1. 实验项目名称：

包分析实验，Wireshark包分析

1. Wireshark的使用
2. Wireshark获取dns数据包
3. Wireshark抓取ftp登录用户名和密码
4. Wireshark抓取Telnet密码信息
5. 实验原理：

Wireshark是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。

1. 实验目的：

练习Wireshark的抓包过程。查看数据包中的信息。

1. 实验器材（设备、虚拟机名称）：

SimpleSPC信息安全云实验系统，

Windows Sever 2008 R2

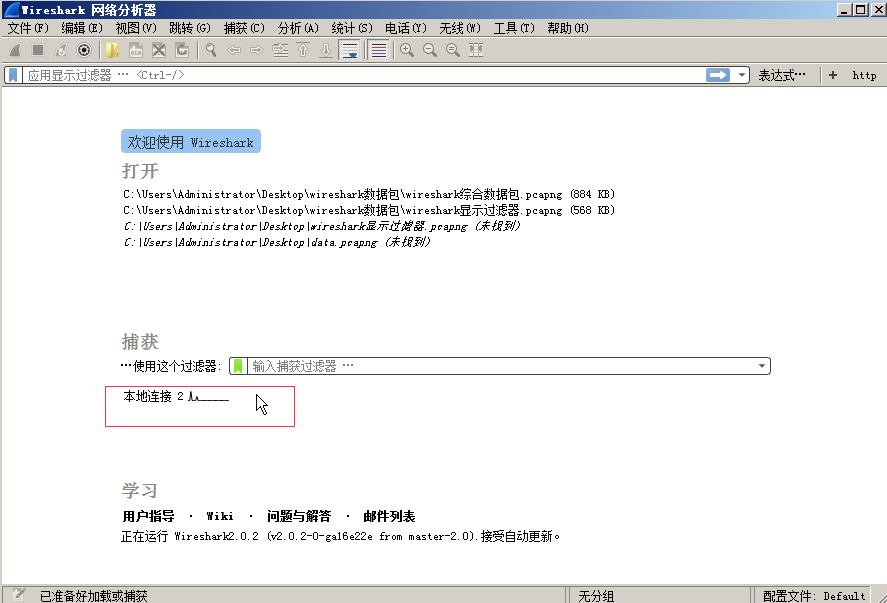
CentOS 6.5

1. 实验步骤：

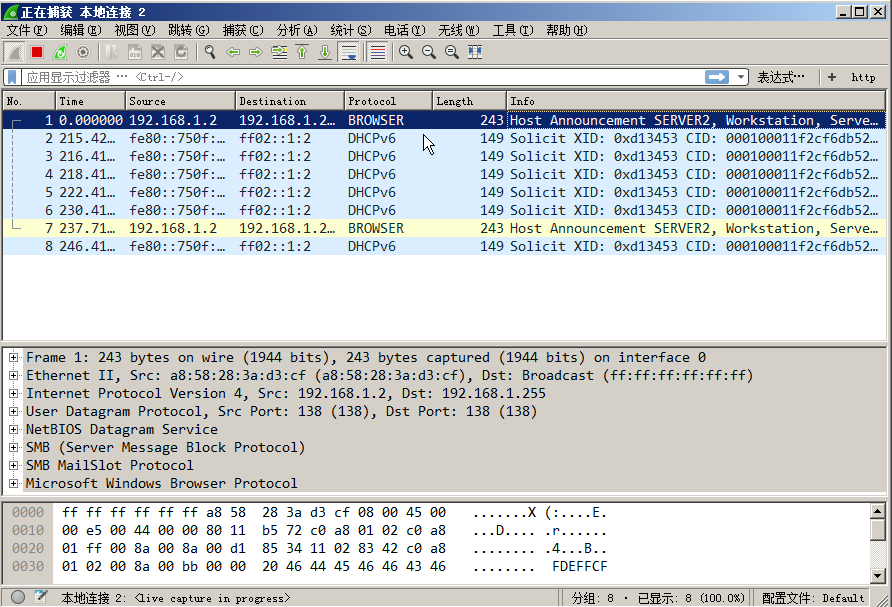
1. Wireshark的使用

1.1 双击运行“Wireshark”.

1.2 双击本地连接，开始自动获取数据包.



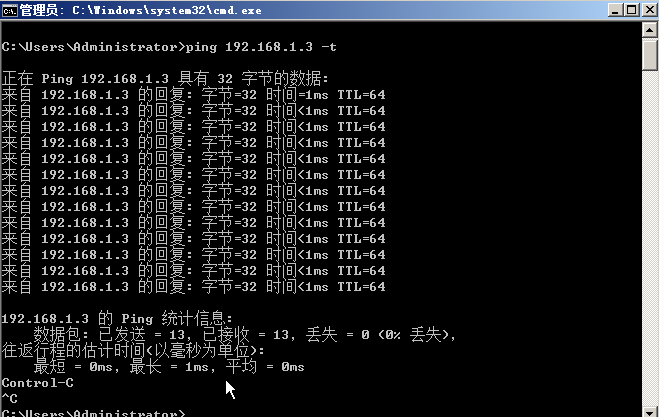
1.3 自动开始捕获数据包主界面.



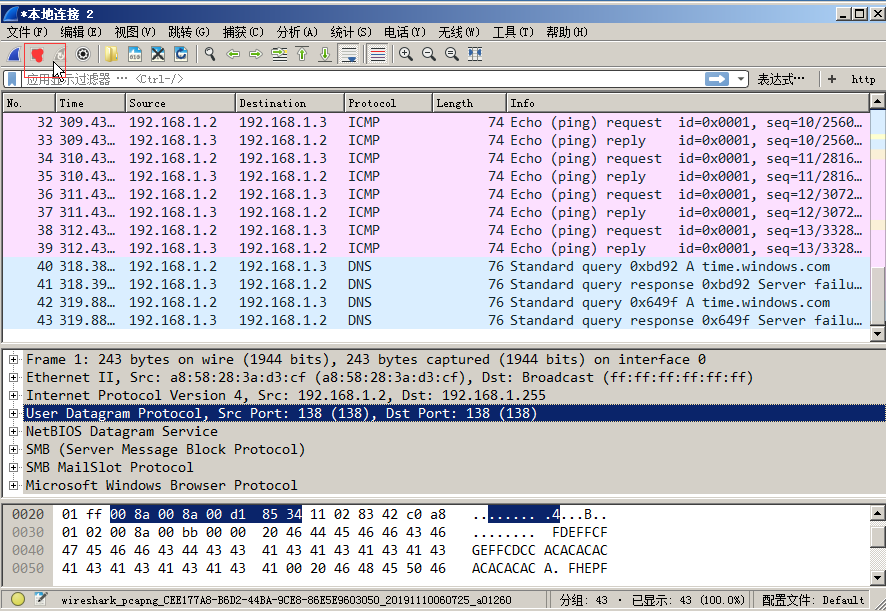
1.4 单击开始，在运行处输入cmd，打开命令行.

