Android RE

1. Step 1: Decompile an Android [JADX](https://github.com/skylot/jadx?ref=hackernoon.com), [Apktool](https://github.com/iBotPeaches/Apktool?ref=hackernoon.com), [Bytecode Viewer](https://github.com/Konloch/bytecode-viewer/?ref=hackernoon.com) or Android Studio.
2. Step 2: Easiest way and normally people do is run Android an Android Studio with Apk Bundle decompiling

A screenshot of a computer

Description automatically generated

1. I went across all the directories and found a unique file named encoded\_chudio.wav

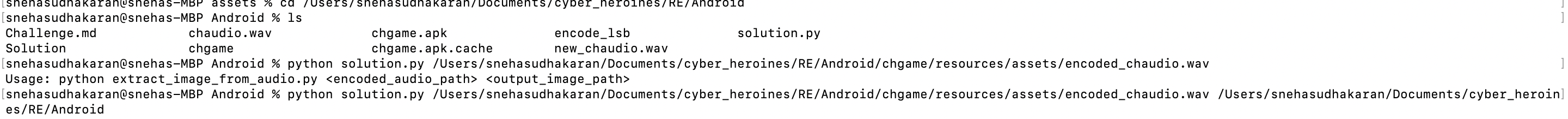
In command line as the decompiled version with jadx-gui gives a folder “chgame”

A close-up of a computer screen

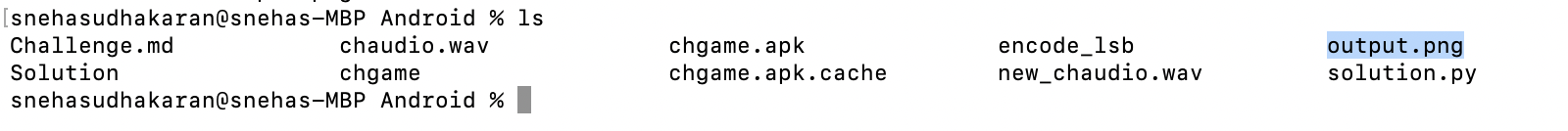
Description automatically generated

1. I kept traversing in all folders to get the actual file in chgame-Resources-assets-encoded\_chaudio.wavA white background with black text

   Description automatically generated
2. Since its encoded, it is linked with trespasser hacker society and clue is that our contest is on the weekend that they created a tool for RE I used



1. I created a solution.py for decoding the audio and the new image(screenshot containing the flags) are now in the new location



A screenshot of a computer

Description automatically generated

Hence the output to win this challenge they can have Flag is

chctf{t53$p@$$35\_h@ck!ng\_$0c!3ty}}