《计算机网络》实验指导

实验五：HTTP 与 DNS 协议分析

一、实验目的

1、了解常用的应用层协议；

2、掌握 HTTP 协议的基本内容，并深入理解 HTTP 协议的通信过程；

3、掌握 DNS 协议的基本内容，并深入理解 DNS 协议的通信过程。

二、实验学时

2 学时

三、实验类型

创新性

四、实验需求

1、硬件

每人配备计算机 1 台，计算机接入实验室局域网。

2、软件

Windows 7 操作系统，安装网络嗅探软件 Wireshark。

3、网络

支持对互联网的访问。

4、工具

无

五、实验理论

1、应用层的基本理论；

2、HTTP 和 DNS 协议的基本原理与通信过程；

3、网络嗅探工具的工作原理。

六、预备知识

1、DNS 域名服务器的类型和作用；

> 要求：
> 请查阅相关资料，说明 DNS 域名服务器的类型和作用，并自行绘制一个表格进行对比分析，将结果填写到实验报告册中。

2、WinPcap 和 Wireshark 软件的基本工作原理与使用方法；

3、请查阅资料，列举八种常见的应用层协议，并填写表 5-1 应用层协议对比分析一览表。

表 5-1 应用层协议对比分析一览表

序号	协议名称	英文标识	默认端口	传输协议	具体用途
1					
2					
3					
4					
5					
6					
7					
8					

要求：

请查阅资料完成表 5-1 的具体内容，并将结果填写到实验报告册中。

七、实验任务

1、完成 DNS 和 HTTP 协议的分析；

2、通过数据报分析 HTTP 协议的通信过程；

3、通过数据报分析 DNS 协议的通信过程。

八、实验内容及步骤

1、DNS 协议分析

（1）打开 Wireshark，在【Filter】选项中输入报文过滤条件“**dns and ip.addr==8.8.8.8**”，选择【Start】，开始进行报文采集，选择左上角红色按钮停止报文采集。如图 5-1 所示。

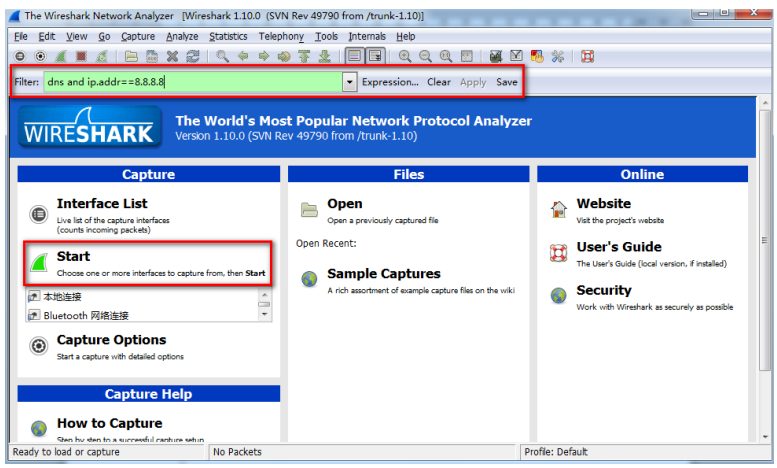

图 5-1 使用 Wireshark 工具进行 DNS 报文采集

（2）打开 Windows 的命令窗体，输入“**nslookup –qt ke.51xueweb.cn 8.8.8.8**”，使用 DNS 服务器“8.8.8.8”对域名记录“ke.51xueweb.cn”进行解析。

如图 5-2 所示。

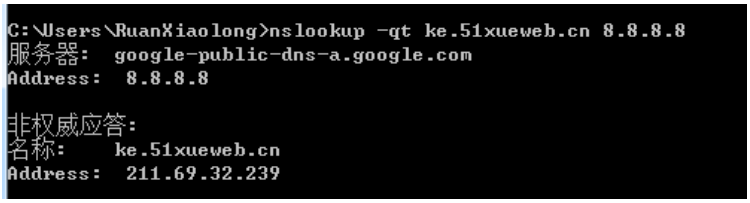

图 5-2 对域名记录 ke.51xueweb.cn 进行 DNS 解析请求

（3）在 Wireshark 窗体中，看到 DNS 解析的过程。如图 5-3 所示。

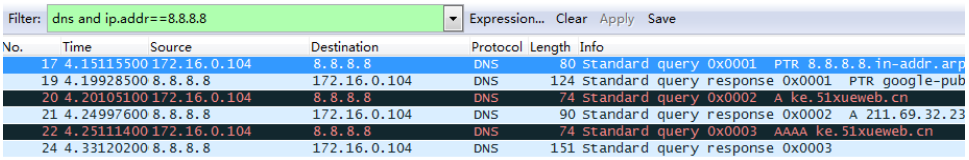

图 5-3 DNS 报文

（4）对采集的数据报文进行分析研究，并完成表 5-2、表 5-3 的填写。

表 5-2 一次 DNS 解析请求过程

序号	发送时间	来源 IP	目的 IP	报文具体作用和描述
1				
2				
3				
4				
5				
6				
...				

