Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

DISKO 1 – PicoCTF

| **Informações do documento** | |
| --- | --- |
| **Referência** | DISKO 1 – PicoCTF |
| **N° Revisão** | 0 |
| **Data de publicação** | 17/05/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/505 |

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

| **Histórico de revisões** | | |
| --- | --- | --- |
| **N°** | **Entregas** | **Descrição** |
| **0** | 17/05/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

| **Informações do CTF** | |
| --- | --- |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Linux, Forense |
| **Plataforma** | PicoCTF |
| **Área** | Red |

**Sumário**

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

[Desenvolvimento 3](#_30j0zll)

Descompactando o arquivo [3](#_2et92p0)

Buscando a flag 3

[Conclusão 3](#_tyjcwt)

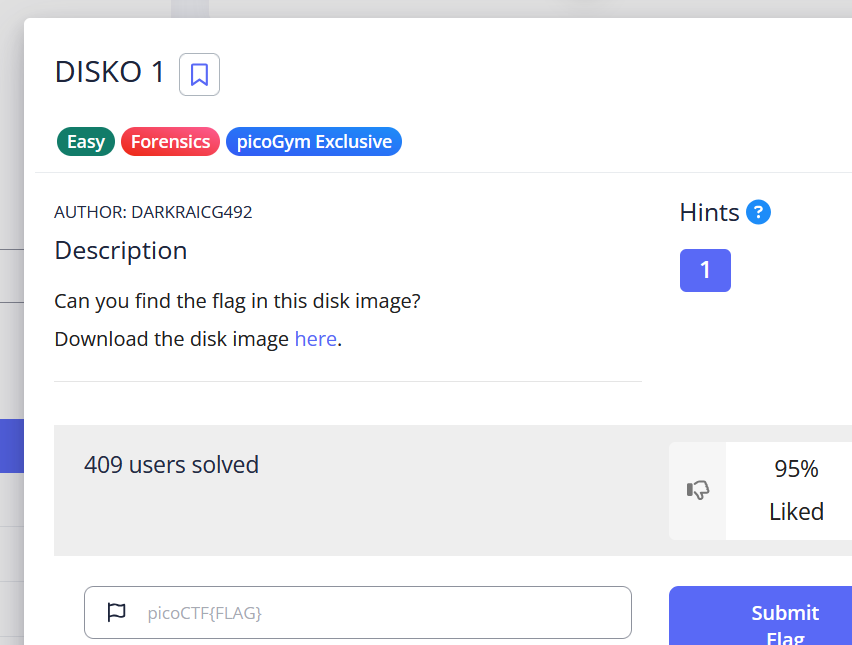
[Referências 3](#_3dy6vkm)

**Contextualização**

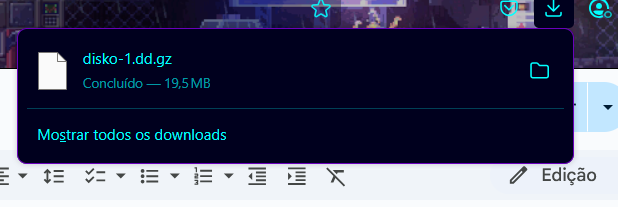
Neste CTF, o foco era aprender um pouco mais sobre extensões de arquivos Linux e como fazer uma análise simples de forense digital. O objetivo era pegar um arquivo de disco compactado, analisar e achar a flag escondida nele, usando ferramentas básicas.

