

ID 22031212122  
NAME xiaoning Shu  
TEAC zhiwei Zhang  
DATE 20230523



西安电子科技大学  
XIDIAN UNIVERSITY

*Experimentation and practice of new generation information technology*

---

## HOMEWORK 2 Network Analysis Technology Experiment

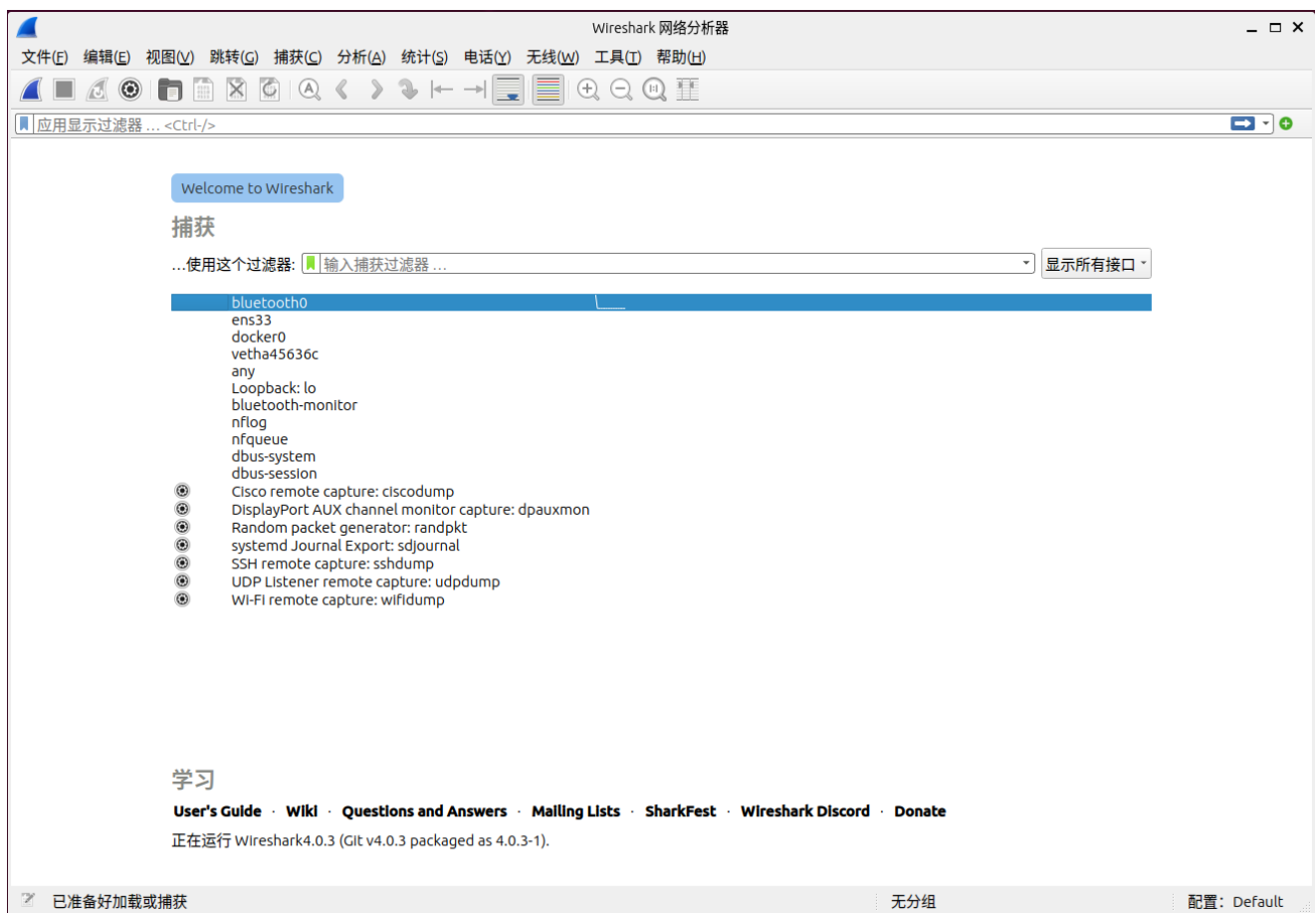
# 网络分析技术实验

### HTTP协议分析实验

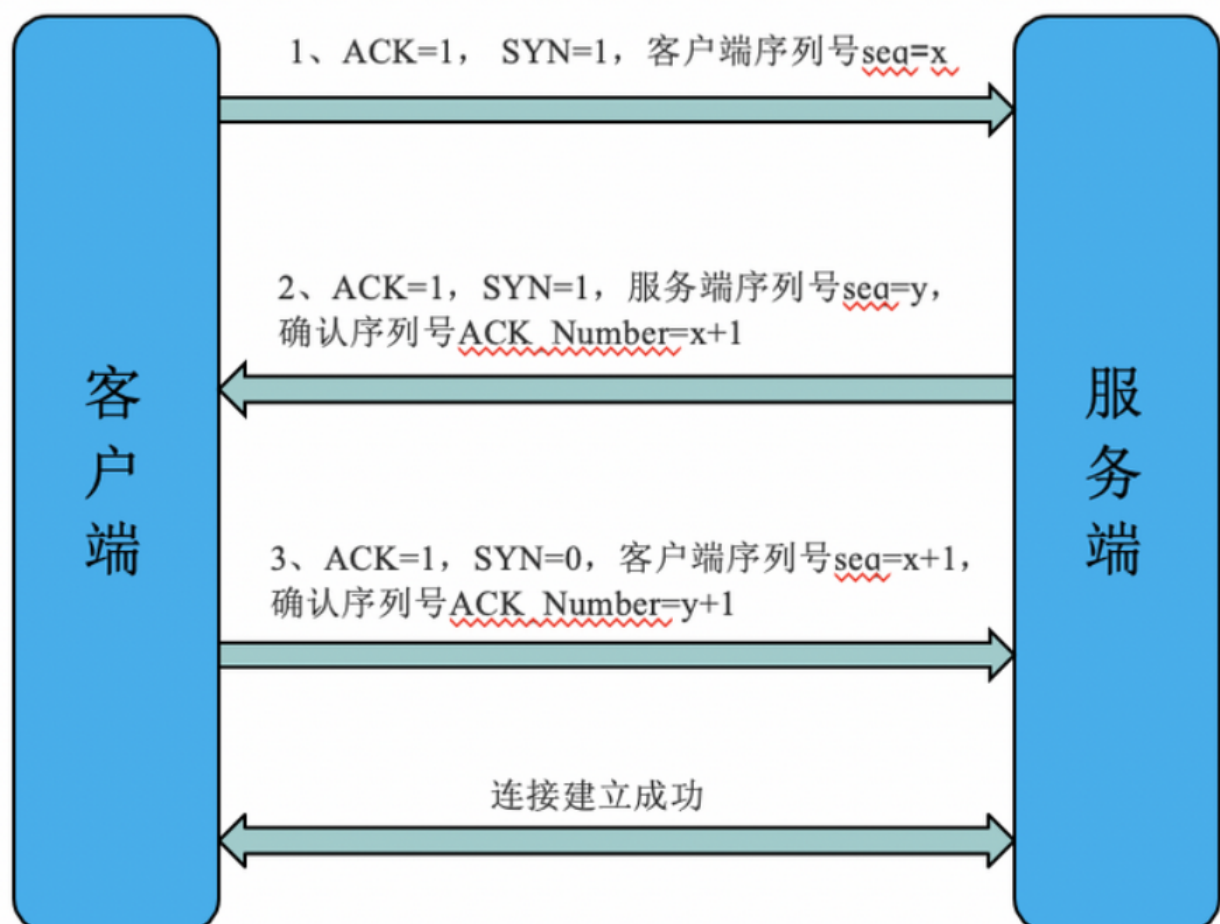
利用实验（一）建立的Web应用（虚拟机和容器两个版本），在用户侧使用网络抓包分析工具进行协议分析，观察并分析BS之间交互的过程和内容，对比虚拟机和容器版本交互内容有无异差。

安装抓包工具Wireshark

```
sudo apt-get install wireshark
```



这是抓包的记录，因为我使用了云MySQL服务器，所以在进行运行登录界面时，会对云MySQL服务器进行握手规则。



1	0.000000000	192.168.107.128	142.251.43.10	TCP	74	49112	- 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4239513423 TSecr=0 WS=128
2	0.004061206	192.168.107.128	142.251.42.234	TCP	74	39002	- 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418188435 TSecr=0 WS=128
3	0.284235017	192.168.107.128	142.251.42.234	TCP	74	39012	- 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418188655 TSecr=0 WS=128
4	0.070409987	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39002 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418190447 TSecr=0 WS=128	
5	0.230047025	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39012 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418190071 TSecr=0 WS=128	
6	0.420155922	192.168.107.128	172.217.103.42	TCP	74	43440	- 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3130484545 TSecr=0 WS=128
7	4.192202177	192.168.107.128	142.251.43.10	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 49112 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4239517615 TSecr=0 WS=128	
8	0.235994245	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39002 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418194607 TSecr=0 WS=128	
9	0.492071420	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39012 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418194803 TSecr=0 WS=128	
10	8.54057461	Vmware_e0:a5:38	Vmware_e0:a5:38	ARP	42	who has 192.168.107.27 Tell 192.168.107.128	
11	8.540851620	Vmware_e0:a5:38	Vmware_e0:a5:38	ARP	60	192.168.107.2 is at 00:50:56:e0:a5:38	
12	9.042074308	172.217.103.42	192.168.107.128	TCP	60	443 - 43440 [RST, ACK] Seq=1 ACK=1 Win=64240 Len=0	
13	0.043000000	192.168.107.128	142.251.42.234	TCP	74	49112	- 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4181917414 TSecr=0 WS=128
14	10.044197837	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 34782 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418198415 TSecr=0 WS=128	
15	12.000000000	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 34782 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418200431 TSecr=0 WS=128	
16	12.390846424	192.168.107.128	142.251.43.10	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 49112 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4239525004 TSecr=0 WS=128	
17	14.408218836	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39002 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418202709 TSecr=0 WS=128	
18	14.084504181	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 39012 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418203955 TSecr=0 WS=128	

