Libpcap 编程环境建立

Libpcap 简介

libpcap 是 unix/linux 平台下的网络数据包捕获函数包，大多数网络监控软件都以它为基础。Libpcap 可以在绝大多数类 unix 平台下工作。官方网站是 http://www.tcpdump.org/。

Libpcap 提供了系统独立的用户级别网络数据包捕获接口，并充分考虑到应用程序的可移植性。Libpcap 可以在绝大多数类 unix 平台下工作。在 windows 平台下，一个与 libpcap 很类似的函数包 winpcap 提供捕获功能，其官方网站是 http://www.winpcap.org/。

Libpcap 下载安装

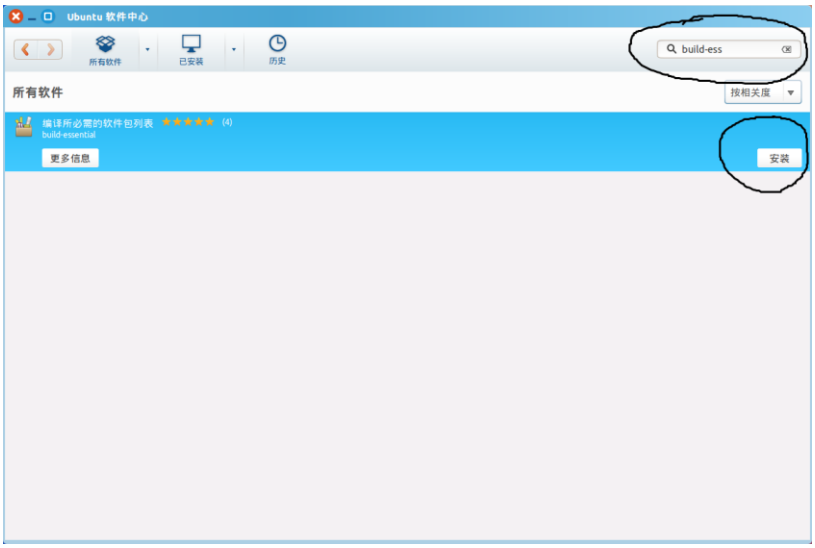
在 http://www.tcpdump.org/ 网站上的 download 中，可以下载到 libpcap-1.7.4.tar.gz 文件。

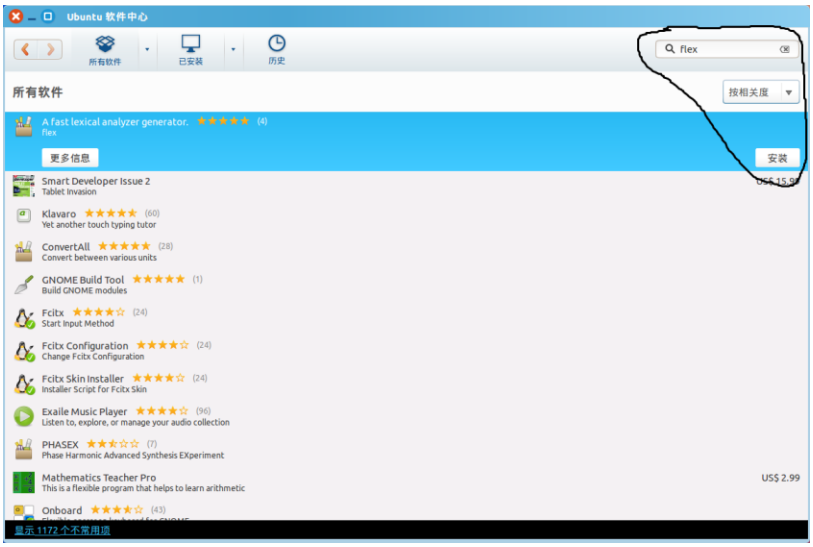
在 Ubuntu 中需要安装这个软件包。Linux 下，“tar.gz”文件的安装方法是，通过以下命令行：

