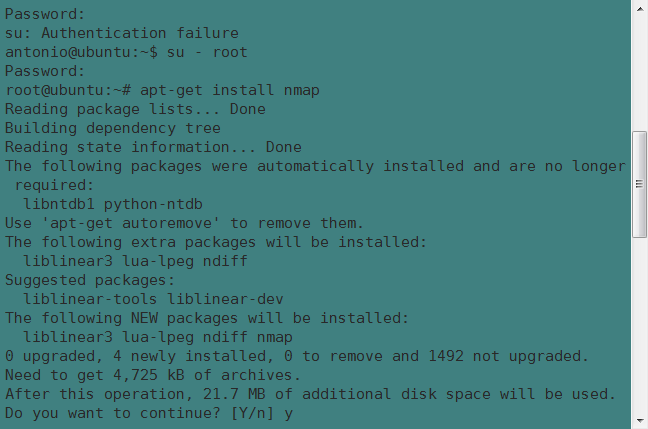
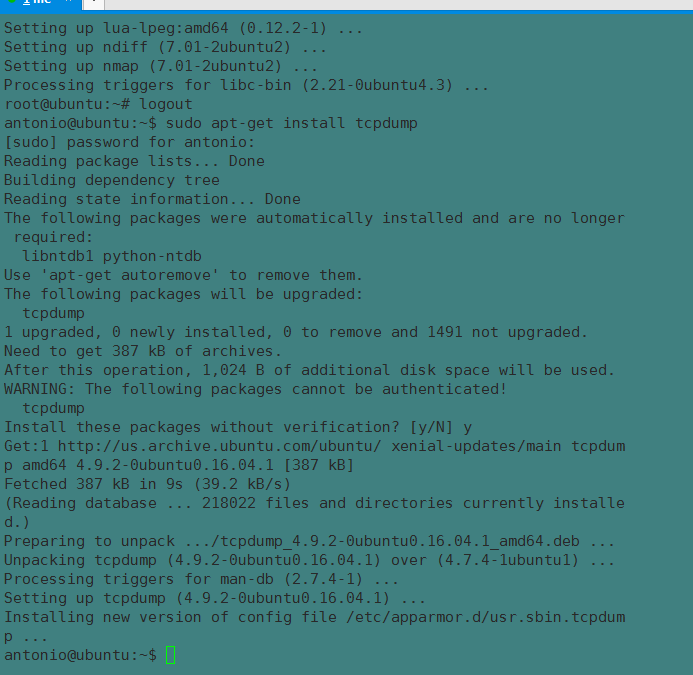
在**Linux**虚拟机上安装**nmap**和**tcpdump**。

提示：

*sudo apt-get install nmap*

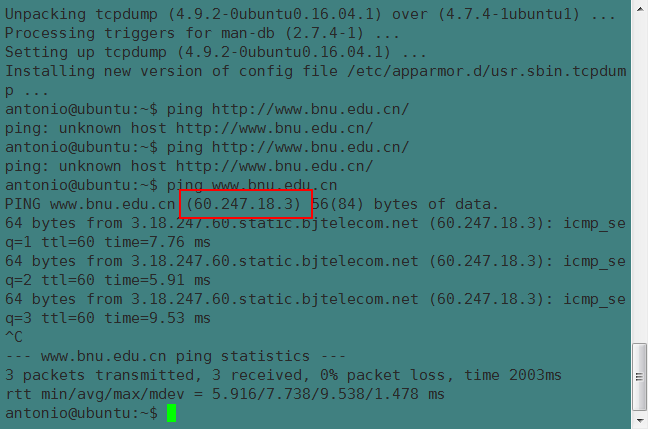


*sudo apt-get install tcpdump*



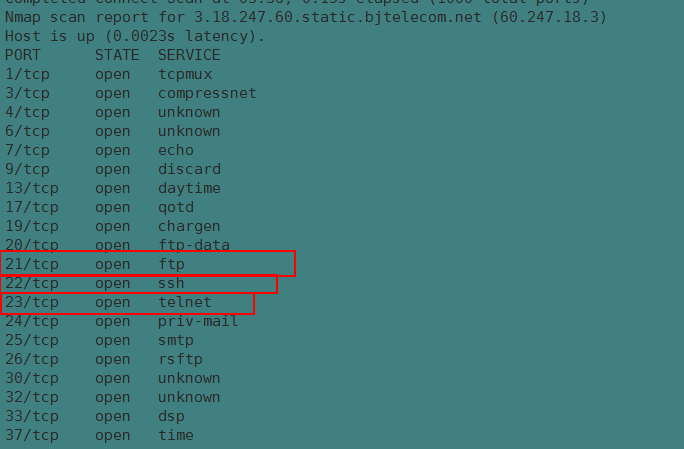
**2.** 使用**nmap**扫描端口。

1) 获得北师大官网的IP地址。如何从http://www.bnu.edu.cn/得到其IP地址？



提示：回忆实验1中的ping命令

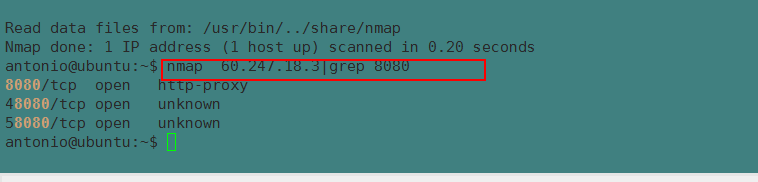
2) 扫描北师大官网所在服务器（以下简称“该主机”）的各个端口。该主机开放了哪些端口？每个端口各运行什么服务？举例说明3个即可。



