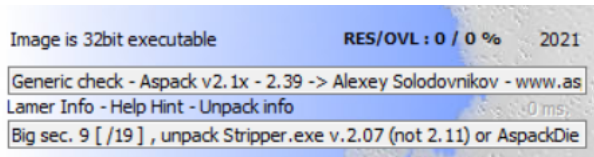
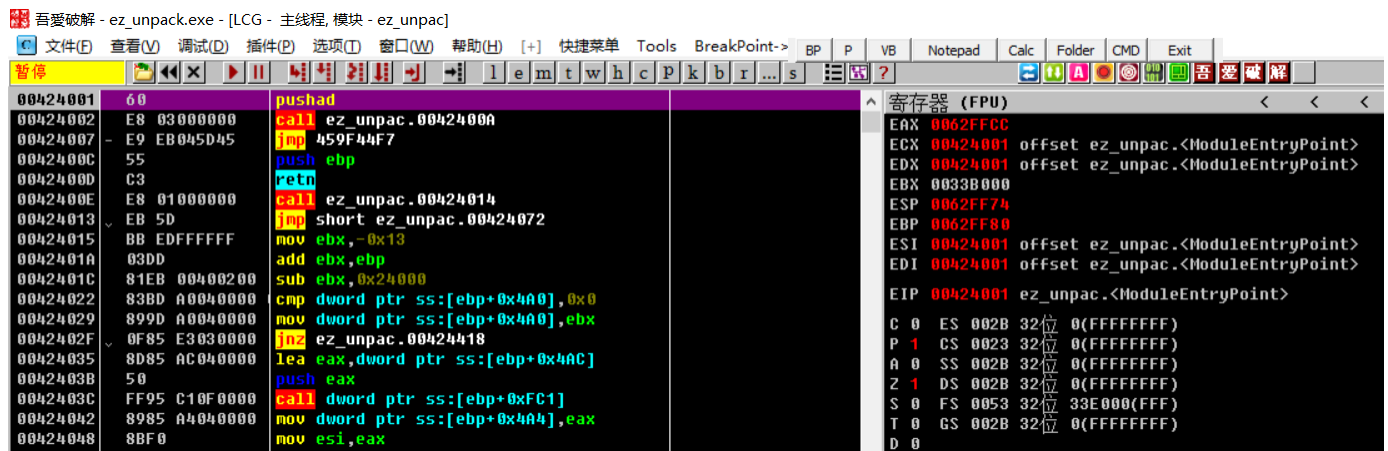


