題目:giveUflag
丟進 IDA 裡面看
Main 裡面有兩個 function:

```
_LIST_ENTRY *sub_401550()
{
  _LIST_ENTRY *Flink; // [rsp+40h] [rbp-20h]
  _LIST_ENTRY *i; // [rsp+58h] [rbp-8h]

  Flink = NtCurrentPeb()->Ldr->InMemoryOrderModuleList.Flink;
  for ( i = Flink->Flink; i != Flink && wcsicmp((const wchar_t *)i[5].Flink, aK); i = i->Flink )
    ;
  return i[2].Flink;
}
```

PEB table,包含了這個 process 所使用的所有的 dll
這個很明顯就是去 PEB table,透過 InMemoryOrderModuleList 找想要的 dll,
wcsicmp((const wchar_t *)i[5].Flink, aK) 就是在做 string compare 的動作,在 x64dgb 裡面可以看到這個 aK 是 kernel32.dll,i[5].Flink 對應到這個 dll 的 name
所以就是 在 PEB table 裡面找到 kernel32.dll 對應的 struct
Return i[2].Flink,就是返回 kernel32.dll 在 mem 裡面的起始位置

```
memcpy(v3, &unk_403040, 0xB4ui64);
memset(Buffer, 0, sizeof(Buffer));
v12 = image_base_address + *(int *)(image_base_address + 60);
EAT = (int *)(image_base_address + *(int *)(v12 + 136));
v10 = image_base_address + EAT[3];
v9 = EAT[5];
addressOfFunctions = (int *)(image_base_address + EAT[7]);
addressOfNames = (int *)(image_base_address + EAT[8]);
for ( i = 0; i < v9; ++i )
{
  String1 = (char *)(image_base_address + addressOfNames[i]);
  if ( !stricmp(String1, "sleep") )
    break;
}
```

這邊就是透過上面拿到的 image,先找出 optional header,得到 export directory 位置,在去 EAT 裡面查 name 是 sleep 的 function

```
  }
  func_ptr_1 = (void (__fastcall *)(__int64))(image_base_address + addressOfFunctions[i]);
  func_ptr_2 = func_ptr_1;
  func_ptr_1(0x240C8400i64);
  puts("https://i.ytimg.com/vi/_T2c8g6Zuq8/maxresdefault.jpg");
  func_ptr_2(604800000i64);
  puts("https://i.ytimg.com/vi/MY4sFW83yxg/maxresdefault.jpg");
  func_ptr_2(604800000i64);
  puts("https://i.ytimg.com/vi/OVuZ4vGxVKE/maxresdefault.jpg");
  for ( j = 0; j <= 44; ++j )
    Buffer[j] = off_403020[j] ^ v3[4 * j];
  puts(Buffer);
  return func_ptr_1;
}
```

這邊的 func_ptr_1 , func_ptr_2 其實就是 sleep
Print 出 flag 之前會 sleep 很久
我們使用 x64dbg 把時間改成 1 秒,flag 就出來了