

重庆邮电大学

学生实验实习报告册

学年学期： 2018-2019 学年 ☐春☒秋学期

课程名称： 计算机网络

学生学院： 软件工程学院

专业班级： 13001603班

学生学号： 2016214052

学生姓名： 姜文泽

联系电话： 17783101834

重庆邮电大学教务处制

实验四：HTTP 和 DNS 分析

一、实验目的

1. 熟悉并掌握 Wireshark 的基本操作，了解网络协议实体间的交互以及报文交换；
2. 分析 HTTP 和 DNS 协议。

二、实验内容

通过使用命令行中的 nslookup 命令和 Wireshark 抓包工具理解 HTTP 和 DNS 协议。

三、实验环境

操作系统：Windows 10 专业版 1809

工具软件：Wireshark 2.6.4

浏览器软件：Google Chrome

网络环境：

无线局域网适配器 WLAN：

连接特定的 DNS 后缀 : lan

本地链接 IPv6 地址. : fe80::3079:5439:d245:e240%9

IPv4 地址 : 192.168.199.175

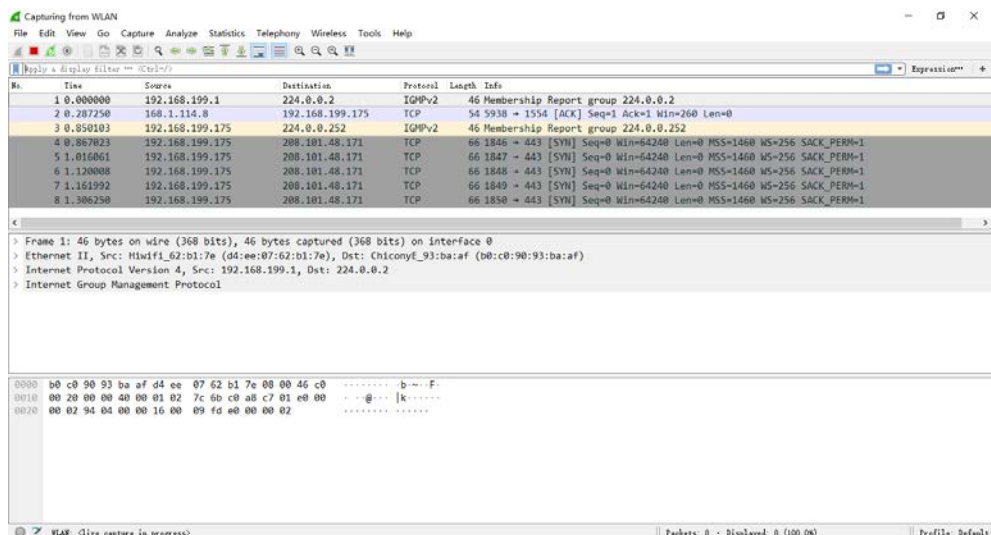
子网掩码 : 255.255.255.0

默认网关. : 192.168.199.1

四、实验步骤

1. HTTP 分析

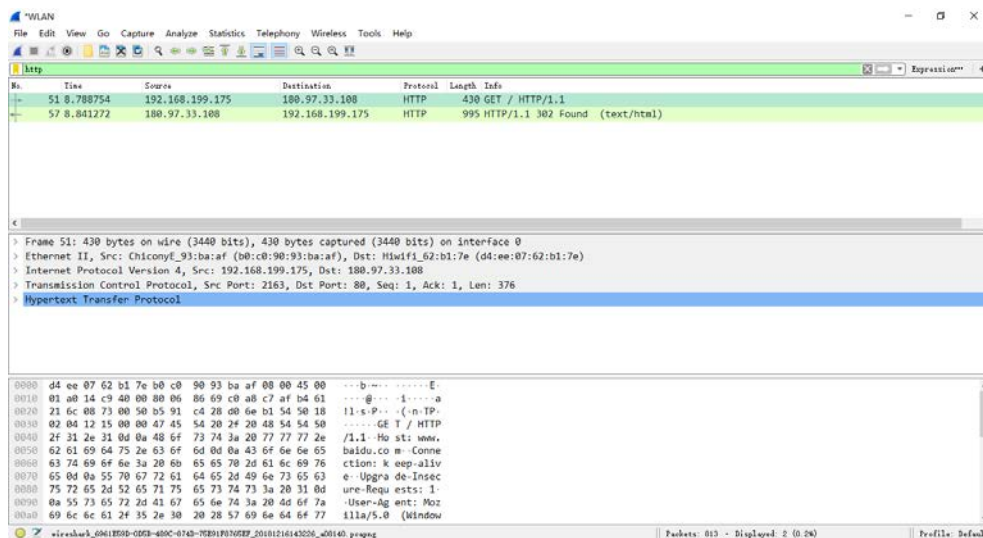
(1) 启动 Wireshark，开始分组捕获；



- (2) 启动主机上的 Chrome 浏览器，在浏览器的地址栏中输入：www.baidu.com；
- 浏览器将显示百度搜索网页；



- (3) 在窗口的显示过滤规则编辑框处输入“http”，分组列表子窗口中将只显示所捕获到的 HTTP 消息。选择分组列表窗口中的第一条 http 报文。它应该是你的计算机发向 www.baidu.com 服务器的 HTTP GET 报文；



- (4) 停止分组捕获，并根据捕获窗口内容，回答“实验报告内容”中的问题。

2. 跟踪并分析 DNS

nslookup 工具允许主机向指定的 DNS 服务器查询某个 DNS 记录。如果没有指明 DNS 服务器，nslookup 将把查询请求发向默认的 DNS 服务器。

```
命令提示符
Microsoft Windows [版本 10.0.17763.194]
(c) 2018 Microsoft Corporation. 保留所有权利。

C:\Users\Wenze>nslookup /?
用法:
nslookup [-opt ...]          # 使用默认服务器的交互模式
nslookup [-opt ...] - server # 使用 "server" 的交互模式
nslookup [-opt ...] host     # 仅查找使用默认服务器的 "host"
nslookup [-opt ...] host server # 仅查找使用 "server" 的 "host"

C:\Users\Wenze>
```

nslookup 的一般格式是: nslookup - option1 - option2 host-to-find