ez_unpack

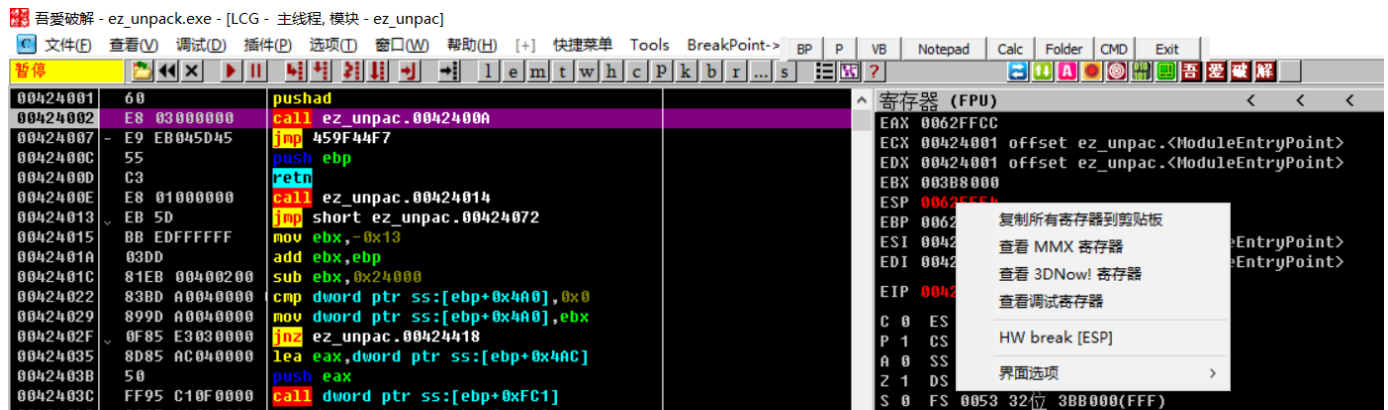
扔进Exeinfo PE, 32位exe, Aspack壳



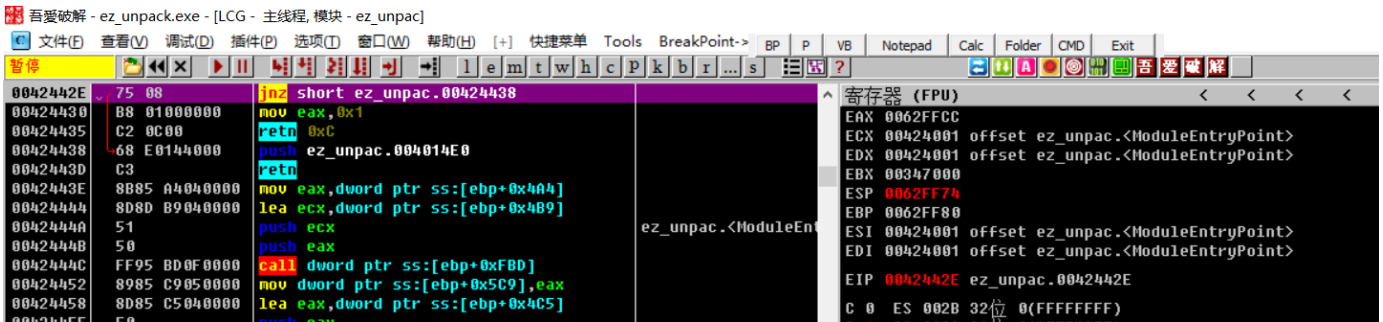
压缩壳一般都会用到pushad指令, ESP定律即可脱壳, 进去按一下F8



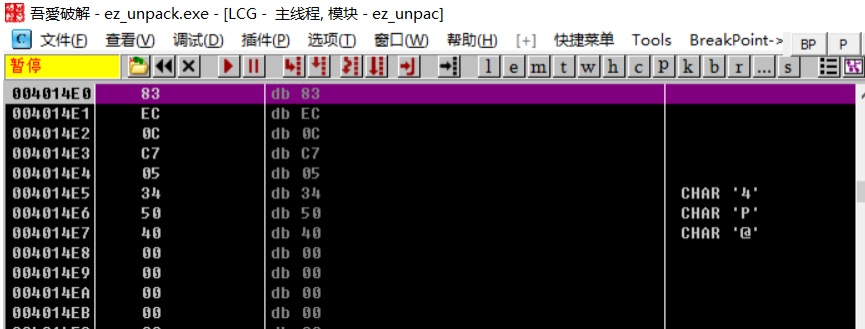
右键ESP寄存器然后选择断点, 即HW break [ESP], 然后按一下F9



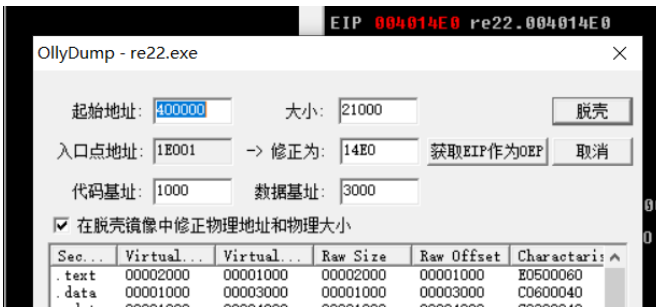
再F8几下进入壳内的exe函数, 然后就找到了程序真正的OEP



OEP



选择 插件->OllyDump, 自动选择了当前EIP作为OEP, 啥都不用选直接按脱壳, 保存为dump.exe



将脱好壳的程序放进ida, 剩下的不细讲了, base64解码一下就是flag

```

sub_4022B0();
puts(Buffer);
printf("Please input your flag:");
scanf("%s", v4);
v9 = v4;
v8 = strlen(v4);
v7 = sub_401500(v9, v8, v6);
v6[v7] = 0;
qmemcpy(v4, "TU9DU0NURntWZXJ5X0V6X1VucDBja19SMHZlcnNlX2hhKmhhfQ==", sizeof(v4));
for ( i = 0; i < v7; ++i )
{
    if ( v6[i] != v4[i] )
    {
        printf("Sorry, plz try again");
        break;
    }
}
printf("Jesus, You are so handsome!!");
return 0;

```

```

1 import base64
2 flag = "TU9DU0NURntWZXJ5X0V6X1VucDBja19SMHZlcnNlX2hhKmhhfQ=="

```

```
3
4 print(base64.b64decode(flag))
5 # M0CSCTF{Very_Ez_Unp0ck_R0verse_ha*ha}
```