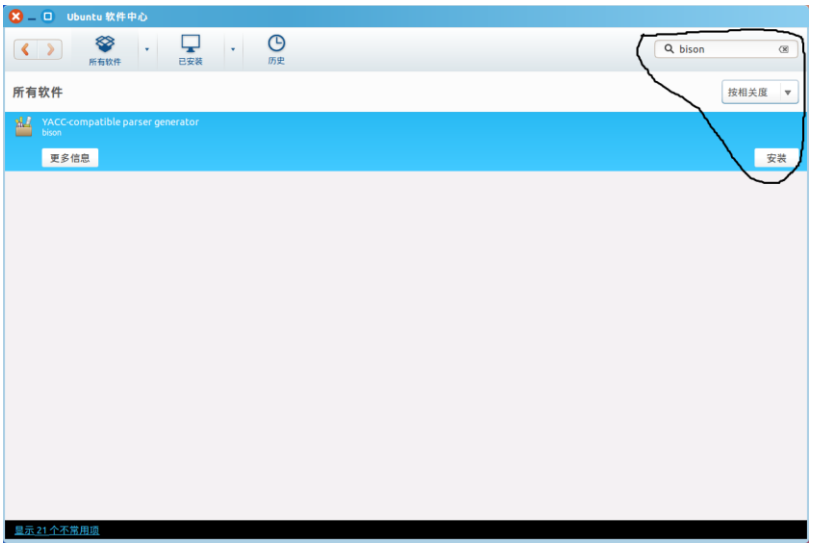
```
./configure
make
make install
```

执行这个三个步骤之前，需要安装几个软件才能顺利安装，build-essential、flex、bison。

安装软件除了通过 apt-get install 命令外，也可以使用图形界面的“Ubuntu 软件中心”。在搜索处输入软件的名字，然后点击安装即可。


Ubuntu 软件中心
所有软件
已安装
历史
build-ess
所有软件
按相关度
编译所必需的软件包列表
build-essential
更多信息
安装


Ubuntu 软件中心
所有软件
已安装
历史
flex
所有软件
按相关度
A fast lexical analyzer generator.
flex
更多信息
安装
Smart Developer Issue 2
Tablet Invasion
Klavaro
Yet another touch typing tutor
ConvertAll
Convert between various units
GNOME Build Tool
Build GNOME modules
Fcitx
Start Input Method
Fcitx Configuration
Change Fcitx Configuration
Fcitx Skin Installer
Installer Script for Fcitx Skin
Exaile Music Player
Listen to, explore, or manage your audio collection
PHASEX
Phase Harmonic Advanced Synthesis EXperiment
Mathematics Teacher Pro
This is a flexible program that helps to learn arithmetic
US$ 2.99
Onboard
显示 1172 个不常用项


Ubuntu 软件中心
所有软件
已安装
历史
bison
所有软件
按相关度
YACC-compatible parser generator
bison
更多信息
安装
显示 21 个不常用项

上述三个软件安装成功后，就可以安装 libpcap 了。首先是解压下载下来的软件包，libpcap-1.7.4.tar.gz。解压的方法可以用命令行：tar xzvf libpcap-1.7.4.tar.gz，也可以在图形界面的文件浏览器中，在文件上“右键->提取到此处”。

