实验八：DNS 协议分析

一、实验目的

1、理解 DNS 的基本原理；

2、理解 DNS 报文格式和各字段含义；

3、理解 DNS 解析的通信过程。

二、实验学时

2 学时

扫码看步骤

三、实验类型

验证性

四、实验需求

1、硬件

每人配备计算机 1 台，不低于双核 CPU、8G 内存、500GB 硬盘。

2、软件

支持 Windows 操作系统，安装 eNSP 仿真软件，安装 Wireshark 网络嗅探软件。

3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问。

4、工具

无。

五、实验任务

1、完成 DNS 报文的采集；

2、完成 DNS 报文结构的分析；

3、完成 DNS 通信过程分析。

六、实验内容及步骤

1、DNS 数据报文分析

（1）获取数据报文

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，如图 8-1 所示。

②打开 Windows 的命令窗体，输入“**nslookup –qt=A internet.hactcm.edu.cn 8.8.8.8**”，使用服务器“8.8.8.8”对域名记录“internet.hactcm.edu.cn”解析，如图 8-2 所示。

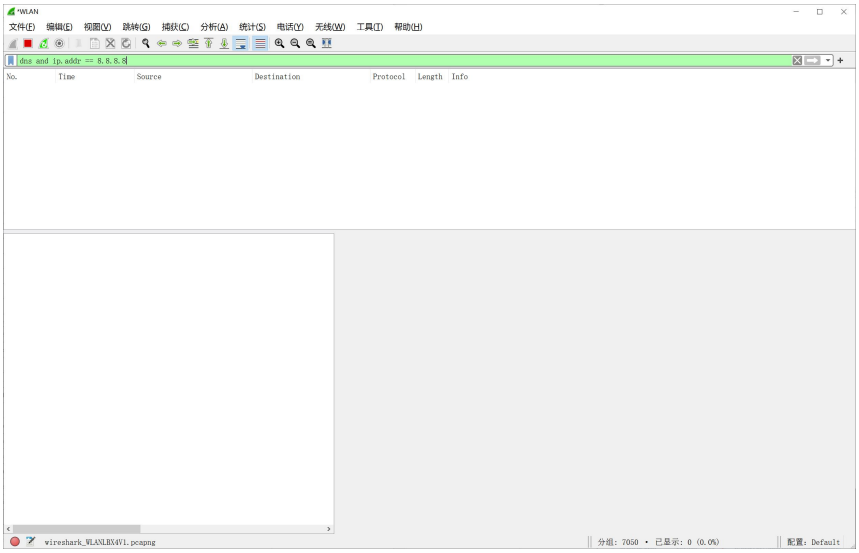

图 8-1 使用 Wireshark 工具进行 DNS 报文采集

图 8-2 对域名记录 internet.hactcm.edu.cn 进行 DNS 解析请求

③在 Wireshark 的抓包窗体中，查看已获取的 DNS 数据报文，如图 8-3 所示。

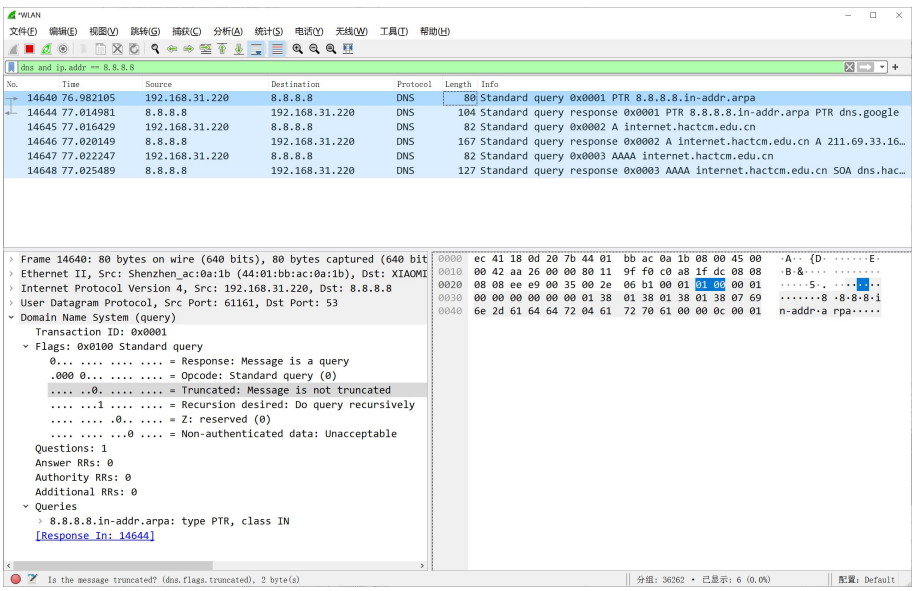

图 7-3 DNS 数据报文

（2）数据报文分析

对采集的数据报文进行分析，并完成表 8-1、表 8-2 的填写。

表 8-1 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 8-2 域名记录 internet.hactcm.edu.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		

2、通信过程中常见请求类型的 DNS 报文分析

（1）NS 记录

①获取 NS 记录请求应答报文。

在 Windows 命令窗体，输入“**nslookup –qt=ns 51xueweb.cn 8.8.8.8**”，使用服务器“8.8.8.8”获取 NS 记录记录结果。

②分析 NA 记录请求应答报文。

在 Wireshark 中查看获取的 NS 记录解析数据报文，对 NS 记录请求应答数据报文进行分析，并根据数据报文内容填写表 8-3 和表 8-4。

表 8-3 NS 记录请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	**Transaction ID**		**第 位**		
2	**Flags**		**第 位**		
3	**Questions**		**第 位**		
4	**Answer RRs**		**第 位**		
5	**Authority RRs**		**第 位**		

6	Additional RRs		第　位		
7	Queries		第　位		
8	抓取数据包的详细内容：				