dns-server;

ipconfig 命令用来显示你当前的 TCP/IP 信息, 包括: 你的地址、DNS 服务器的地址、适配器的类型等信息。

如果要显示与主机相关的信息用命令: ipconfig/all;

```
命令提示符
C:\Users\Wenze>ipconfig /all

Windows IP 配置

   主机名 . . . . . : AZE-Windows
   主 DNS 后缀 . . . . . : 
   节与类型 . . . . . : 混合
   IP 路由已启用 . . . . . : 否
   WINS 代理已启用 . . . . . : 否
   DNS 后缀搜索列表 . . . . . : lan

以太网适配器 以太网:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : Realtek PCIe FE Family Controller
   物理地址 . . . . . : 
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是

无线局域网适配器 本地连接* 1:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . : 
   描述 . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   物理地址 . . . . . : 
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是

无线局域网适配器 本地连接* 2:
```

如果要查看 DNS 缓存中的记录用命令: ipconfig/displaydns

```
命令提示符
C:\Users\Wenze>ipconfig /displaydns

Windows IP 配置

array704-prod.do.dsp.mp.microsoft.com
-----
记录名称 . . . . . : array704-prod.do.dsp.mp.microsoft.com
记录类型 . . . . . : 1
生存时间 . . . . . : 2926
数据长度 . . . . . : 4
部分 . . . . . : 答案
A (主机)记录 . . . . . : 52.229.168.53

accounts.google.com
-----
记录名称 . . . . . : accounts.google.com
记录类型 . . . . . : 1
生存时间 . . . . . : 190
数据长度 . . . . . : 4
部分 . . . . . : 答案
A (主机)记录 . . . . . : 216.58.200.77

ocsp2.digicert.com
-----
记录名称 . . . . . : ocsp2.digicert.com
记录类型 . . . . . : 5
生存时间 . . . . . : 995
数据长度 . . . . . : 8
```