1.5 在cmd下输入命令“ping 192.168.1.3 -t”，并回车，

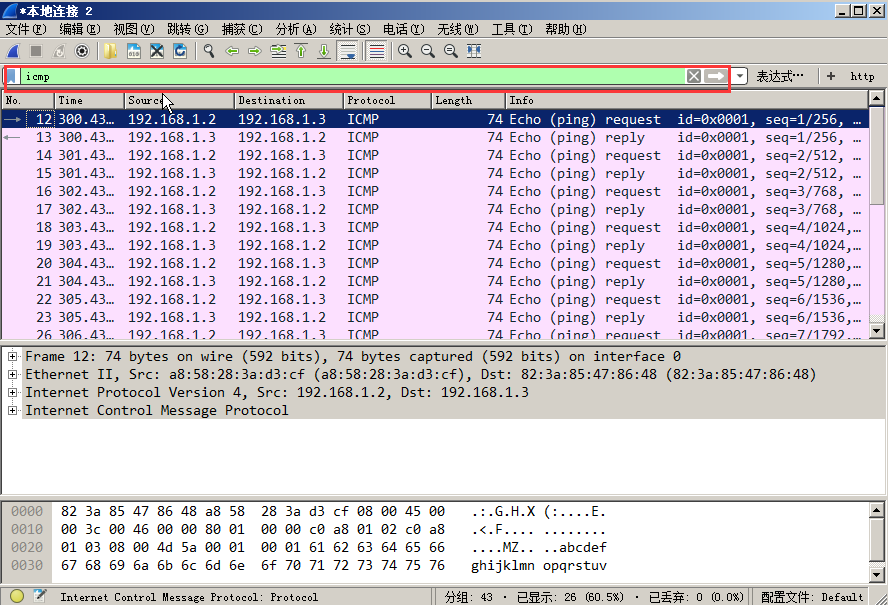
1.6按Ctrl+C停止命令，如下图所示



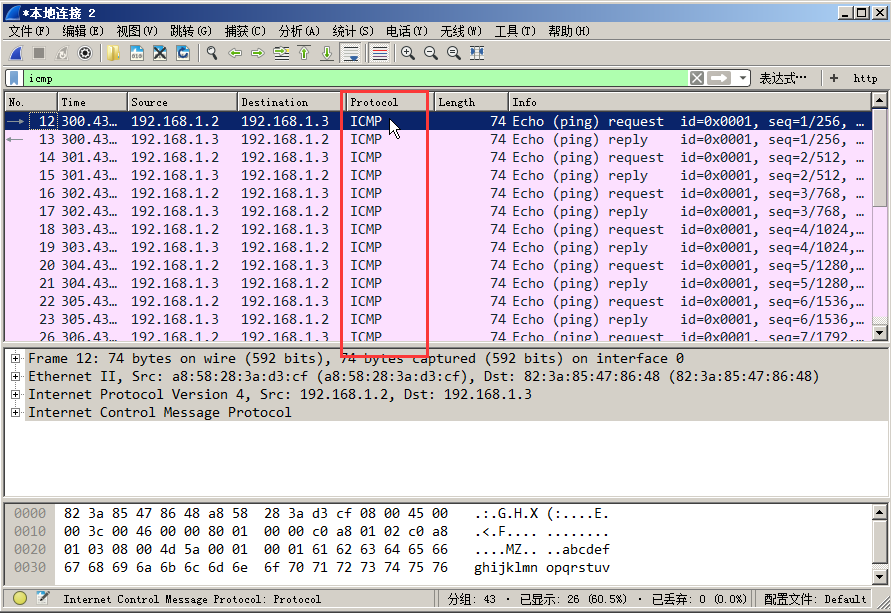
1.7 返回wireshark主界面，单击左上角红色正方形按钮停止捕获数据包，如下图所示：



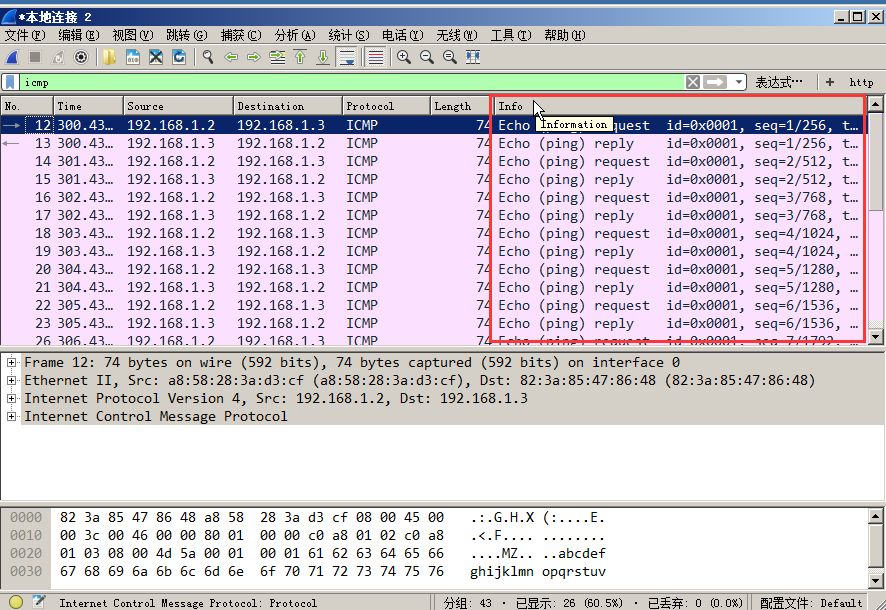
1.8 在显示过滤器中输入icmp.



