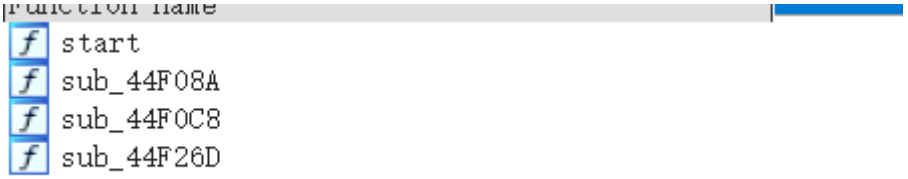
使用upx进行加壳

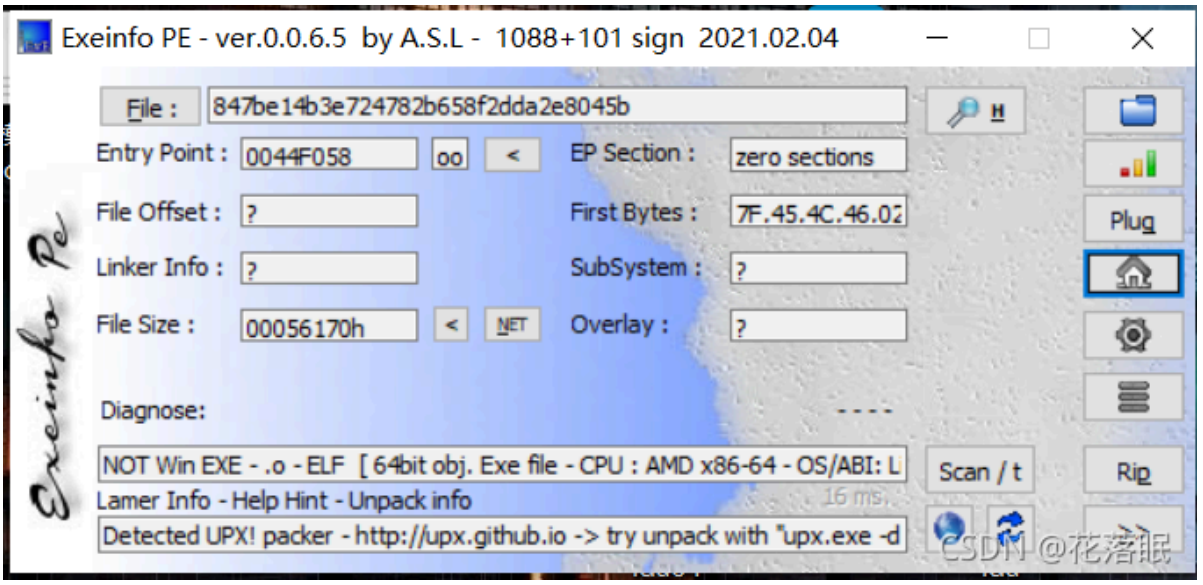
先查壳

一般做到逆向的部分题的时候，把文件丢进ida会发现函数特别少，大部分都是加壳了

ida打开只有四个函数



丢入ExeinfoPe里面
发现有壳（最下面那行显示是upx壳）



脱壳

首先安装工具，解压完之后进入到最里层文件夹中复制下来此时的地址，cmd打开命令行先cd把地址转换，之后直接输入upx.exe -h安装完成
会出现这样（一大串）

```
Microsoft Windows [版本 10.0.19043.1237]
(c) Microsoft Corporation。保留所有权利。

C:\Users\10439>cd C:\Users\10439\Desktop\software\ida\upx-3.96-win64\upx-3.96-win64

C:\Users\10439\Desktop\software\ida\upx-3.96-win64\upx-3.96-win64>upx.exe -h
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

Commands:
  -1     compress faster                   -9    compress better
  --best compress best (can be slow for big files)
  -d     decompress                        -l    list compressed file
  -t     test compressed file              -V    display version number
  -h     give this help                    -L    display software license

Options:
  -q     be quiet                          -v    be verbose
  -oFILE write output to 'FILE'
  -f     force compression of suspicious files
  --no-color, --mono, --color, --no-progress   change look

Compression tuning options:
  --brute             try all available compression methods & filters [slow]
  --ultra-brute       try even more compression variants [very slow]

Backup options:
  -k, --backup        keep backup files
  --no-backup         no backup files [default]

Overlay options:
  --overlay=copy      copy any extra data attached to the file [default]
  --overlay=strip     strip any extra data attached to the file [DANGEROUS]
  --overlay=skip      don't compress a file with an overlay

Options for djgpp2/coff:
  --coff              produce COFF output [default: EXE]

Options for dos/com:
  --8086              make compressed com work on any 8086

Options for dos/exe:
  --8086              make compressed exe work on any 8086
  --no-reloc          put no relocations in to the exe header

Options for dos/sys:
  --8086              make compressed sys work on any 8086

Options for ps1/exe:
  --8-bit             uses 8 bit size compression [default: 32 bit]
  --8mib-ram          8 megabyte memory limit [default: 2 MiB]
  --boot-only         disables client/host transfer compatibility
  --no-align          don't align to 2048 bytes [enables: --console-run]

Options for watcom/le:
  --le                produce LE output [default: EXE]

Options for win32/pe, win64/pe, rtm32/pe & arm/pe:
  --compress-exports=0    do not compress the export section
  --compress-exports=1    compress the export section [default]
  --compress-icons=0      do not compress any icons
  --compress-icons=1      compress all but the first icon
  --compress-icons=2      compress all but the first icon directory [default]
  --compress-icons=3      compress all icons