然后是我的主机像我的Tomcat服务器进行三次握手规则。后面进行了登陆之后的信息传输。

21	14.784266015	192.168.107.128	185.125.190.18	TCP	74	53486	- 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3014288261 TSecr=0 WS=128
22	15.107814006	185.125.190.18	192.168.107.128	TCP	60	80	- 53486 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
23	15.167905400	192.168.107.128	185.125.190.18	TCP	54	53486	- 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
24	16.168122403	192.168.107.128	185.125.190.18	HTTP	142	GET / HTTP/1.1	
25	15.168250824	185.125.190.18	192.168.107.128	TCP	60	80	- 53486 [ACK] Seq=1 Ack=89 Win=64240 Len=0
26	15.614158852	185.125.190.18	192.168.107.128	HTTP	243	HTTP/1.1 204 No Content	
27	15.614669955	192.168.107.128	185.125.190.18	TCP	54	53486	- 80 [FIN, ACK] Seq=89 Ack=191 Win=64059 Len=0
28	15.615132750	185.125.190.18	192.168.107.128	TCP	60	80	- 53486 [ACK] Seq=191 Ack=90 Win=64239 Len=0
29	19.220302534	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 34782 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=418204591	
30	16.568787466	192.168.107.128	124.222.251.11	TCP	59	57204	- 72738 [PSH, ACK] Seq=1 Ack=1 Win=63076 Len=5
31	16.569340849	124.222.251.11	192.168.107.128	TCP	60	72738	- 57204 [ACK] Seq=1 Ack=6 Win=64240 Len=0
32	16.579484294	124.222.251.11	192.168.107.128	TCP	65	27238	- 57204 [PSH, ACK] Seq=1 Ack=6 Win=64240 Len=11
33	16.579652928	192.168.107.128	124.222.251.11	TCP	54	57204	- 72738 [ACK] Seq=6 Ack=12 Win=63076 Len=0
34	16.583083102	192.168.107.128	124.222.251.11	TCP	459	57204	- 72738 [PSH, ACK] Seq=6 Ack=12 Win=63076 Len=405
35	16.584072104	124.222.251.11	192.168.107.128	TCP	60	27238	- 57204 [ACK] Seq=12 Ack=411 Win=64240 Len=0
36	16.594021353	124.222.251.11	192.168.107.128	TCP	1020	27238	- 57204 [PSH, ACK] Seq=12 Ack=411 Win=64240 Len=966
37	16.602516594	192.168.107.128	124.222.251.11	TCP	298	57204	- 72738 [PSH, ACK] Seq=411 Ack=978 Win=63076 Len=244
38	16.602909342	124.222.251.11	192.168.107.128	TCP	60	27238	- 57204 [ACK] Seq=978 Ack=655 Win=64240 Len=0
39	16.612307499	124.222.251.11	192.168.107.128	TCP	626	27238	- 57204 [PSH, ACK] Seq=978 Ack=655 Win=64240 Len=572
40	16.620831114	192.168.107.128	124.222.251.11	TCP	973	57204	- 72738 [PSH, ACK] Seq=655 Ack=1550 Win=63076 Len=919
41	16.621936872	124.222.251.11	192.168.107.128	TCP	60	27238	- 57204 [ACK] Seq=1550 Ack=1574 Win=64240 Len=0
42	16.633844435	124.222.251.11	192.168.107.128	TCP	13194	27238	- 57204 [ACK] Seq=1550 Ack=1574 Win=64240 Len=13140
43	16.634339958	124.222.251.11	192.168.107.128	TCP	565	27238	- 57204 [PSH, ACK] Seq=14690 Ack=1574 Win=64240 Len=511
44	16.635274787	192.168.107.128	124.222.251.11	TCP	54	57204	- 72738 [ACK] Seq=1574 Ack=15201 Win=55480 Len=0
45	16.652878542	192.168.107.128	124.222.251.11	TCP	75	57204	- 72738 [PSH, ACK] Seq=1574 Ack=15201 Win=62780 Len=21
46	16.653125986	124.222.251.11	192.168.107.128	TCP	60	27238	- 57204 [ACK] Seq=15201 Ack=1595 Win=64240 Len=0
47	16.662596698	124.222.251.11	192.168.107.128	TCP	65	27238	- 57204 [PSH, ACK] Seq=15201 Ack=1595 Win=64240 Len=11
48	16.676068839	192.168.107.128	124.222.251.11	TCP	258	57204	- 72738 [PSH, ACK] Seq=1595 Ack=15212 Win=62780 Len=204
49	16.676226009	124.222.251.11	192.168.107.128	TCP	60	27238	- 57204 [ACK] Seq=15212 Ack=1799 Win=64240 Len=0

以上是8080端口的idea登录方式。以下证明docker形式的登录。

1	0.000000000	192.168.107.128	104.26.11.240	TCP	54	56038	- 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
2	0.000118756	104.26.11.240	192.168.107.128	TCP	60	[TCP ACKed unseen segment] 443 - 56038 [ACK] Seq=1 Ack=2 Win=64240 Len=0	
3	1.150086478	192.168.107.128	192.168.107.2	DNS	102	Standard query 0xf788 A content-autofill.googleapis.com OPT	
4	1.150461170	192.168.107.128	192.168.107.2	DNS	102	Standard query 0x6cea HTTPS content-autofill.googleapis.com OPT	
5	1.164782212	192.168.107.2	192.168.107.128	DNS	159	Standard query response 0x6cea HTTPS content-autofill.googleapis.com SOA ns1.google.com OPT	
6	1.164782580	192.168.107.2	192.168.107.128	DNS	150	Standard query response 0xf788 A content-autofill.googleapis.com A 142.251.42.234 A 172.217.160.7	
7	1.167832783	192.168.107.128	142.251.42.234	TCP	74	42400	- 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=419808319 TSecr=0 WS=128
8	1.283025136	31.13.76.99	192.168.107.128	TCP	60	443 - 38226 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0	
9	1.406080122	192.168.107.128	142.251.42.234	TCP	74	42402	- 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=419808558 TSecr=0 WS=128
10	1.436757140	31.13.76.99	192.168.107.128	TCP	60	443 - 38228 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0	
11	1.530478486	31.13.76.99	192.168.107.128	TCP	60	443 - 38234 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0	
12	1.711554343	31.13.76.99	192.168.107.128	TCP	60	443 - 38244 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0	
13	1.916638728	31.13.76.99	192.168.107.128	TCP	60	443 - 38256 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0	
14	2.17570753	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 42400 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460	
15	2.432190715	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 42402 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460	
16	2.989994093	31.13.76.99	192.168.107.128	TCP	60	443 - 38262 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0	
17	4.139398589	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 42400 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460	
18	4.448139004	192.168.107.128	142.251.42.234	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 42402 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460	