如果要清空 DNS 缓存用命令：ipconfig /flushdns

```
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.65

记录名称. . . . . : redirector.gvt1.com
记录类型. . . . . : 1
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.72

记录名称. . . . . : redirector.gvt1.com
记录类型. . . . . : 1
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.71

C:\Users\Wenze>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\Wenze>
```

运行以上命令需要进入 MSDOS 环境。(开始菜单->运行->输入命令“cmd”)

- (1) 利用 ipconfig 命令清空主机上的 DNS 缓存。启动 Chrome 浏览器，并将浏览器的缓存清空：

```
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.65

记录名称. . . . . : redirector.gvt1.com
记录类型. . . . . : 1
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.72

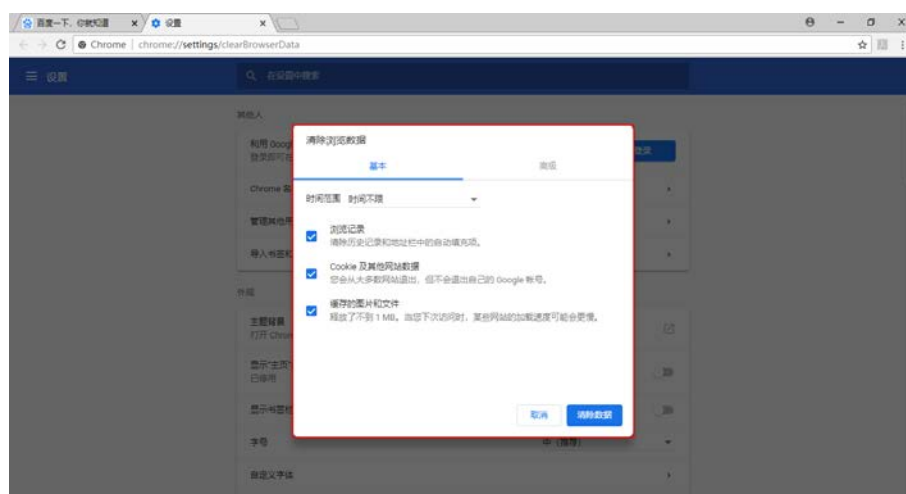
记录名称. . . . . : redirector.gvt1.com
记录类型. . . . . : 1
生存时间. . . . . : 107
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 203.208.40.71

C:\Users\Wenze>ipconfig /flushdns

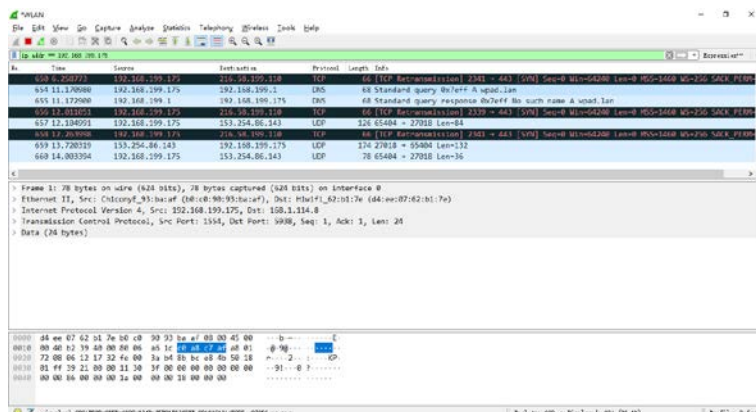
Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\Wenze>
```



- (2) 启动 Wireshark，在显示过滤筛选规则编辑框处输入：
“ip.addr == your_IP_address” (如: ip.addr==10.17.7.23);



- (3) 过滤器将会删除所有目的地址和源地址与指定 IP 地址都不同的分组;
(4) 开始 Wireshark 分组捕获;
(5) 在 Chrome 浏览器的地址栏中输入: www.baidu.com 后, 回车;
(6) 停止分组捕获;
(7) 开始 Wireshark 分组捕获。
(8) 在 www.baidu.com 上进行 nslookup 即执行命令: nslookup www.baidu.com;
(9) 停止分组捕获。

