# Informix 数据库协议分析

## Informix数据库安装

Informix是IBM推出的一款关系型数据库。目前informix版本为12.10。我们这次研究的数据库是informix 12.10 developer version。

由于缺少资料，导致在ubuntu 16.04 lts上安装informix数据库遇到了很多的困难。根据IBM官网和自己的尝试，我总结的步骤如下：

1，在https://www.ibm.com/analytics/informix 上注册并下载informix。注意在注册时要填写自己所在城市，街道，邮编。否则将无法下载。

1. 解压下载文件。
2. 创造informix用户和用户组：由于informix利用pam技术登录，所以这个账户就是登录informix数据库的账户

sudo groupadd informix

sudo useradd -g informix -d /opt/informix -m -s /bin/bash informix

1. 在解压后的文件中，执行sudo ./ids\_install -i gui，打开gui安装界面。按照提示安装即可。
2. 切换到informix用户。否则会有非常多的bug出现。
3. 网上很多文档都是过时的，现在的informix不需要配置类似config.std也可直接运行。

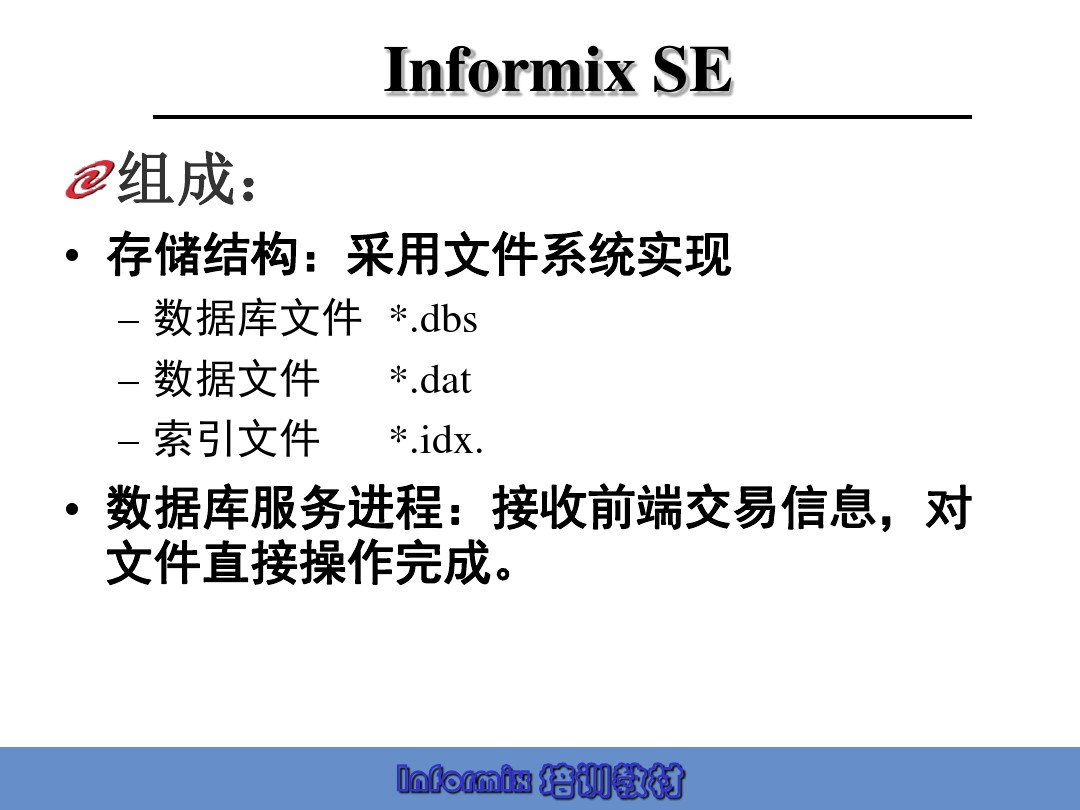
把source /opt/Informix\_Software\_Bundle/ol\_informix1210.ksh命令写入.bashrc，这样开机会自动加载环境变量。

