Disko 2

The challenge came with a raw disk image that had multiple partitions. The flag was not visible directly – it was not possible to scan the whole binary file. A clue was provided: “How can you extract or isolate a partition?” This provided a hint that the flag was located in a particular partition. The disk image had a Linux ext4 partition and a FAT32 partition. It was provided that the Linux partition had the flag.

Steps to solve it:

Uncompress and analyze the disk image. Use file to analyze the disk image. The Linux partition was from sector 2048 to sector 51,200.

Extract the partition using dd:

dd if=disko-2.dd of=part1.img bs=512 skip=2048 count=51200

This extracted the Linux partition into part1.img.

Search for the flag using strings and grep:

strings part1.img | grep picoCTF

The flag was found

The moral of the story: disk forensics is not about searching for the flag in the data. The knowledge of the data structure, that the disk image is divided into several partitions, makes it easier to search for the flag in the correct location. This exercise has reinforced an important lesson in cybersecurity: it is not always the difficulty level that is important, but the tool that is being used. A series of logical steps led to the solution.