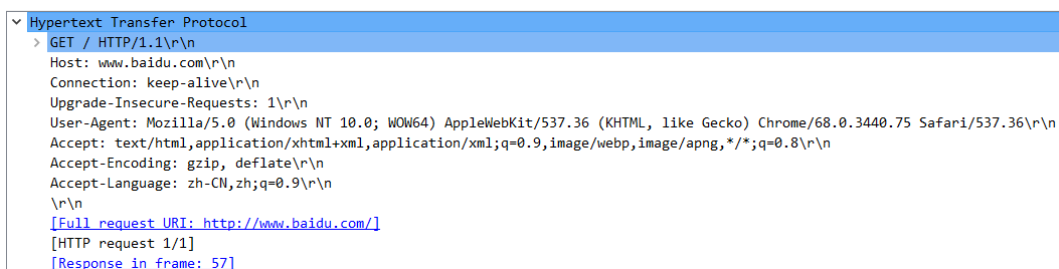
3. HTTP 分析实验结果

- (1) 从发出 HTTP GET 消息到接收到 HTTP OK 响应报文共需要多长时间? (在默认的情况下, 分组列表窗口中 Time 列的值是从 Wireshark 开始追踪到分组被捕获时总的时间, 以秒为单位。若要按 time-of-day 格式显示 Time 列的值, 需选择 View 下拉菜单, 再选择 Time Display Format, 然后选择 Time-of-day。)

No.	Time	Source	Destination	Protocol	Length	Info
51	8.788754	192.168.199.175	180.97.33.108	HTTP	430	GET / HTTP/1.1
57	8.841272	180.97.33.108	192.168.199.175	HTTP	995	HTTP/1.1 302 Found (text/html)

接收到 HTTP Found: $T = 8.841272 - 8.788754s = 0.052518s = 52.518ms$

- (2) 写出第 3 步所显示的 HTTP 消息头部行信息并说明其含义?



GET 该消息类型以及具体协议

Host 发出请求的页面所在的域

Connection 浏览器与服务器之间连接的类型

Upgrade-Insecure-Requests 告知服务器，浏览器可以处理 https 协议，与服务器返回的 Content-Security-Policy 相对应，可以将该网址（http）升级为 https 协议。

User-Agent 浏览器的用户代理字符串

Accept 浏览器能够处理的内容类型

Accept-Encoding 浏览器能够处理的压缩编码

Accept-Language 浏览器当前设置的语言

等等

- (3) 你的浏览器使用的是 HTTP1.0，还是 HTTP1.1？你所访问的 Web 服务器所用 HTTP 协议的版本号是多少？

```
Info
GET / HTTP/1.1
HTTP/1.1 302 Found (text/html)
```