如上图 北师大开启了21：ftp 22：ssh 23：telnet

提示：*nmap IP*地址

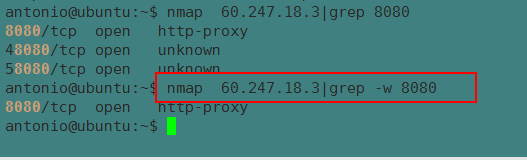
3) 如下命令的执行结果如何？请解释其原因。

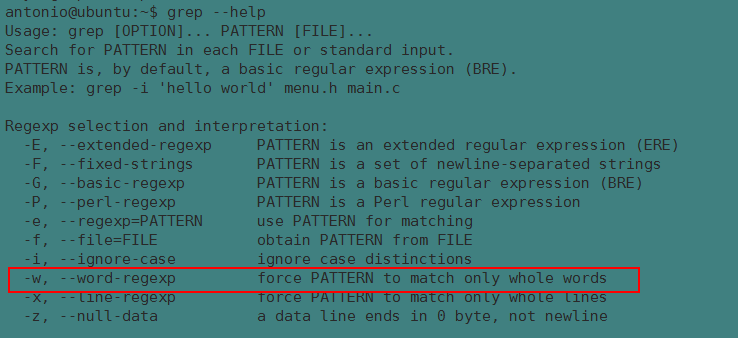


*nmap* 北师大官网*IP | grep 8080*

提示：管道命令| 、grep命令

4) 如下命令的执行结果如何？请解释其原因。

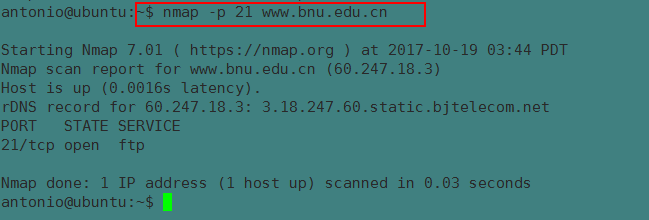




只显示已知的端口，如上图。

*nmap* 北师大官网*IP | grep –w 8080*

5) 扫描指定端口。如何只扫描该主机的80端口?请给出两种方法。



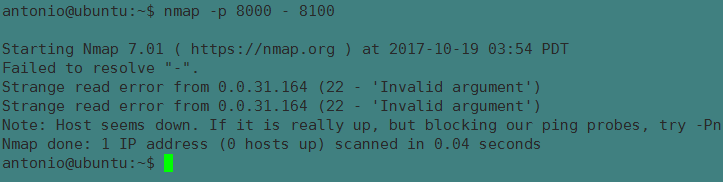
提示：

*nmap –p* 端口号



管道命令+ grep

6) 扫描指定范围的端口。如何只扫描该主机介于8000至8100这一范围的端口?



