数据包嗅探实验（Packet Sniffering）

任务0. wireshark下载和安装

下载地址：<https://www.wireshark.org/#download>

任务1. 水木论坛登录密码嗅探

1.1登录[www.newsmth.net](http://www.newsmth.net)，并用注册新用户后退出。

1.2启动wireshark，并重新使用新注册的用户名和密码登录论坛。

使用wireshark分析上一步的登录过程。

分析数据流回答下列问题：

Q1. newsmth.net的ip地址什么？

Q2. 如何根据ip地址过滤访问newsmth.net的流量?给出显示过滤规则及结果截图

1.3尝试在命令行运行下面的telnet命令，使用刚才注册的新用户来登录水木论坛，并启动wireshark捕获该登录过程。

命令行远程登录命令：C:\>telnet newsmth.net

分析数据流，你能找到刚才输入的登录用户和登录密码吗？

1.4 分析telnet登录过程发送的telnet数据包，找到刚才输入的密码。

分析数据流回答下列问题：

Q3. 如何获取刚才的输入密码？给出方法及结果截图。提示可以跟踪TCP流。

任务2. 登录学校主页：<http://www.nenu.edu.cn>

分析数据流回答系列问题：

Q1：学校主页的ip地址是什么？

Q2：在浏览器和web服务器之间的通信过程中，找到一次完整的TCP连接建立的三次握手过程，以及一对http请求和http响应数据包。

任务3（可不做此部分）. 使用kali流量监视工具，监视无线路由器与电脑之间的802.11数据包，实验中的wifi数据包见bb平台的附件。在Virtual Box上加载Kali虚拟机，并使用 aircrack-ng来破解wifi的登录密码。

Kali Linux下载地址：<https://www.kali.org/downloads/>

回答下列问题：

Q7. 尝试过滤EAPOL协议，并解释过滤出来的数据包含义。

Q8. 给出Wifi登录密码的破解结果，及详细实验步骤截图。

wificrack参考文档：

<https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-aircrack-ng-0148366/>