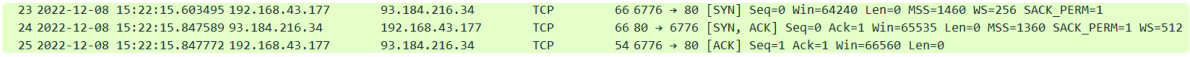
实验四报告

姓名：牟真伟　　学号：PB20051061

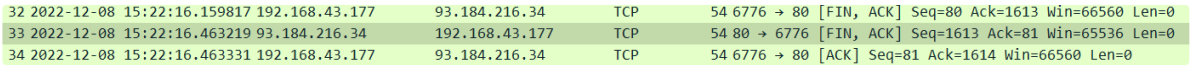
实验内容

TCP

TCP连接建立时三次握手的数据包：



TCP连接释放时的数据包(只有三次挥手)：

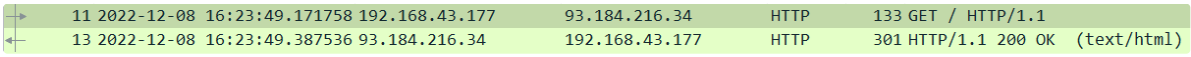


项目	数据
发送方IP地址和端口号	192.168.43.177:6776
接收方IP地址和端口号	93.184.216.34:80

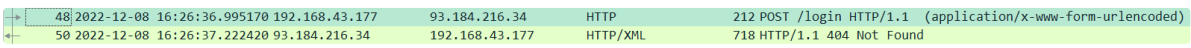
项目	握手包1	握手包2	握手包3	释放包1	释放包2	释放包3
Seq号	0	0	1	80	1613	81
Ack号	无	1	1	1613	81	1614
Flags	SYN	SYN,ACK	ACK	FIN,ACK	FIN,ACK	ACK

HTTP/HTTPS

`curl -4 -v http://www.example.com` HTTP数据包：

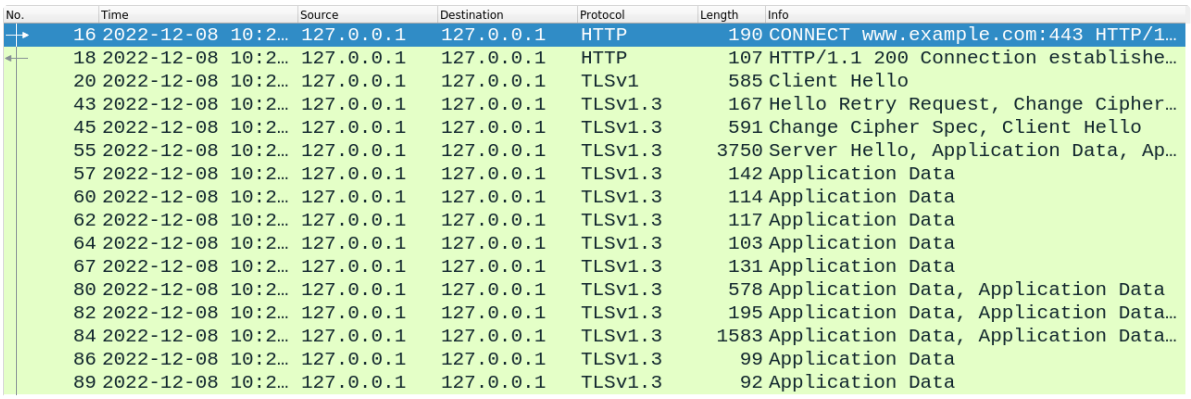


`curl -4 -v -d "user=test" http://example.com/login` HTTP数据包：



指令	协议版本	方法类型	状态码	回复包内容类型
`curl -4 -v http://www.example.com`	HTTP/1.1	GET	200	text/html
`curl -4 -v -d "user=test" http://example.com/login`	HTTP/1.1	POST	404	text/html

