实验七：DNS 报文分析

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

三、实验类型

验证型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 Wireshark 网络嗅探软件。

3、网络

实验室局域网支持，能够访问校园网，能够访问互联网。

4、工具

无。

五、实验理论

1、DNS 基本原理；

2、DNS 解析过程。

六、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。

七、实验内容及步骤

1、DNS 数据包分析

（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 7-1 所示。

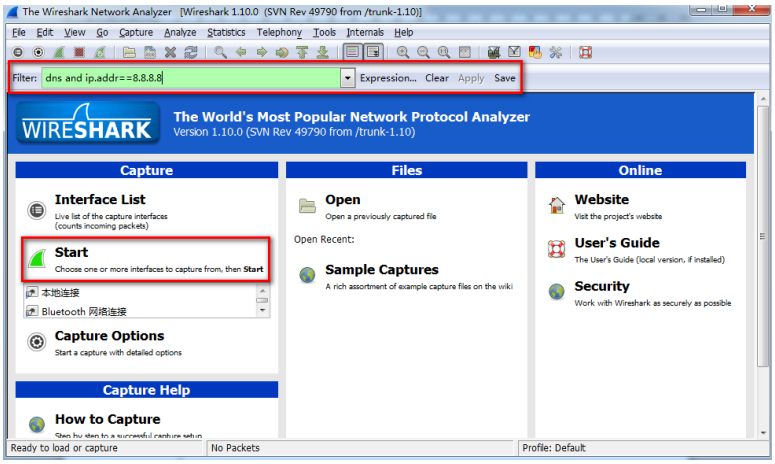

图 7-1 使用 Wireshark 工具进行 DNS 报文采集

②打开 Windows 的命令窗体，输入“nslookup –qt network.ke.51xueweb.cn 8.8.8.8”，使用 DNS 服务器“8.8.8.8”对域名记录“network.ke.51xueweb.cn”进行解析，如图 7-2 所示。

图 7-2 对域名记录 network.ke.51xueweb.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 7-3 所示。

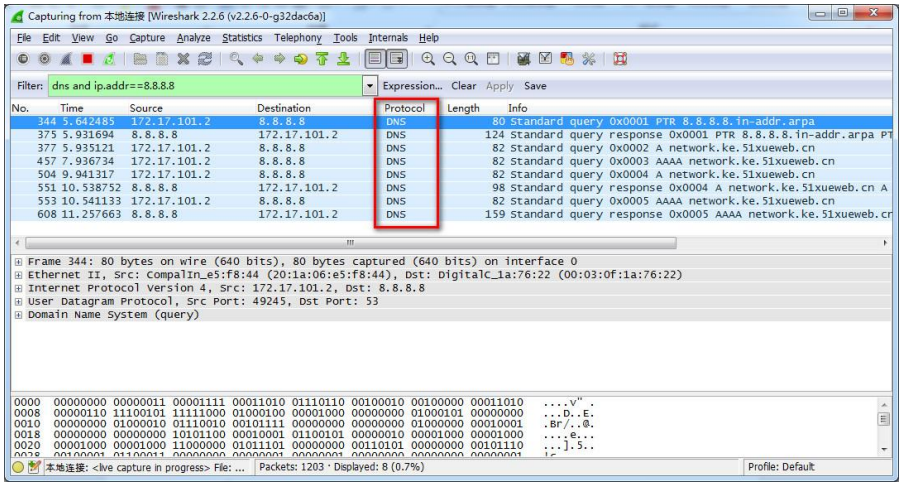

图 7-3 DNS 数据报文

（2）数据报文分析

对采集的数据报文进行分析，并完成表 7-1、表 7-2 的填写。

表 7-1 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 7-2 域名记录 network.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	Primary name Server		
7	Responsible authority's mailbox		
8	Serial Number		
9	Refresh Interval		
10	Retry Interval		
11	Expire Limit		
12	Minimum TTL		

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。打开 Windows 的命令窗体，输入“nslookup –qt=ns network.ke.51xueweb.cn 8.8.8.8”，使用 DNS 服务器“8.8.8.8”获取 NS 记录记录结果，如图 7-4 所示。