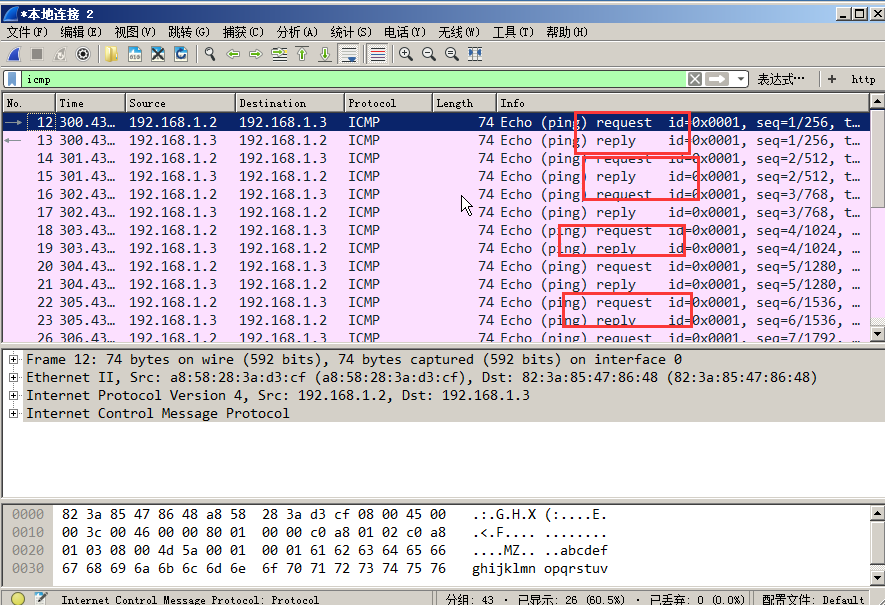
1.9 在显示过滤器输入命令后发先封包列表中，所有protocol变成了icmp协议的数据包.



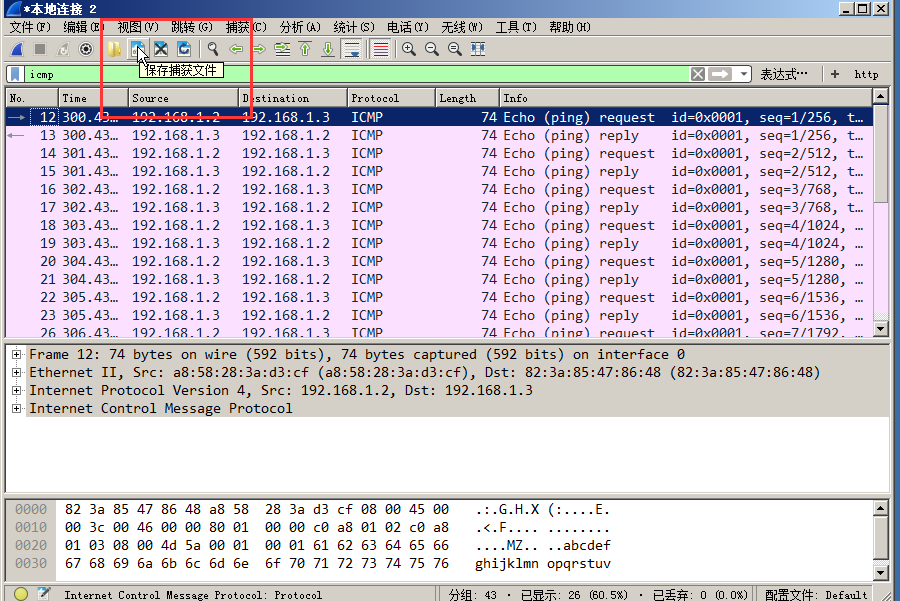
1.10 调整封包列表的条目大小，查看info信息.



1.11 通过显示过滤器的过滤，剩余的icmp全是关于ping命令的请求和应答.

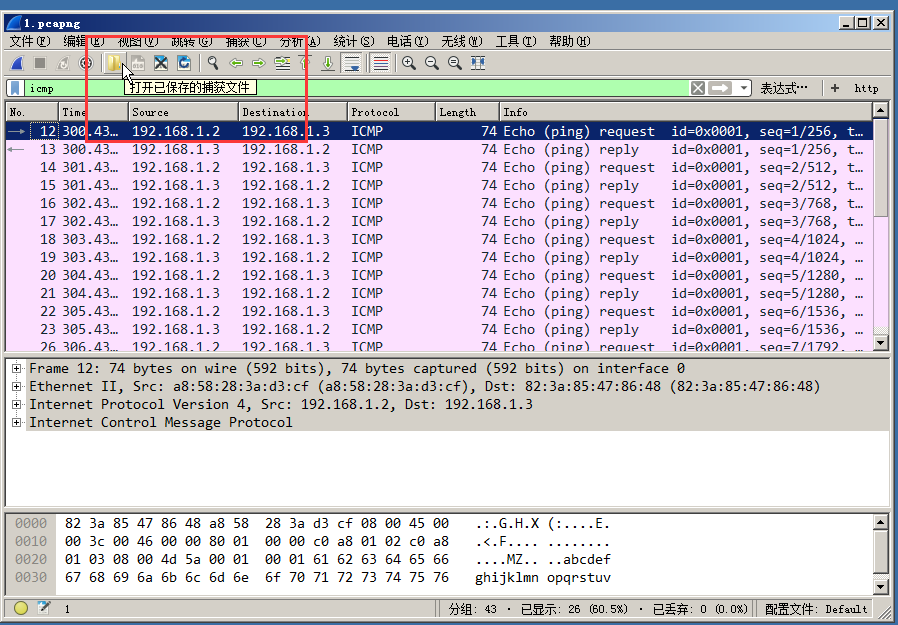


1.12 保存捕获的数据包，再次点击开始按钮或者点击“保存捕获文件”.



1.13 弹出保存文件窗口，选择路径保存.

