Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

hideme – PicoCTF

| **Informações do documento** | |
| --- | --- |
| **Referência** | hideme – PicoCTF |
| **N° Revisão** | 0 |
| **Data de publicação** | 25/04/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/350?category=4&difficulty=2&page=1 |

| **Redação** | Matheus da Cunha Castilho | Estudante |
| --- | --- | --- |
| **Revisão** | Sérgio Guidi Trovo | Orientador |
| **Aprovação** | Sérgio Guidi Trovo | Diretor |

| **Histórico de revisões** | | |
| --- | --- | --- |
| **N°** | **Entregas** | **Descrição** |
| **0** | 25/04/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

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

**Sumário**

[Contextualização](#_gjdgxs) [3](#_1t3h5sf)

[Desenvolvimento 3](#_30j0zll)

Busca da flag 3

[Conclusão 3](#_tyjcwt)

[Referências 3](#_3dy6vkm)

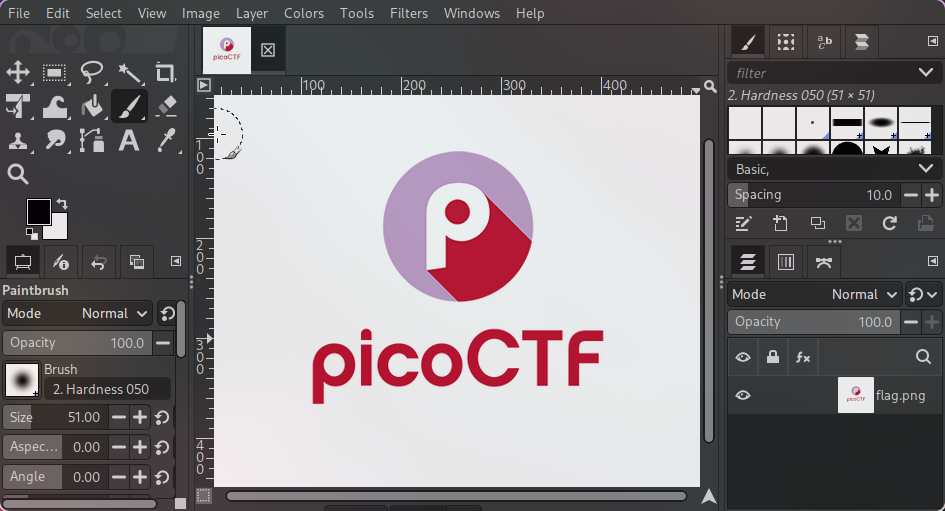
**Contextualização**

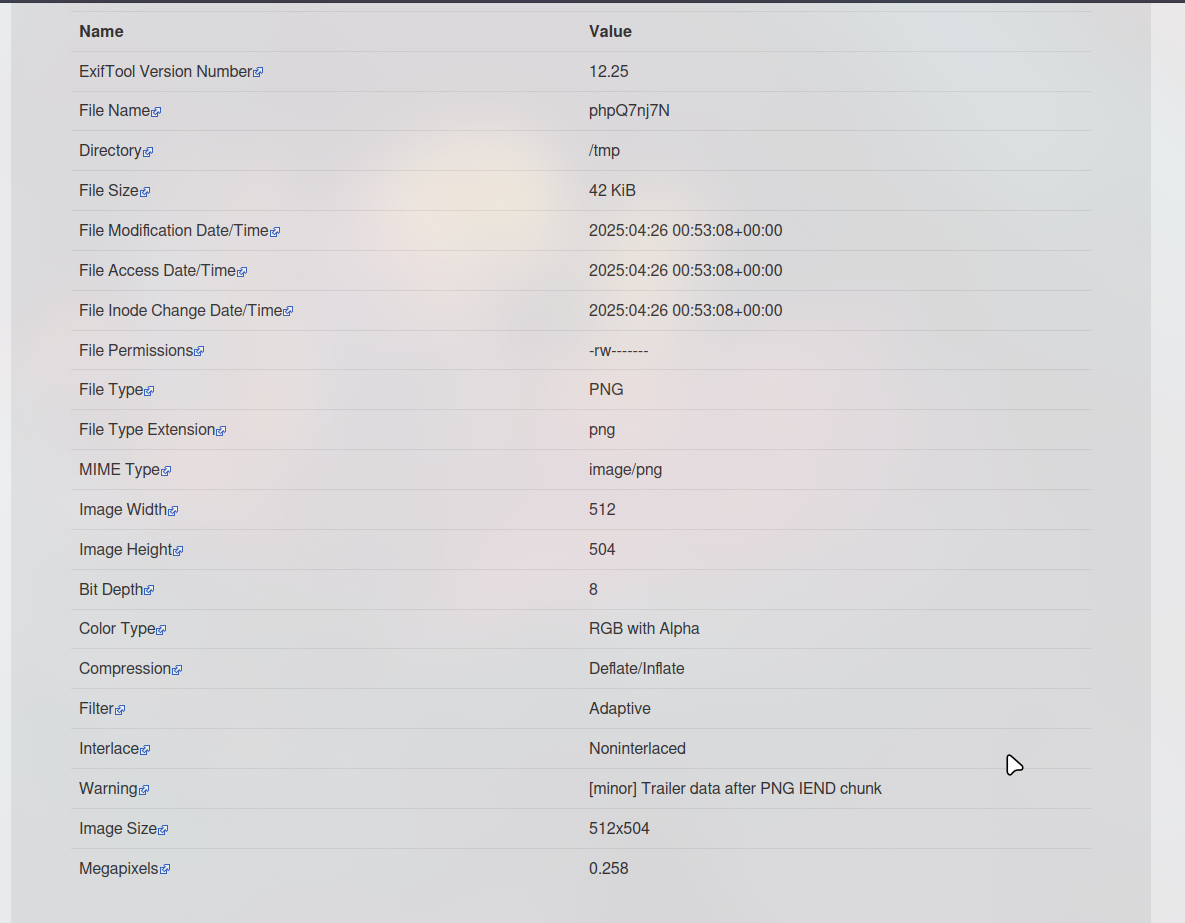
O desafio hideme do PicoCTF envolve esteganografia, ou seja, esconder dados dentro de arquivos. O objetivo aqui era encontrar uma flag escondida dentro de uma imagem, o que exige o uso de ferramentas específicas para análise e extração de dados ocultos. É um bom exemplo de como arquivos simples podem esconder informações importantes.