图 7-4 进行 DNS 的 NS 记录解析请求

在 Wireshark 的抓包窗体中，查看已获取的 DNS 的 NS 记录解析数据报文，如图 7-5 所示。

②NS 记录请求应答报文分析。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 7-3 和表 7-4。

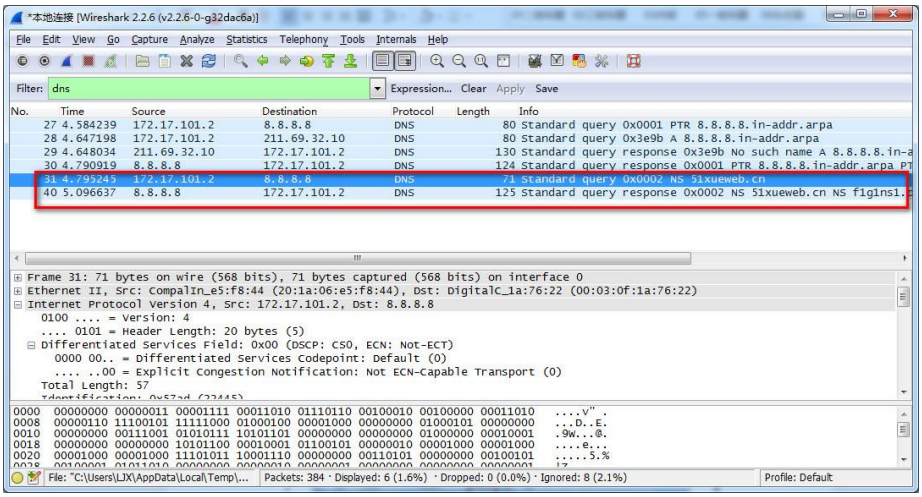

图 7-5 NS 记录请求应答报文

表 7-3 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 7-4 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。打开 Windows 的命令窗体，输入“nslookup –qt=cname network.xg.hactcm.edu.cn 8.8.8.8”，使用 DNS 服务器“8.8.8.8”获取 CNAME 记录记录结果，如图 7-6 所示。

```
C:\Users\RuanXiaolong>nslookup -qt=cname network.xg.hactcm.edu.cn 8.8.8.8
服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

非权威应答:
network.xg.hactcm.edu.cn        canonical name = network.ke.51xueweb.cn
```

图 7-6 CNAME 记录解析请求

在 Wireshark 的抓包窗体中，查看已获取的 CNAME 记录解析数据报文，如图 7-7 所示。

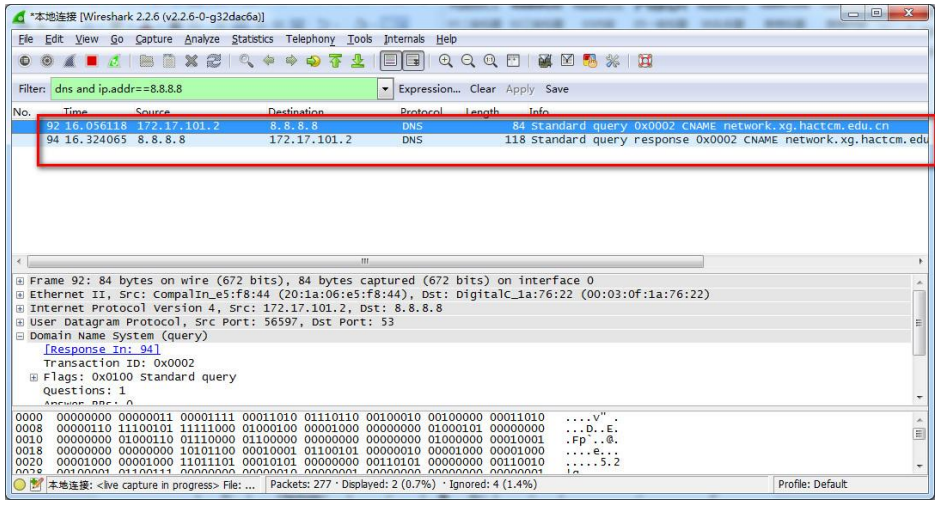

图 7-7 DNS 协议 NS 请求应答报文

②CNAME 记录请求应答报文分析。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 7-5 和表 7-6。

表 7-5 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 7-6 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：				

（3）MX 记录

①获取 MX 记录请求应答报文。打开 Windows 的命令窗体，输入“nslookup –qt=mx hactcm.edu.cn 8.8.8.8”，使用 DNS 服务器“8.8.8.8”获取 CNAME 记录记录结果，如图 7-8 所示。

```
C:\Users\RuanXiaolong>nslookup -qt=mx hactcm.edu.cn 8.8.8.8
服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

非权威应答:
hactcm.edu.cn    MX preference = 10, mail exchanger = mailgate.hactcm.edu.cn
```

图 7-8 进行 DNS 的 MX 记录解析请求

在 Wireshark 的抓包窗体中，查看已获取的 MX 记录解析数据报文，如图 7-9 所示。

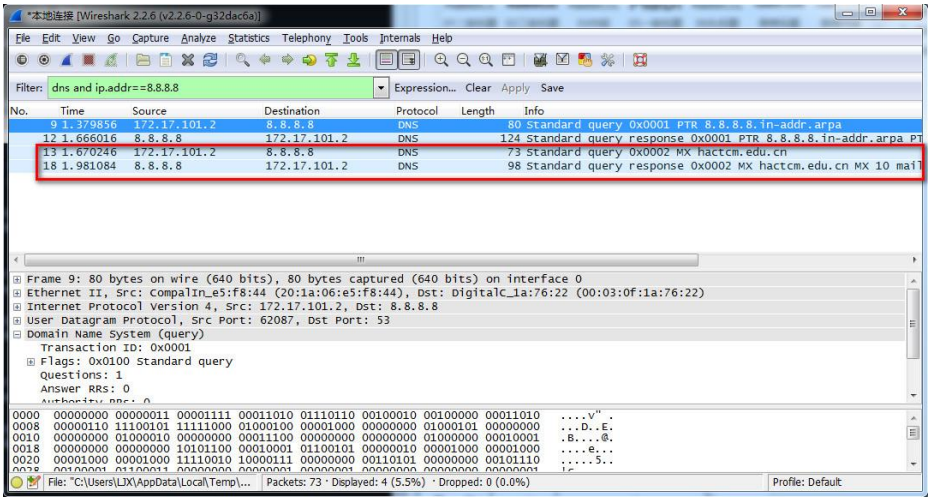

图 7-9 MX 记录请求应答报文

②MX 记录请求应答报文分析。对 MX 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 7-7 和表 7-8。

表 7-7 MX 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 7-8 MX 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：				

八、实验分析

1、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？

2、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？