提示：*nmap –p* 开始端口*-*结束端口

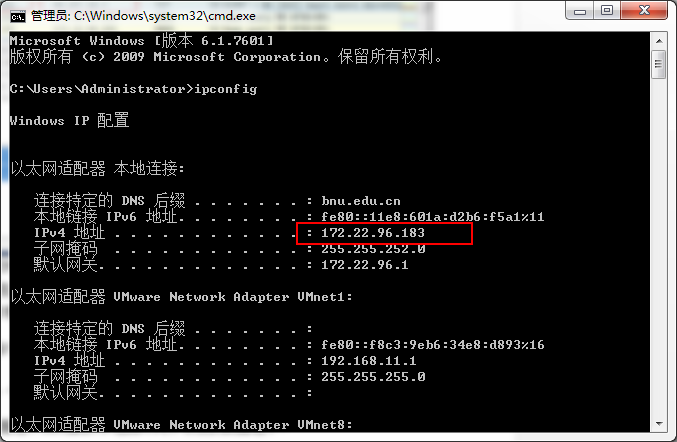
**3.** 使用**Wireshark**抓包。

1) 在Windows虚拟机上安装Wireshark。注意，在安装时，需要勾选“Install WinPcap”。

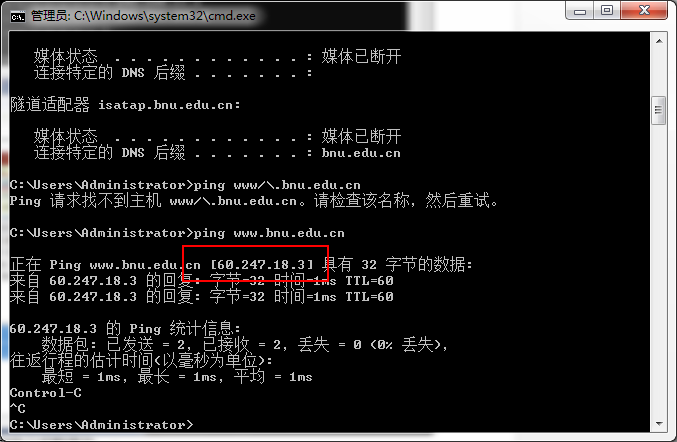


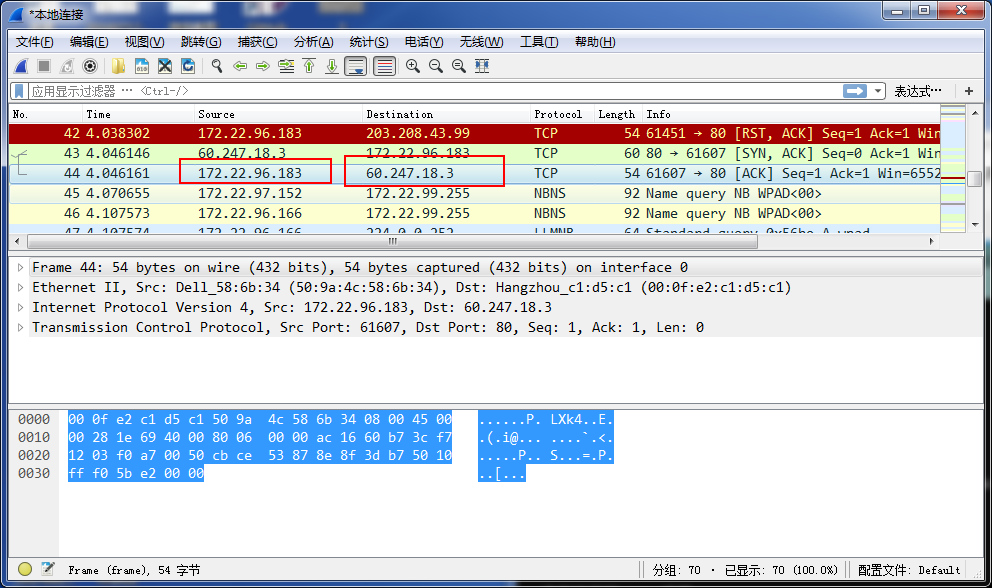
2) 访问北师大官网，捕获Windows虚拟机与官网服务器之间的数据包。

主机地址

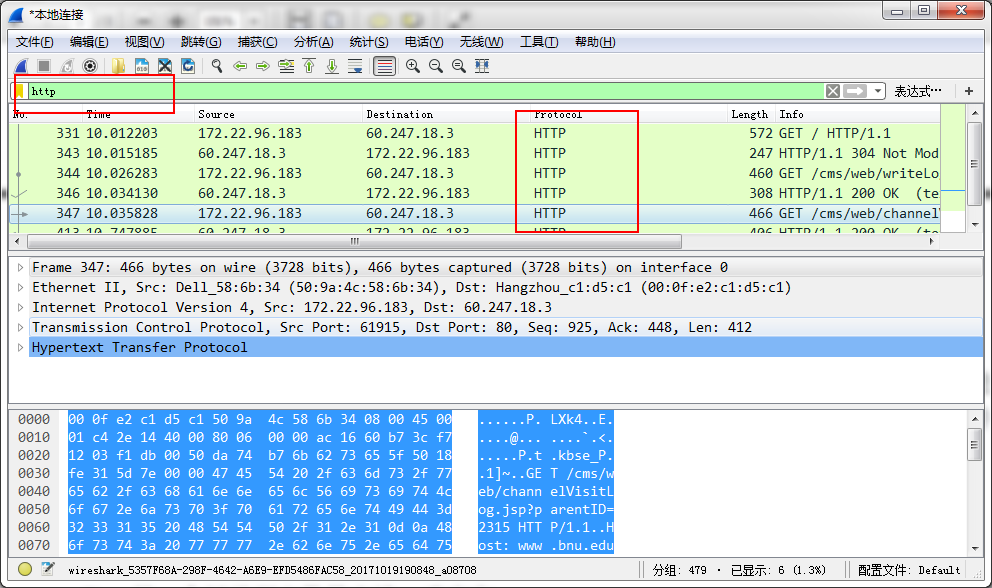


