**SeeSee软件说明**

**一、开发目的**

由于linux下抓包的tcpdump只能在命令行模式且数据量大时只能存成文件，不具有实时性，所以设计此软件，以达到数据共享与数据的实时跟踪。本软件包据两部分，一部分是服务器端（linux下运行），另一部分是客户端（windows平台），开发测试过程中可以通过客户端直观的进行抓包条件定制与查看数据包情况。

**二、本软件的特色**

**1：**本软件可以通过客户端直观的查看linux端的数据包情况。

**2：**网络版功能，多个客户端可同时登录服务器，可以分享其他客户端抓包数据，此功能主要针对不同开发人员或不同模块之间的数据共享，以达到一个联调的功能。

**三、开发介绍**

1: 服务器端基于linux 平台，开发语言C，抓包库基于开源库pcap、iksemel（XML解释库）。

2：客户端基于windows平台VC6.0，开发语言C++，基于MFC库、iksemel。

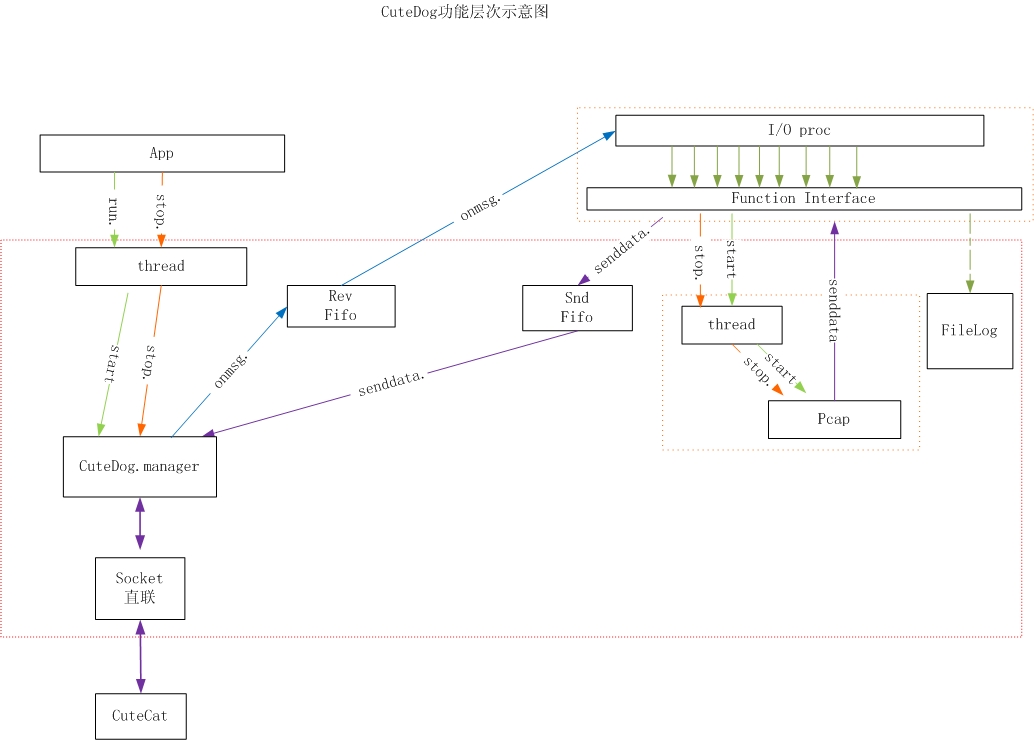
**四、涉及名词介绍**

本系统统称SeeSee,服务器端名称CuteDog；客户端名称CuteCat。

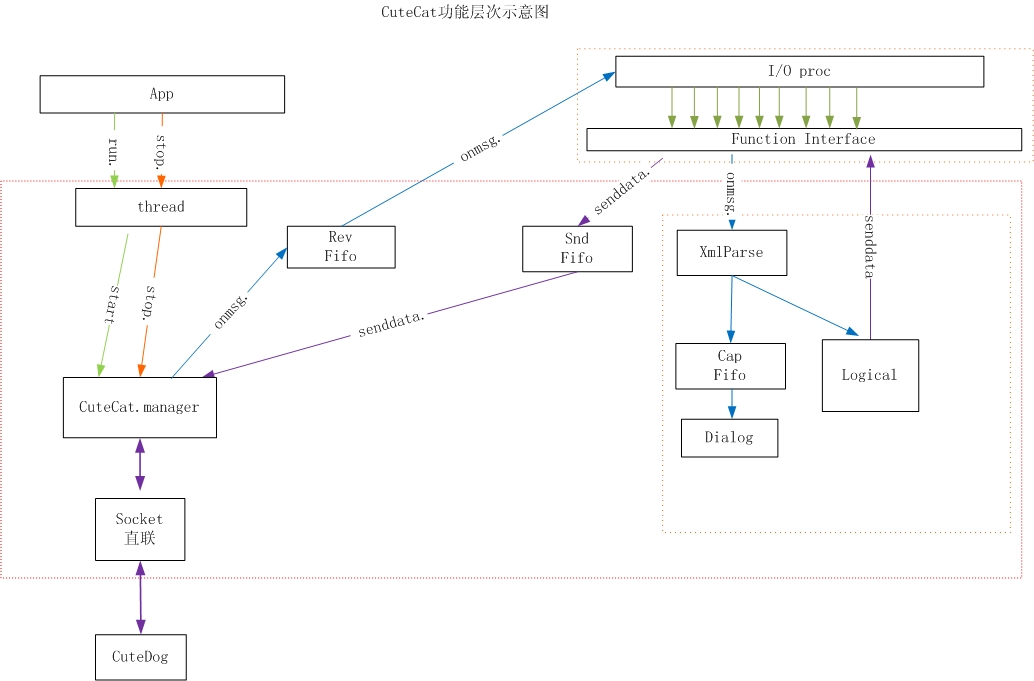
Pionner :指先行者模式，需指定抓包条件Hooker指享有查模式，可直接共享Pionner的数据。