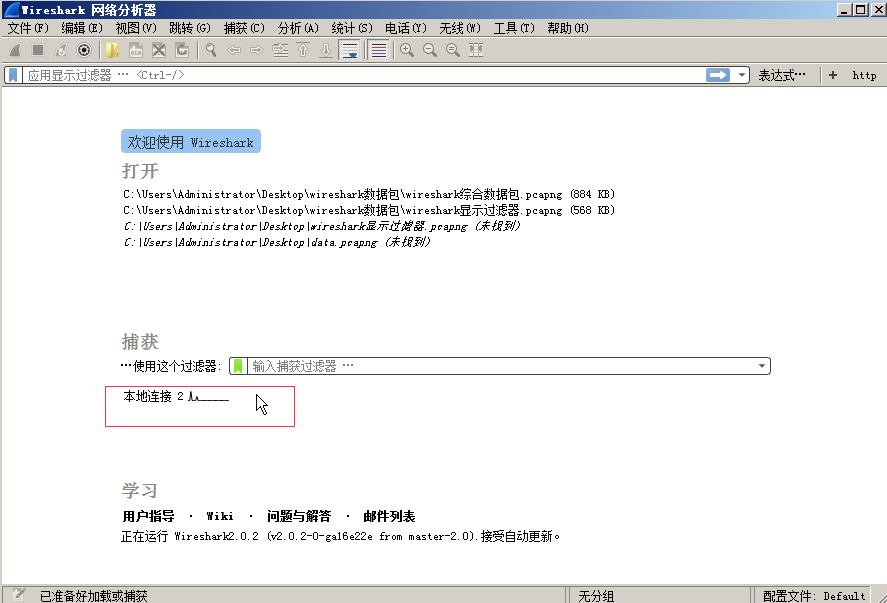
1.14 当再次想对该数据包进行分析时，点击“打开已保存的捕获文件”，即可打开上次保存的抓包信息.



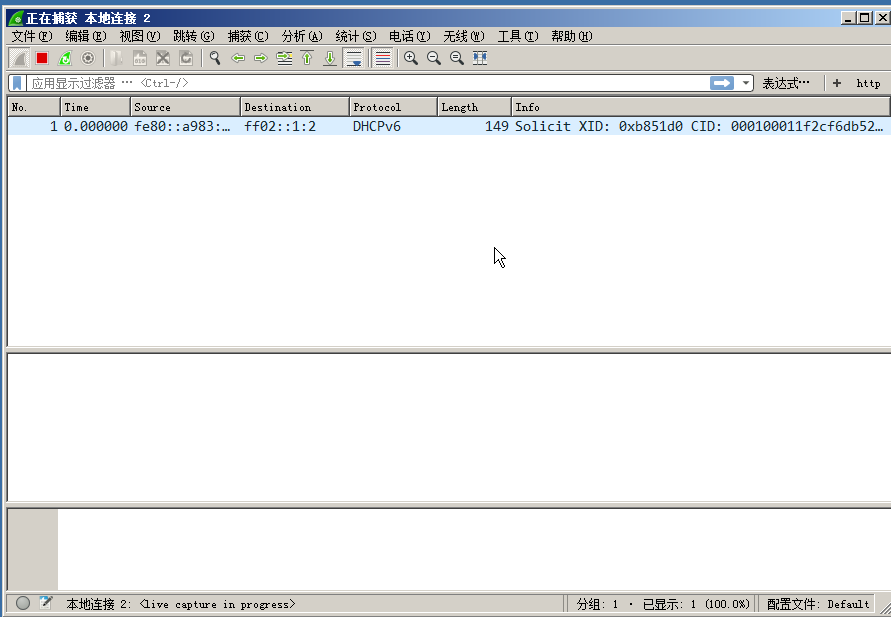
2. Wireshark获取dns数据包

2.1 双击“wireshark”图标.

2.2 双击本地连接.

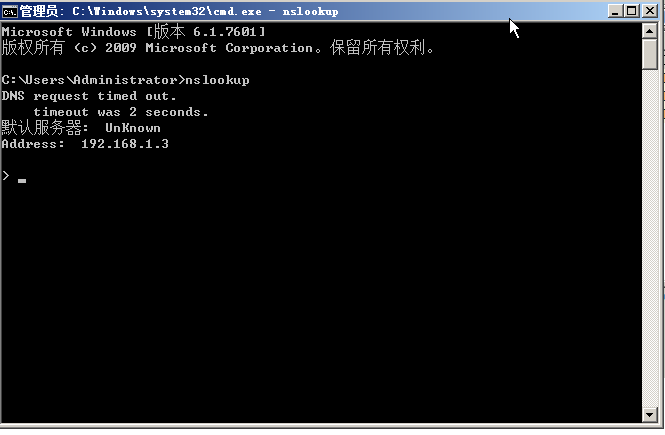


2.3 wireshark以本地连接为接口开始自动抓取数据包.

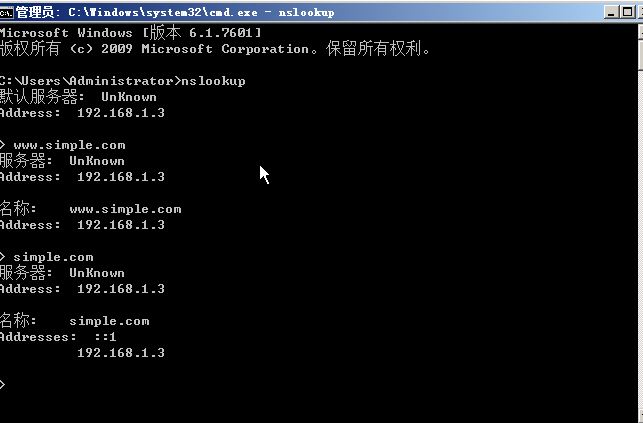


2.4 单击开始，在运行处输入cmd并回车.