[www.bnu.edu.cn的ip](http://www.bnu.edu.cn的ip)地址

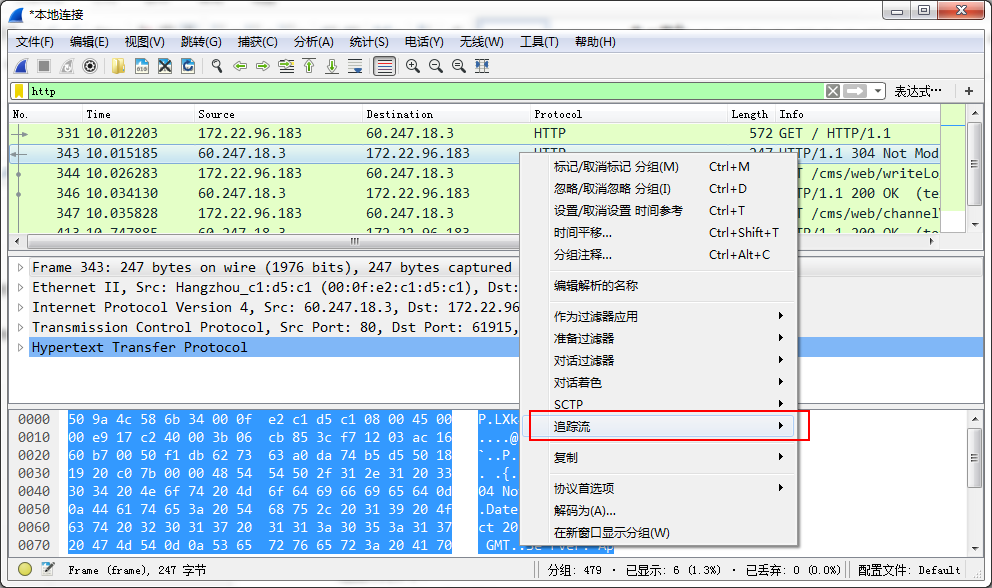


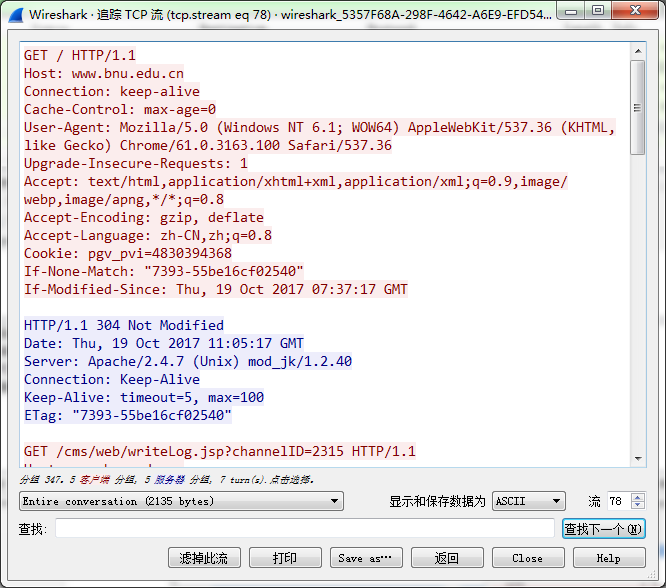


3) 应用过滤器，筛选出HTTP协议的数据包。

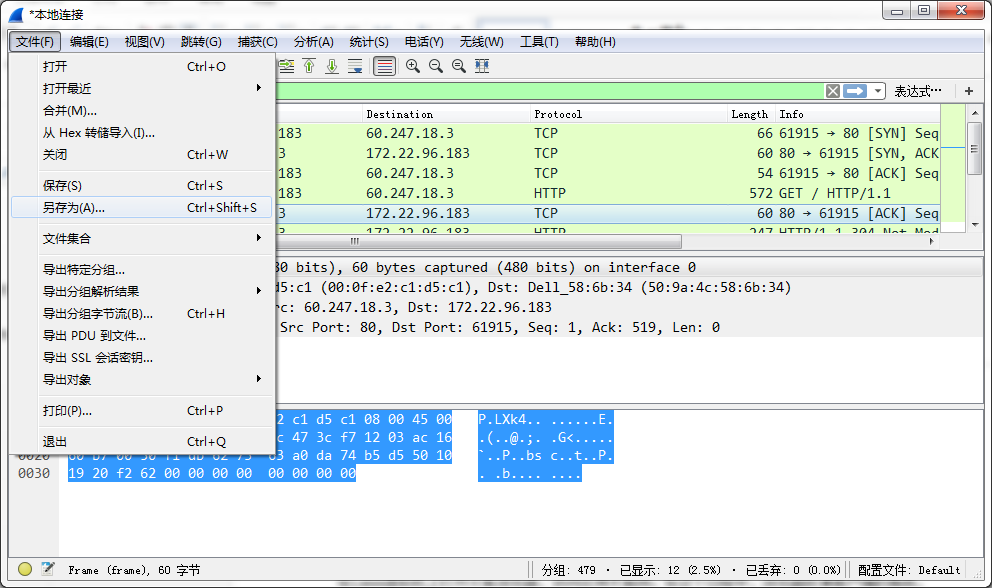


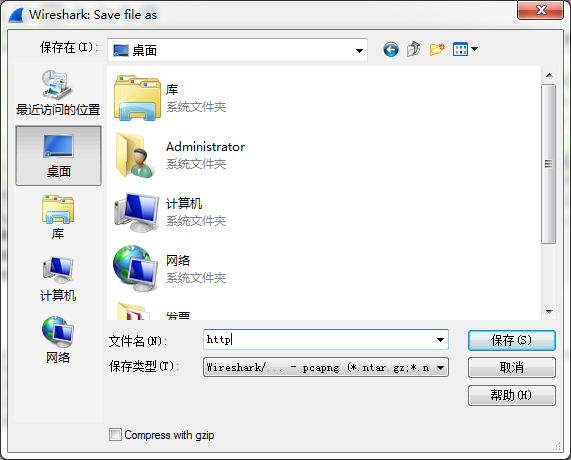
4) 找到感兴趣的HTTP数据包，“右键->追踪流->TCP流”，分析数据包内容。