均为 HTTP 1.1

- (4) 从服务器向你的浏览器返回 response 消息的状态代码是多少？表示什么意思？

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 302 Found\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n]
      Response Version: HTTP/1.1
      Status Code: 302
      [Status Code Description: Found]
      Response Phrase: Found
```

302：请求的资源现在临时从不同的 URI 响应请求。由于这样的重定向是临时的，客户端应当继续向原有地址发送以后的请求。只有在 Cache-Control 或 Expires 中进行了指定的情况下，这个响应才是可缓存的。

4. 跟踪并分析 DNS 实验结果

- (1) 定位到 DNS 查询消息和查询响应报文，这两种报文的发送是基于 UDP 还是基于 TCP 的？

No.	Time	Source	Destination	Protocol	Length	Info
4	2.564828	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CNAME www.a.shifen.com A 188.97.33.1
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xc259 A b1.bstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xc7b2 A s1.bstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0xc204 A t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0xc4151 A s11.bstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4217 A sp0.baidu.com CNAME www.a.shifen.com A 188.97.33.1
86	2.730303	192.168.199.1	192.168.199.175	DNS	130	Standard query response 0xc7b2 A s1.bstatic.com CNAME www.a.shifen.com A 188.97.33.1

Internet Protocol Version 4, Src: 192.168.199.175, Dst: 192.168.199.1						
0180 = Version: 4						
... 0181 = Header Length: 20 bytes (5)						
Differential Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 59						
Identification: 0x2e4a (11002)						
Flags: 0x0000						
Time to live: 128						
Protocol: UDP (17)						
Header checksum: 0xfcf5 [validation disabled]						
[Header checksum status: Unverified]						
Source: 192.168.199.175						
Destination: 192.168.199.1						

这两种报文的发送是基于 UDP 的

(2) DNS 查询消息的目的端口是多少？DNS 查询响应消息的端口号是多少？

No.	Time	Source	Destination	Protocol	Length	Info
4	2.564828	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CNAME www.a.shifen.com A 188.97.33.1
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xc259 A b1.bstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xc7b2 A s1.bstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0xc204 A t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0xc4151 A s11.bstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4217 A sp0.baidu.com CNAME www.a.shifen.com A 188.97.33.1
86	2.730303	192.168.199.1	192.168.199.175	DNS	130	Standard query response 0xc7b2 A s1.bstatic.com CNAME www.a.shifen.com A 188.97.33.1

Frame 4: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0						
Ethernet II, Src: Chicony_E93:ba:af (08:c0:90:93:ba:af), Dst: Huiwifl_62:bi:7e (04:ee:07:62:bi:7e)						
Internet Protocol Version 4, Src: 192.168.199.175, Dst: 192.168.199.1						
User Datagram Protocol, Src Port: 55077, Dst Port: 53						
Domain Name System (query)						

No.	Time	Source	Destination	Protocol	Length	Info
4	2.564828	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CNAME www.a.shifen.com A 188.97.33.1
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xc259 A b1.bstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xc7b2 A s1.bstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0xc204 A t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0xc4151 A s11.bstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4217 A sp0.baidu.com CNAME www.a.shifen.com A 188.97.33.1
86	2.730303	192.168.199.1	192.168.199.175	DNS	130	Standard query response 0xc7b2 A s1.bstatic.com CNAME www.a.shifen.com A 188.97.33.1

Frame 5: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0						
Ethernet II, Src: Huiwifl_62:bi:7e (04:ee:07:62:bi:7e), Dst: Chicony_E93:ba:af (08:c0:90:93:ba:af)						
Internet Protocol Version 4, Src: 192.168.199.1, Dst: 192.168.199.175						