1. 执行oninit -i初始化，查看onstat -i，如果出现如下图的情况，说明安装成功。

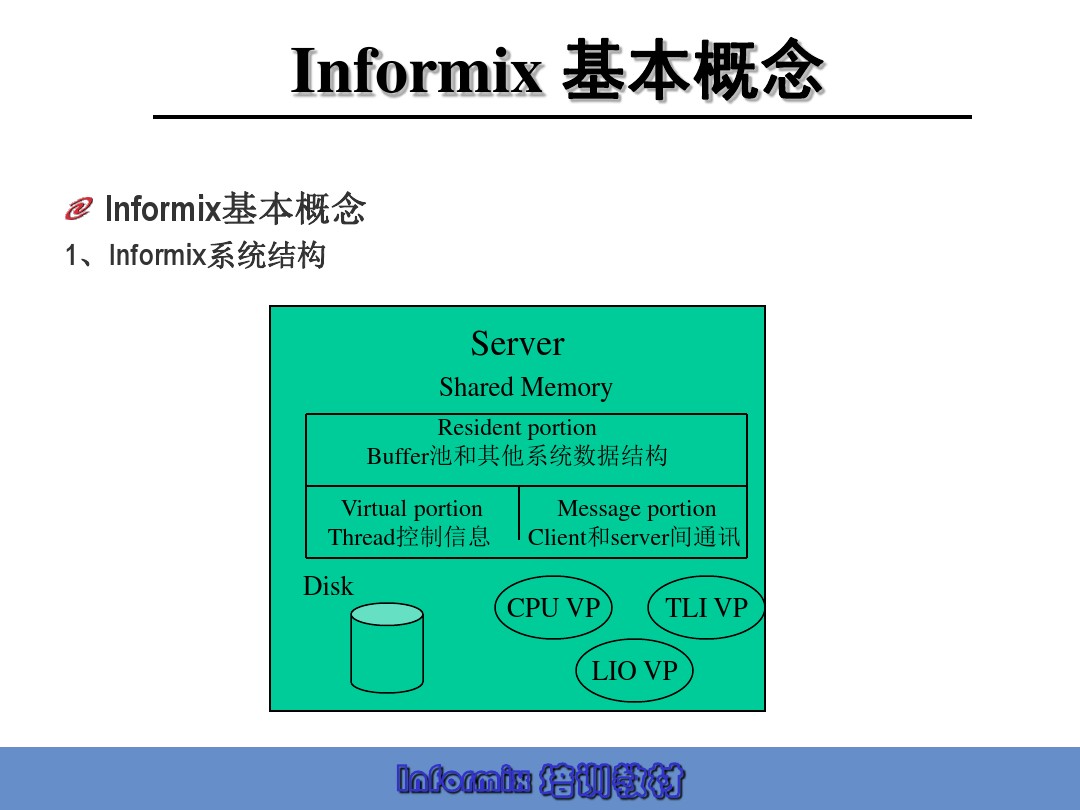
## 

## Informix系统基本介绍

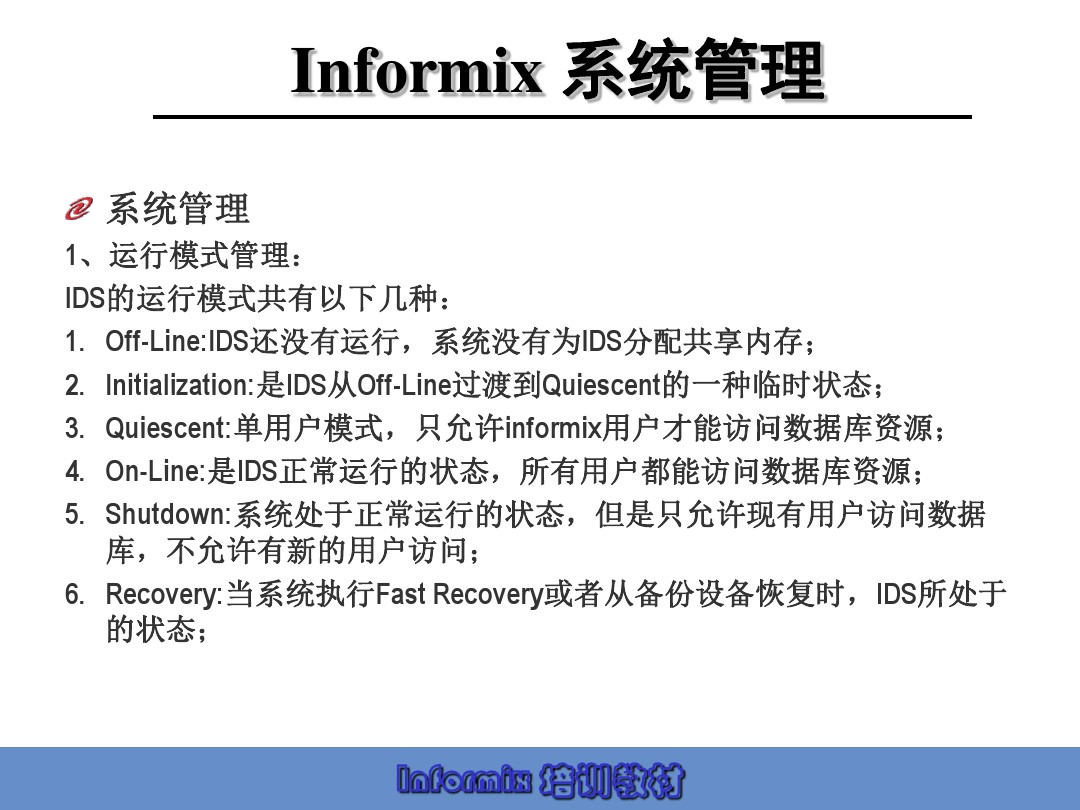
根据网上的资料，informix基础和其他的数据库没有什么不同：



Informix主要分为三类vp（虚拟处理器），处理进程，shared memory以及实际的disk。



这些都和其他的数据库没有太大的区别。真正区别在于informix的运行模式：



所以和mysql或者sqlserver直接用守护进程的方式连接不同，informix必须手动启动才能正常工作。具体的状态用onmode指令切换：