5) 将本次抓包结果保存在本地文件。

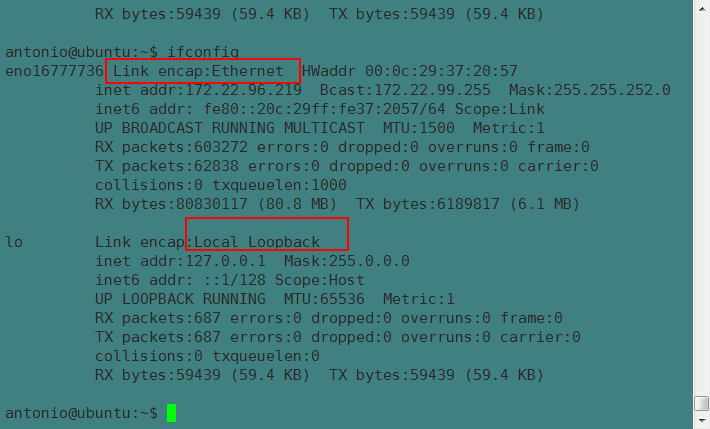






**4.** 使用**tcpdump**抓包。

1) 查看网卡。使用ifconfig命令，查看Linux虚拟机安装了哪些网卡。如何识别其中的以太网卡和本地回环网卡？

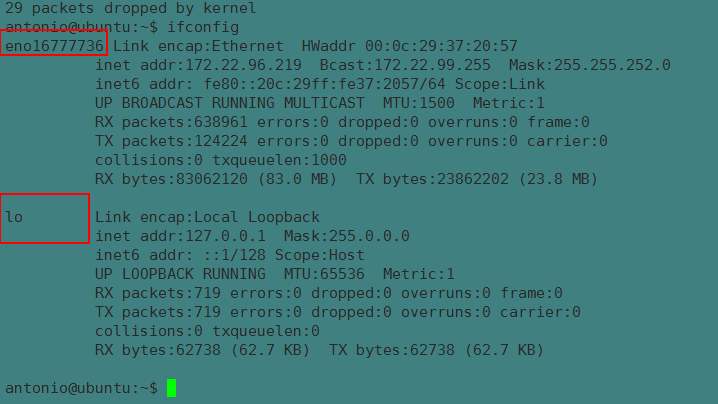


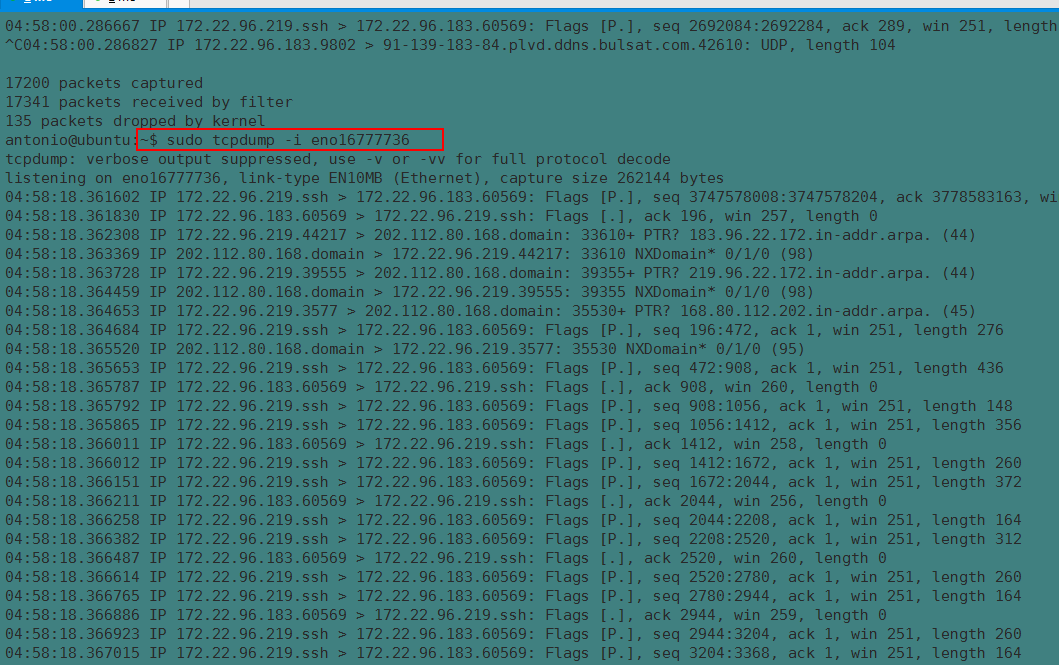
上边的红框为以太网卡，下边的为回环地址

2) tcpdump抓包：指定网卡。

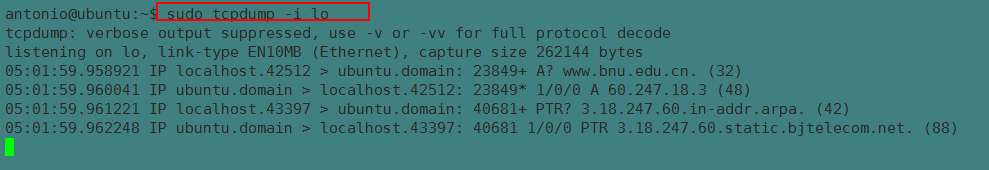
如何截获以太网卡收发的数据包？如何截获本地回环网卡收发的数据包？

提示：*tcpdump -i* 网卡