  --compress-resources=0  do not compress any resources at all
  --keep-resource=list    do not compress resources specified by list
  --strip-relocs=0        do not strip relocations
  --strip-relocs=1        strip relocations [default]

Options for linux/elf:
  --preserve-build-id     copy .gnu.note.build-id to compressed output

file..   executables to (de)compress

This version supports:
    amd64-darwin.dylib                  dylib/amd64
    amd64-darwin.macho                  macho/amd64
    amd64-linux.elf                     linux/amd64
    amd64-linux.kernel.vmlinux          vmlinux/amd64
    amd64-win64.pe                      win64/pe
    arm-darwin.macho                    macho/arm
    arm-linux.elf                       linux/arm
```

```
    arm-linux.kernel.vmlinux            vmlinux/arm
    arm-linux.kernel.vmlinuz            vmlinuz/arm
    arm-wince.pe                        arm/pe
    arm64-darwin.macho                  macho/arm64
    arm64-linux.elf                     linux/arm64
    armeb-linux.elf                     linux/armeb
    armeb-linux.kernel.vmlinux          vmlinux/armeb
    fat-darwin.macho                    macho/fat
    i086-dos16.com                      dos/com
    i086-dos16.exe                      dos/exe
    i086-dos16.sys                      dos/sys
    i386-bsd.elf.execve                 bsd.exec/i386
    i386-darwin.macho                   macho/i386
    i386-dos32.djgpp2.coff              djgpp2/coff
    i386-dos32.tmt.adam                 tmt/adam
    i386-dos32.watcom.le                watcom/le
    i386-freebsd.elf                    freebsd/i386
    i386-linux.elf                      linux/i386
    i386-linux.elf.execve               linux.exec/i386
    i386-linux.elf.shell                linux.sh/i386
    i386-linux.kernel.bvmlinuz          bvmlinuz/i386
    i386-linux.kernel.vmlinux           vmlinux/i386
    i386-linux.kernel.vmlinuz           vmlinuz/i386
    i386-netbsd.elf                     netbsd/i386
    i386-openbsd.elf                    openbsd/i386
    i386-win32.pe                       win32/pe
    m68k-atari.tos                      atari/tos
    mips-linux.elf                      linux/mips
    mipsel-linux.elf                    linux/mipsel
    mipsel.r3000-ps1                    ps1/exe
    powerpc-darwin.macho                macho/ppc32
    powerpc-linux.elf                   linux/ppc32
    powerpc-linux.kernel.vmlinux        vmlinux/ppc32
    powerpc64-linux.elf                 linux/ppc64
    powerpc64le-darwin.macho            macho/ppc64le
    powerpc64le-linux.elf               linux/ppc64le
    powerpc64le-linux.kernel.vmlinux    vmlinux/ppc64le

UPX comes with ABSOLUTELY NO WARRANTY; for details visit https://upx.github.io

C:\Users\10439\Desktop\software\ida\upx-3.96-win64\upx-3.96-win64>
```