这是docker 8080端口进行登录时的对云MySQL的连接。可以看到进行了握手规则。

下面是对Tomcat服务器以及登录后渲染界面的信息传输。

19	8.156853417	192.168.107.128	124.222.251.11	TCP	59	54022	- 72738 [PSH, ACK] Seq=1 Ack=1 Win=63076 Len=5
20	8.157358950	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=1 Ack=6 Win=64240 Len=0
21	8.165978181	124.222.251.11	192.168.107.128	TCP	65	27238	- 54022 [PSH, ACK] Seq=1 Ack=6 Win=64240 Len=11
22	8.166068596	192.168.107.128	124.222.251.11	TCP	54	54022	- 72738 [ACK] Seq=6 Ack=12 Win=63076 Len=0
23	8.172243569	192.168.107.128	124.222.251.11	TCP	459	54022	- 72738 [PSH, ACK] Seq=6 Ack=12 Win=63076 Len=405
24	8.172521856	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=12 Ack=411 Win=64240 Len=0
25	8.182247060	124.222.251.11	192.168.107.128	TCP	1020	27238	- 54022 [PSH, ACK] Seq=12 Ack=411 Win=64240 Len=966
26	8.191261880	192.168.107.128	124.222.251.11	TCP	298	54022	- 72738 [PSH, ACK] Seq=411 Ack=978 Win=63076 Len=244
27	8.191662741	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=978 Ack=655 Win=64240 Len=0
28	8.200534356	124.222.251.11	192.168.107.128	TCP	626	27238	- 54022 [PSH, ACK] Seq=978 Ack=655 Win=64240 Len=572
29	8.211403341	192.168.107.128	124.222.251.11	TCP	973	54022	- 72738 [PSH, ACK] Seq=655 Ack=1550 Win=63076 Len=919
30	8.211713481	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=1550 Ack=1574 Win=64240 Len=0
31	8.222372017	124.222.251.11	192.168.107.128	TCP	13705	27238	- 54022 [PSH, ACK] Seq=1550 Ack=1574 Win=64240 Len=13651
32	8.222683465	192.168.107.128	124.222.251.11	TCP	54	54022	- 72738 [ACK] Seq=1574 Ack=15201 Win=55480 Len=0
33	8.258904240	192.168.107.128	124.222.251.11	TCP	75	54022	- 72738 [PSH, ACK] Seq=1574 Ack=15201 Win=62780 Len=21
34	8.259264793	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=15201 Ack=1595 Win=64240 Len=0
35	8.260251412	124.222.251.11	192.168.107.128	TCP	65	27238	- 54022 [PSH, ACK] Seq=15201 Ack=1595 Win=64240 Len=11
36	8.276032711	192.168.107.128	124.222.251.11	TCP	256	54022	- 72738 [PSH, ACK] Seq=1595 Ack=15212 Win=62780 Len=202
37	8.276255426	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=15212 Ack=1797 Win=64240 Len=0
38	8.284879548	124.222.251.11	192.168.107.128	TCP	67	27238	- 54022 [PSH, ACK] Seq=15212 Ack=1797 Win=64240 Len=13
39	8.292828536	192.168.107.128	124.222.251.11	TCP	65	54022	- 72738 [PSH, ACK] Seq=1797 Ack=15225 Win=62780 Len=11
40	8.293188097	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=15225 Ack=1808 Win=64240 Len=0
41	8.303920444	124.222.251.11	192.168.107.128	TCP	65	27238	- 54022 [PSH, ACK] Seq=15225 Ack=1808 Win=64240 Len=11
42	8.304973498	192.168.107.128	124.222.251.11	TCP	75	54022	- 72738 [PSH, ACK] Seq=1808 Ack=15236 Win=62780 Len=21
43	8.305163551	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=15236 Ack=1829 Win=64240 Len=0
44	8.314245009	124.222.251.11	192.168.107.128	TCP	65	27238	- 54022 [PSH, ACK] Seq=15236 Ack=1829 Win=64240 Len=11
45	8.348505849	192.168.107.128	124.222.251.11	TCP	129	54022	- 72738 [PSH, ACK] Seq=1829 Ack=15247 Win=62780 Len=75
46	8.348081729	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=15247 Ack=1904 Win=64240 Len=0
47	8.350710151	124.222.251.11	192.168.107.128	TCP	1666	27238	- 54022 [PSH, ACK] Seq=15247 Ack=1904 Win=64240 Len=1612
48	8.359756156	192.168.107.128	124.222.251.11	TCP	54	54022	- 72738 [ACK] Seq=1904 Ack=16859 Win=62780 Len=0
49	8.381970266	192.168.107.128	124.222.251.11	TCP	92	54022	- 72738 [PSH, ACK] Seq=1904 Ack=16859 Win=62780 Len=38
50	8.382482440	124.222.251.11	192.168.107.128	TCP	60	27238	- 54022 [ACK] Seq=16859 Ack=1942 Win=64240 Len=0
51	8.392782158	124.222.251.11	192.168.107.128	TCP	65	27238	- 54022 [PSH, ACK] Seq=16859 Ack=1942 Win=64240 Len=11

Frame 133: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0 (ens33)

Section number: 1

Encapsulation type: Ethernet (1)

Arrival Time: May 21, 2023 09:13:42.781799300 CST

[Time delta from previous captured frame: 0.000000000 seconds]

Epoch Time: 1684631622.781799300 seconds

[Time delta from previous displayed frame: 0.589968175 seconds]

[Time since reference or first frame: 9.333605540 seconds]

Frame Number: 133

Frame Length: 102 bytes (816 bits)

Capture Length: 102 bytes (816 bits)

0000 00 50 e0 a5 38 00 0c 29 9b ee a3 08 00 45 00 PV: 8... ).....E

0010 00 58 ac e9 00 00 40 11 75 d8 c0 ab 6b 00 c0 ab X...@...k...