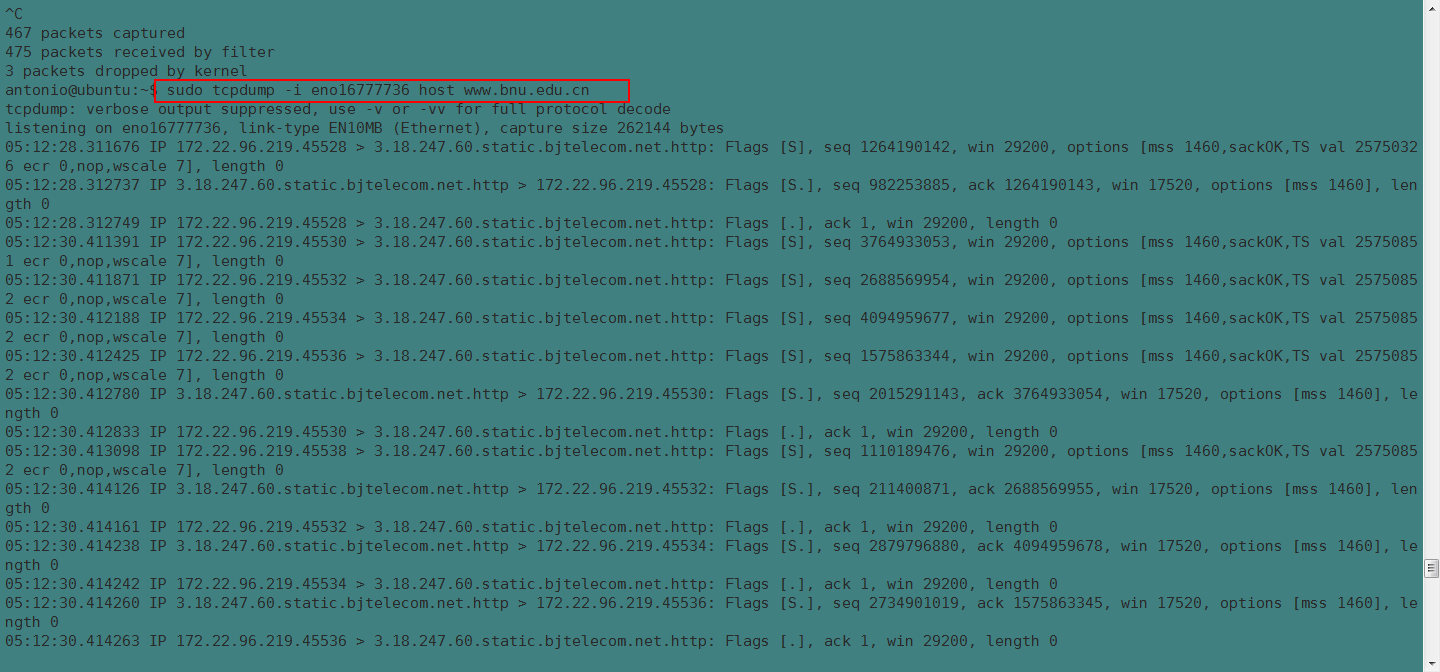




提示：在测试本地回环网卡时，如果没有截获到收发数据包，可打开另一个终端窗口，执行*ping localhost*命令，人为制造数据包。



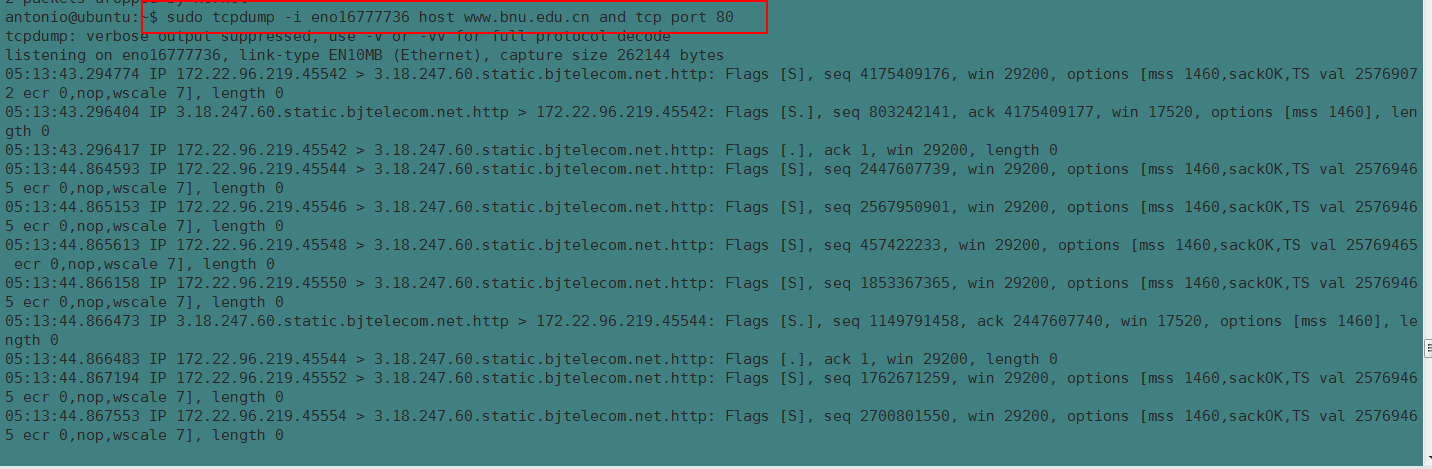
3) tcpdump抓包：指定IP。



在Linux虚拟机上打开火狐浏览器，访问北师大官网。在这个过程中，浏览器扮演客户端的角色，而北师大主机扮演服务器的角色。客户端向服务器发起请求，指明渲染页面所需要的资源；服务器接收请求并进行处理，然后向客户端发送响应；客户端得到响应，完成渲染并呈现给用户。那么，如何利用tcpdump，截获Linux虚拟机与北师大主机之间传输的数据包？你能从抓包情况分析出哪些信息呢？

