PicoCTF Hurry up! Wait! 100 points

<https://mercury.picoctf.net/static/df4efca50acbb7c5e829f8fd472fb796/svchost.exe>

No explanation other than this link. Its an exe file I’m assumed to reverse engineer to find the file inside. For this I’ll be using Ghidra!

When going through the file most files are just short functions but there is one function standing out which is: FUN\_0010298a

Graphical user interface

Description automatically generated

When opening each function we see one function:

Graphical user interface, application

Description automatically generated

Clicking this fist thing redirects me to P, then going back and doing the same for the next function redirects me to I, looks like we found the solution!

Now in order to extract this I could go over everything manually but in the writeup down below made its own script! And I’m a big fan of making scripts to solve these types of problems because it’s a massive learning experience to just copy paste it and look into how everything works!

Graphical user interface, text, application, email

Description automatically generated

And so I received the flag!

Honestly I do not understand how this works, even though I’m quite adept to Python… But knowing the possibility of scripting in Ghidra will be a strong asset for me in the future!

picoCTF{d15a5m\_ftw\_87e5ab1}