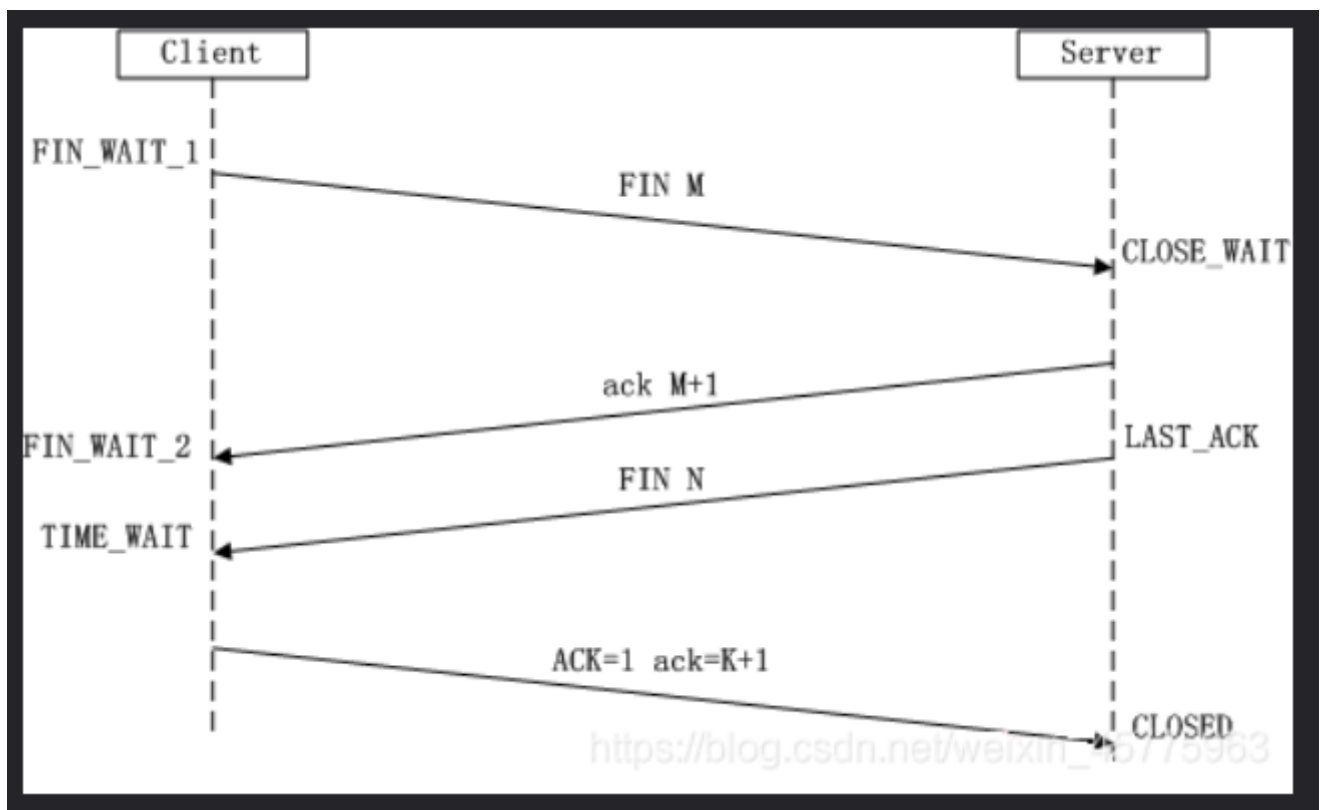
0020 6b 02 c8 59 00 35 00 44 58 29 1c 9c 01 00 00 1 k...Y.5 D X).....c

0030 00 00 00 00 00 01 10 63 6f be 74 65 0e 74 2d 01 .. content-a

0040 75 74 6f be 6c 65 01 70 00 00 00 00 00 00 00 00 utfoll goog leap

0050 69 73 83 63 6f 6d 00 00 01 01 00 00 29 05 c0 is com

0060 00 00 00 00 00 00 00 00 .....



内容之间的交互差异：

除了网络之外，文件也是重要的进行数据交互的资源。在以往的虚拟机中，我们通常直接采用虚拟机的文件系统作为应用数据等文件的存储位置。然而这种方式其实并非完全安全的，当虚拟机或者容器出现问题导致文件系统无法使用时，虽然我们可以很快的通过镜像重置文件系统使得应用快速恢复运行，但是之前存放的数据也就消失了。

为了保证数据的独立性，我们通常会单独挂载一个文件系统来存放数据。这种操作在虚拟机中是繁琐的，因为我们不但要搞定挂载在不同宿主机中实现的方法，还要考虑挂载文件系统兼容性，虚拟操作系统配置等问题。值得庆幸的是，这些在 Docker 里都已经为我们轻松的实现了，我们只需要简单的一两个命令或参数，就能完成文件系统目录的挂载。

能够这么简单的实现挂载，主要还是得益于 Docker 底层的 Union File System 技术。在 UnionFS 的加持下，除了能够从宿主操作系统中挂载目录外，还能够建立独立的目录持久存放数据，或者在容器间共享。

在 Docker 中，通过这几种方式进行数据共享或持久化的文件或目录，我们都称为数据卷 (Volume)。

通过挂载数据卷的方式，我们可以让宿主机的文件数据和容器中的文件数据进行交互，可以得知容器内部发生的情况，还可以通过容器之间继承数据卷的方式，实现容器集群共享数据。



# HTTPS协议分析实验

- 在HTTP实验选择的Web应用版本基础上（虚拟机和容器两个版本），开启HTTPS服务；在用户侧使用网络抓包分析工具进行协议分析，观察并分析BS之间交互的过程和内容，对比虚拟机和容器版本交互内容有无异差。