`curl -4 -v https://www.example.com`HTTPS数据包：



No.	Time	Source	Destination	Protocol	Length	Info
16	2022-12-08 10:2…	127.0.0.1	127.0.0.1	HTTP	190	CONNECT www.example.com:443 HTTP/1…
18	2022-12-08 10:2…	127.0.0.1	127.0.0.1	HTTP	107	HTTP/1.1 200 Connection establishe…
20	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1	585	Client Hello
43	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	167	Hello Retry Request, Change Cipher…
45	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	591	Change Cipher Spec, Client Hello
55	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	3750	Server Hello, Application Data, Ap…
57	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	142	Application Data
60	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	114	Application Data
62	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	117	Application Data
64	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	103	Application Data
67	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	131	Application Data
80	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	578	Application Data, Application Data
82	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	195	Application Data, Application Data…
84	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	1583	Application Data, Application Data…
86	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	99	Application Data
89	2022-12-08 10:2…	127.0.0.1	127.0.0.1	TLSv1.3	92	Application Data

DNS

查询目标	命令	结果
www.baidu.com 的 IPv4 地址	`dig www.baidu.com @8.8.8.8`	14.215.177.39或14.215.177.38
202.38.75.11 的域名	`dig -x 202.38.75.11 @8.8.8.8`	infonet.ustc.edu.cn
jw.ustc.edu.cn 的 IPv6 地址（AAAA）	`dig -t aaaa jw.ustc.edu.cn @8.8.8.8`	2001:da8:d800:642::248
mail.ustc.edu.cn 的邮件交换记录（MX）	`dig mx mail.ustc.edu.cn @8.8.8.8`	5 smtp1.ustc.edu.cn,10 smtp.ustc.edu.cn,10 smtp2.ustc.edu.cn
i.ustc.edu.cn 的别名记录（CNAME）	`dig cname i.ustc.edu.cn @8.8.8.8`	revproxy.ustc.edu.cn
example.com 的域名服务器记录（NS）	`dig ns example.com @8.8.8.8`	a.iana-servers.net,b.iana-servers.net

dig查询根服务器：

```
aweary@LAPTOP-07C8FQOM:/mnt/d/Linux$ dig @8.8.8.8

; <<>> DiG 9.16.1-Ubuntu <<>> @8.8.8.8
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16153
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       17221   IN      NS      g.root-servers.net.
.                       17221   IN      NS      j.root-servers.net.
.                       17221   IN      NS      e.root-servers.net.
.                       17221   IN      NS      l.root-servers.net.
.                       17221   IN      NS      d.root-servers.net.
.                       17221   IN      NS      a.root-servers.net.
.                       17221   IN      NS      b.root-servers.net.
.                       17221   IN      NS      i.root-servers.net.
.                       17221   IN      NS      m.root-servers.net.
.                       17221   IN      NS      h.root-servers.net.
.                       17221   IN      NS      c.root-servers.net.
.                       17221   IN      NS      k.root-servers.net.
.                       17221   IN      NS      f.root-servers.net.

;; Query time: 98 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Dec 08 20:32:08 CST 2022
;; MSG SIZE  rcvd: 239
```

dig查询<your-student-id>.ustc.edu.cn ：

```
aweary@aweary-computer:~$ dig pb20051061.ustc.edu.cn

; <<>> DiG 9.16.15-Ubuntu <<>> pb20051061.ustc.edu.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 4996
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;pb20051061.ustc.edu.cn.                IN      A

;; Query time: 12 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Dec 08 10:36:26 EST 2022
;; MSG SIZE  rcvd: 51
```

status字段为NXDOMAIN

FTP

主动模式：

```
    192.168.43.177.33670 > 202.38.64.10.21: Flags [P.], cksum 0xfba8 (correct), seq 406753
356:406753385, ack 2724399643, win 501, options [nop,nop,TS val 4000109685 ecr 1433901973]
, length 29: FTP, length: 29
        PORT 192,168,43,177,192,151
        0x0000:  4510 0051 df8f 4000 4006 647d c0a8 2bb1  E..Q..@.@.d}..+.
        0x0010:  ca26 400a 8386 0015 183e 904c a263 0a1b  .&@......>.L.c..
        0x0020:  8018 01f5 fba8 0000 0101 080a ee6c d475  .............l.u
        0x0030:  5577 9b95 504f 5254 2031 3932 2c31 3638  Uw..PORT.192,168
        0x0040:  2c34 332c 3137 372c 3139 322c 3135 310d  ,43,177,192,151.
        0x0050:  0a                                       .
```

