HTTP & DNS 实验

王嵘晟

PB17111614

一. HTTP 实验

1. The Basic HTTP GET/response interaction

根据实验要求上的操作步骤进行实验，打开 Chrome 浏览器，按照实验一的方法配置 wireshark，等待一分钟，开始捕捉，点开链接，停止捕捉。

问题：

1. HTTP 1.1　　HTTP 1.1
2. zh-CN,zh;q=0.9\r\n
3. 192.168.43.195　　128.119.245.12
4. 200
5. Mon, 23 Sep 2019 14:55:27 GMT
6. 539 bytes (capture lenth)　209 bytes(file data)
7. Protocol

2. The HTTP CONDITIONAL GET/response interaction

根据实验要求上的操作步骤进行试验，打开 chrome 浏览器，清除缓存，开始捕捉，点开链接后迅速刷新网页，然后停止捕捉。

问题：

8. 没有
9. 是，200 表示正常返回了，且返回了文件
10. 是，第一次 get 得到文件的时间
11. 304 没有，第一次访问时已经返回了，第二次没有改变

3. Retrieving Long Documents

根据实验要求上的操作步骤进行试验，打开 chrome 浏览器，清除缓存，开始捕捉，点开链接，然后停止捕捉。

问题：

12. 2
13. 4
14. 200 OK
15. 没有

4. HTML Documents with Embedded Objects

根据实验要求上的操作步骤进行试验，打开 chrome 浏览器，清除缓存，开始捕捉，点开链接，然后停止捕捉。

问题：

16. 3　　128.119.245.12

```
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file4.html
Request Version: HTTP/1.1
Request Method: GET
Request URI: /pearson.png
Request Version: HTTP/1.1
Request Method: GET
Request URI: /~kurose/cover_5th_ed.jpg
Request Version: HTTP/1.1
```

17. 连续的下载，因为时间不同

5. HTTP Authentication

根据实验要求上的操作步骤进行试验，打开 chrome 浏览器，清除缓存，关闭，再打开浏览器。开始捕捉，点开链接，输入账号和密码，然后停止捕捉。

问题：

18. 401 unauthorized
19.

```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
```

二. DNS 实验

1. nslookup

打开 windows 命令行，分别输入三条指令完成实验

问题：

1.

```
C:\Users\acer>nslookup www.baidu.com
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
名称:    www.a.shifen.com
Addresses:  182.61.200.6
          182.61.200.7
Aliases:  www.baidu.com
```

2.

```
C:\Users\acer>nslookup -type=NX tu-dresden.de
unknown query type: NX
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
名称:    tu-dresden.de
Address:  141.76.16.182
```

3.

```
C:\Users\acer>nslookup -type=MX www.yahoo.com
服务器:  mx.ustc.edu.cn
Address:  202.38.64.56

非权威应答:
www.yahoo.com   canonical name = atsv2-fp-shed.wg1.b.yahoo.com

wg1.b.yahoo.com
        primary name server = yf1.yahoo.com
        responsible mail addr = hostmaster.yahoo-inc.com
        serial  = 1569328304
        refresh = 30 (30 secs)
        retry   = 30 (30 secs)
        expire  = 86400 (1 day)
        default TTL = 300 (5 mins)
```

2. ipconfig

在 Windows 命令行下输入相关指令熟悉 ipconfig

3. Tracing DNS with Wireshark

先通过 ipconfig/flushdns 清除 dns 缓存，然后清除浏览器缓存，打开 wireshark 并在 filter 栏输入 ip.addr==192.168.43.195，开始捕捉，打开链接，关闭捕捉。

问题：

4. UDP

5.

```
User Datagram Protocol, Src Port: 54868 (54868), Dst Port: domain (53)
    Source Port: 54868 (54868)
    Destination Port: domain (53)
```

6. 192.168.43.1

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . : Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC
   物理地址. . . . . . . . . . . . : C8-3D-D4-A3-2D-0F
   DHCP 已启用 . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . : 2408:84ee:c016:b609:908d:83d0:4f2a:6536(首选)
   临时 IPv6 地址. . . . . . . . . : 2408:84ee:c016:b609:6891:3394:c3a1:3892(首选)
   本地链接 IPv6 地址. . . . . . . : fe80::908d:83d0:4f2a:6536%16(首选)
   IPv4 地址 . . . . . . . . . . . : 192.168.43.195(首选)
   子网掩码 . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . : 2019年9月24日 15:49:29
   租约过期的时间  . . . . . . . . : 2019年9月24日 22:06:15
   默认网关. . . . . . . . . . . . : fe80::3274:96ff:fe71:7574%16
                                     192.168.43.1
   DHCP 服务器 . . . . . . . . . . : 192.168.43.1
   DHCPv6 IAID . . . . . . . . . . : 113786324
   DHCPv6 客户端 DUID  . . . . . . : 00-01-00-01-21-98-73-90-FC-45-96-94-BA-6E
   DNS 服务器  . . . . . . . . . . : 192.168.43.1
                                     2408:84ee:c016:b609::63
   TCPIP 上的 NetBIOS  . . . . . . : 已启用
```

相同

7. Type A 没有应答
8. 3 个，name type class time date CANME address
9. 不一致
10. 没有

接下来用 nslookup

开始捕获，用 nslookup 访问 www.mit.edu，关闭捕获

问题：

11.

```
User Datagram Protocol, Src Port: 61919 (61919), Dst Port: domain (53)
   Source Port: 61919 (61919)
   Destination Port: domain (53)
```

12. 192.168.43.1 是
13. Type A 没有
14. 3 个，name type class time date CANME address
15.

```
C:\Users\LENOVO>nslookup www.mit.edu
服务器:  UnKnown
Address:  192.168.43.1

非权威应答:
名称:    e9566.dscb.akamaiedge.net
Addresses:  2600:1400:c000:2b1::255e
          104.118.76.78
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

更换命令重新试验（1）

问题：

16. 192.168.43.1 相同
17. type NS 没有回答

18. 8 个 MIT 名字服务器，没有地址
19.

```
C:\Users\LENOVO>nslookup -type=NS mit.edu
服务器:  UnKnown
Address:  192.168.43.1

非权威应答:
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use5.akam.net
```

更换命令重新试验（2）

问题：

20. 192.168.43.1 一致
21. Type A 没有回答
22. 一个回答，name type class time data address
23.

```
C:\Users\LENOVO>nslookup www.aiit.edu
服务器:  UnKnown
Address:  192.168.43.1

非权威应答:
名称:    www.aiit.edu
Address:  202.71.129.70
```