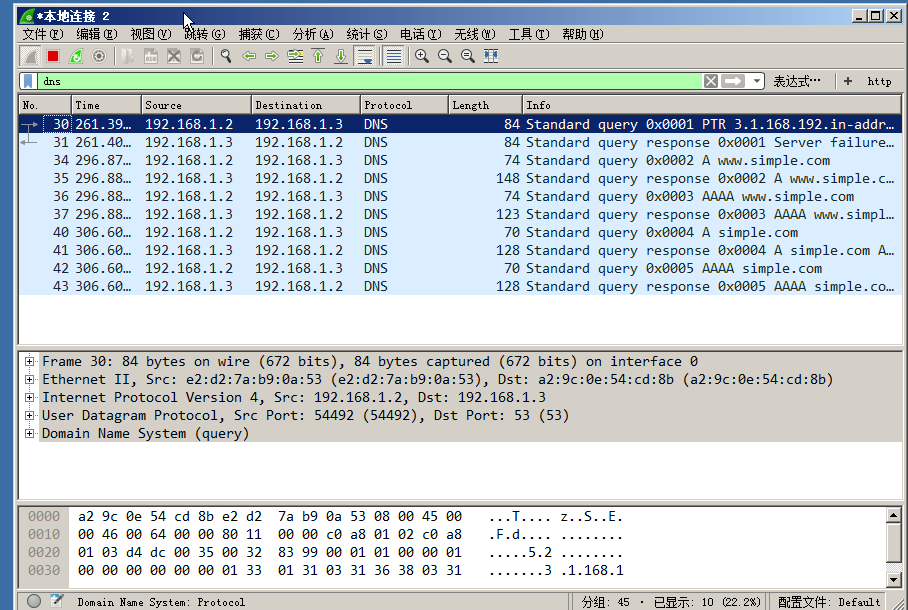
2.5 在命令行下输入nslookup，回车，进入nslookup模式.



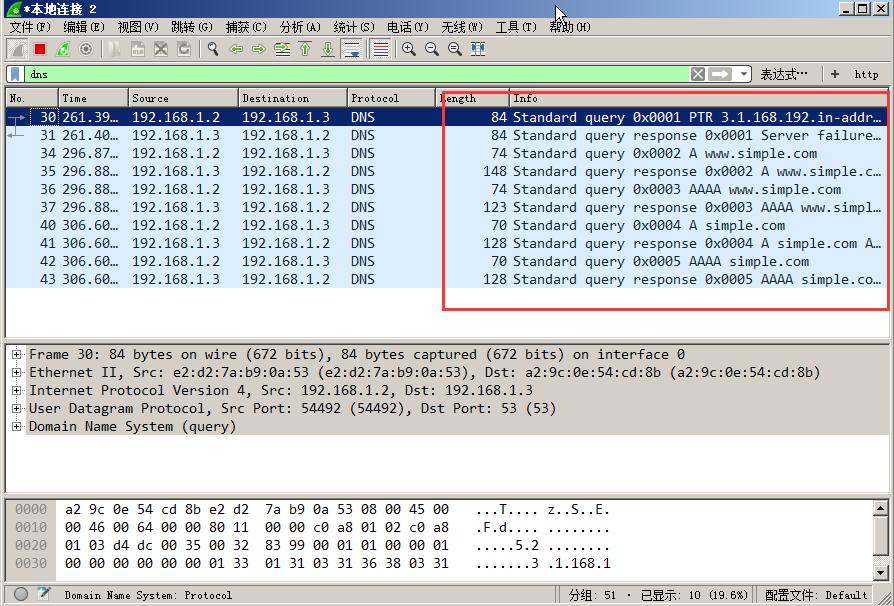
2.6 输入要解析的域名并回车，比如“www.simple.com”，“simple.com”



2.7 返回wireshark的主界面，在过滤器中输入dns.



2.8 查看info信息.根据下图中内容可以观察到dns的请求解析过程.

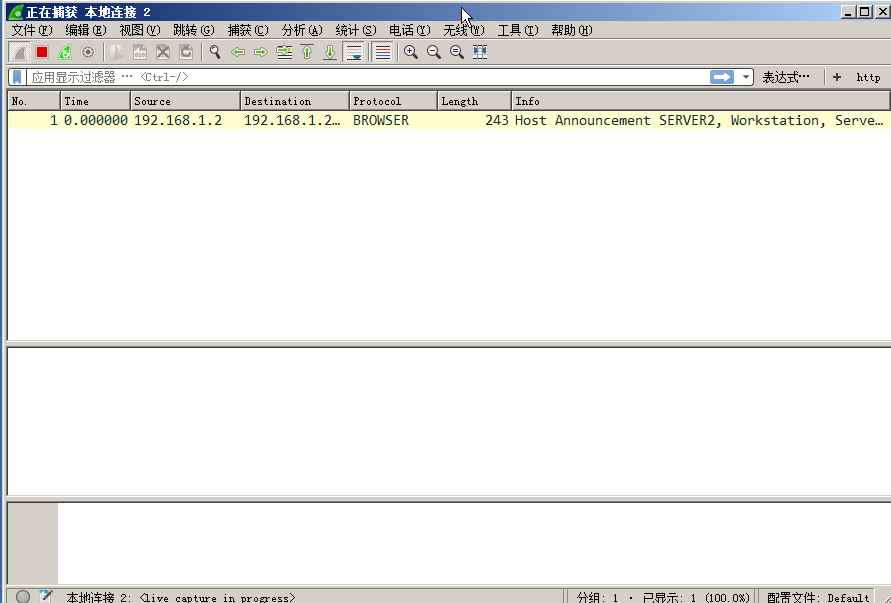


3.Wireshark抓取ftp登录用户名和密码

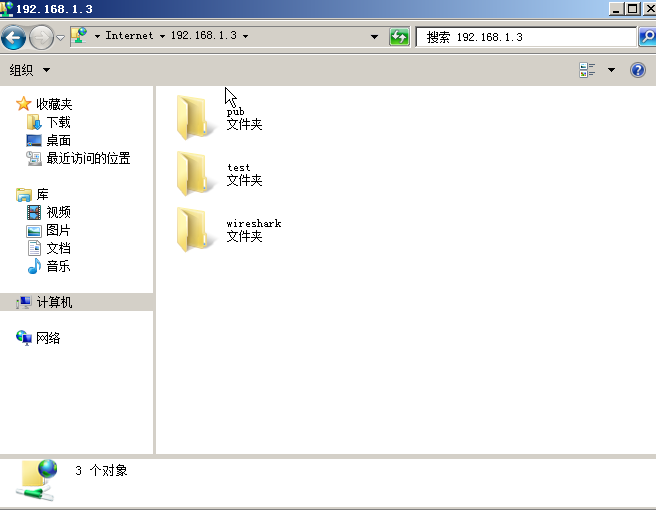
3.1 双击桌面上的“wireshark”图标.

