Winpcap 使用教程

0x00 安装

1 百度 winpcap ， 下载安装包并安装，或者直接下载并安装 wireshark（推荐）

2 下载 winpcap 的开发包

官网：http://www.winpcap.org/

百度网盘 ： 链接：http://pan.baidu.com/s/1eQx0gRS 密码：p9mf

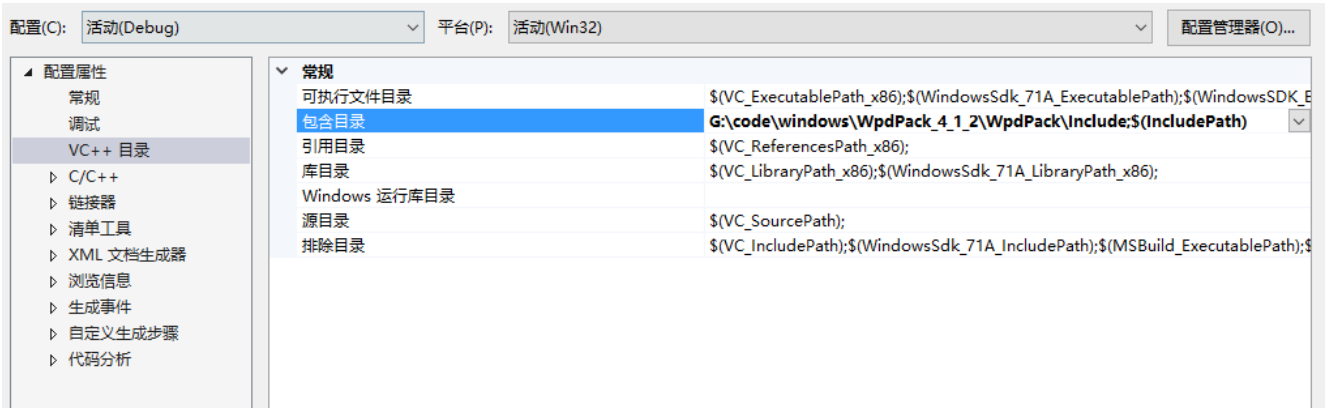
3 IDE ： vs, codeblocks 等等

0x01 开发包导入

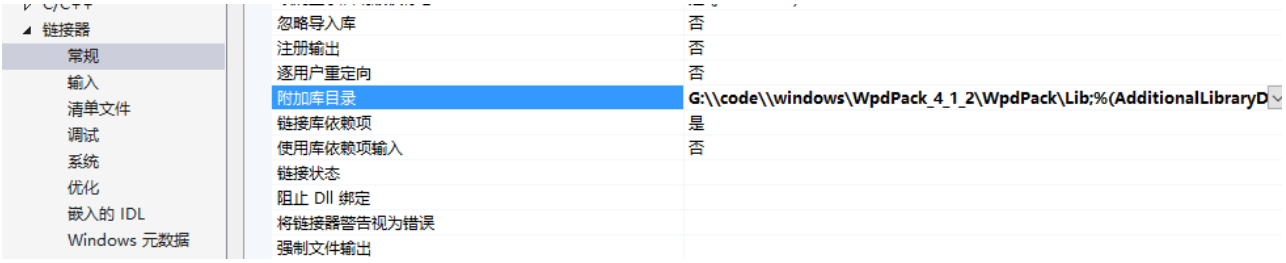
N: 这里我以 vs 为例， 其他 IDE 也类似

1 新建一个控制台工程，通过项目->添加新项 添加一个.cpp 或.c 文件

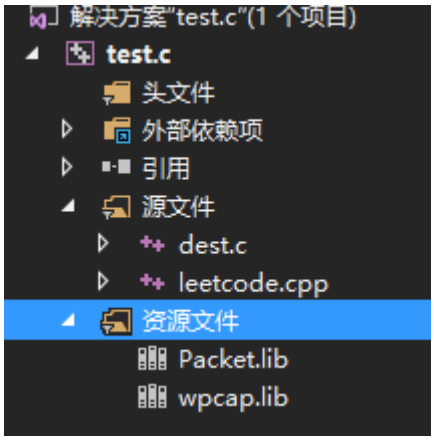
2 在项目->属性->VC++ 目录中，添加一个开发包的绝对路径



3 在链接器的常规中，加入 lib 的绝对路径



然后在资源中添加两个文件



以上，导入就完成了 。

0x11 使用

在代码文件中加入#include “pcap.h” 即可使用。
百度网盘里是我写的（其实是官网 Copy 的- -）代码， 抓包部分已经完成 ， 部分代码我也做了相应的注释。
对 winpcap 感兴趣的可以去官网查看 Documentation
以下是两个灰常详细的链接
http://www.ferrisxu.com/WinPcap/html/index.html
http://www.winpcap.org/docs/docs_412/html/main.html ，

另外 linux 下可以使用 libpcap 进行开发 http://www.tcpdump.org/#documentation

链接：http://pan.baidu.com/s/1hqFCUcW 密码：v9qr