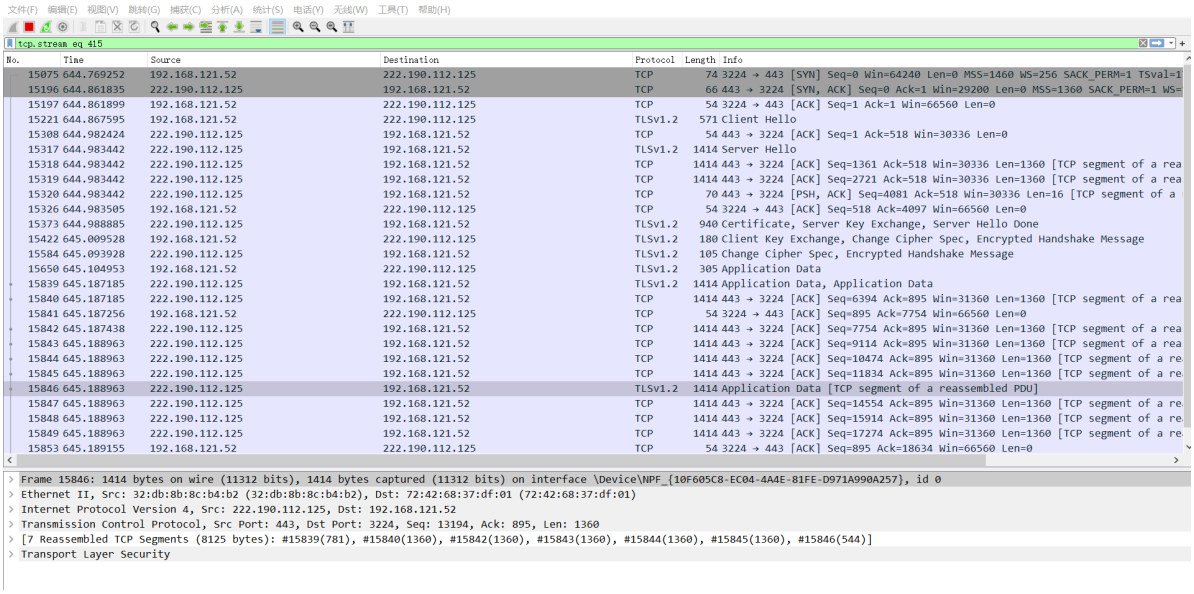
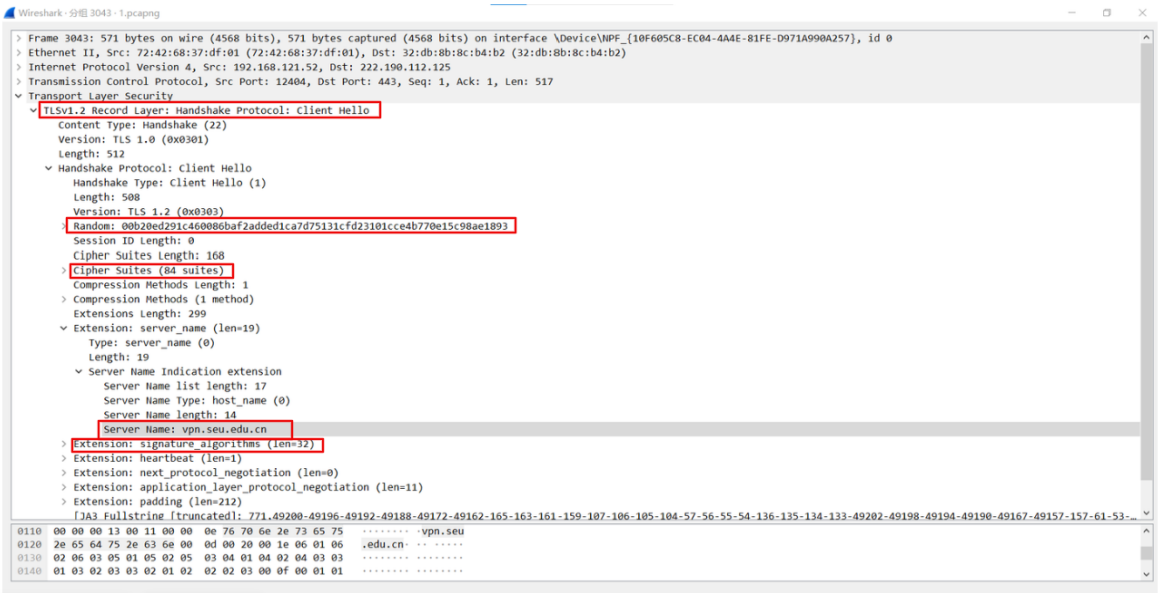
VPN连接过程：

该VPN的服务器IP为222.190.112.125，当我们从客户端连接VPN时，首先与服务器进行三次握手，建立TCP连接，然后进行TLS协议四次握手，连接建立，通过TLSv1.2实现本机和VPN服务器之间的身份认证、密钥协商、数据传输，建立起客户端和服务器端之间的数据传输隧道。



1.第一次

首先由客户端发起第一次握手，即Client Hello报文，其中包括用于密钥协商的Random，服务器域名Server name，支持的加密算法，支持的签名算法等等。



