Archive: note.zip
[note.zip] note.txt password:
extracting: note.txt

(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# ls
cereals.svg  kep.txt  note.txt  note.zip  secrets.kdbx

(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# cat note.txt
GCSC{p4$sw0rD_cr4ck1nG_br34kZ_GPUs}
```

---

## SOUDAN

**Enoncé** : Décidemment, c'est la guerre numérique entre la CyberBadCorp et notre pays. Un nouvel agent ayant pris fonction ce matin au sein de la Police Scientifique Guinéenne se plaint de son antivirus qui n'arrête pas d'alerter toutes les 5s. Il décide de le désactiver pour se concentrer sur son enquête. Cette ouverture a permis à un membre de la CyberBadCorp de s'introduire dans sa machine et dumper les données d'identification (SAM et SYS) qu'il prévoit d'utiliser pour élever ses droits. Ils ont relevé cette chaîne de caractères dans une de leurs attaques postérieures à celle-ci: "Asdfg". Elle pourrait certainement te servir à compléter l'évidence qui te manque.

**Solution** : Pour ce chall, j'ai tout de suite utilisé **samdump2** pour extraire le **hash** dans un fichier en output.

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# samdump2 system sam -o hash.txt
HDS
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# cat hash.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4cc54d1e22e6f25a6d8afb31b38fce8f:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::ked
```

A la suite de ça, j'ai utilisé **hashcat** pour obtenir le mot de passe correspondant.

**Flag** : `GCSC2022{12345Asdfg}`

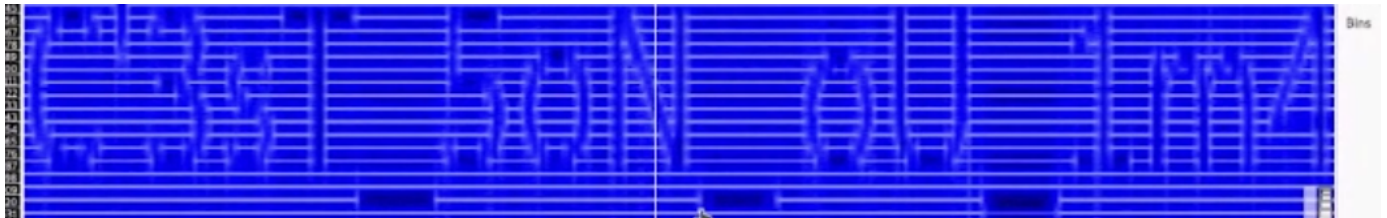
---

## ANGOLA

Les membres de la CyberBadCorp décident de célébrer leur dernier coup qui a permis l'arrêt de nombreux SI de l'administration guinéenne. Sur la mission depuis plusieurs semaines, tu sais qu'ils communiquent par tous les moyens. Alors tu tentes le coup par le coup : tu t'y invites et enregistres

toutes les musiques jouées à cette soirée. Tu as vu combien ils étaient en feu particulièrement sur cette musique. Analyse-la et dis-nous ce que tu trouves.

**Solution** : Bon je n'avais j'amaais fait de **stégano** jusqu'à ce jour et pour résoudre ce mystère, j'ai d'abord et comme toujours utilisé mon ami **Google** pour savoir comment extraire une information dans un audio **mp3**. J'ai tout de suite vu beaucoup d'outil mais j'ai finalement préféré **sonic-visualiser** (je ne sais pas pourquoi moi je voulais juste avoir le **flag** haha 😁😎). En balançant l'audio dans **sonic-visualiser** et en effectuant manips que j'ai vu [ici](#), j'ai réussi à obtenir ça :



**Flag** : GCSC2022{C'3sT\_5oN\_Ou\_1m4g3?}

---

## BRAZIL

Les membres de a CyberBadCorp viennent d'avoir accès a une infrastructure critique de la Guinée. Leurs premières actions a été d'effacer les fichiers log dans le but de se maintenir incognito. Heureusement, l'ANSSI-Guinée avait pris des mesures en amont pour journaliser les actions des éventuels intrus dans ce système en répliquant le fichier de log au fur et à mesure dans l'image du Président. Nous mettons cette jolie photo à ta disposition pour voir ce qui a pu se passer tout au long de de cette cyberattaque attaque.

Ces questions pas-à-pas te permettront de vite les retrouver.

- 1- Quel est le nom du hacker ?
  - 2- Quel est le commentaire laissé par le hacker?
  - 3- Quel est le mot de passe pour extraire le fichier exfiltré par le hacker?
  - 4- Quel est le nom original ainsi que le mot de passe de ce fichier archivé extrait précédemment?
- Format attendu : fichier.txt, password
- 5- Quel est la preuve de l'intrusion (flag)?