3.2 双击本地连接.

3.3 wireshark以本地连接为接口开始自动抓取数据包.

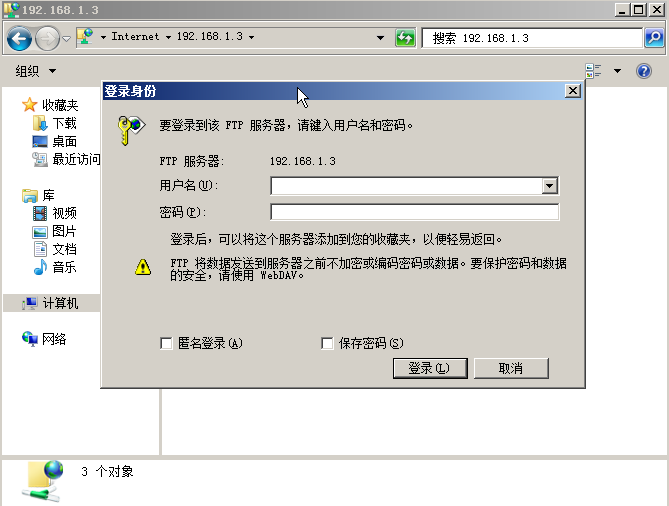


3.4 在桌面双击打开“计算机”，在地址栏输入ftp：//192.168.1.3 并回车.

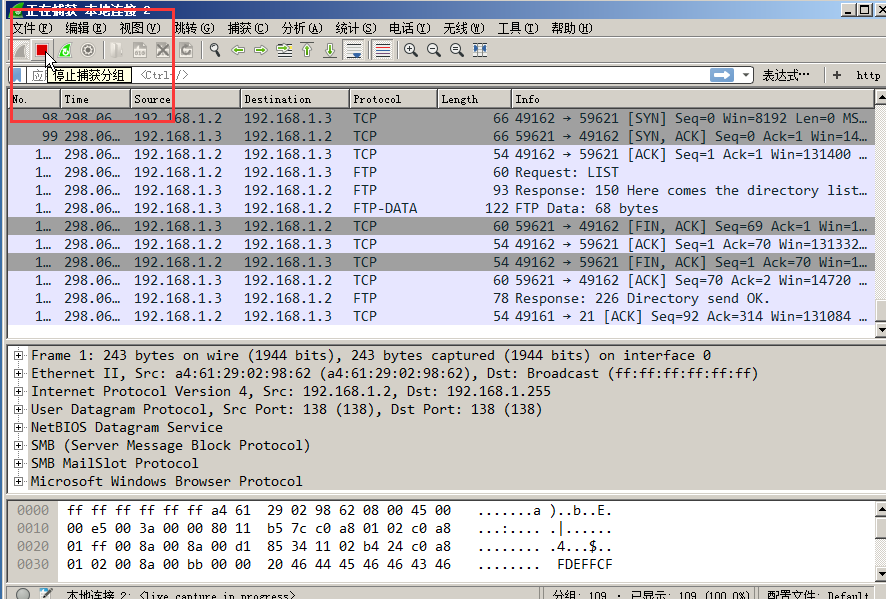


3.5 右键单击空白处，选择登陆.

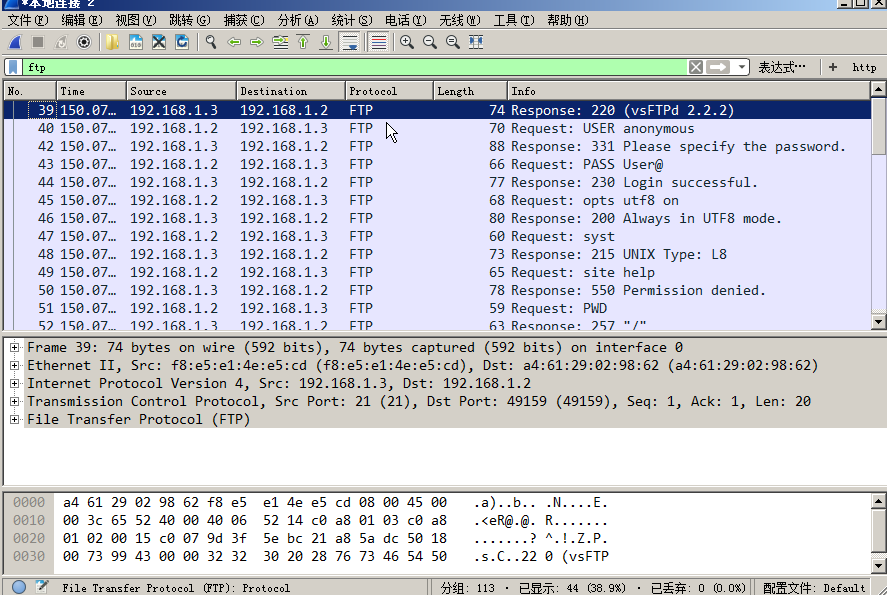
3.6 输入用户名：wireshark和密码Simplexue123.



