## Solution à : USB51

Il y a une zone 51 dans le désert d'octets banals véhiculés par les trames de trafic réseau du source : capture.pcapng. Cette zone se trouve être un fichier pdf avec du texte à extraire ; dans lequel se trouve elle-même une phrase binaire.

```
(kali@kali)-[/mnt/Share/404CTF2025/Analyse Forensique/USB 51]
$ hexdump -C capture.pcapng | grep -a -b "%PDF"
22280:000011b0 00 00 00 00 00 00 00 00 00 00 00 25 50 44 46 |.............%PDF|
   -(kali®kali)-[/mnt/Share/404CTF2025/Analyse Forensique/USB 51]
$ grep -aob "%PDF" capture.pcapng
4540:%PDF
(kali@ kali)-[/mnt/Share/404CTF2025/Analyse Forensique/USB 51]
$ dd if=capture.pcapng of=extracted.pdf bs=1 skip=4540
61736+0 records in
61736+0 records out
61736 bytes (62 kB, 60 KiB) copied, 25.2925 s, 2.4 kB/s
   -(kali@kali)-[/mnt/Share/404CTF2025/Analyse Forensique/USB 51]
_$`ls -l
total 292
drwxrwx — 1 root vboxsf 4096 Jun 7 17:51 assets
-rwxrwx — 1 root vboxsf 40687 May 12 07:01 'Capture d'écran 2025-05-12 130057.png'
-rwxrwx- 1 root vboxsf 60596 May 12 07:04 'Capture d'écran 2025-05-12 130441.png'
-rwxrwx — 1 root vboxsf 4439 May 12 07:05 'Capture d'écran 2025-05-12 130528.png' aléatoire a
-rwxrwx- 1 root vboxsf 66276 May 10 17:14 capture.pcapng
-rwxrwx— 1 root vboxsf 47777 May 12 06:56 exfiltrated_document.pdf
-rwxrwx- 1 root vboxsf 61736 Jun 7 18:07 extracted.pdf
   (kali@kali)-[/mnt/Share/404CTF2025/Analyse Forensique/USB 51]
_$ file extracted.pdf
xdg-open extracted.pdf # ou evince extracted.pdf
extracted.pdf: PDF document, version 1.7, 4 page(s)
   (kali@kali)-[/mnt/Share/404CTF2025/Analyse Forensique/USB 51]
_$ file extracted.pdf
xdg-open extracted.pdf # ou evince extracted.pdf
extracted.pdf: PDF document, version 1.7, 4 page(s)
   (kali@kali)-[/mnt/Share/404CTF2025/Analyse Forensique/USB 51]
$ foremost -i capture.pcapng -o sortie_docs
Processing: capture.pcapng
                            1. Synthèse de la découverte
                            L'analyse des dernières données spectrométriques issues du télescope spatial Ariel et du radiotélescope
                            LOFAR révèle des anomalies atmosphériques sur Kepler-442b-X (désignation temporaire). Contrairement
                            aux prévisions initiales, cette exoplanète présente des niveaux significatifs d'oxygène libre (O2) et de
                            méthane (CH<sub>4</sub>) en cohabitation stable, ce qui pourrait être un indicateur indirect d'une activité biologique.
                            2. Présence d'une structure artificielle ?
                            Un signal radiofréquence faible, mais répétitif, a été capté par le radiotélescope de Nançay et confirmé par
                            le réseau LOFAR à une fréquence de 1420.40575 MHz (ligne de l'hydrogène). Une analyse approfondie
                            indique un motif non aléatoire avec une séquence récurrente tous les 6,27 heures.
                            Données brutes :
                                  00110100 00110000 00110100 01000011 01010100 01000110 01111011 01010111
                                  L'analyse du signal écarte l'hypothèse du hasard, surtout au vu de son message une fois décodé.
                            3. Menace potentielle?
                            Le spectre d'absorption planétaire a également révélé des variations soudaines qui suggèrent une émission
                            thermique intense, localisée dans une région précise de la planète (coordonnées approximatives : +12.45,
```