客户端开启的数据通道的端口号为192*256+151=49303

被动模式：

```
    192.168.43.177.33672 > 202.38.64.10.21: Flags [P.], cksum 0xbd72 (correct), seq 311125
2502:3111252508, ack 3888007598, win 501, options [nop,nop,TS val 4001032656 ecr 143500946
0], length 6: FTP, length: 6
        PASV
        0x0000:  4510 003a dc75 4000 4006 67ae c0a8 2bb1  E..:.u@.@.g...+.
        0x0010:  ca26 400a 8388 0015 b971 f216 e7be 49ae  .&@......q....I.
        0x0020:  8018 01f5 bd72 0000 0101 080a ee7a e9d0  .....r.......z..
        0x0030:  5588 81b4 5041 5356 0d0a                 U...PASV..
10:00:45.977968 wlp1s0 In  IP (tos 0x0, ttl 49, id 11981, offset 0, flags [DF], proto TCP
(6), length 102)
    202.38.64.10.21 > 192.168.43.177.33672: Flags [P.], cksum 0x5cd9 (correct), seq 1:51,
ack 6, win 181, options [nop,nop,TS val 1435044484 ecr 4001032656], length 50: FTP, length
: 50
        227 Entering Passive Mode (202,38,64,10,181,105)
        0x0000:  4500 0066 2ecd 4000 3106 243b ca26 400a  E..f..@.1.$;.&@.
        0x0010:  c0a8 2bb1 0015 8388 e7be 49ae b971 f21c  ..+.......I..q..
        0x0020:  8018 00b5 5cd9 0000 0101 080a 5589 0a84  ....\.......U...
        0x0030:  ee7a e9d0 3232 3720 456e 7465 7269 6e67  .z..227.Entering
        0x0040:  2050 6173 7369 7665 204d 6f64 6520 2832  .Passive.Mode.(2
        0x0050:  3032 2c33 382c 3634 2c31 302c 3138 312c  02,38,64,10,181,
        0x0060:  3130 3529 0d0a                           105)..
```

服务端开启的数据端口的端口号为181*256+105=46441，与后续数据包一致

```
    192.168.43.177.38678 > 202.38.64.10.46441: Flags [S], cksum 0xa378 (correct), seq 1701
259123, win 64240, options [mss 1460,sackOK,TS val 4001033014 ecr 0,nop,wscale 7], length
0
        0x0000:  4500 003c e003 4000 4006 642e c0a8 2bb1  E..<..@.@.d...+.
        0x0010:  ca26 400a 9716 b569 6567 2773 0000 0000  .&@....ieg's....
        0x0020:  a002 faf0 a378 0000 0204 05b4 0402 080a  .....x..........
        0x0030:  ee7a eb36 0000 0000 0103 0307            .z.6........
```

思考题

1. 解释 HTTP 中的幂等是什么意思？GET 操作是幂等的吗？POST 呢？

HTTP方法的幂等性是指一次和多次请求某一个资源应该具有同样的副作用，GET方法只是获取特定资源，并不会对该资源做出修改，因此GET操作是幂等的.

POST方法会对资源做出修改，调用多次POST方法得到的结果不同，因此POST方法不是幂等的.

2. HTTPS 抓到的数据包与之前 HTTP 中抓到的有何不同？这是什么原因导致的？

HTTPS抓到的数据包使用TLS协议传输，且传输的数据为加密后的数据，因为HTTPS运行在SSL/TLS上，会对传输的数据进行加密.

3. FTP 实验中使用的 `sudo tcpdump -i any -vvnX host home.ustc.edu.cn` 指令整体可以达到什么效果？其中每个参数的含义分别是什么？

在所有网络接口上,抓取ip地址为home.ustc.edu.cn对应地址的数据包,并输出详细的报文信息

`-i any`:监听所有端口

`host`:抓取ip地址为home.ustc.edu.cn对应地址的数据包

`-vv`:输出详细的报文信息

`-n`:不把网络地址转换成名字

`-X`:以16进制和ASCII码形式显示每个报文（去掉链路层报头）

4. 解释从输入网址，到浏览器显示网页，在客户端的应用层依次发生了什么？

应用层首先发起DNS请求,查询到输入网址域名所对应的IP地址,应用层的HTTP协议对输入网址的资源发出HTTP请求,服务器处理请求并返回HTTP响应报文,得到服务器端的资源文件后,浏览器将资源文件渲染成网页,并显示出来.