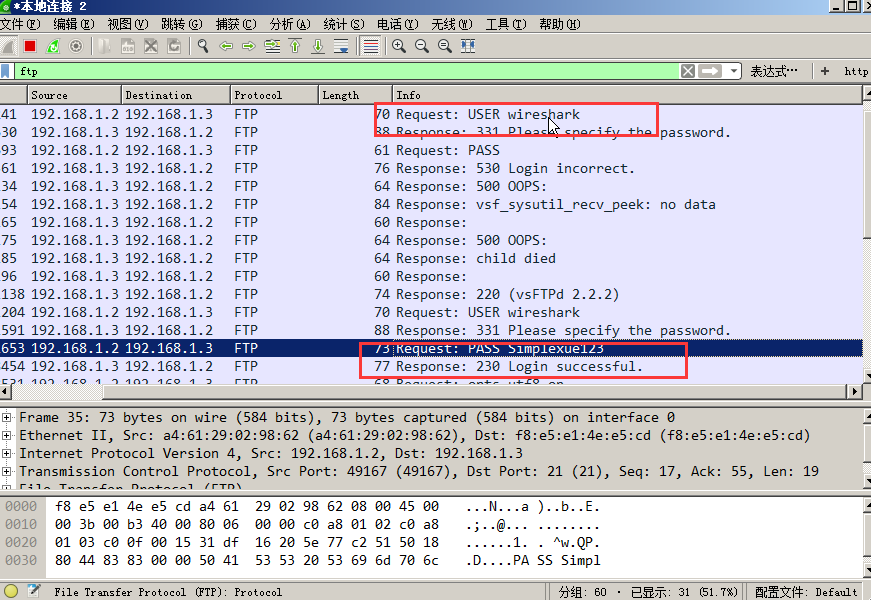
3.7 登陆成功后，返回wireshark界面，单击停止抓包.



3.8 在过滤器中输入ftp并回车，查看所有ftp协议数据包.



3.9可以看出输入用户名和密码后成功登陆.



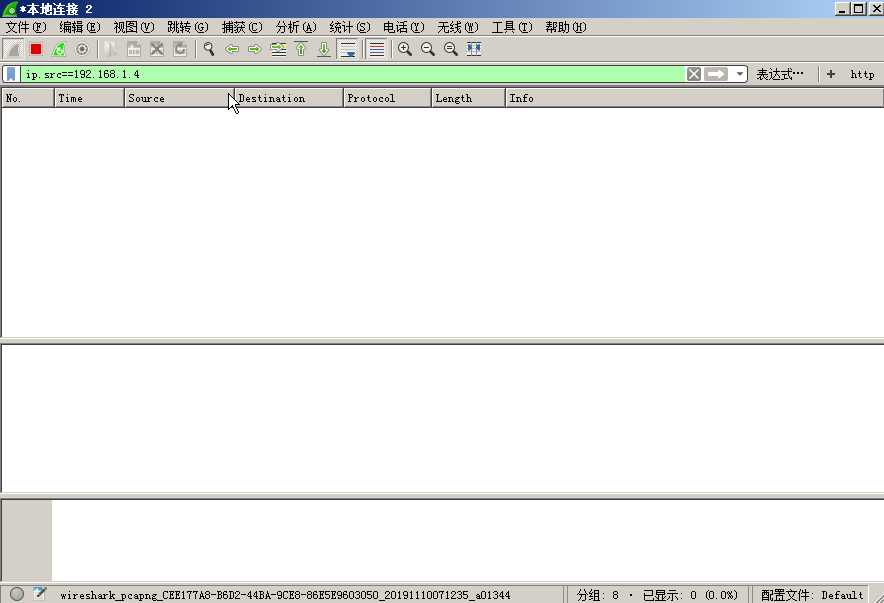
4.Wireshark抓取Telnet

4.1 双击打开wireshark.

4.2 双击本地连接.

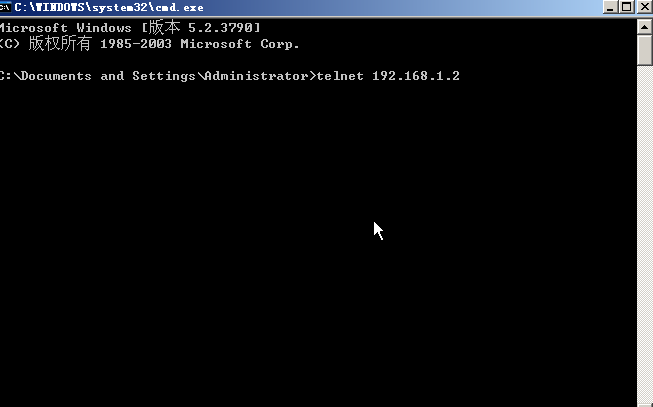
4.3 wireshark开始抓包

4.4 过滤器中输入“ip.src == 192.168.1.4”.



4.5 切换到用户机，192.168.1.4.

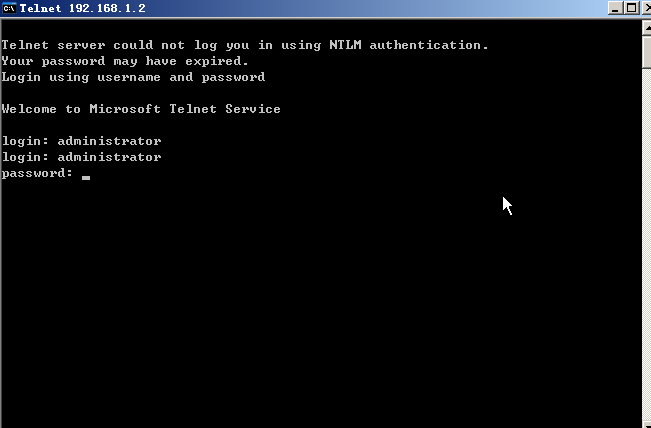
4.6 在用户机的cmd界面输入telnet 192.168.1.2 然后回车.