**Desenvolvimento**

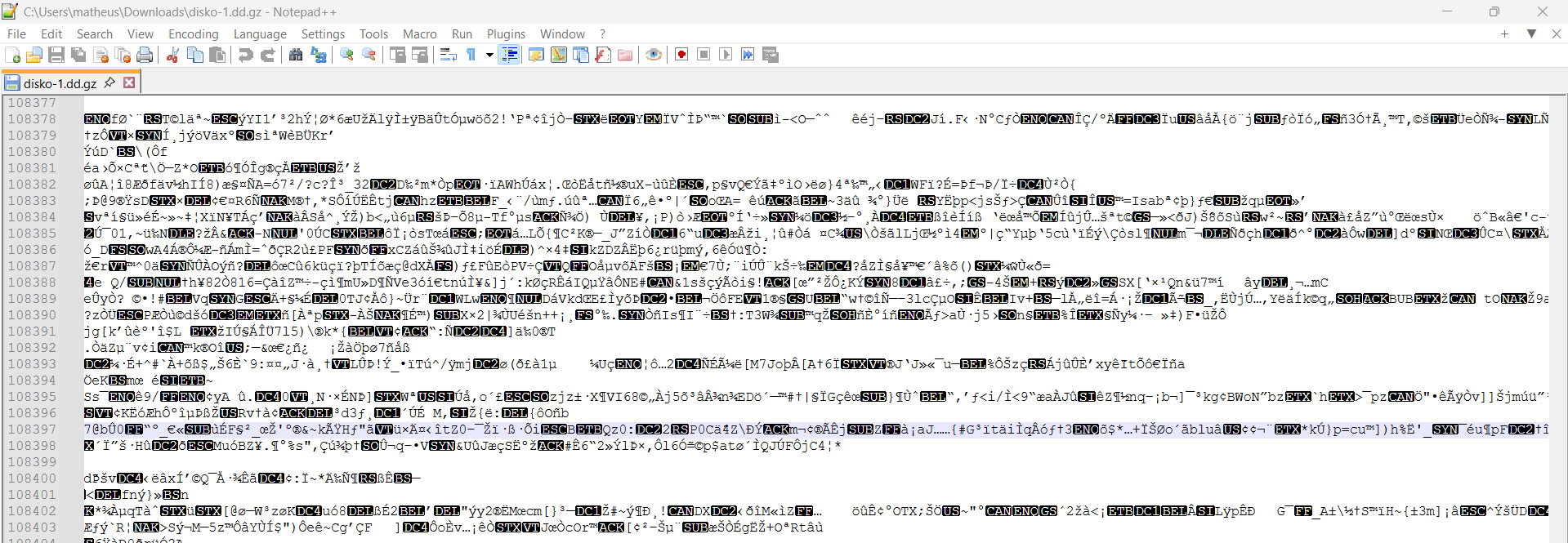
**Descompactando o arquivo**



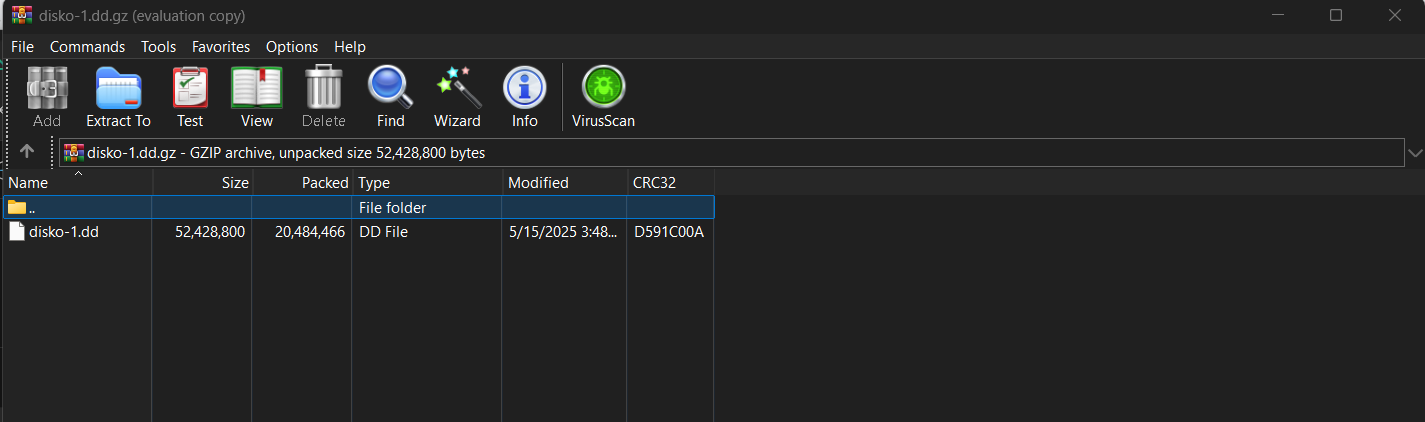
Ao iniciar o CTF, obtemos um arquivo .[dd.gz](http://dd.gz).



Neste arquivo, encontrei alguns textos não legíveis, e ao buscar por algo referente a flag, como “PicoCTF”, não encontrei nada de relevante.