提示：*tcpdump -i* 网卡host IP地址

4) tcpdump抓包：指定端口。



思考：如何从给定的URL分析出其端口号？可以就如下两个URL说明：

http://www.website.com/path/to/index.html?query1=value1&query2=value2

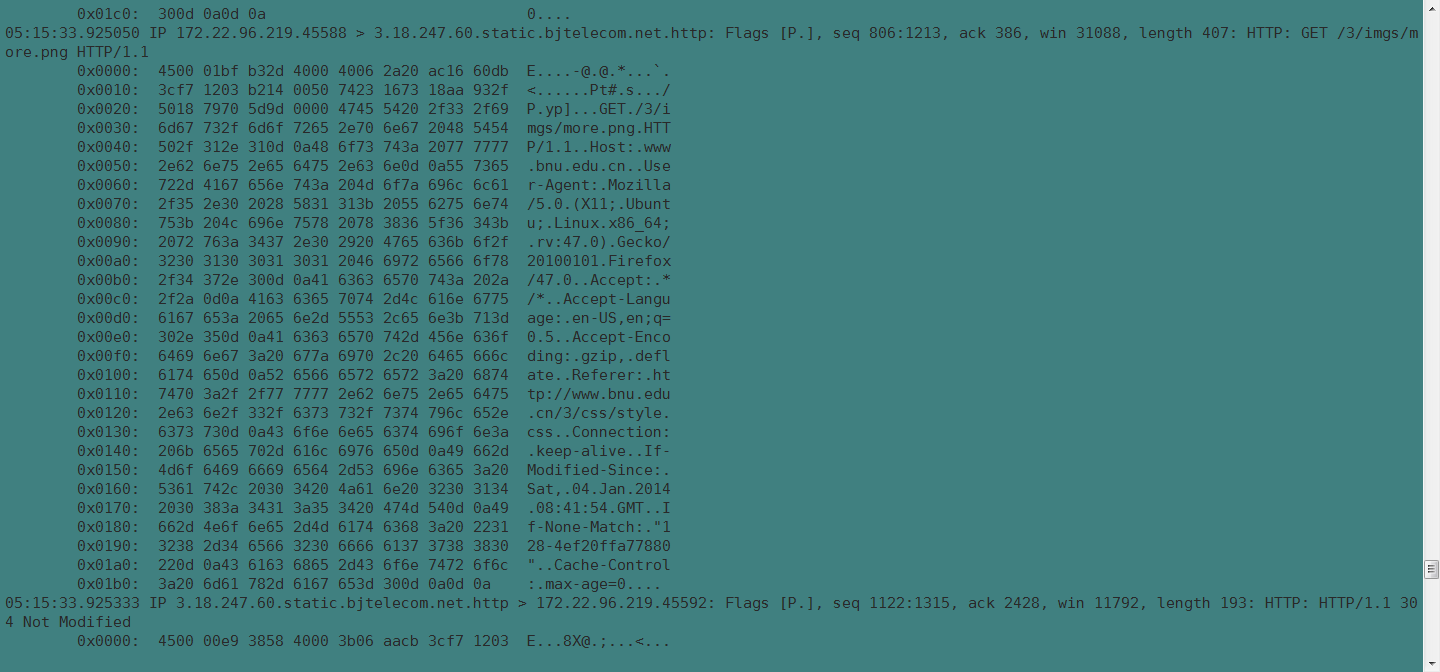
http://www.website.com:8080/path/to/index.html?query1=value1&query2=value2

北师大官网的URL为http://www.bnu.edu.cn，其占用所在服务器的哪一个端口？如何利用tcpdump，截获Linux虚拟机与北师大主机的该端口之间传输的数据包？如果监听北师大主机的8080端口，刷新浏览器，会抓取到数据包吗?