我在上海，仔细看了看网址，好像需要登录VPN，要是不打不开网页。

这是HTTP协议抓的包：

1	0.000000000	VHware-sh0e:a3	VHware-sh0e:a3	ARP	42 who has 192.168.107.2 Tell 192.168.107.128
2	0.000270082	VHware-sh0e:a3	VHware-sh0e:a3	ARP	60 192.168.107.2 is at 60:50:56:e0:a5:38
3	1.020635467	192.168.107.128	142.251.42.234	TCP	74 60024 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=420627824 TSecr=0 WS=128
4	1.020635467	192.168.107.128	142.251.42.234	TCP	74 60024 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=420627824 TSecr=0 WS=128
5	1.076904490	192.168.107.128	192.168.107.2	DNS	82 Standard query 0x2700 A www.xdqv.com OPT
6	1.076904490	192.168.107.128	192.168.107.2	DNS	82 Standard query 0x3bf5 HTTPS www.xdqv.com OPT
7	1.010675333	192.168.107.2	192.168.107.128	DNS	114 Standard query response 0x2700 A www.xdqv.com A 104.21.78.45 A 172.67.210.6 OPT
8	1.010675333	192.168.107.2	192.168.107.128	DNS	161 Standard query response 0x3bf5 HTTPS www.xdqv.com HTTPS OPT
9	1.015484205	192.168.107.128	104.21.78.45	TCP	74 43454 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=444940158 TSecr=0 WS=128
10	1.050642705	192.168.107.128	192.168.107.128	TCP	60 443 - 43454 [FIN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
11	1.952917511	192.168.107.128	104.21.78.45	TCP	54 43454 - 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
12	1.953048709	192.168.107.128	104.21.78.45	TLVSl.3	571 Client Hello
13	1.953037024	192.168.107.128	192.168.107.128	TCP	60 443 - 43454 [ACK] Seq=1 Ack=518 Win=64240 Len=0
14	1.973878784	192.168.107.128	104.21.78.45	QUIC	1292 Initial, DCID=75ac43ed388df059, PKN: 1, PING, PING, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PADDING
15	1.974239114	192.168.107.128	104.21.78.45	QUIC	120 e-RTT, DCID=75ac43ed388df059
16	1.974544471	192.168.107.128	104.21.78.45	QUIC	480 e-RTT, DCID=75ac43ed388df059
17	1.992838244	104.21.78.45	192.168.107.128	TLVSl.3	2170 Server Hello, Change Cipher Spec, Application Data
18	1.992880734	192.168.107.128	104.21.78.45	TCP	54 43454 - 443 [ACK] Seq=518 Ack=2123 Win=62780 Len=0
19	1.994999481	192.168.107.128	104.21.78.45	TLVSl.3	118 Change Cipher Spec, Application Data
20	1.994384307	104.21.78.45	192.168.107.128	TCP	60 443 - 43454 [ACK] Seq=2123 Ack=582 Win=64240 Len=0
21	2.012499810	104.21.78.45	192.168.107.128	QUIC	1242 Protected Payload (KPo)
22	2.015869175	104.21.78.45	192.168.107.128	QUIC	1242 Protected Payload (KPo)
23	2.015869602	104.21.78.45	192.168.107.128	QUIC	1242 Handshake, SCID=8168dc123e93bf7af126a9a120d938b06c1e1e48
24	2.015869605	104.21.78.45	192.168.107.128	QUIC	892 Handshake, SCID=8168dc123e93bf7af126a9a120d938b06c1e1e48
25	2.014651886	192.168.107.128	104.21.78.45	QUIC	1292 Protected Payload (KPo), DCID=8168dc123e93bf7af126a9a120d938b06c1e1e48
26	2.017573451	192.168.107.128	104.21.78.45	QUIC	128 Handshake, DCID=8168dc123e93bf7af126a9a120d938b06c1e1e48
27	2.024095453	104.21.78.45	192.168.107.128	TLVSl.3	582 Application Data, Application Data
28	2.048983845	192.168.107.128	142.251.42.228	TCP	74 46358 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1955346431 TSecr=0 WS=128
29	2.054433813	192.168.107.128	192.168.107.128	QUIC	570 Protected Payload (KPo)
30	2.054433813	104.21.78.45	192.168.107.128	QUIC	66 Protected Payload (KPo)
31	2.054433879	104.21.78.45	192.168.107.128	QUIC	66 Protected Payload (KPo)
32	2.054433946	104.21.78.45	192.168.107.128	QUIC	91 Protected Payload (KPo)
33	2.050685504	192.168.107.128	104.21.78.45	QUIC	85 Protected Payload (KPo), DCID=8168dc123e93bf7af126a9a120d938b06c1e1e48
34	2.057291057	192.168.107.128	104.21.78.45	QUIC	89 Protected Payload (KPo), DCID=8168dc123e93bf7af126a9a120d938b06c1e1e48