onmode -ky  完全关闭数据库 (y是对一切回答为yes,去掉提示)

onmode -sy  宽限的切换到静态方式

onmode -uy 马上切换到静态方式

onmode -my 从静态方式切换到联机方式

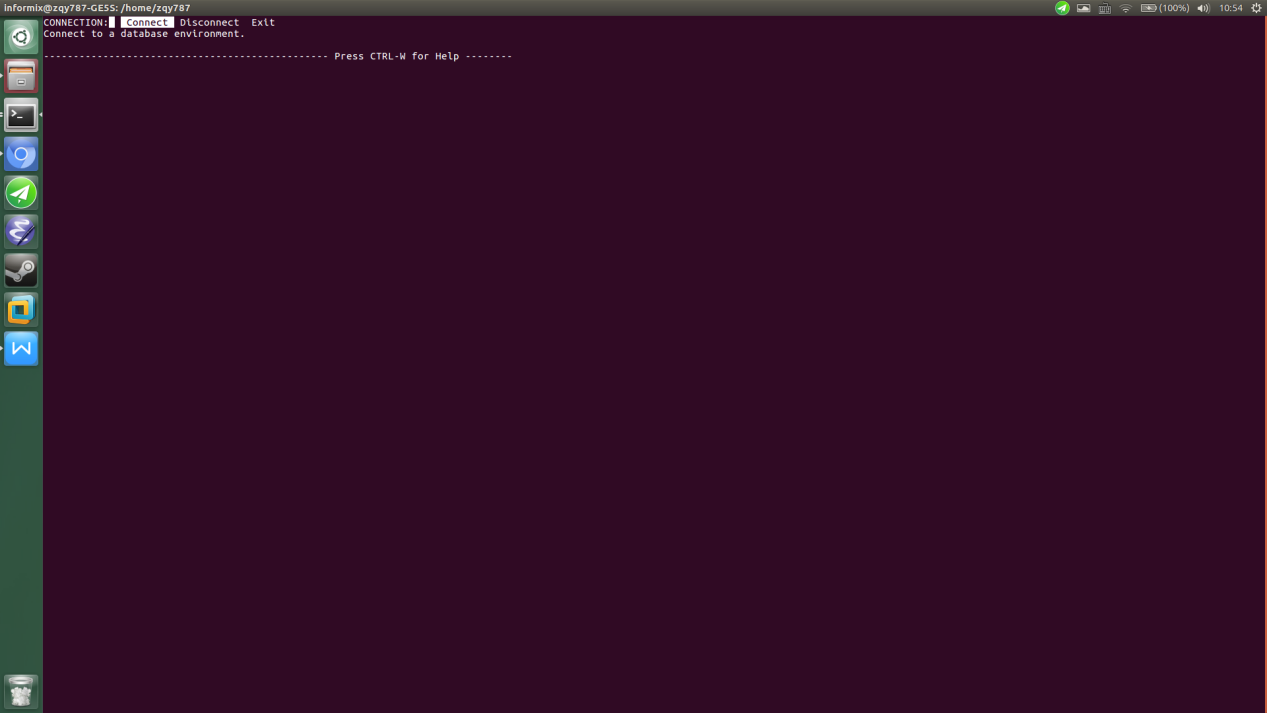
说明：联机方式：用户可以连接 (可以用onmode -uy切到静态， 用onmode -ky关闭)   
           静态方式：用户不可以连接，但可以使用实用程序进行访问IDS  (比如onstat)  (可以用onmode -m切换到联机)   
           完全关闭：没有启动服务，什么都不能访问(可以用oninit切换到联机) 