表 5-3 域名记录 ke.51xueweb.cn 的 A 记录的 DNS 解析内容

序号	字段名	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data Length		
6	Addr		

要求：

请按照上述要求进行抓包和数据包分析，完成表 5-2、5-3 的填写，并将分析结果填写到实验

报告册中。

（5）打开 Windows 的命令窗体，输入“**nslookup –qt 51xueweb.cn 8.8.8.8**”，使用 DNS 服务器“8.8.8.8”对域名“51xueweb.cn”进行解析。如图 5-4 所示。

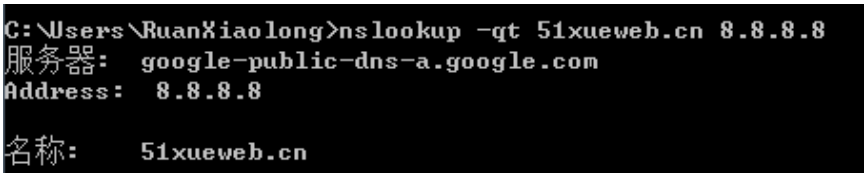

图 5-4 对域名 51xueweb.cn 进行 DNS 解析请求

（6）对采集的数据报文进行分析研究，并完成表 5-4 的填写。

表 5-4 域名 51xueweb.cn 的 DNS 解析内容

序号	字段名	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data length		
6	Primary name Server		
7	Responsible authority’s mailbox		
8	Serial Number		
9	Refresh Interval		
10	Retry Interval		
11	Expire Limit		
12	Minimum TTL		

要求：

请按照上述要求进行抓包和数据包分析，完成表 5-4 的填写，并将分析结果填写到实验报告册中。

2、HTTP 协议分析

（1）打开 Wireshark，在【Filter】选项中输入报文过滤条件“**http contains “http://ke.51xueweb.cn”**”，选择【Start】，开始进行报文采集，选择左上角红色按钮停止报文采集。如图 5-5 所示。

（2）打开浏览器，在地址栏中输入“http://ke.51xueweb.cn”，进行网页访问。

（3）分析采集到的数据报文，并分别填写表 5-5、表 5-6。

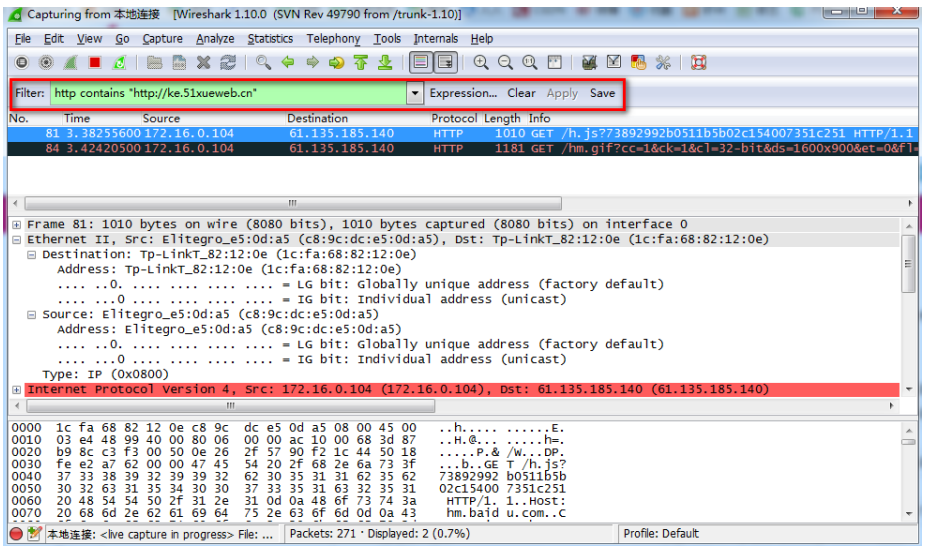

图 5-5 使用 Wireshark 工具进行 HTTP 报文采集

表 5-5 一次 Get 请求的过程

序号	发送时间	来源 IP	目的 IP	报文具体作用和描述
1				
2				
3				
4				
5				
…				

表 5-6 HTTP 的 Get 请求解析内容（HTML 文档）

序号	字段名	字段值	字段解释和说明
1	Request Version		
2	Status code		
3	Response Phrase		
4	Content-Length		
5	Content-Type		
6	Content-Location		
7	Last-Modified		
8	Accept-Ranges		
9	ETag		
10	Server		

