

# LE DÉCODEUR

## Rapport d'Analyse Forensique d'Images

### Informations Générales

Image analysée: test\_steno.png

Chemin: E:\ENSET\Digital\_Skills\_Py\TheDecoder\test\_steno.png

Date d'analyse: 2026-01-03T19:16:09.422900

### Résultats d'Analyse

Méthode	Résultat	Détails
OCR (Tesseract)	■ NON	-
OCR (EasyOCR)	■ NON	-
LSB Stéganographie	✓ OUI	Message cache : TEST FORENSIC
Métadonnées EXIF	■ NON	0 éléments suspects
Chaînes ASCII	■ NON	0 chaînes trouvées
Signatures binaires	✓ OUI	10 signatures
Anomalies bit-planes	■ NON	Entropie: 0.190
Anomalies histogramme	■ NON	-

### Conclusion

Niveau de suspicion: **LOW**

Méthodes avec résultats: LSB, SIGNATURES

Nombre total de découvertes: 2

Extraction directe: Réussie

# Analyse Intelligente (LLM + NLP)

Métrique	Valeur
Score de suspicion IA	20/100
Niveau de danger	LOW
Nature du contenu	benign
Modèle LLM	meta-llama/llama-3.1-405b-instruct:free
Tokens utilisés	900

## Résumé de l'analyse :

Le texte extrait par stéganalyse contient un message caché qui semble être un test de capacités forensiques. L'analyse révèle que le contenu est probablement anodin, mais certaines caractéristiques techniques pourraient indiquer une intention plus complexe.

## Recommandations :

- 1. Effectuer une analyse plus approfondie des signatures binaires pour déterminer leur origine et leur objectif.
- 2. Rechercher d'autres indices ou messages cachés dans le fichier ou les communications associées.