🚀 Writeup - Challenge "USB 51" (404CTF) - Étudiant 2600 - Morad Halmi 🌐

📝 Introduction

Le fichier **capture.pcapng** contient une capture réseau où un document confidentiel a été exfiltré de l'ESA (Agence Spatiale Européenne). Objectif : identifier le document exfiltré et récupérer les informations cachées.

🕵️ Étape 1 : Analyse du fichier PCAP

Ouverture et analyse initiale

```
wireshark capture.pcapng
```

- Filtrage des protocoles courants pour détecter une exfiltration :

```
http || ftp || ssh || smb
```

- Aucune de ces méthodes de transfert classique n'a été détectée.

Identification des données suspectes

En parcourant les paquets, un flux contenant une séquence binaire a été identifié. Cette séquence a immédiatement attiré l'attention.

📜 Étape 2 : Extraction du document exfiltré

1. Export des objets HTTP dans Wireshark :

```
File > Export Objects > HTTP
```

2. Sauvegarde du fichier nommé **exfiltrated_document.pdf**.

Contenu du document PDF

- Rapport confidentiel de l'ESA sur l'exoplanète **Kepler-442b-X**.
- Le document contient une séquence binaire cachée :

```
00110100 00110000 00110100 01000011 01010100 01000110 01111011 01010111
00110011 01011111 01100011 00110000 01001101 01000101 01011111 01001001
01001110 01011111 01110000 00110011 01100001 01000011 00110011 01111101
```

🗝️ Étape 3 : Décodage de la séquence binaire

- La séquence binaire a été convertie en texte avec un script Python simple :

```
binary_data = "00110100 00110000 00110100 01000011 01010100 01000110 01111011 010101
decoded = ''.join([chr(int(b, 2)) for b in binary_data.split()])
print(decoded)
```

- Résultat du décodage :

```
404CTF{W3_c0ME_IN_p3aC3}
```

✅ Étape 4 : Conclusion

- Document exfiltré identifié : **exfiltrated_document.pdf**.
- Message caché extrait et décodé.
- Flag final récupéré.

🚩 Flag :

```
404CTF{W3_c0ME_IN_p3aC3}
```

🚀 Commandes clés utilisées :

- `wireshark capture.pcapng` : Analyse du PCAP.
- `File > Export Objects > HTTP` : Extraction du document exfiltré.
- `python` : Décodage de la séquence binaire.

📝 Remarques :

- Toujours vérifier les données cachées dans les fichiers.
- Le binaire est souvent utilisé pour cacher des informations sensibles.