**Desenvolvimento**

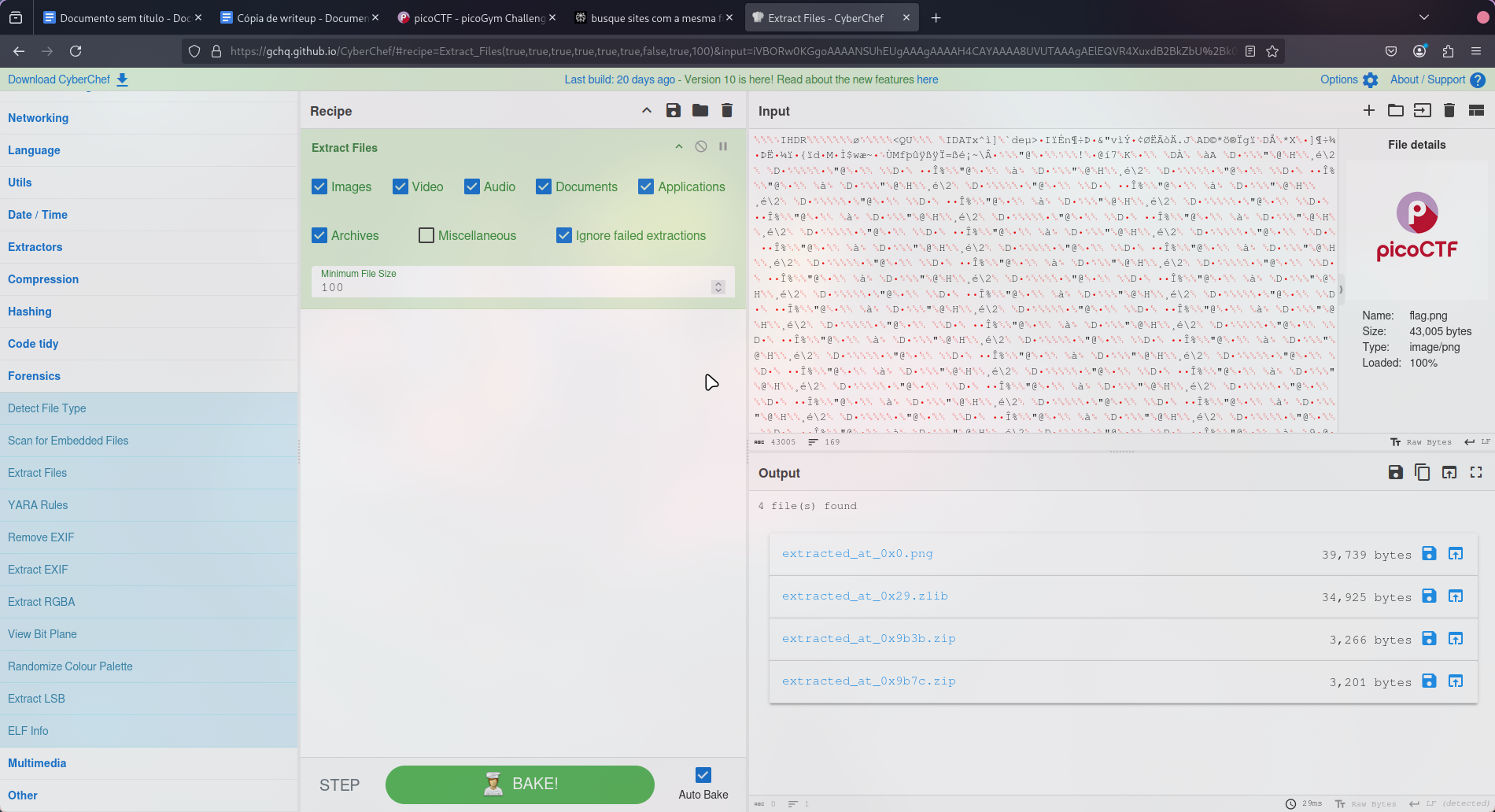
**Busca da flag**

Ao baixar o arquivo, obtemos essa imagem.

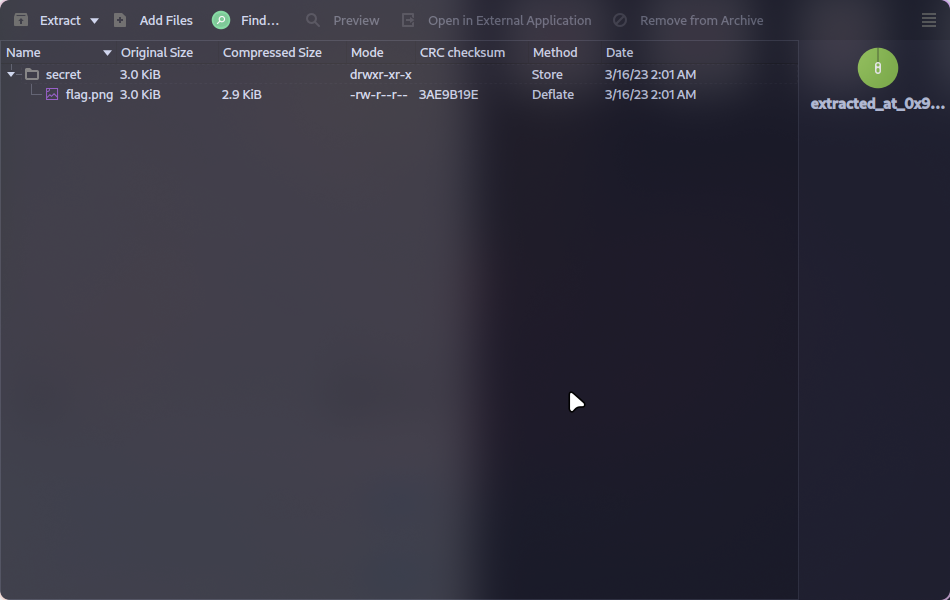


Ao analisar com o exiftools, não conseguimos encontrar nenhuma informação útil.  


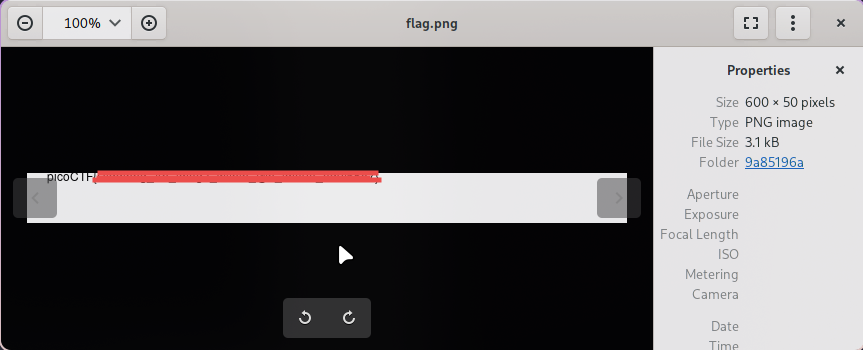
Agora, ao colocar no CyberChef, utilizando a opção de “Extract Files”, da qual podemos extrair possíveis arquivos escondidos na imagem, obtivemos quatro arquivos. Dois deles, são responsáveis pela imagem que está sendo mostrada, já os outros dois, para outra imagem, dentro desta.



Ao baixar o zip, encontrei uma pasta com uma outra imagem.



Ao abrir, obtemos a flag



**Conclusão**

Esse CTF pode ser considerado uma boa prática para iniciantes e intermediários em esteganografia. Apesar de simples, mostrou como ferramentas como o CyberChef podem revelar arquivos escondidos dentro de imagens e é um ótimo exercício para quem está começando na área de segurança e quer entender como investigar arquivos de forma mais técnica.

**Referências**

<https://gchq.github.io/CyberChef>

<https://exif.tools/>