The first step of this challenge is finding a way of decompiling the ios app. After looking through a few things, I found out **7zip** can easily do it, so I used it to unzip the app.

Inside the app, we can find the “d” folder mentioned in the challenge description, so we read the instructions. The base64 string tells us to look for **SC_Info**. There are 3 such folders, however only one contains a **Manifest.pslist** file. Inside this file we can find a message telling us the next step is… a hash.

Breaking this hash (bcrypt) can be done using hashcat and rockyou.txt:

hashcat -m 3200 -a 0 -o cracked.txt hash.txt /usr/share/wordlists/rockyou.txt

Afterwards, after a little wait we find out the initial text is asterix. Looking for files named “asterix” in the app folder returns an image named **asterix.jpg**

Inside this image we can discover a weird string, reminding me on Brainfuck: “++++[++++>---<]>++.--.>-[--->+<]>--.--[->++++<]>-.-----[->++<]>-.-[->+++++<]>.[-->+<]>+++++.----[->++<]>.-.-[------>+<]>--.------...--..[->++<]>.+.+[-->+<]>.+.++.++.-----[->++<]>-..+[-->+<]>+++.--[->++<]>.---.+[-->+<]>++++.---.+++.-----[->++<]>-.+[-->+<]>+++.--[->++<]>.--.+++.+[-->+<]>+.---.[->++<]>-.-[-->+<]>.+.[->++<]>.[-->+<]>++++++.------[->++<]>-.+[-->+<]>++..--[->++<]>.[-->+<]>++++.+++.-----.-[->++<]>.[-->+<]>--.++++.-.--[->++<]>-.+[-->+<]>++++++.----[->++<]>.++[->+++<]>.-.-------.-[--->+<]>+.[-->+<]>.+..----.++++++.+++.--.----[->++<]>-.-[-->+<]>.+++++.>--[-->+++<]>.”

Turns out this is in fact brainfuck, and executing this code returns the flag.

Made with love by: AndreiCat