实验一：网络抓包与协议分析

一、实验目的

通过实验，掌握 Wireshark 网络抓包工具的使用方法，在真实网络环境下捕捉和分析网络应用数据包，掌握 HTTP、DNS、TCP、UDP 等应用层及传输层协议报文的结构，深入理解相关协议的特点与工作原理，培养学生网络故障检测、网络性能改进和网络安全分析的能力。

二、实验内容

1. 学习 Wireshark 网络抓包工具的基本操作，掌握捕获过滤器和显示过滤器的使用方法。

2. 访问 Web 网站并捕捉数据包，分析 HTTP 协议报文格式和交互过程，观察 TCP 协议报文格式，分析 TCP 协议采用的可靠传输机制、以及 TCP 连接建立和关闭的交互过程。

3. 使用 nslookup 命令查询域名并捕捉数据包，分析 DNS 协议报文格式和交互过程，同时分析 UDP 协议报文格式和交互过程。

三、实验环境

Windows 7 + Wireshark

四、实验要求

1. 实验时间为两周（10 月 31 日——11 月 13 日）。

2. 应独立完成实验、独立撰写实验报告，严禁抄袭和拷贝。

3. 除了 HTTP、DNS 应用层协议，鼓励对其他应用层协议进行数据包分析，并酌情给予加分。

4. 完成实验内容后应联系助教进行验收，并登记成绩。

5. 助教验收通过后，提交电子版的实验报告给助教，实验报告格式要求及提交方式见《计算机网络课程实验报告（模板）》。