表 8-4 NS 记录应答报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Transaction ID		第　位		
2	Flags		第　位		
3	Questions		第　位		
4	Answer RRs		第　位		
5	Authority RRs		第　位		
6	Additional RRs		第　位		
7	Queries		第　位		
8	Answers		第　位		
9	抓取数据包的详细内容：				

（2）CNAME 记录

①获取 CNAME 记录请求应答报文。

在 Windows 命令窗体，输入“nslookup –qt=cname www.baidu.com 8.8.8.8”，使用服务器“8.8.8.8”获取 CNAME 记录记录结果。

②分析 CNAME 记录请求应答报文。

在 Wireshark 中查看获取的 CNAME 记录解析数据报文，对 CNAME 记录请求应答数据报文进行分析，并根据数据报文内容填写表 8-5 和表 8-6。

表 8-5 CNAME 记录请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Transaction ID		第　位		
2	Flags		第　位		
3	Questions		第　位		

4	**Answer RRs**		**第　位**		
5	**Authority RRs**		**第　位**		
6	**Additional RRs**		**第　位**		
7	**Queries**		**第　位**		
8	**抓取数据包的详细内容：**				

表 8-6 CNAME 记录应答报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	**Transaction ID**		**第　位**		
2	**Flags**		**第　位**		
3	**Questions**		**第　位**		
4	**Answer RRs**		**第　位**		
5	**Authority RRs**		**第　位**		
6	**Additional RRs**		**第　位**		
7	**Queries**		**第　位**		
8	**Answers**		**第　位**		
9	**抓取数据包的详细内容：**				

七、设计任务（实验考核）

1、任务说明

（1）按照要求完成 Wireshark 报文分析。

（1）按照要求对 DNS 报文进行分析，并进一步理解 DNS 协议。

2、任务要求

要求 1：使用 Wireshark 采集报文；

要求 2：实现对 DNS 协议报文的分析（A 记录、NS 记录、CNAME 记录）。

3、考核要求

题目 1：提供 A 记录的 Wireshark 报文采集的界面截图（格式参考图 8-1），完成分析后并填写表 8-1、表 8-2，将表格转为截图后提交。（共计提交 3 张图片，且内容应对应）

题目 2：提供 NS 记录的 Wireshark 报文采集的界面截图（格式参考图 8-1），完成分析后并填写表 8-3、表 8-4，将表格转为截图后提交。（共计提交 3 张图片，且内容应对应）

题目 3：提供 CNAME 记录的 Wireshark 报文采集的界面截图（格式参考图 8-1），完成分析后并填写表 8-5、表 8-6，将表格转为截图后提交。（共计提交 3 张图片，且内容应对应）