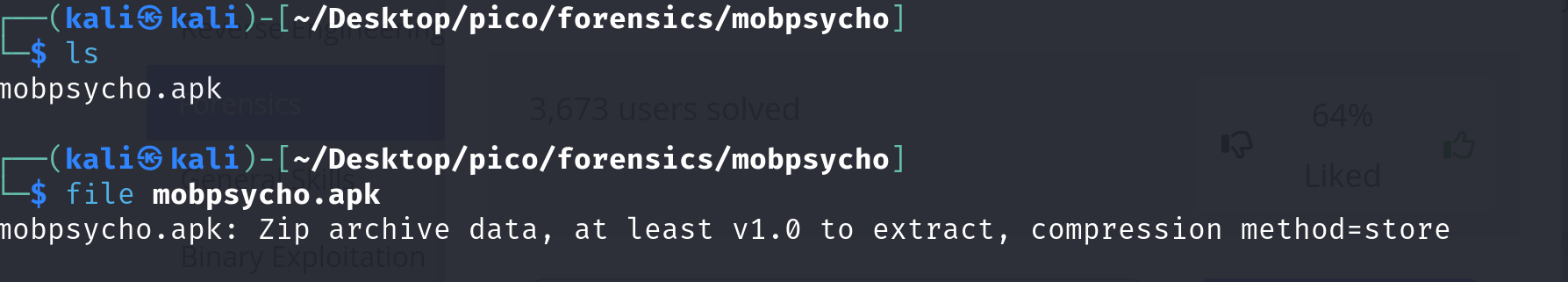
MOB PSYCHO APK Forensics Challenge Write-up

In this challenge, we were given an Android APK file called mobpsycho.apk. The goal was to analyze and extract the flag hidden within the APK. The following steps describe how we approached and solved the challenge.

**Step 1**: Identifying the APK structure



Android APK files are essentially ZIP archives. We confirmed this by running the file command, which identified mobpsycho.apk as a ZIP archive.

**Step 2:** Extracting the APK contents

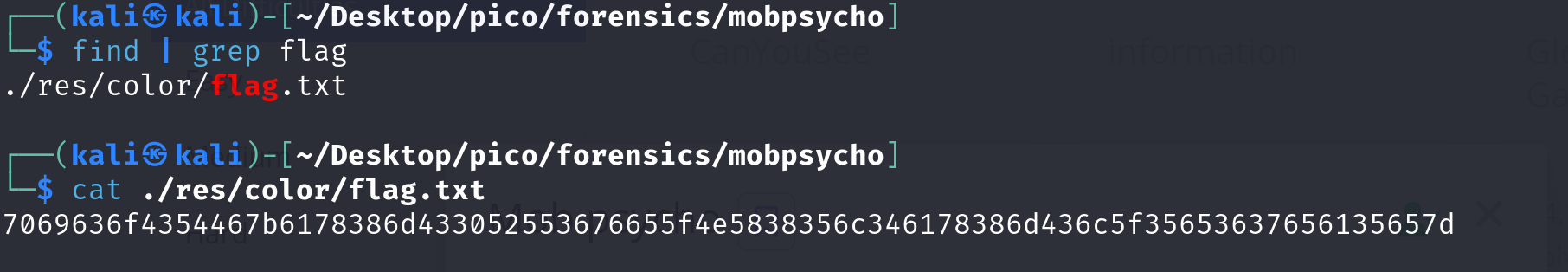
Using unzip, we extracted the contents of the APK:



This resulted in a directory containing various files, such as the AndroidManifest.xml and a number of resource files.

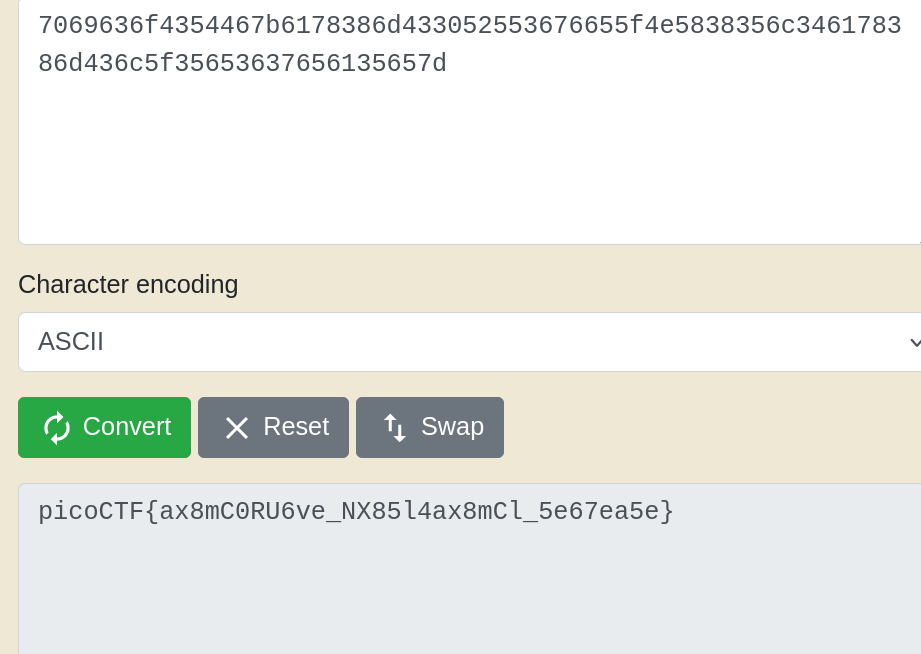
**Step 3**: Searching for hidden data

To find any hidden data, we used the find command to search through the extracted files. Specifically, we were looking for files containing potential flags or encoded data:

This search revealed a hexadecimal string in one of the files, which appeared to be part of the flag.

**Step 4**: Converting the hexadecimal data

The hexadecimal string found looked like this: "6865782d6e756d62657273...". We suspected that this was part of the flag encoded in hex. To decode it, we used a hex-to-text conversion tool:



**Step 5**: The final flag

The final flag was: picoCTF{ax8mC0RU6ve\_NX85l4ax8mCl\_5e67ea5e}