从脱机切换到静态方式：oninit -s  
 从脱机切换到联机方式：oninit -v  
 从静态切换到联机方式：onmode -m  
 从联机切换到静态方式(让用户完成处理，但不允许新用户连接)：onmode -s  
 从联机切换到静态方式(让所有用户对话立即终止)：onmode -u  
 从任何方式切换到脱机方式(让所有用户会话立即终止)：onmode -k

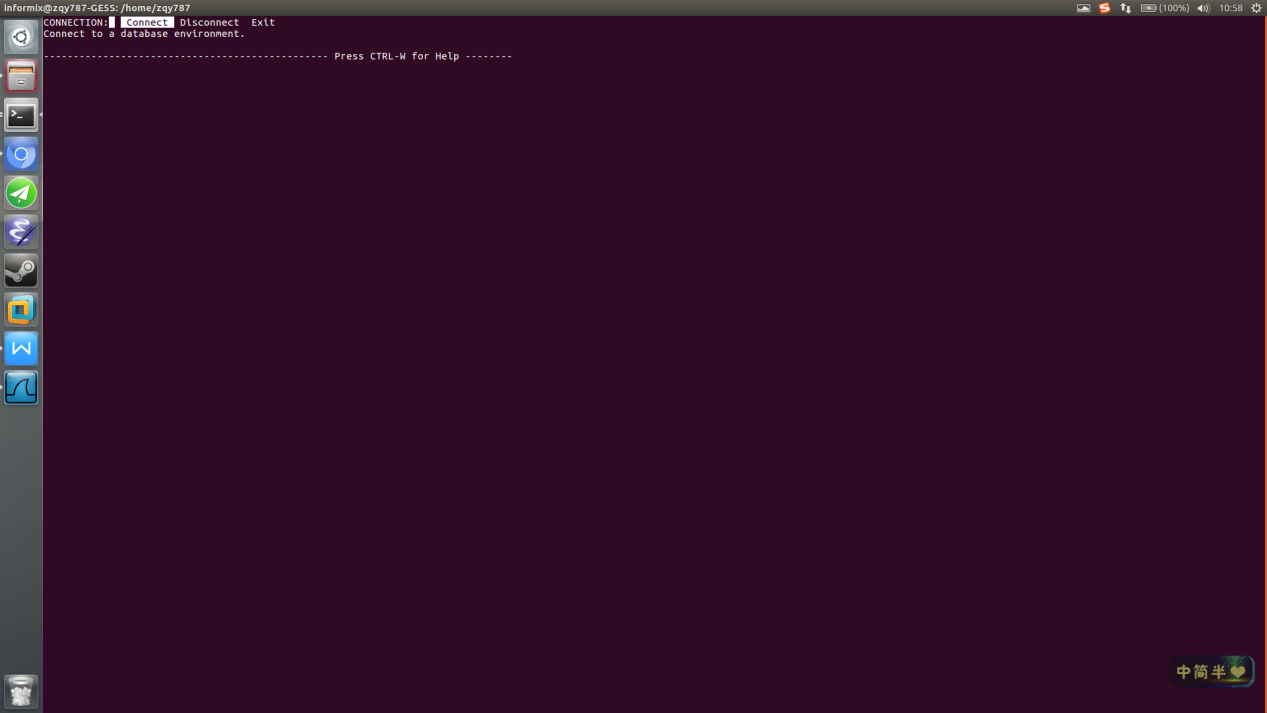
## Informix连接协议分析

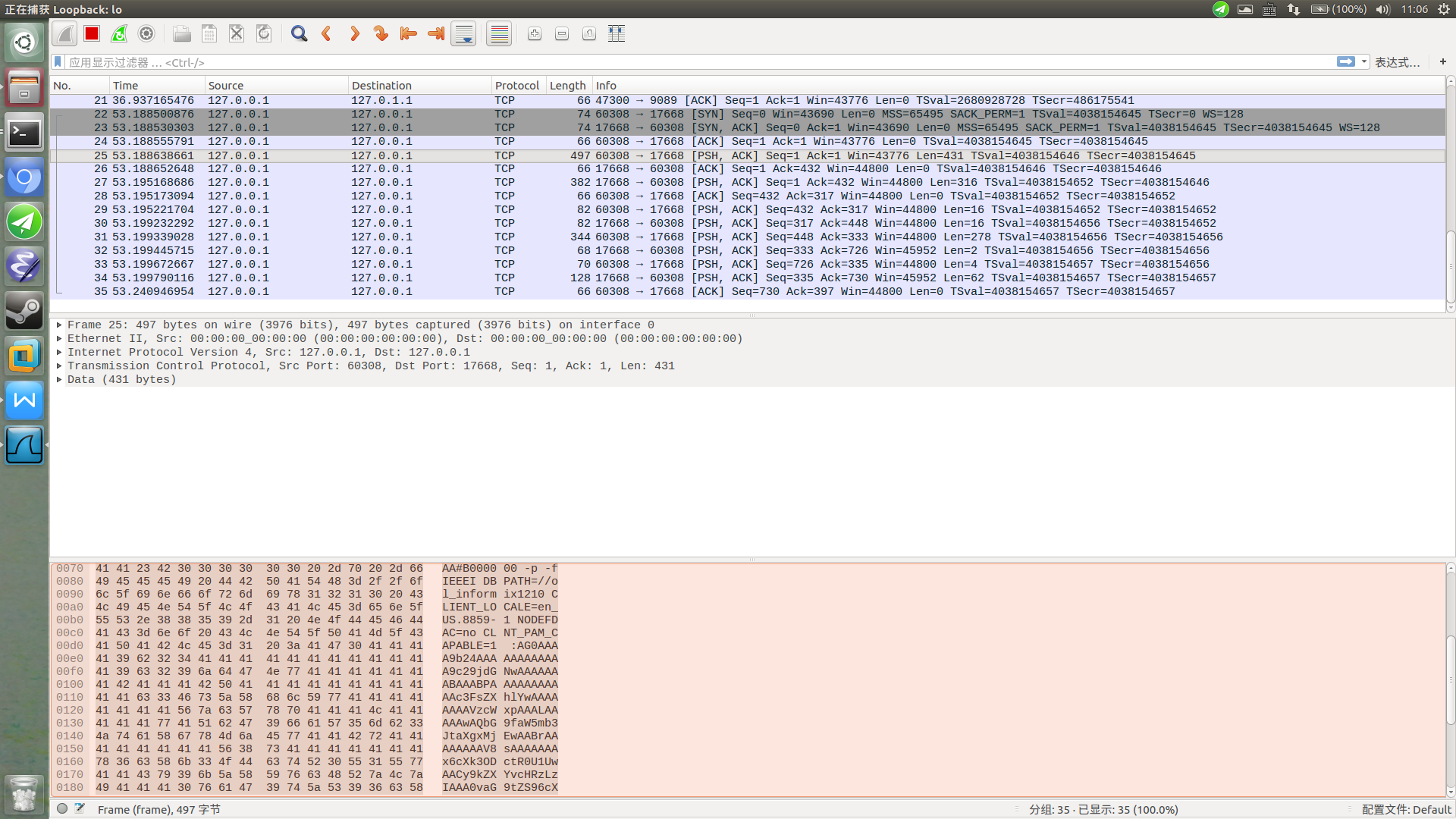
连接数据库用dbacess命令连接。由于采用了pam技术，所以dbacess不需要再进行账户认证。因此，在登录阶段，并不用利用通讯技术去提供账号密码。所以这一阶段没有协议进行分析。

进一步分析我们发现，在dbacess中提供了一种类似登录的接口：



由于这个是在客户端登录，我们猜测是有连接的。因此我们尝试输入informix的账号与密码，并用wireshark进行抓包：



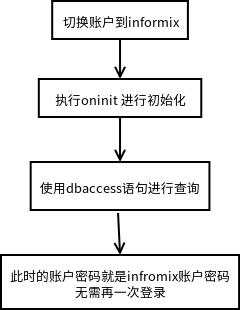


可以看到，我们并没有使用什么协议，而是简单的利用tcp传递了一个命令进行登录而已。并且我们发现，在账号密码错误的情况下，我们并不会发包。因此我们明确了内部登录流程：