**五、系统概要设计**

1：服务器端



2：客户端

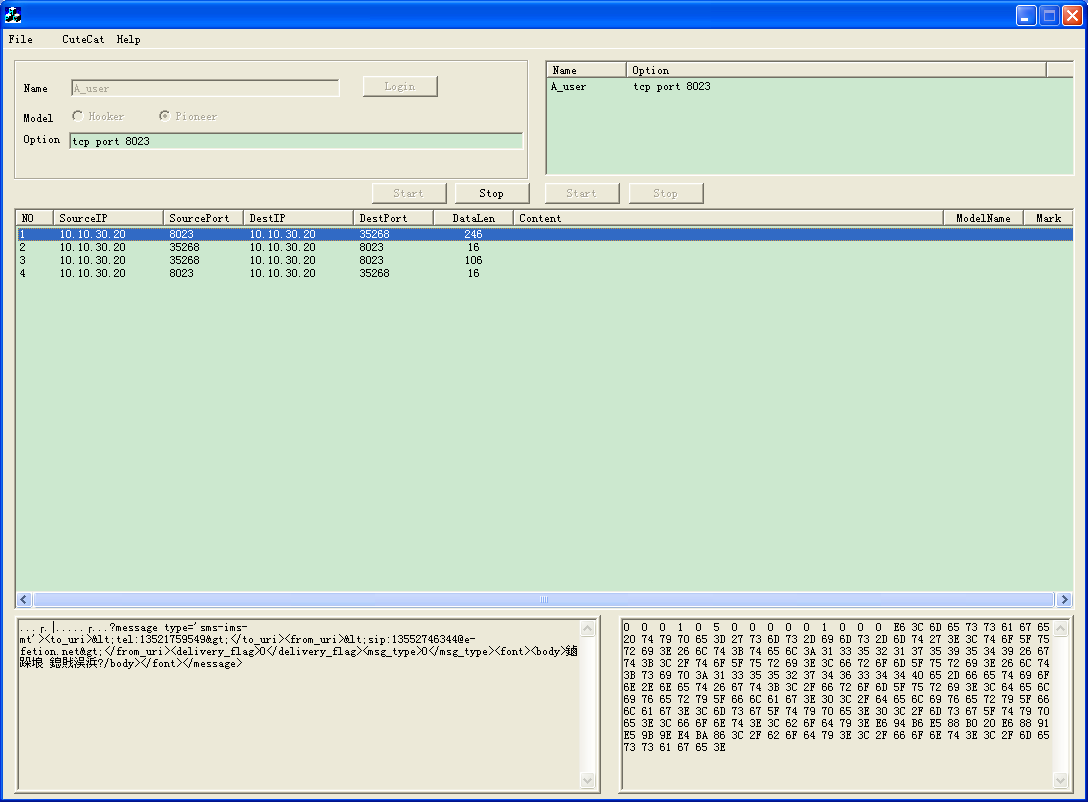


**六、使用举例**

1：背景：用户user1与user2，user1负责开发模块A;user2负责开发模块B,且A 与B通过tcp 8023通讯，此时user1 与user2 进行通讯协议联调。 A、 B 模块都在linux 服务器上。User1 user2 都是在windows 上用终端与linux 相连。

