**《计算机网络安全》实验报告**

**实验（4） 安全防护实验**

学生姓名： 陈华豪 学 号： 6130116238 专业班级： 网络工程161班

实验类型：■ 验证 □ 综合 □ 设计 实验日期：  实验成绩：

**实验目的**

了解**Sniffer/Wireshark**软件的监听原理，掌握**Sniffer/Wireshark**软件的使用方法，学会使用**Sniffer/Wireshark**软件进行数据包和协议分析。

**试验内容**

（1）安装**Sniffer/Wireshark**软件

（2）配置**Sniffer/Wireshark**

（3）创建过滤器

（4）捕获网络信息数据包，然后通过解码进行检测分析

**3．实验过程**

3．1实验环境

（1）**Sniffer**软件

（2）**Wireshark**软件

3．2关键实验步骤及配置

（1）打开浏览器，显示主页

（2）启动wireshark，看到开始界面：

**图片包含 屏幕截图

描述已自动生成**

（3） **定时：一小时：**

图片包含 屏幕截图

描述已自动生成

（4）**抓取：**

图片包含 屏幕截图

描述已自动生成

（5）**筛选 特定 http**

图片包含 屏幕截图

描述已自动生成

（6）**特定 http 包详情**

图片包含 屏幕截图

描述已自动生成

（7）**协议**

图片包含 屏幕截图

描述已自动生成

（8）地址

图片包含 屏幕截图

描述已自动生成

（9）存活时间

图片包含 屏幕截图

描述已自动生成

（10）筛选tcp

图片包含 屏幕截图

描述已自动生成

**实验结果**

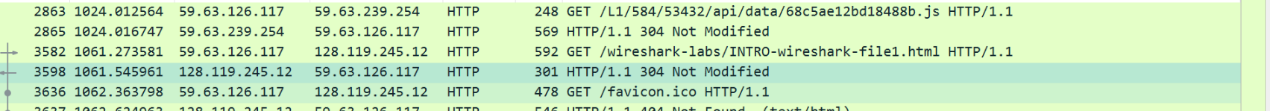
试着用工具分具体问题：

从发送HTTP GET消息到收到HTTP OK回复需要多长时间？ （默认情况下，数据包列表窗口中时间列的值是自Wireshark跟踪开始以来的时间量（以秒为单位）。要以时间格式显示时间字段，请选择Wireshark View下拉菜单，然后选择时间显示格式，然后选择时间。）

答：先下载一个页面：<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

get-ok

**得出：**

****

**选中查看到达时间：**

**图片包含 屏幕截图

描述已自动生成**

**选中查看回复时间：**

**图片包含 屏幕截图

描述已自动生成**

**到达时间: Oct 28, 2018 09:43:29.933311000 中国标准时间**  
  
**回复时间: Oct 28, 2018 09:43:30.205691000 中国标准时间**  
  
相减得 0.27238s

**实验总结**

利用成熟的抓包工具进行数据包分析让学习者可以在真实环境下体会到网络工作流程以及

网络协议的具体细节，通过学习使用工具也可以达到网络故障分析实践的目的，利用创造的网络攻击时间分析常见网络攻击是一个很好的方法。

这次实验我选择了使用wireshark来进行网络抓包及分析。在之前学习过网络协议分析课程后对这个软件的应用也有了基本了解。