利用PAM技术查询账号是否存在 -> 不存在直接报错，连接断开。 -> 存在则生成一条登录命令，包装在tcp内部发送。

现在还不清晰时候这个技术也是直接利用了PAM现有的框架进行操作的，但是我们认为可能性很大。

登录流程如图：

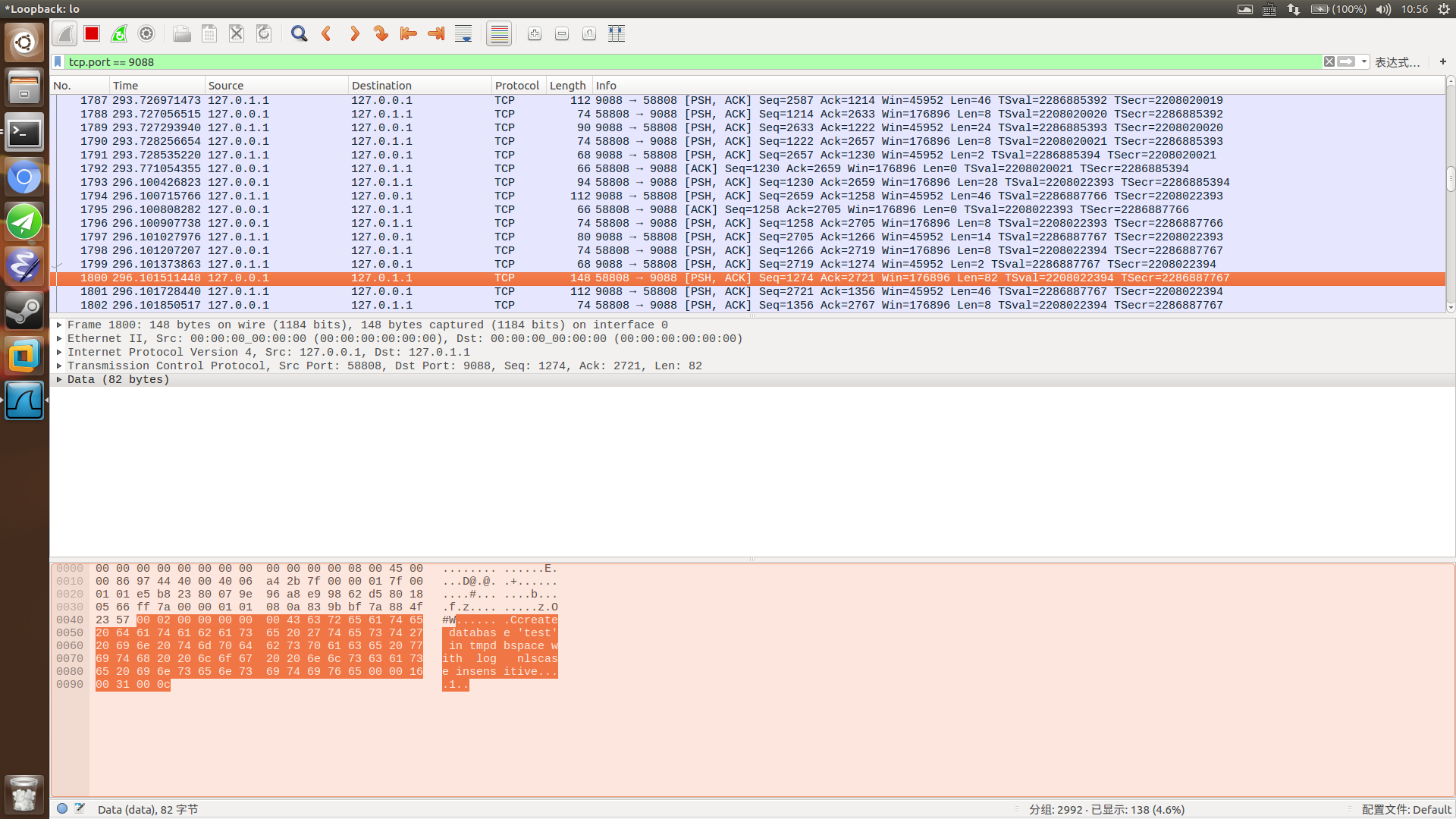


所以想要获取informix账户用户密码，我们只需要获取操作系统的账户名密码即可。

## Infromix 通讯协议分析

根据相关文章，informix使用的是drda通讯协议。和db2协议一样。

自己抓包发现，informix协议并不能被识别。但是我们可以手动对比，发现确实它使用的是drda协议。和db2数据库是一套协议 -- 他们都是IBM公司开发的，所以也可以理解。



虽然我们的wireshark并不能识别infromix的协议，但是对比可以看出infromix协议和db2协议一致。可以直接使用db2的分析。