35	2.072761540	192.168.107.128	104.21.78.45	QUIC	54 43454 - 443 [ACK] Seq=582 Ack=2051 Win=62780 Len=0
36	2.093450122	104.21.78.45	192.168.107.128	QUIC	70 Protected Payload (KPo)
37	2.093787688	192.168.107.128	104.21.78.45	QUIC	540 Protected Payload (KPo), DCID=8168dc123e93bf7af126a9a120d938b06c1e1e48
38	2.131720150	104.21.78.45	192.168.107.128	QUIC	66 Protected Payload (KPo)
39	2.142600625	104.21.78.45	192.168.107.128	QUIC	1242 Protected Payload (KPo)
40	2.142600625	104.21.78.45	192.168.107.128	QUIC	1067 Protected Payload (KPo)
41	2.143001194	192.168.107.128	104.21.78.45	QUIC	85 Protected Payload (KPo), DCID=8168dc123e93bf7af126a9a120d938b06c1e1e48
42	2.146025193	192.168.107.128	192.168.107.2	DNS	91 Standard query 0xc039 A a.nel.cloudflare.com OPT
43	2.146740209	192.168.107.128	192.168.107.2	DNS	91 Standard query 0x531a HTTPS a.nel.cloudflare.com OPT
44	2.178249199	192.168.107.2	192.168.107.128	DNS	107 Standard query response 0xc039 A a.nel.cloudflare.com A 35.190.80.1 OPT
45	2.178724986	192.168.107.2	192.168.107.128	DNS	170 Standard query response 0x531a HTTPS a.nel.cloudflare.com SOA colemans.n.cloudflare.com OPT
46	2.184397811	192.168.107.128	35.190.80.1	QUIC	Initial, SCID=722ab8b1fed473, PKN: 1, PADDING, PING, PADDING, CRYPTO, PADDING, PING, PING, PING, PING, PING
47	2.197214258	192.168.107.128	35.190.80.1	TLVSl.2	237 Application Data
48	2.197405096	192.168.107.128	35.190.80.1	TLVSl.2	93 Application Data
49	2.197405096	35.190.80.1	192.168.107.128	TCP	60 443 - 44338 [ACK] Seq=1 Ack=184 Win=64240 Len=0
50	2.197405096	35.190.80.1	192.168.107.128	TCP	60 443 - 44338 [ACK] Seq=1 Ack=223 Win=64240 Len=0
51	2.236356981	35.190.80.1	192.168.107.128	QUIC	1292 Protected Payload (KPo)
52	2.240145027	192.168.107.128	35.190.80.1	QUIC	206 Protected Payload (KPo), DCID=F22ab8b1fed473
53	2.240727215	192.168.107.128	104.21.78.45	QUIC	455 Protected Payload (KPo), DCID=8168dc123e93bf7af126a9a120d938b06c1e1e48
54	2.268417967	35.190.80.1	192.168.107.128	TLVSl.2	93 Application Data
55	2.277631636	35.190.80.1	192.168.107.128	QUIC	560 Protected Payload (KPo)
56	2.277632307	35.190.80.1	192.168.107.128	QUIC	163 Protected Payload (KPo)
57	2.281242166	192.168.107.128	35.190.80.1	QUIC	74 Protected Payload (KPo), DCID=F22ab8b1fed473
- Frame 29: 570 bytes on wire (4560 bits), 570 bytes captured (4560 bits) on interface -					
Section number: 1					
Interface id: 0 (ens33)					
Encapsulation type: Ethernet (1)					
Arrival Time: May 21, 2023 09:36:35.150100112 CST					
[Time shift for this packet: 0.000000000 seconds]					
Epoch Time: 1684832335.150100112 seconds					
[Time delta from previous captured frame: 0.000530073 seconds]					
0000	00 0c 29 9b ee a3 5c 30 31 e0 a5 38 08 00 45 00	->	00 0c 29 9b ee a3 5c 30 31 e0 a5 38 08 00 45 00	->	
0010	02 2c 84 09 00 00 88 11 d2 15 68 15 4e 2d c9 a8	->	02 2c 84 09 00 00 88 11 d2 15 68 15 4e 2d c9 a8	->	
0020	60 88 01 b1 bf 82 18 4b a5 46 03 03 70 39 9d	->	60 88 01 b1 bf 82 18 4b a5 46 03 03 70 39 9d	->	
0030	4f dc 00 25 42 8f 81 80 24 40 50 00 95 45 32 05	->	4f dc 00 25 42 8f 81 80 24 40 50 00 95 45 32 05	->	
0040	ac ce eb a2 26 23 8a 95 03 00 57 e5 84 28 f6 60	->	ac ce eb a2 26 23 8a 95 03 00 57 e5 84 28 f6 60	->	
0050	02 03 92 02 92 ea 47 8f e4 64 9c 70 na c0 ce 2c	->	02 03 92 02 92 ea 47 8f e4 64 9c 70 na c0 ce 2c	->	
0060	8f 47 e1 02 81 1b af 06 b9 25 ce 00 3f ef b4 b4	->	8f 47 e1 02 81 1b af 06 b9 25 ce 00 3f ef b4 b4	->	
0070	6f 77 47 25 ad 29 b3 22 b4 74 92 00 ce 1b 7c b2	->	6f 77 47 25 ad 29 b3 22 b4 74 92 00 ce 1b 7c b2	->	
0080	8f 07 18 c1 a5 91 91 61 1d 08 3f 32 06 0a 33 07	->	8f 07 18 c1 a5 91 91 61 1d 08 3f 32 06 0a 33 07	->	

