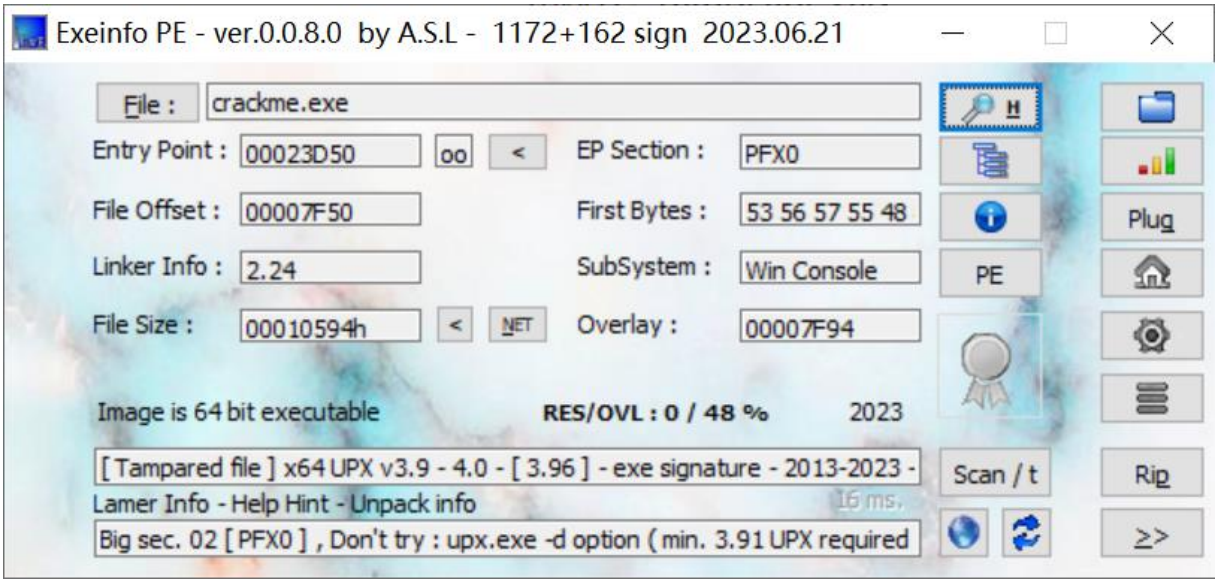
crackme-wp

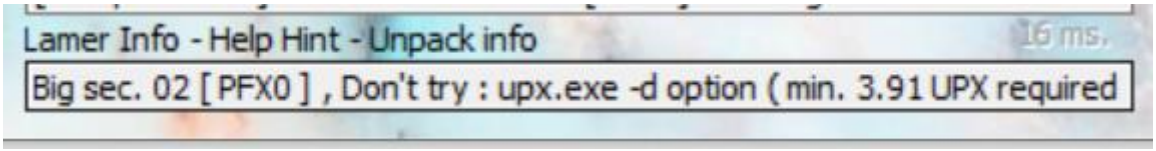
出题人：D0UBL3SEV3N

学校：大理大学

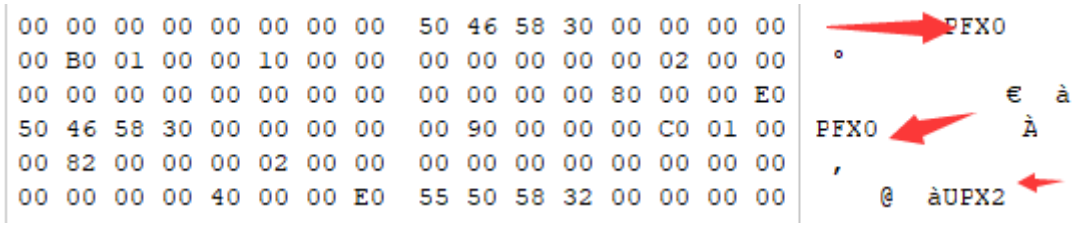
下载附件后拖入 Exeinfo PE 查壳



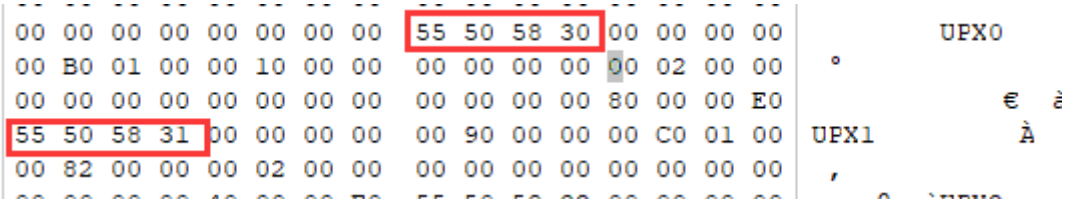
首先看到是 upx 壳，但是提示不要尝试用 upx.exe -d 去脱：



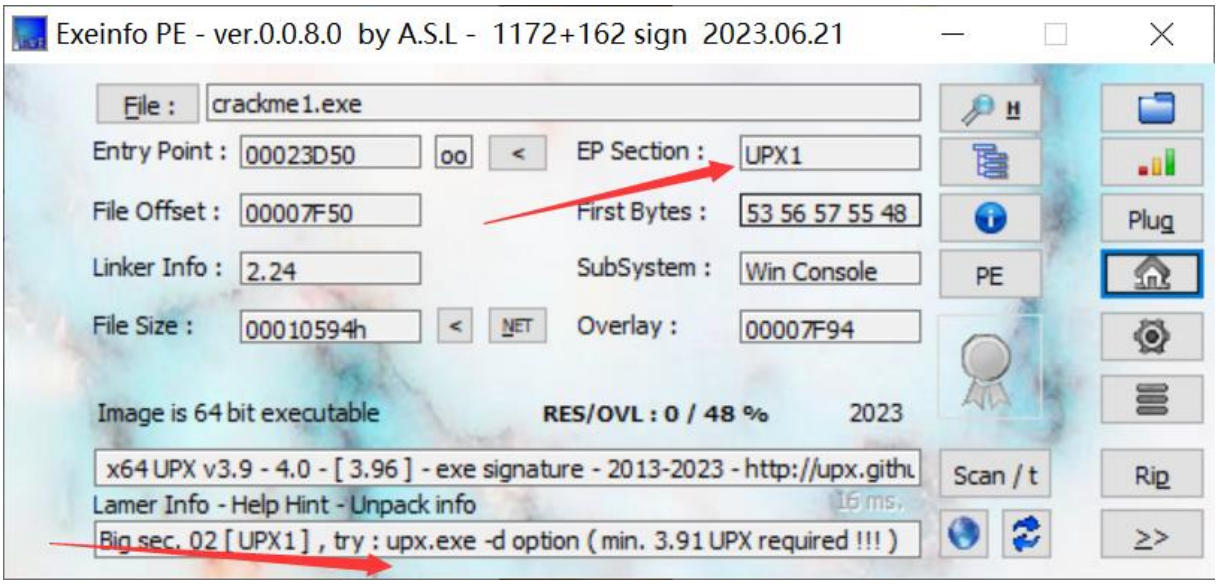
EP section 不对，是被改了，winhex 查看：



改对应的 16 进制，让第一个 PFX0 变成 UPX0，第二个 PFX0 变成 UPX1，也就是把第一个 50 46 58 30 改成 55 50 58 30；第二个 50 46 58 30 改成 55 50 58 31 如下：



再去查一下是否正常了。



显示正常，脱壳：

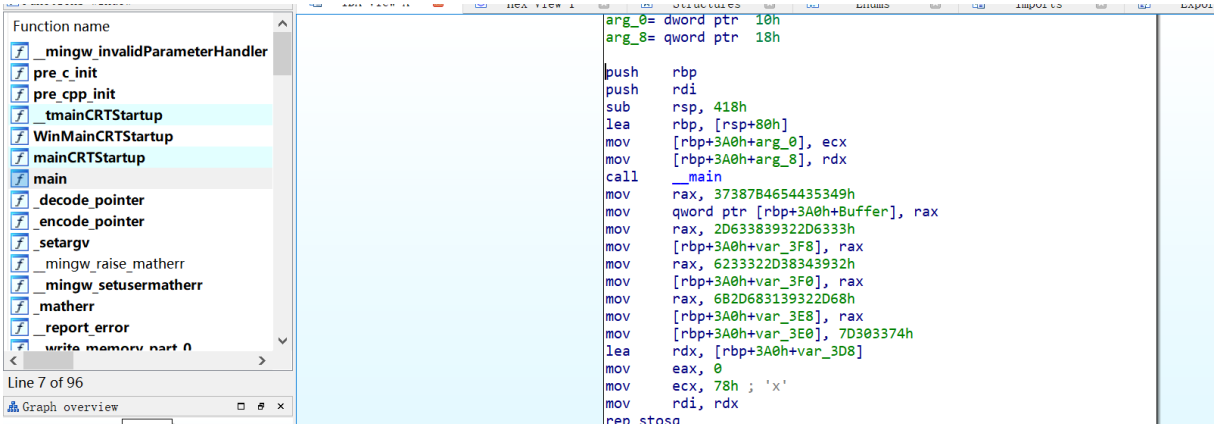
```
C:\Users\86198\Desktop\challenge\isctf2023出题人\crackme>upx.exe -d crackme1.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2022
UPX 4.0.0       Markus Oberhumer, Laszlo Molnar & John Reiser   Oct 28th 2022

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    130964 <-     66964   51.13%    win64/pe      crackme1.exe

Unpacked 1 file.

C:\Users\86198\Desktop\challenge\isctf2023出题人\crackme>
```

然后载入 ida64 找到主函数，反编译



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char Buffer[8]; // [rsp+20h] [rbp-60h]
  char v5; // [rsp+48h] [rbp-38h]

  _main();
  strcpy(Buffer, "ISCTF{873c-298c-2948-23bh-291h-kt30}");
  memset(&v5, 0, 0x3C0ui64);
  puts(Buffer);
  return 0;
}
```

拿到 flag

```
ISCTF{873c-298c-2948-23bh-291h-kt30}
```