CTF WRITE-UP PORTFOLIO (FULL COMMAND VERSION)

Author: IllumeMindID
Focus: Digital Forensics, Steganography, Encoding

This document contains complete CTF write-ups with full command-line evidence, following CTFtime-style forensic documentation.

Challenge 1: Riddle Registry

Category: PDF Forensics
Description: Hidden flag inside PDF metadata.
Commands:

```
sudo apt install poppler-utils
pdfinfo confidential.pdf
echo "cGljb0NURntwdXp6bDNkX20zdGFkYXRhX2YwdW5kIV80MjQ0MGM3ZH0=" | base64 --decode
```

Flag: picoCTF{puzzl3d_m3tadata_f0und!_42440c7d}

Challenge 2: Hidden in Plain Sight

Category: Steganography
Description: Image hides steghide payload.
Commands:

```
sudo apt install libimage-exiftool-perl steghide
exiftool img.jpg
echo "c3RlZ2hpZGU6Y0VGNmVuZHZjbVE9" | base64 --decode
echo "cEF6endvcmQ=" | base64 --decode
steghide extract -sf img.jpg
```

Flag: picoCTF{h1dd3n_1n_1m4g3_656e4d79}

Challenge 3: Flag in Flame

Category: Forensics
Description: Base64 log reveals image and hex flag.
Commands:

```
base64 --decode logs.txt > output.png
file output.png
echo "7069636F4354467B666F72656E736963735F616E616C797369735F69735F616D617A696E675F37383265353563
```

Flag: picoCTF{forensics_analysis_is_amazing_782e55c9}