CTF WRITE-UP PORTFOLIO

Author: IllumeMindID
Focus Area: Digital Forensics & Steganography
Style: CTFtime (English)

This portfolio contains detailed Capture The Flag (CTF) write-ups focusing on forensic analysis, metadata inspection, encoding detection, and steganographic extraction.

Challenge 1: Riddle Registry

Category: PDF Forensics
Description: A PDF document contains a hidden flag within its metadata.
Solution:
The PDF metadata was inspected using pdfinfo. A Base64 encoded string was found in the Author field. Decoding the string revealed the flag.
Flag: picoCTF{puzzl3d_m3tadata_f0und!_42440c7d}

Challenge 2: Hidden in Plain Sight

Category: Steganography
Description: A JPG image hides a secret payload protected by layered encoding.
Solution:
Image metadata was inspected using exiftool. A Base64 encoded comment revealed a steghide hint and password. The hidden file was extracted using steghide, revealing the flag.
Flag: picoCTF{h1dd3n_1n_1m4g3_656e4d79}

Challenge 3: Flag in Flame

Category: Forensics
Description: A suspicious log file contains encoded data hiding the true payload.
Solution:
The log file was identified as Base64 encoded data. Decoding the file produced a PNG image. Within the image, a hexadecimal string was found and decoded to reveal the flag.
Flag: picoCTF{forensics_analysis_is_amazing_782e55c9}

Conclusion:
These challenges highlight common forensic techniques used in CTF competitions, including metadata analysis, encoding recognition, and steganography.