之后就可以脱壳了，还在这个窗口，因为刚刚已经把地址转到了upx脱壳工具这里了，所以这下不用再转，（下次打开需要重新转）

先打操作指令

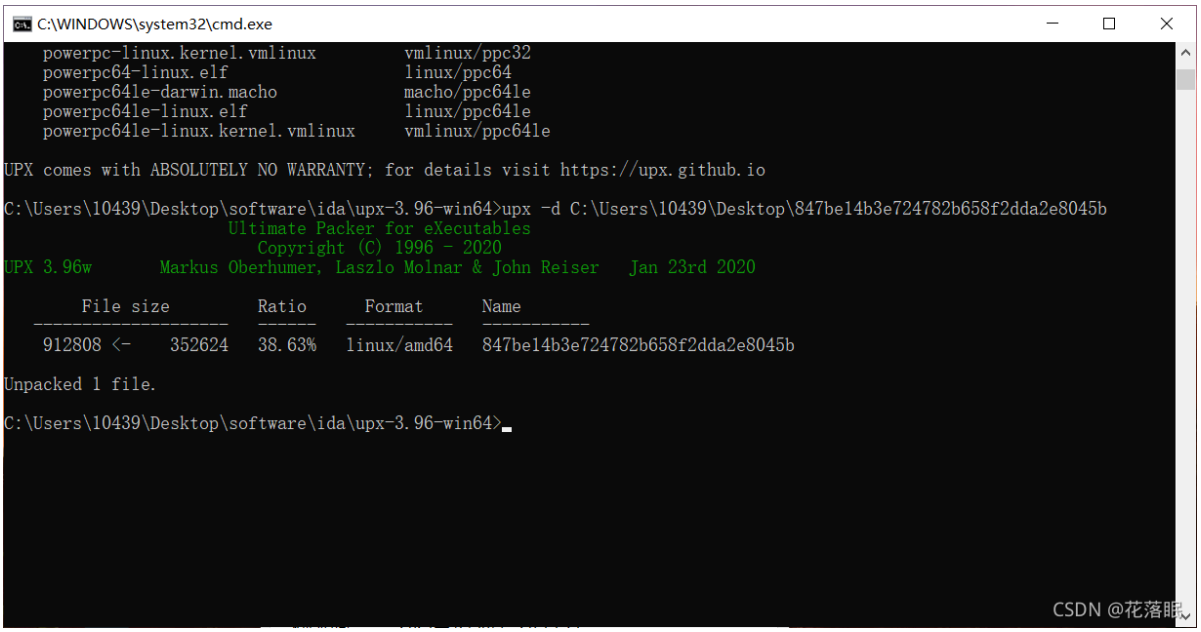
```
Commands:
  -1     compress faster                    -9    compress better
  --best compress best (can be slow for big files)
  -d     decompress                         -l    list compressed file
  -t     test compressed file               -V    display version number
  -h     give this help                     -L    display software license
```