**Solution** : Le premier outil que j'ai utilisé pour ce **chall** était **Exiftool** pour voir quelles infos contiennent l'image donnée :



```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# exiftool mamadi-doumbouya.jpg
ExifTool Version Number      : 12.39
File Name                    : mamadi-doumbouya.jpg
Directory                    : .
File Size                    : 79 KiB
File Modification Date/Time   : 2022:02:20 13:14:48+01:00
File Access Date/Time        : 2022:02:24 22:00:38+01:00
File Inode Change Date/Time   : 2022:02:23 00:47:18+01:00
File Permissions              : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : inches
X Resolution                  : 96
Y Resolution                  : 96
Exif Byte Order               : Big-endian (Motorola, MM)
Image Description             : GCSC
Make                         : Iphone 15
Camera Model Name             : Iphone 15
Artist                       : John TRUMP
XD Title                      : GCSC
XP Comment                    : 55 6e 33 5f 31 6d 34 67 65 5f 70 33 75 74 5f 63 34 63 68 33 72 5f 34 75 74 72
33 5f 63 68 30 73 33
XP Author                     : John TRUMP
XP Subject                    : GCSC
Padding                       : (Binary data 2060 bytes, use -b option to extract)
About                         : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Creator                      : John TRUMP
Title                         : GCSC
Description                   : GCSC
Image Width                   : 768
Image Height                  : 694
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling          : YCbCr4:2:0 (2 2)
Image Size                    : 768x694
Megapixels                    : 0.533
```

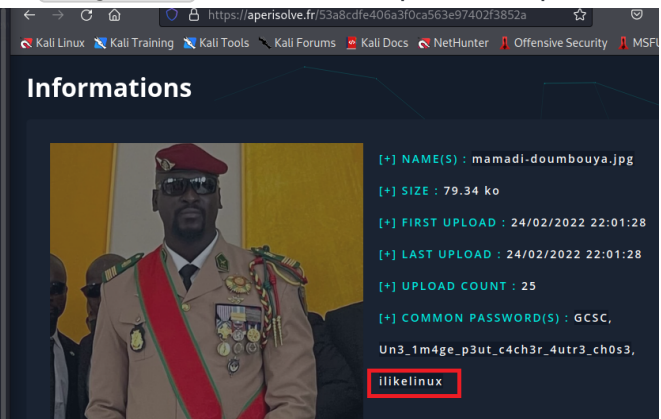
L'utilisation d'**exiftool** m'a déjà permis de répondre aux deux premières questions. Cependant, le commentaire était en hexadécimal, il fallait donc le convertir pour savoir ce qu'il a laissé comme commentaire. Pour ce faire, j'ai procédé comme suit :

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# echo 55 6e 33 5f 31 6d 34 67 65 5f 70 33 75 74 5f 63 34 63 68 33 72 5f 34 75 74 72 33 5f 63 68 30 73 33 | xxd -r -p
Un3_1m4ge_p3ut_c4ch3r_4utr3_ch0s3
```

**Note** : j'ai également utilisé **Aperisolve** pour obtenir plus de détails possible, il m'a aussi permis de voir le commentaire à droite de l'image. Toutefois, pour extraire le fichier archivé, il fallait utiliser la mot de passe **ilikelinux**. Pour cela, j'ai utilisé le fameux outil **steghide** avec le mot de passe en question.

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# steghide extract -sf mamadi-doumbouya.jpg
Entrez la passphrase:
*écriture des données extraites dans "secret.zip".

(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
```



**Informations**

- [+] NAME(S) : mamadi-doumbouya.jpg
- [+] SIZE : 79.34 ko
- [+] FIRST UPLOAD : 24/02/2022 22:01:28
- [+] LAST UPLOAD : 24/02/2022 22:01:28
- [+] UPLOAD COUNT : 25
- [+] COMMON PASSWORD(S) : GCSC, Un3\_1m4ge\_p3ut\_c4ch3r\_4utr3\_ch0s3, **ilikelinux**

Une fois le fichier **zip** extrait, j'ai voulu le dézipper malheureusement, il me fallait encore de nouveau mot de passe.

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# unzip secret.zip
Archive: secret.zip
[secret.zip] flag.txt password:
skipping: flag.txt                incorrect password
```

Comme je ne savais plus quoi faire, j'ai utilisé du **bruteforce** avec **fcrackzip** (un outil spécifique pour bruteforcer les fichiers **zip**).

```
(ctf@kali)-[~/Téléchargements/GUINEAN]
$ fcrackzip -u -D -p '/usr/share/wordlists/rockyou.txt' secret.zip

PASSWORD FOUND!!!!: pw = love2linux
```

A la suite de mon bruteforce, j'ai obtenu le mot de passe **love2linux** qui m'a finalement permis de dézipper **secret.zip** et obtenir **flag.txt**.

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# unzip secret.zip
Archive: secret.zip
[secret.zip] flag.txt password:
extracting: flag.txt
```

Dans **flag.txt**, le text était en **base64**, il ne restait plus qu'à décoder le message.