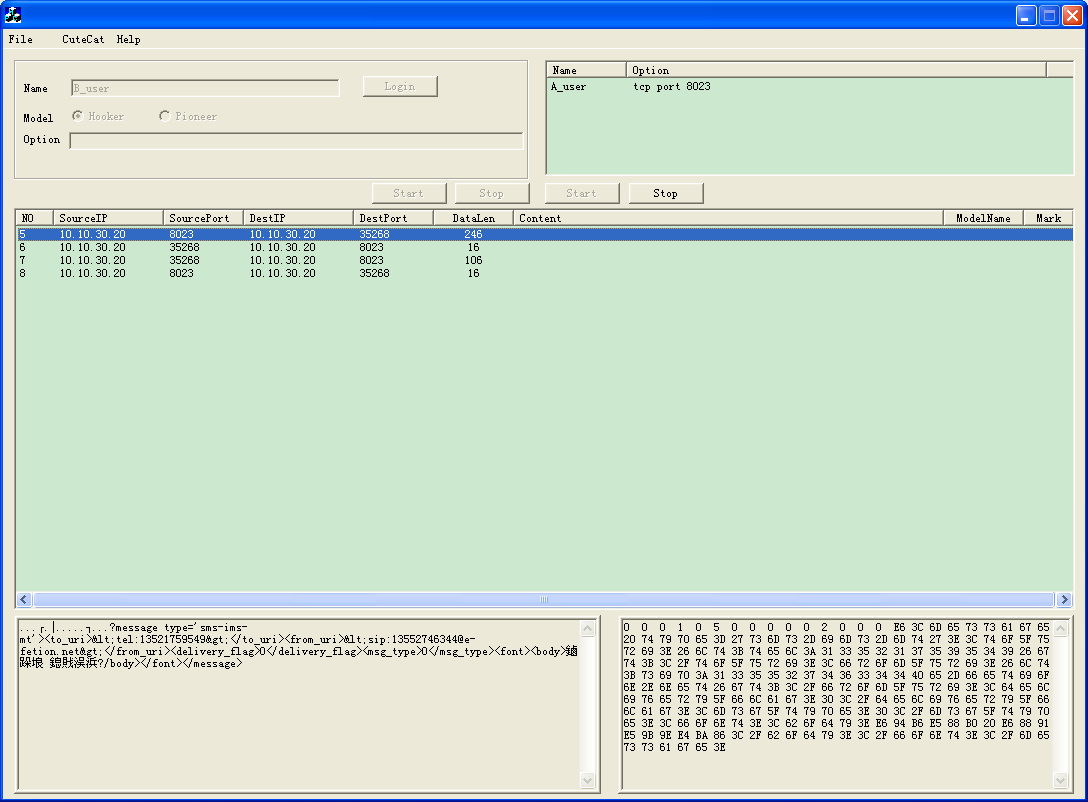
2: 在linux 服务器上， SeeSee 服务器端已在运行。

3：此时为了实时跟踪TCP数据，user1启动客户端，[name]栏输入名字，登录服务器端，成功model 栏变成可选，选择pionner,此时opition变成可写，输入抓包条件tcp port 8023,然后点击[start],右栏会出现“A\_user tcp port 8023“字样，此时A 与B 进行通讯，就会抓到相应数据，如图示：