11	X-Powered-By		
12	Date		
13	Time Since Request		

要求：

1、请按照上述要求进行抓包和数据包分析，完成表 5-5、5-6 的填写，并将分析结果填写到实验报告册中。

2、请分析 HTTP 针对 HTML、CSS、PNG、JS 文件的 Get 请求是否相同？并将分析结果填写到实验报告册中。

（4）请设计 Head 请求的实验，并对报文进行分析。

要求：

1、请设计 Head 请求的实验方案，将实验方案填写到实验报告册中。

2、请按照实验方案开展实验，并设计表格记录实验过程和实验分析，将实验记录表与实验分析表填写到实验报告册中。

（5）请设计 Post 请求的实验，并对报文进行分析。

要求：

1、请设计 Post 请求的实验方案，将实验方案填写到实验报告册中。

2、请按照实验方案开展实验，并设计表格记录实验过程和实验分析，将实验记录表与实验分析表填写到实验报告册中。

九、实验分析

1、通过 HTTP 使用浏览器访问网站时，浏览器是否只向目的主机发送一次 HTTP 请求？如何查看这些请求？

要求：

请查阅相关资料，回答上述问题，并将答案填写到实验报告册中。

2、每访问一个网站都需要进行域名解析，域名解析的效率直接决定了网站访问的效率，如何为本地主机配置一个高效率的 DNS 服务器对于网站访问至关重要，那么如何查找和评估对自己来讲效率最高的 DNS 服务器呢？

要求：

请查阅相关资料，回答上述问题，并将答案填写到实验报告册中。

3、域名记录和域名的关系

（1）什么是域名，什么是域名记录？二者之间的关系是什么？

（2）域名记录有几种类型？

（3）如何申请一个自己的域名？

要求：
请查阅相关资料，回答上述 3 个问题，并将答案填写到实验报告册中。

4、Head、Get、Post 请求

（1）本实验是在 HTTP 的客户端进行的，那么 HTTP 服务器端的 HTTP 报文结构和客户端的报文结构一致么？

（2）HTTP 发送的 Head、Get、Post 请求的报文结构有什么不同，请对比分析。

（3）HTTP 发送 Head、Get、Post 请求的过程是否不同？请对比分析。

要求：
1、请按照（1）（2）2 个要求，对比分析 Head、Get、Post 请求的报文结构，并将分析结果填写在实验报告册中。
2、请查阅相关资料，回答（3）的问题，并将结果填写到实验报告册中。

十、课外自主实验

1、HTTP 和 HTTPs 协议

（1）请设计实验，分析 HTTPs 协议。

（2）分析 HTTPs 协议的报文结构，和 HTTP 协议的报文结构进行对比，并绘制对比表。

（3）分析 HTTPs 协议的通信过程，和 HTTP 协议的通信过程进行对比，并绘制对比表。

要求：
1、请按照上述（1）的要求，进行具体实验，并将实验过程的具体内容填写到实验报告册中。
2、请按照上述（2）（3）2 个要求，将实验分析的具体内容填写到实验报告册中。

2、SMTP、POP3、IMAP 协议

（1）请设计实验，对比分析电子邮件服务的 SMTP、POP3、IMAP 协议。

（2）请通过数据报文，分析 SMTP、POP3、IMAP 协议的报文结构。

（3）请分析 SMTP、POP3、IMAP 协议的通信过程。

要求：
1、请按照上述（1）的要求，完成该实验，并将实验设计的合理性和具体内容填写到实验报告册中。
2、请按照上述（2）的要求，完成对 SMTP、POP3、IMAP 报文结构的分析，并将具体的分析结果填写到实验报告册中。
3、请按照上述（3）的要求，完成对 SMTP、POP3、IMAP 通信过程的分析，并将具体的分析结果填写到实验报告册中。

3、浏览器与 HTTP

（1）大多数浏览器都使用多标签页（Tab）的工作模式，那么浏览器是如何把不同的 HTTP 请求返回给不同的标签页（Tab）呢？

（2）浏览器访问网页结束后，为什么要断开与服务器的 TCP 连接？

（3）访问一个网站时，浏览器如何进行 HTTP 版本的选择？

十一、实验扩展资源

1、图书

（1）网络协议分析与实现 胡维华 高等教育出版社

（2）网络协议教程 陈明 清华大学出版社

（3）网络协议分析 寇晓蕤，罗军勇，蔡延荣 机械工业出版社

2、文章

（1）基于 HTTP 协议的多线程下载工具的实现 李晶媛 韩慧莲 《电脑开发与应用》 2009 年 10 期

（2）DNS 协议分析与安全检测 吴海涛 郭丽红 《计算机安全》 2009 年 04 期

（3）浅析 DNS 协议 邵明珠 解瑞云 《甘肃科技》 2006 年 05 期

（4）基于 HTTP 协议与 XML 技术的远程数据访问 张玉祥 高昆元 王魁生 《计算机工程与设计》 2005 年 05 期

3、互联网资源

（1）协议分析网：http://www.cnpaf.net/Class/ProtocolAll/

（2）网易公开课：

http://c.open.163.com/coursera/courseIntro.htm?cid=105&tabNoJmp=1#/courseIntro

（3）Wireshark 官方文档：http://www.wireshark.org/docs/

（4）科来网络分析系统：http://www.colasoft.com.cn/products/capsa.php

4、电子资源下载

课程网站：ke.51xueweb.cn/Network.html