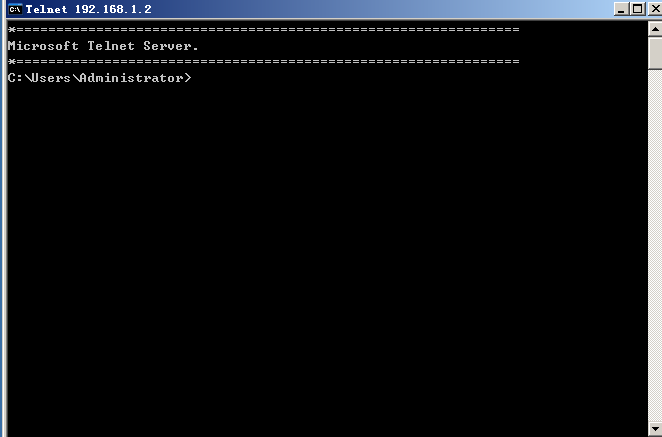
4.7 输入y



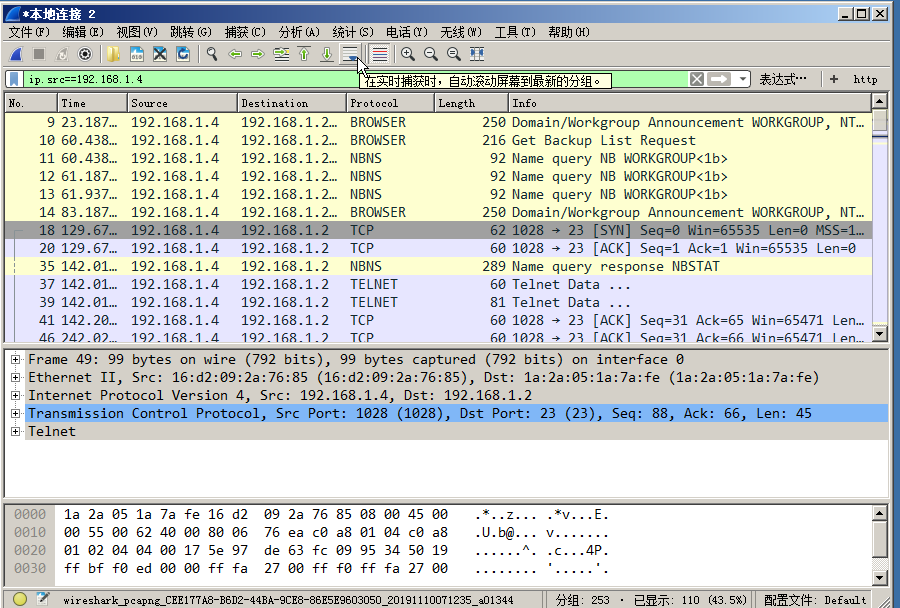
4.8 输入用户名“administrator”，密码“Simplexue123”



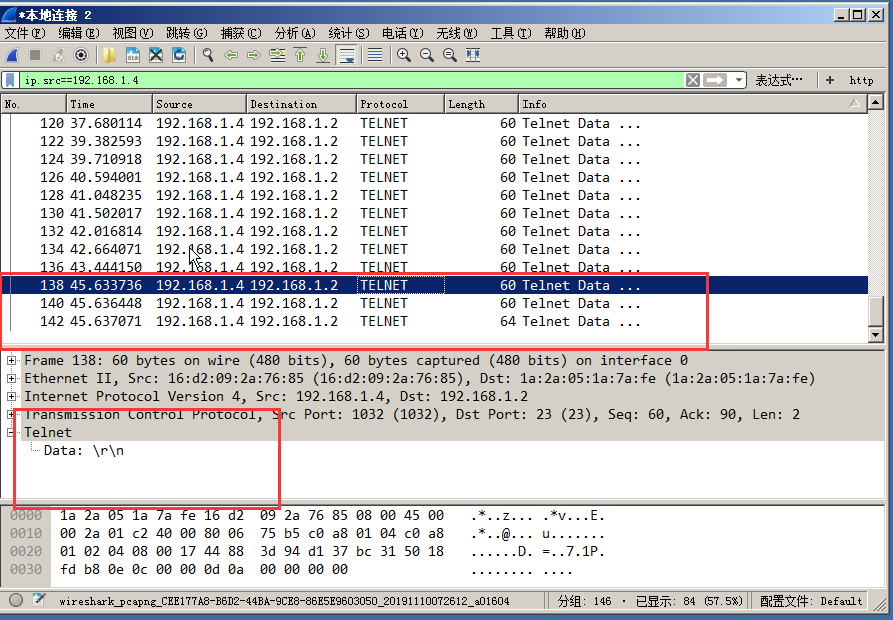
* 1. 输入密码后回车确认，如下图所示：



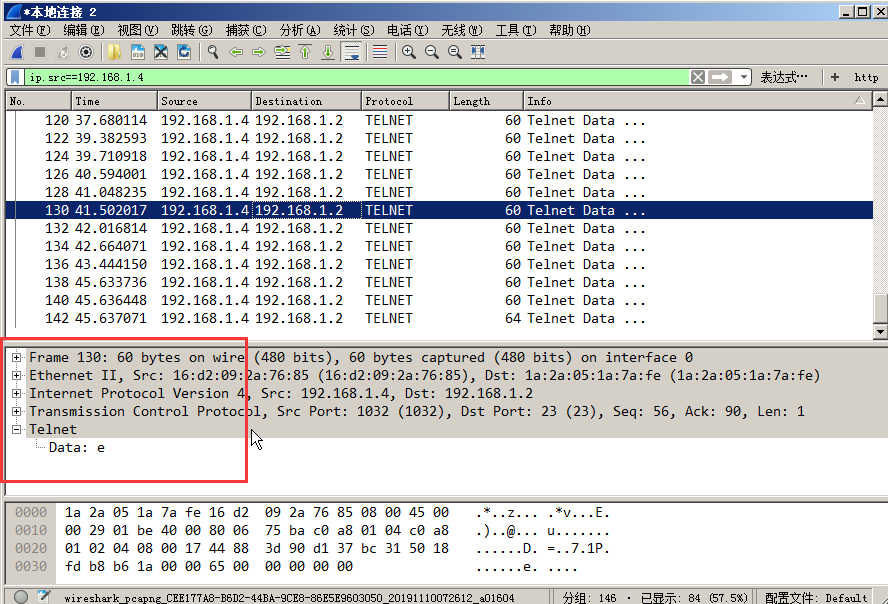
* 1. 返回192.168.1.2机器，在wireshark界面停止抓包.
  2. 单击转到最新分组按钮.



4.12倒着查看info的Telnet data信息，倒数第三个数据包中有data标签.



4.13 “\r\n”意思为回车，并重开一行，继续查看前面三行data信息，分别得到3、2、1.继续查看得到e.



4.14 将信息连起来就是用户名administrator和密码Simplexue123.

1. 实验结果及分析：
2. 总结及心得体会：