这是在HTTPS上抓的包：

1	0.000000000	192.168.107.128	172.217.160.100	TCP	74 46056 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2859142984 TSecr=0 WS=128
2	2.040784416	192.168.107.128	108.160.166.42	TCP	74 56600 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3017284835 TSecr=0 WS=128
3	2.190410416	192.168.107.128	192.168.107.2	DNS	84 Standard query 0x2da1 A www.xdqv.com OPT
4	2.190911649	192.168.107.128	192.168.107.2	DNS	84 Standard query 0xb7f0 HTTPS www.xdqv.com OPT
5	2.283493313	192.168.107.2	192.168.107.128	DNS	100 Standard query response 0x2da1 A www.xdqv.com A 127.0.0.1 OPT
6	2.283657365	192.168.107.2	192.168.107.128	DNS	84 Standard query response 0xb7f0 HTTPS www.xdqv.com OPT
7	6.000383847	192.168.107.128	108.160.166.42	TCP	74 56600 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3017285340 TSecr=0 WS=128
8	6.032079495	192.168.107.128	35.190.80.1	QUIC	1292 Initial, DCID=e18ef8b8b8661dad, PKN: 1, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, CRYPTO, PING, PADDING
9	6.832871195	192.168.107.128	35.190.80.1	TLVSl.2	233 Application Data
10	6.832939362	192.168.107.128	35.190.80.1	TLVSl.2	93 Application Data
11	6.833405426	35.190.80.1	192.168.107.128	TCP	60 443 - 44338 [ACK] Seq=1 Ack=180 Win=64240 Len=0
12	6.833405614	35.190.80.1	192.168.107.128	TCP	60 443 - 44338 [ACK] Seq=1 Ack=219 Win=64240 Len=0
13	6.904180583	35.190.80.1	192.168.107.128	TLVSl.2	93 Application Data
14	6.947892512	192.168.107.128	35.190.80.1	TCP	54 44338 - 443 [ACK] Seq=219 Ack=40 Win=62780 Len=0
15	6.014931427	192.168.107.128	35.190.80.1	QUIC	1292 Initial, DCID=e18ef8b8b8661dad, PKN: 3, PING, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING, PING, PADDING, CRYPTO, CRYPTO, PADDING
16	6.039943602	35.190.80.1	192.168.107.128	TLVSl.2	149 Application Data
17	6.040090950	192.168.107.128	35.190.80.1	TCP	54 44338 - 443 [ACK] Seq=219 Ack=135 Win=62780 Len=0
18	6.040598852	192.168.107.128	35.190.80.1	TLVSl.2	93 Application Data
19	6.040649577	192.168.107.128	35.190.80.1	TLVSl.2	89 Application Data
20	6.040731293	35.190.80.1	192.168.107.128	TCP	60 443 - 44338 [ACK] Seq=135 Ack=258 Win=64240 Len=0
21	6.040731343	35.190.80.1	192.168.107.128	TCP	60 443 - 44338 [ACK] Seq=135 Ack=293 Win=64240 Len=0
22	6.040758825	192.168.107.128	35.190.80.1	TLVSl.2	228 Application Data
23	6.040806864	192.168.107.128	35.190.80.1	TLVSl.2	483 Application Data
24	6.040903839	35.190.80.1	192.168.107.128	TCP	60 443 - 44338 [ACK] Seq=135 Ack=467 Win=64240 Len=0
25	6.040903861	35.190.80.1	192.168.107.128	TCP	60 443 - 44338 [ACK] Seq=135 Ack=896 Win=64240 Len=0
26	6.080456375	35.190.80.1	192.168.107.128	QUIC	1292 Handshake, SCID=e18ef8b8b8661dad
27	6.080456719	35.190.80.1	192.168.107.128	QUIC	1292 Handshake, SCID=e18ef8b8b8661dad
28	6.080456757	35.190.80.1	192.168.107.128	QUIC	1292 Handshake, SCID=e18ef8b8b8661dad
29	6.080456797	35.190.80.1	192.168.107.128	QUIC	458 Protected Payload (KPo)
30	6.080970102	192.168.107.128	35.190.80.1	QUIC	81 Handshake, DCID=e18ef8b8b8661dad
31	6.080992936	192.168.107.128	35.190.80.1	QUIC	201 Protected Payload (KPo), DCID=e18ef8b8b8661dad
32	6.179520653	192.168.107.128	104.21.78.45	TCP	54 43454 - 443 [FIN, ACK] Seq=1 Ack=1 Win=62780 Len=0
33	6.178026095	192.168.107.128	108.160.166.42	TCP	74 51138 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3017288966 TSecr=0 WS=128
34	6.179832547	104.21.78.45	192.168.107.128	TCP	60 443 - 43454 [ACK] Seq=1 Ack=2 Win=64239 Len=0
35	6.210507063	104.21.78.45	192.168.107.128	TCP	60 443 - 43454 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=0
36	6.211500740	192.168.107.128	104.21.78.45	TCP	54 43454 - 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
37	6.260608568	35.190.80.1	192.168.107.128	QUIC	1292 Handshake, SCID=e18ef8b8b8661dad
38	6.261095810	192.168.107.128	35.190.80.1	QUIC	197 Protected Payload (KPo), DCID=e18ef8b8b8661dad
39	6.267747850	35.190.80.1	192.168.107.128	TCP	1292 Handshake, SCID=e18ef8b8b8661dad
40	6.268208545	192.168.107.128	35.190.80.1	QUIC	199 Protected Payload (KPo), DCID=e18ef8b8b8661dad
41	6.292339960	35.190.80.1	192.168.107.128	TLVSl.2	131 Application Data
42	6.292943009	192.168.107.128	35.190.80.1	TLVSl.2	93 Application Data
43	6.293369294	35.190.80.1	192.168.107.128	TCP	60 443 - 44338 [ACK] Seq=212 Ack=935 Win=64240 Len=0
44	6.293423562	192.168.107.128	35.190.80.1	TLVSl.2	89 Application Data
45	6.293660093	192.168.107.128	35.190.80.1	TCP	60 443 - 44338 [ACK] Seq=212 Ack=970 Win=64240 Len=0
46	6.342648997	35.190.80.1	192.168.107.128	QUIC	560 Protected Payload (KPo)
47	6.343094753	192.168.107.128	35.190.80.1	QUIC	75 Protected Payload (KPo), DCID=e18ef8b8b8661dad
48	6.345262906	35.190.80.1	192.168.107.128	QUIC	170 Protected Payload (KPo)
49	6.345587167	192.168.107.128	35.190.80.1	QUIC	75 Protected Payload (KPo), DCID=e18ef8b8b8661dad
50	6.514522486	35.190.80.1	192.168.107.128	QUIC	67 Protected Payload (KPo)
51	6.521782244	35.190.80.1	192.168.107.128	QUIC	69 Protected Payload (KPo)
52	7.209312998	192.168.107.128	108.160.166.42	TCP	74 [TCP Retransmission] [TCP Port numbers reused] 51138 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3017289896 TSecr=0 WS=128
53	7.209360000	192.168.107.128	172.217.160.100	TCP	74 46056 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2859150641 TSecr=0 WS=128
54	7.209394343	192.168.107.128	108.160.166.42	TCP	74 [TCP Retransmission] [TCP Port numbers reused] 4850 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2859151100 TSecr=0 WS=128
55	9.216422223	192.168.107.128	108.160.166.42	TCP	74 [TCP Retransmission] [TCP Port numbers reused] 51138 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3017292802 TSecr=0 WS=128
56	9.216428262	192.168.107.128	108.160.166.42	TCP	74 [TCP Retransmission] [TCP Port numbers reused] 5666 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3017293802 TSecr=0 WS=128
57	9.216591760	192.168.107.128	108.160.166.42	TCP	74 [TCP Retransmission] [TCP Port numbers reused] 5667 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3017293542 TSecr=0 WS=128

## • 比较分析HTTP和HTTPS协议的差异

TTP协议以明文方式发送内容，不提供任何方式的数据加密。HTTP协议不适合传输一些敏感信息，比如：信用卡号、密码等支付信息。https则是具有安全性的ssl加密传输协议。http和https使用的是完全不同的连接方式，用的端口也不一样，前者是80，后者是443。并且https协议需要到ca申请证书。HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，要比http协议安全。

HTTPS协议的主要作用可以分为两种：一种是建立一个信息安全通道，来保证数据传输的安全；另一种就是确认网站的真实性。HTTPS在HTTP的基础上加入了SSL协议，SSL依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。

### 实验说明

- 域名为 <http://www.xdv.com>、<http://www.xdc.com> 和 <https://www.xdqdv.com>、<https://xdqdc.com>
- 网络抓包分析工具不限，公钥证书等工具不限
- 分析范围为用户发去页面请求到用户登录成功或失败期间，浏览器与服务器之间所有的网络交互，至少应包括应用层、传输层和网络层的协议内容。