Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

hideme - PicoCTF

| **Informações do documento** | |
| --- | --- |
| **Referência** | Renan Schiavotello |
| **N° Revisão** | 1 |
| **Data de publicação** | 20/10/2025 |
| **Link** | [Link para acessar o CTF](https://play.picoctf.org/practice/challenge/350?page=1&search=hideme&solved=0) |

| **Redação** | Renan Schiavotello | Estudante |
| --- | --- | --- |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

| **Histórico de revisões** | | |
| --- | --- | --- |
| **N°** | **Entregas** | **Descrição** |
| **0** | DD/MM/AAAA | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

| **Informações do CTF** | |
| --- | --- |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | steganography |
| **Plataforma** | PicoCTF |
| **Área** | Red |

**Sumário**

[Contextualização](#_mecptipwlz0) 2

[Desenvolvimento 3](#_2xvtpvhpbim5)

flag? [3](#_q2hj9skrrm4j)

[Conclusão](#_b2sbrgcpd986) 5

[Referências](#_kzmiwsvo7889) 5

**Contextualização**

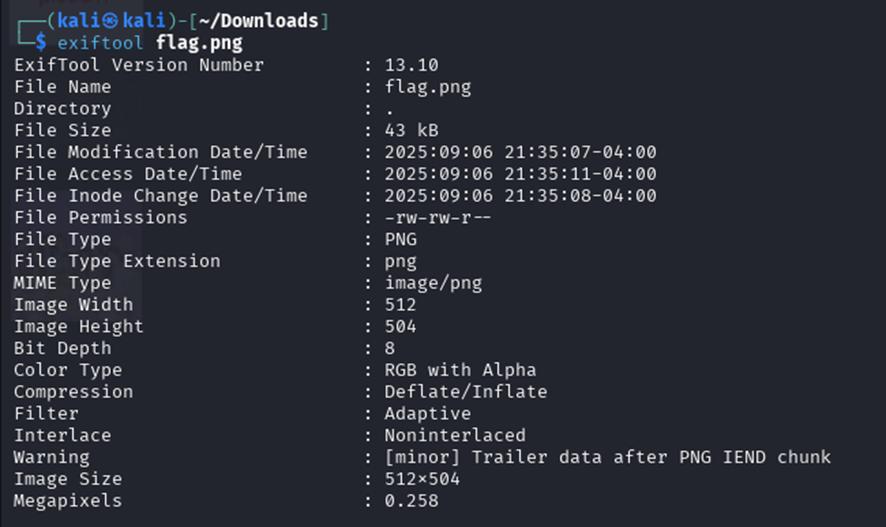
**Esse ctf envolve steganography (esteganografia), ou seja, esconder dados em imagem.**

**Desenvolvimento**

Começamos com uma imagem baixada, a qual contém uma flag a ser descoberta.

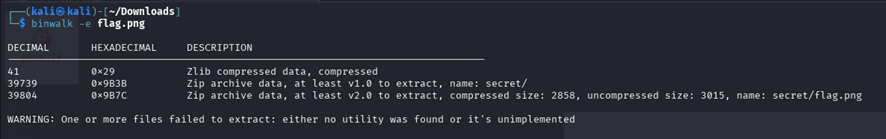
1. **Inspeção inicial (metadados)**

* Comando: exiftool imagem.png
* Objetivo: checar campos úteis e detectar anexos fora do padrão.
* Resultado: nada realmente útil em metadados. A observação de *“Trailer data after PNG IEND chunk”* apenas confirma que há conteúdo anexado ao final do arquivo — algo já esperado em esteganografia.

****

**2. Extração de artefatos embutidos**

* Comando: binwalk -e imagem.png
* Objetivo: varrer o binário e extrair automaticamente qualquer bloco reconhecível.
* Resultado: o binwalk criou um diretório de extração com arquivos adicionais encontrados.



**3. Localização da flag**

* Acessei a pasta gerada pelo binwalk e percorri a estrutura;
* Dentro do diretório secret/ havia uma imagem flag.png contendo a flag do desafio.

**Conclusão**

**É um CTF direto, mas exige noções básicas de esteganografia e familiaridade com ferramentas de análise de arquivos. O fluxo “verificar metadados → procurar dados anexados → extrair e inspecionar a árvore gerada” foi suficiente para recuperar a flag.**

**Referências**

* **Guia introdutório sobre encontrar dados ocultos em imagens (InfoSec Write-ups).**
* **Documentação/ajuda de Exiftool e binwalk.**
* **Plataforma: Pico CTF.**