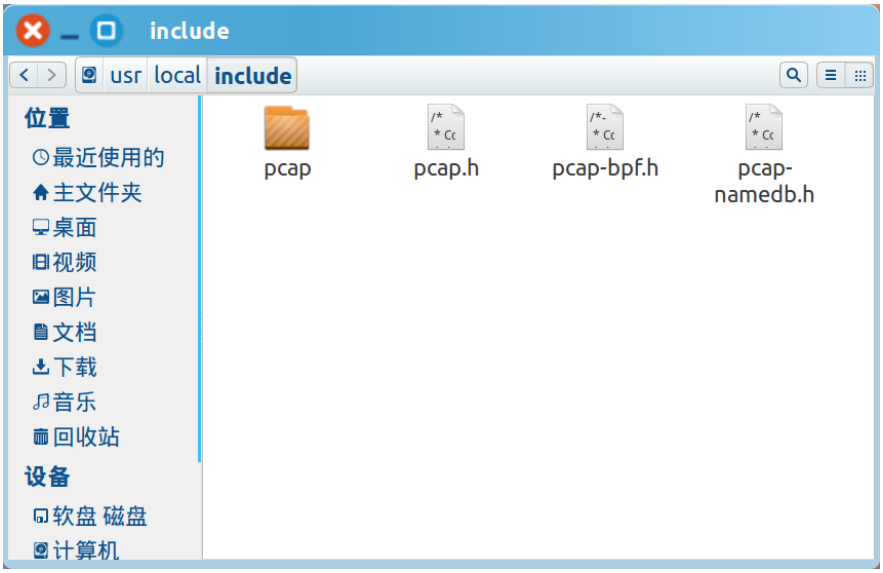
解压出一个文件目录 libpcap.1.7.4，在此目录内运行命令行：

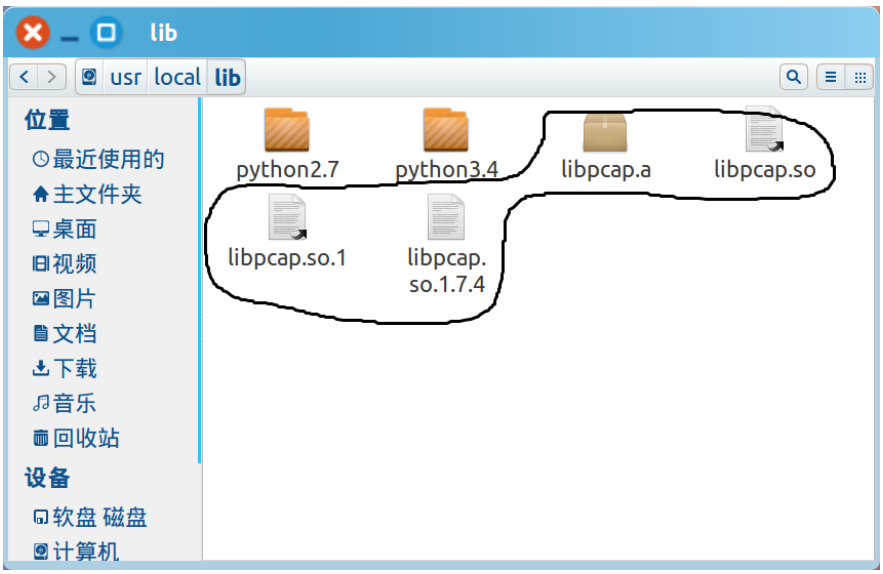
./configure

make

sudo make install

这里需要注意，make install 的时候，使用使用 sudo，因为安装文件的时候需要用到管理员权限。提示需要输入管理员密码，我们的虚拟机的密码是六个 1。软件安装到了/usr/local 目录下。可以看考/usr/local/include 和/usr/local/lib 目录下有了我们需要的头文件和 lib 文件。





安装成功后，通过一个简单的应用程序来验证一下是否安装成功。

```
#include <stdio.h>

#include <stdlib.h>
```

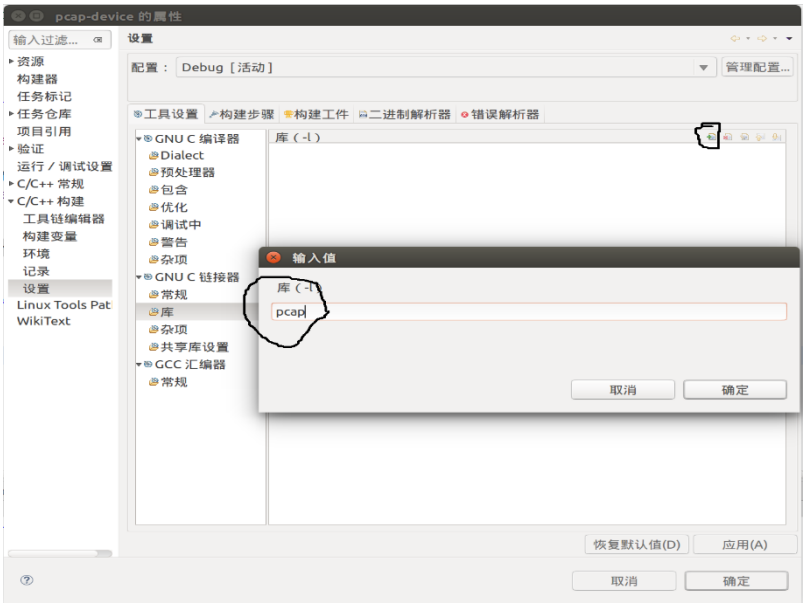
```c
#include <unistd.h>
#include <pcap/pcap.h>

int main(int argc,char *argv[])
{
    char *dev, errbuf[PCAP_ERRBUF_SIZE];
    dev=pcap_lookupdev(errbuf);
    if(dev==NULL)
    {
        fprintf(stderr,"couldn't find default
device: %s\n",errbuf);
        return(2);
    }
    printf("Device: %s\n",dev);
    return(0);
}
```

用 gedit 编辑器，输入上述代码，保存为 device.c。通过命令行来编译：
gcc -I/usr/local/include -L/usr/local/lib -o device device.c -lpcap
编译成功，就表明编程环境安装正确。

编译成功后，执行程序时，首先在命令行中运行一下 ldconfig，ldconfig 执行时通常需要 sudo ldconfig。然后再./device。

上过网络软件设计课程的同学，当然也可以使用 eclipse 来编辑代码，编译。

建立一个 C 项目，ANSI C Project，把代码拷贝到源文件里面。编译的时候，需要链接 pcap 库。设置项目属性，按照下图提示加入 pcap 库，即可编译成功。



使用 libpcap 编程

如何使用 libpcap 编程，需要到官方网站 http://www.tcpdump.org/查看相关文档。但是文档基本都是英文的。为了更容易上手，建议大家参考 winpcap 的一个中文文档——《WinPcap 中文技术文档.chm》，winpcap 是 libpcap 的 windows 版本，大部接口功能都是相同的，可以通过 winpcap 入手，了解 libpcap 如何编程。

example.c 代码是从文档《WinPcap 中文技术文档.chm》中的“分析数据包”部分直接抄下的代码，我们把这份代码编译成功，执行，直接就可以抓到包。这很方便大家进行学习。

Linux 下图形界面编程

推荐大家使用 QT 来编写 Linux 下的图形界面。