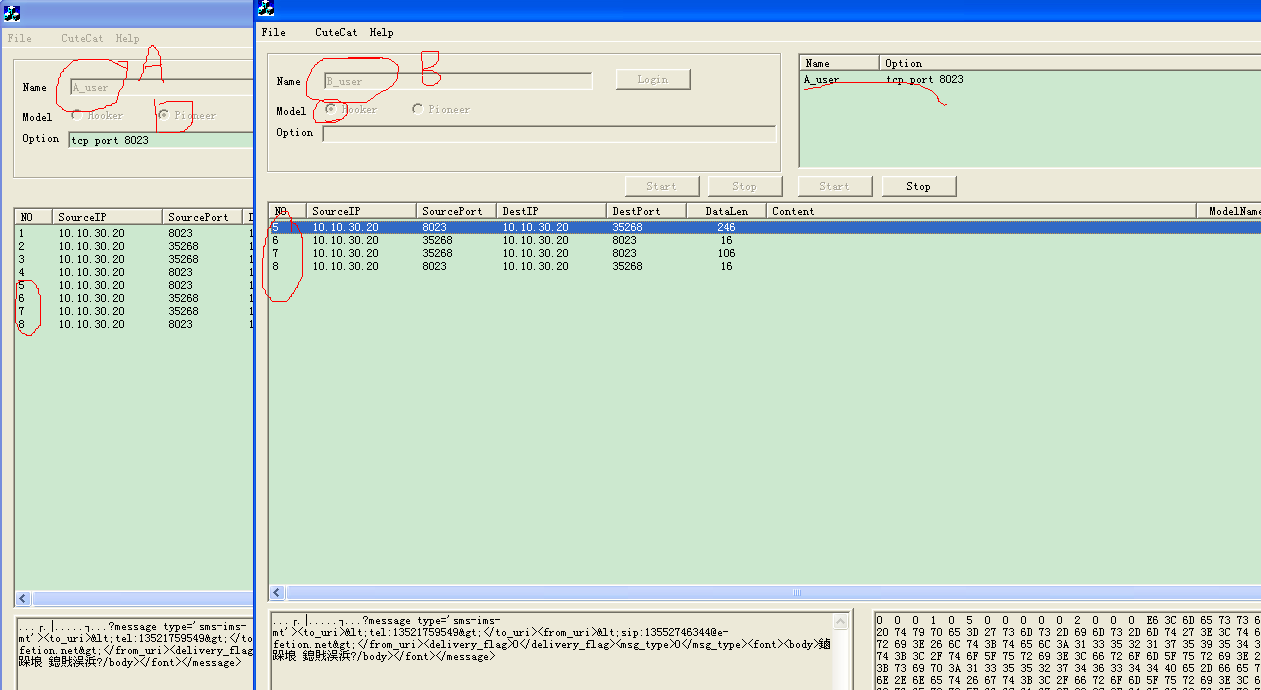


这是一条短信的交互情况，点选记录，下面会详细显示包的16进制和字符串格式，可以看出是13552746344发给13521759549的一条短信。

4：若user2也要查看TCP数据，也可以起动客户端，同样[name]栏输入名字，登录服务器端，成功model 栏变成可选，选择Hooker(此为默认选项)，右栏会同样看到“A\_user tcp port 8023“字样，点击选择此记录，看到[start]变得可用，点击[start] OK，此时再发一条信息，会看到user2也收到同样的信息。如图示



User2用户界面记录是从5开始的，这时user1 user2 数据就是同步的。如下图所示user1 user2二个界面



**七、其他说明**

1：服务端程序启运需要Root 权限。

2：抓包条件（opition）同Wireshark, 本软件与Wireshark使用同一抓包库pcap

应用举例:

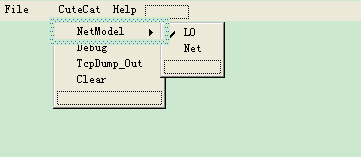
ip dst host 10.10.20.133

ip dst host 10.10.20.133 and port 6666

tcp dst port 8804 or src port 8023

tcp dst port 8023 or src port 8023 or dst port 8020

3：关于网卡模式，本系统支持环回地址上的抓包，当模块都在服务器端时选择[L0]，如下图，否则选[Net]。



八、参考

本软件运用了pcap开源库，iksemel XML开源库，MFC 界面库，并借鉴了源码tcpdump中打印输出，iksemel Base64 相关函数。

八、总结

本软件本人业余爱好之作，由于个人能力及投入精力有限，本软件还在不断完善升级中，软件难免存在不足之处，望指正。联系人：宋延涛 sytwss@163.com