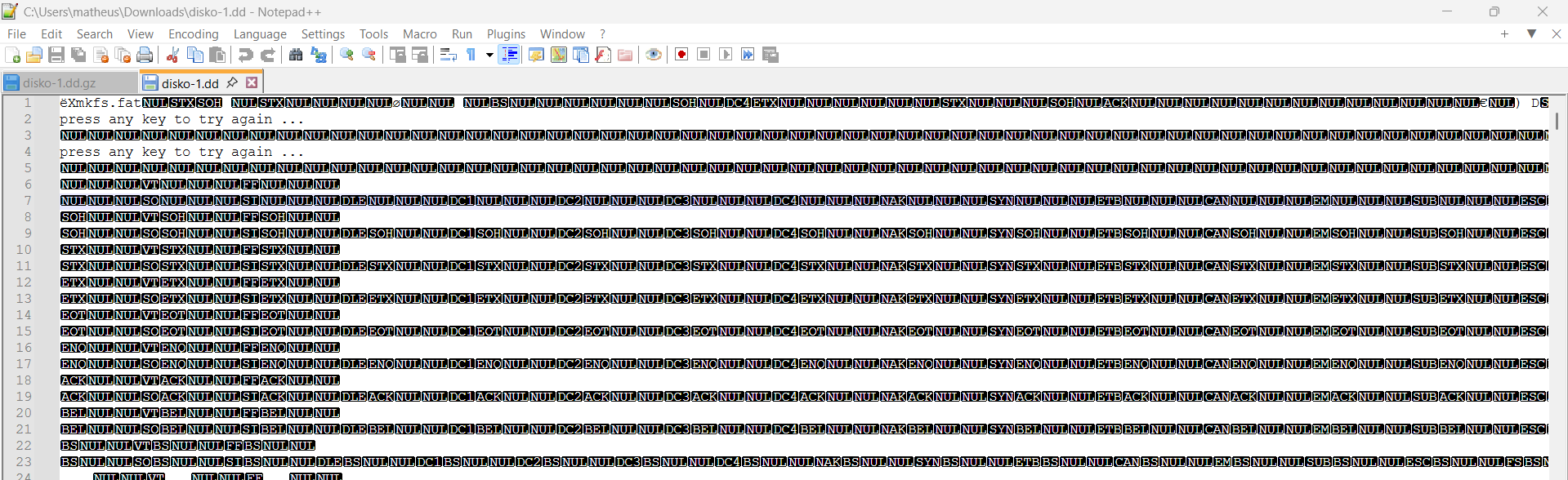


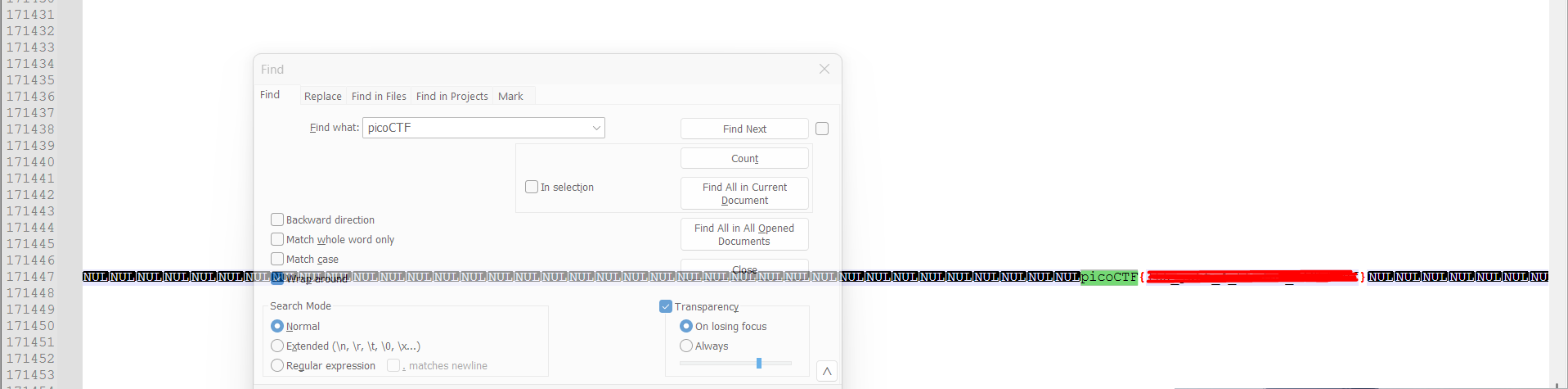
Foi então que pensei na extensão .gz, como uma extensão de arquivo compactado. Com isso, utilizei o WinRaR para descompactar e obtive o arquivo completo.



**Buscando a flag**

Nele, foi possível buscar o texto “PicoCTF”, e encontrar a flag.





**Conclusão**

Ao resolver o desafio, ficou claro como é importante saber lidar com diferentes tipos de arquivos e usar programas simples para abrir e procurar informações. Primeiro, precisei descompactar o arquivo .gz para conseguir acessar o conteúdo. Depois, bastou procurar pelo texto “PicoCTF” para encontrar a flag. Esse exercício mostrou que, mesmo em situações de CTF, o conhecimento básico de manipulação de arquivos e o uso de ferramentas como WinRAR e editores de texto já ajudam bastante na resolução do problema.

**Referências**

<https://www.win-rar.com>

<https://notepad-plus-plus.org>