这些是指令，其中-d是这次要用到的脱壳指令

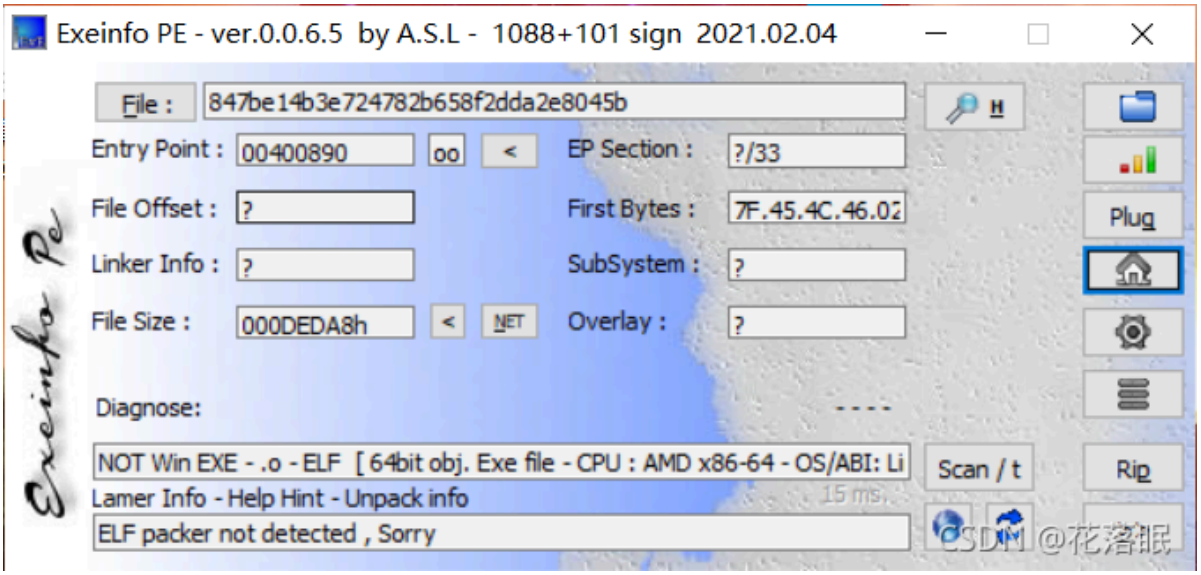
先打好指令upx -指令名 文件位置和名称
这样打

```
>upx -d C:\Users\10439\Desktop\847be14b3e724782b658f2dda2e8045b - 副本
```

脱壳成功



好接下来再丢到ExeinfoPe查看，已经没壳了



再重新放入ida，出现了很多函数，f5操作一下

补充一些其他的UPX命令

压缩可执行文件：UPX XXX.exe
解压缩可执行文件：UPX -d XXX.exe

1. upx.exe –o 别名.exe –d 现名.exe
2.
3. -o：表示输出；
4.
5. -o 别名.exe：表示以别名.exe作为脱壳后的输出；
6.
7. -d 现名.exe：表示以现名.exe作为脱壳前的输入

列表：UPX -l sample.exe

```
D:\Learning_tools\逆向工具\upx-3.95-win64>upx -1 sample_mal.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
     58880 ->     36864   62.61%    win32/pe     sample_mal.exe

D:\Learning_tools\逆向工具\upx-3.95-win64>
```

测试压缩过的可执行文件：UPX -t sample.exe

```
D:\Learning_tools\逆向工具\upx-3.95-win64>upx -t sample_mal.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

testing sample_mal.exe [OK]

Tested 1 file.

D:\Learning_tools\逆向工具\upx-3.95-win64>
```

显示版本号：upx -V （注意区分大小写）

```
D:\Learning_tools\逆向工具\upx-3.95-win64>upx -V
upx 3.95
NRV data compression library 0.84
UCL data compression library 1.03
zlib data compression library 1.2.3
LZMA SDK version 4.43
Copyright (C) 1996-2018 Markus Franz Xaver Johannes Oberhumer
Copyright (C) 1996-2018 Laszlo Molnar
Copyright (C) 2000-2018 John F. Reiser
Copyright (C) 2002-2018 Jens Medoch
Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler
Copyright (C) 1999-2006 Igor Pavlov
UPX comes with ABSOLUTELY NO WARRANTY; for details type 'upx -L'.
                                                    https://blog.csdn.net/qq_43633973
D:\Learning_tools\逆向工具\upx-3.95-win64>
```