提示：*tcpdump -i* 网卡host IP地址*and tcp port* 端口号

5) tcpdump抓包：显示数据包内容。

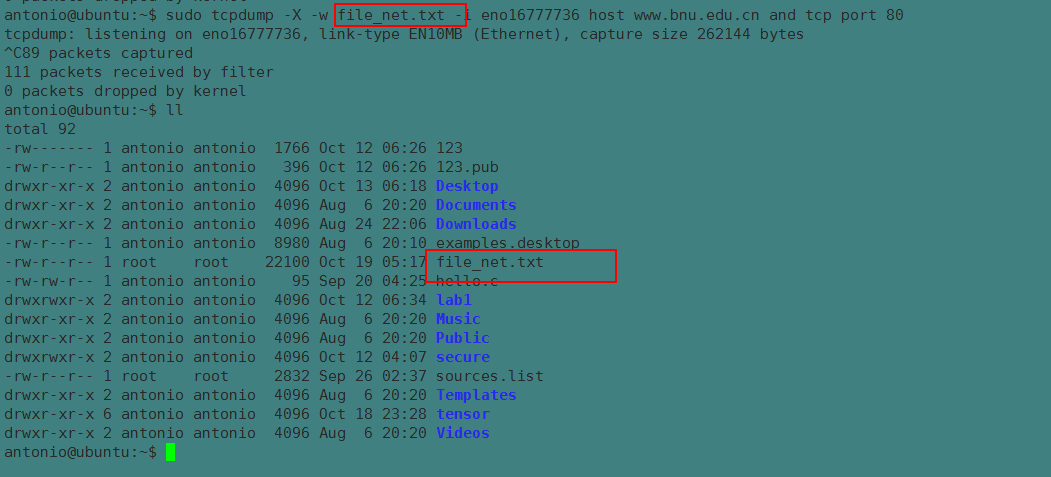




如何显示Linux虚拟机与北师大主机之间每个数据包的内容？请从众多的数据包中，找出任意一个HTTP协议的请求，你能分析出哪些信息？请从众多的数据包中，找出任意一个HTTP协议的响应，你能分析出哪些信息？

提示：*tcpdump -X -i* 网卡host IP地址*and tcp port* 端口号

6) tcpdump抓包：记录到文件。



从上面tcpdump的输出可以看出，tcpdump对截获的数据并没有进行彻底解码，数据包内的大部分内容是使用十六进制的形式直接打印输出的。显然这不利于分析网

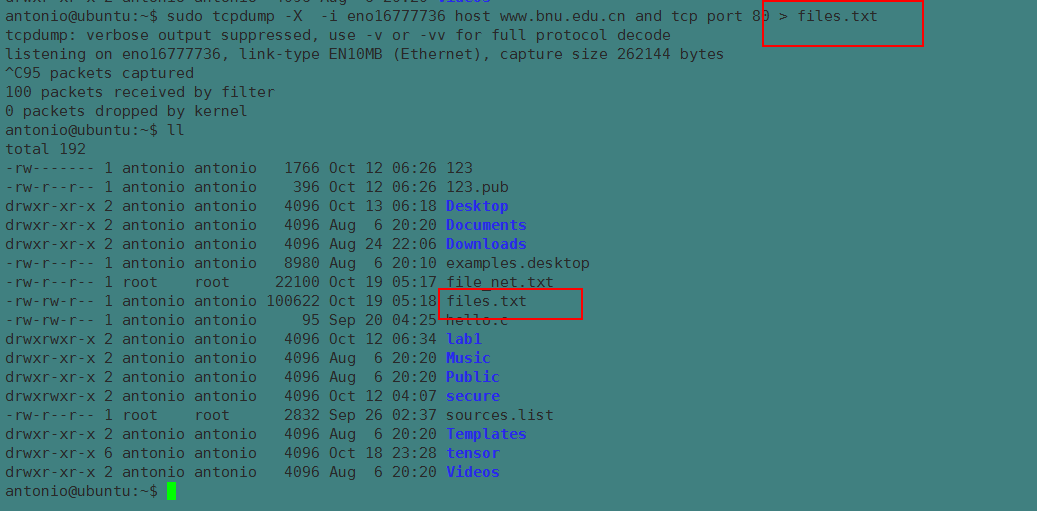
络故障，通常的解决办法是先将截获数据并保存到文件中，然后再使用其他程序进行解码分析。如何将抓包结果，保存到本地日志文件中？如何实时追踪该日志文件的动态变化？

提示：

*tcpdump -X -w* 文件-i 网卡host IP地址*and tcp port* 端口号

*tail -f* 文件

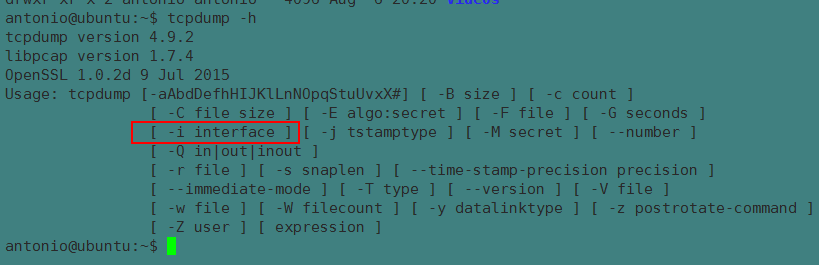
7) 另一个记录到文件的方法：重定向



如果不想在屏幕上显示, 而是想把输出结果直接存储在指定的文件中，可以使用> 或>>。> 将输出结果以“覆盖”的形式存储在指定的文件中，若文件不存在则自动创建；>> 将输出结果以“追加”的形式存储在指定的文件中，若文件不存在则自动创建。如何利用重定向命令，将抓包结果保存到本地日志文件中？如何实时追踪该日志文件的动态变化？

提示：*tcpdump -X -i* 网卡host IP地址*and tcp port* 端口号> 文件

8) 查阅tcpdump命令手册，解释如下命令的含义：



*tcpdump -i* 网卡src IP地址

*tcpdump -*