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# cat flag.txt
Bravo, voici le flag : TDRfc3QzZzRuMGdyNHBoMTNfcDNybTN0X2QzX2M0Y2gzUl9kM3NfbTNzczRnZXMh
```

Et boooooom !!! On a ça :

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# echo 'TDRfc3QzZzRuMGdyNHBoMTNfcDNybTN0X2QzX2M0Y2gzUl9kM3NfbTNzczRnZXMh' | base64 --decode
L4_st3g4n0gr4ph13_p3rm3t_d3_c4ch3R_d3s_m3ss4ges!
```

```
GCSC2022{John TRUMP_Un3_1m4ge_p3ut_c4ch3r_4utr3_ch0s3!_ilikelinux_secret.zip,
love2linux_L4_st3g4n0gr4ph13_p3rm3t_d3_c4ch3R_d3s_m3ss4ges!}
```

## NIGERIA

**Énoncé** : Les régions minières du pays attirent de plus en plus la CyberBadCorp. Trois de leurs membres décident de s'installer dans la région de Kamsar afin de dépouiller le plus d'entreprises d'exploitation. En cours de chemin, ils s'arrêtent un moment dans un village pour manger et se reposer avant de reprendre la route. Ils en profitent aussi pour recharger leurs appareils dans un télécentre. Le gérant du télécentre, agent secret, dump le contenu de leurs téléphones qu'il te transmet à des fins d'analyse pour des questions de sécurité nationale. Lors de tes analyses, tu remarques qu'à un moment donné, tous les trois ont utilisé le même téléphone pour se connecter à une application de messagerie instantanée étrange. Tu as vite retrouvé la base de données reliée à cette application. Maintenant, trouve leurs mots de passe.

Flag: GCSC2022{Password1\_Password2\_Password3}

**Solution** : Pour ce chall, j'ai utilisé **sqlite3** pour extraire des infos dans la base de données :

```
(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# file BD\application\mobile.db
BD application mobile.db: SQLite 3.x database, last written using SQLite version 3028000, file counter 6, database pages 3, cookie 0x1, schema 4, largest root page 3, UTF-8, version-valid-for 6

(root@kali)-[/home/ctf/Téléchargements/GUINEAN]
# sqlite3 BD\application\mobile.db
SQLite version 3.37.2 2022-01-06 13:25:41
Enter ".help" for usage hints.
sqlite> .tables
users
sqlite> select * from tables;
Error: in prepare, no such table: tables (1)
sqlite> select * from users;
John|0DI3MDQMGWzTKQMTExZDExZmFmMzg1NTI1Nzc4ZTc=
Marie|NDFkNTMAYTcxYjJhYTUwMDRkNTMOMjM3NzEwNDFjOWMk
Luc|NGVmy2RhYzgiYzZjNDk0YjNjZWY4NzgY2M2MzK4MDUK
sqlite>
```

Pour John on a :



Recipe	Input
<div>From Base64</div> <div>Alphabet A-Za-z0-9+/=</div> <div><input checked="" type="checkbox"/> Remove non-alphabet chars</div>	ODI3MDQ0MGMwZTk0MTExZDExZmFmMzg1MTI1Nzc4ZTc=
	<div>Output</div> <div>8270440c0e94111d11faf385125778e7</div>

8270440c0e94111d11faf385125778e7 : p1ntap

Pour Marie on a :

Recipe	Input
<div>From Base64</div> <div>Alphabet A-Za-z0-9+/=</div> <div><input checked="" type="checkbox"/> Remove non-alphabet chars</div>	NDFkNTM4YTcxYjJhYTlwMDRkNTM0MjM3NzEwNDFjOWMK
	<div>Output</div> <div>41d538a71b2aa6004d53423771041c9c</div>

41d538a71b2aa6004d53423771041c9c fd1972

Pour Luc on a :

ipe

Base64

habet  
Za-z0-9+/=

Remove non-alphabet chars

Input

NGVmY2RhYzg1YzZjNDk0YjNjZWY4Nzg1Y2M2Mzk4MDUK

Output

4efcdac85c6c494b3cef8781cc639805

4efcdac85c6c494b3cef8781cc639805 : AdDiCtIoN

Flag : GCSC2022{p1ntap\_fd1972\_AdDiCtIoN}

## MADAGASCAR

**Énoncé** : N'oublie pas d'accéder au serveur Discord!

**Solution** : C'était juste un cadeau donné. Il fallait juste mettre le lien du discord de GCSTF