User Datagram Protocol, Src Port: 53, Dst Port: 55077						
Domain Name System (response)						

查询消息的目的端口是 53；响应消息的目的端口号是 55077。

(3) DNS 查询消息发送的目的地址 IP 是多少？利用 ipconfig 命令(ipconfig/all)

查看你主机的本地 DNS 服务器的 IP 地址。这两个地址相同吗？

No.	Time	Source	Destination	Protocol	Length	Info
4	2.564828	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CNAME www.a.shifen.com A 188.97.33.1
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xc259 A b1.bstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0xc7b2 A s1.bstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0xc204 A t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0xc4151 A s11.bstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4217 A sp0.baidu.com CNAME www.a.shifen.com A 188.97.33.1
86	2.730303	192.168.199.1	192.168.199.175	DNS	130	Standard query response 0xc7b2 A s1.bstatic.com CNAME www.a.shifen.com A 188.97.33.1

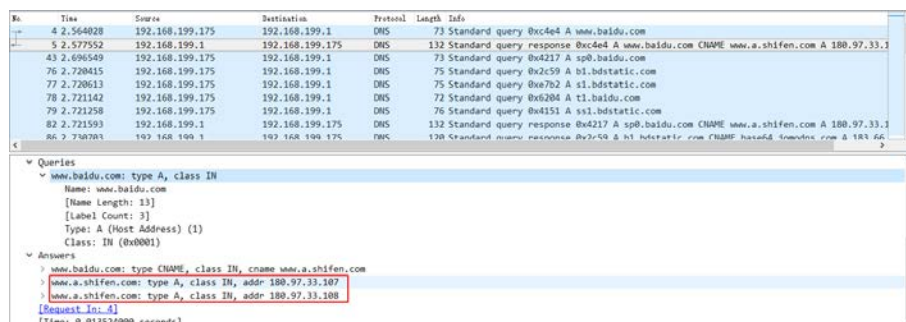
Frame 4: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0						
Ethernet II, Src: Chicony_E93:ba:af (08:c0:90:93:ba:af), Dst: Huiwifl_62:bi:7e (04:ee:07:62:bi:7e)						
Internet Protocol Version 4, Src: 192.168.199.175, Dst: 192.168.199.1						
User Datagram Protocol, Src Port: 55077, Dst Port: 53						
Domain Name System (query)						

命令提示符		媒体状态	
连接特定的 DNS 后缀	:	TeamViewer_VPN_Adapter	: 媒体已断开连接
描述	:	TeamViewer_VPN_Adapter	:
物理地址	:	80-00-00-00-00-00	:
DHCP 已启用	:	是	:
自动配置已启用	:	是	:
无线局域网适配器 WLAN:			
连接特定的 DNS 后缀	:	lan	:
描述	:	Dell Wireless 1705 802.11b/g/n (2.4GHz)	:
物理地址	:	E0-C0-90-93-BA-AF	:
DHCP 已启用	:	是	:
自动配置已启用	:	是	:
本地连接 IPv6 地址	:	fe80::3079:5439:d245:a240%9(首选)	:
IPv4 地址	:	192.168.199.175(首选)	:
子网掩码	:	255.255.255.0	:
获得租约的时间	:	2018-12-16 14:19:49	:
租约已过期时间	:	2018-12-17 2:19:50	:
默认网关	:	192.168.199.1	:
DHCP 服务器	:	192.168.199.1	:
DHCPv6 IAD	:	162578576	:
DHCPv6 客户端 DUID	:	00-01-00-01-23-80-52-F5-20-47-47-5F-08-68	:
DNS 服务器	:	192.168.199.1	:
TCP/IP 上的 NetBIOS	:	已启用	:

DNS 查询消息发送的目的地址 IP 为：192.168.199.1

主机的本地 DNS 服务器的 IP 地址为：192.168.199.1，IP 地址相同。

- (4) 考虑一下你的主机随后发送 TCP SYN Segment，包含 SYN Segment 的 IP 分组头部中目的 IP 地址是否与在 DNS 查询响应消息中提供的某个 IP 地址相对应？



No.	Time	Source	Destination	Protocol	Length	Info
4	2.564028	192.168.199.175	192.168.199.1	DNS	73	Standard query 0xc4e4 A www.baidu.com
5	2.577552	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0xc4e4 A www.baidu.com CHAME www.a.shifen.com A 180.97.33.107
43	2.696549	192.168.199.175	192.168.199.1	DNS	73	Standard query 0x4217 A sp0.baidu.com
76	2.720415	192.168.199.175	192.168.199.1	DNS	75	Standard query 0x2c59 A bl.bdstatic.com
77	2.720613	192.168.199.175	192.168.199.1	DNS	75	Standard query 0x67b2 A sl.bdstatic.com
78	2.721142	192.168.199.175	192.168.199.1	DNS	72	Standard query 0x6204 A t1.baidu.com
79	2.721258	192.168.199.175	192.168.199.1	DNS	76	Standard query 0x4151 A ssl.bdstatic.com
82	2.721593	192.168.199.1	192.168.199.175	DNS	132	Standard query response 0x4217 A sp0.baidu.com CHAME www.a.shifen.com A 180.97.33.108
86	2.730701	192.168.199.1	192.168.199.175	DNS	120	Standard query response 0x2c59 A bl.bdstatic.com CHAME www.a.shifen.com A 180.97.33.107

Queries

- www.baidu.com: type A, class IN
- Name: www.baidu.com
- [Name Length: 13]
- [Label Count: 3]
- Type: A (Host Address) (1)
- Class: IN (0x0001)

Answers

- www.baidu.com: type CHAME, class IN, cname www.a.shifen.com
- www.a.shifen.com: type A, class IN, addr: 180.97.33.107
- www.a.shifen.com: type A, class IN, addr: 180.97.33.108
- [Request In: 4]
- [Time: 0.013524000 seconds]

可能为 180.97.33.108 或 180.97.33.107

五、实验结论

收获 1. DNS 全称 Domain Name System，即域名系统，可以将域名解析为对应的 IP 地址。

收获 2. DNS 协议是基于 UDP 协议的，使用端口号为常用端口号 53。