2.第二次

服务器端返回第一次握手报文，即Server Hello,由客户端根据双方支持的协议情况，对相关方法进行决定，包括TLS版本（1.2），加密套件，压缩方法等等，同时Server端也传回了自己的Random。

```
Wireshark · 分组 3115 · 1.pcapng
> Frame 3115: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on interface \Device\NPF_{10F605C8-EC04-4A4E-81FE-D971A990A257}, id 0
> Ethernet II, Src: 32:db:8b:8c:b4:b2 (32:db:8b:8c:b4:b2), Dst: 72:42:68:37:df:01 (72:42:68:37:df:01)
> Internet Protocol Version 4, Src: 222.190.112.125, Dst: 192.168.121.52
> Transmission Control Protocol, Src Port: 443, Dst Port: 12404, Seq: 1, Ack: 518, Len: 1360
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 101
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 97
        Version: TLS 1.2 (0x0303)
      > Random: 2e80499e7e6b5882b7b93d01558f03972969339429bc68110827813a97cdbcd1
        Session ID Length: 32
        Session ID: 4225191269da0013649473eb2a311042917e76fb0da74ef3378fff0848a7d3b9
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 25
      > Extension: renegotiation_info (len=1)
      > Extension: heartbeat (len=1)
      > Extension: application_layer_protocol_negotiation (len=11)
        [JA3S Fullstring: 771,49200,65281-15-16]
        [JA3S: fa6a4b9265e7f95f0ff89f0f4f068d01]

0080  d3 b9 c0 30 00 00 19 ff  01 00 01 00 00 0f 00 01   ···0···· ********
0090  01 00 10 00 0b 00 09 08  68 74 74 70 2f 31 2e 31   ******** http/1.1
```

Server端第一次握手继续传递第二个报文，其中包含三个主要Message：Certificate，Server Key Exchange和Server Hello Done。

```
> Frame 3122: 940 bytes on wire (7520 bits), 940 bytes captured (7520 bits) on interface \Device\NPF_{10F605C8-EC04-4A4E-81FE-D971A990A257}
> Ethernet II, Src: 32:db:8b:8c:b4:b2 (32:db:8b:8c:b4:b2), Dst: 72:42:68:37:df:01 (72:42:68:37:df:01)
> Internet Protocol Version 4, Src: 222.190.112.125, Dst: 192.168.121.52
> Transmission Control Protocol, Src Port: 443, Dst Port: 12404, Seq: 4097, Ack: 518, Len: 886
> [5 Reassembled TCP Segments (4529 bytes): #3115(1254), #3117(1360), #3118(1360), #3120(16), #3122(539)]
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Certificate
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

其中Certificate向客户端展示自己的数字证书，包含签名权威机构，认证算法，个人签名，以向客户端证明自身身份。这里可以看到东大VPN的域名信息。Server Key Exchange向客户端传递自己的公钥，同时传递选择使用的算法。Server Hello Done用于结束本次握手。

```
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4524
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 4520
        Certificates Length: 4517
      v Certificates (4517 bytes)
          Certificate Length: 1585
        v Certificate: 3082062d30820515a003020102021100 99da415e7297b10fcc77c5d46b4d6277300d0609… (id-at-commonName=*.vpn.seu.edu.cn)
          > signedCertificate
          > algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted: be515dc2067d917aaa1985ae5f506c5d9c963e21cedfc96625ee5175f826be346aea84d2…
          Certificate Length: 1510
        > Certificate: 308205e2308203caa003020102021100d56e246c94ed63abb146efc196b64fb0300d0609… (id-at-commonName=WoTrus DV Server CA  [Run by the Issuer]
          Certificate Length: 1413
        > Certificate: 3082058130820469a003020102021039 72443af922b751d7d36c10dd313595300d06092a… (id-at-commonName=USERTrust RSA Certification Authority,id
```

```
Transport Layer Security
v TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 333
  v Handshake Protocol: Server Key Exchange
      Handshake Type: Server Key Exchange (12)
      Length: 329
    v EC Diffie-Hellman Server Params
        Curve Type: named_curve (0x03)
        Named Curve: secp256r1 (0x0017)
        Pubkey Length: 65
        Pubkey: 046663917cbd9713a5c4d98b013d6cd9aeb81be7857f48f84cfee3f9ceb6ed12c2e1c2e9…
      > Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
        Signature Length: 256
        Signature: 6f7b3d728d505e7cd9df739df7cb56db1003c6ae1e0299f7bb51f584b5093fcc0ed63d2f…
```

3.第三次

Client端进行第二次握手，其中包含三个主要Message：Client Key Exchange，Change Cipher Spec和Encryed Handshake Message。Client端确定证书有效后，向Server端发送自己的公钥，同时Change Cipher Spec用于告知使用密钥，Encryed Handshake Message为使用密钥加密的信息，对端进行校验，可以用于确认密钥的正确性。

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 66
      EC Diffie-Hellman Client Params
          Pubkey Length: 65
          Pubkey: 04d2d71c488ab4681b382fe0d5f0a7e9eaa0aad1b92d4bede87aa30f593c5cf0969bc18c…
  TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
```

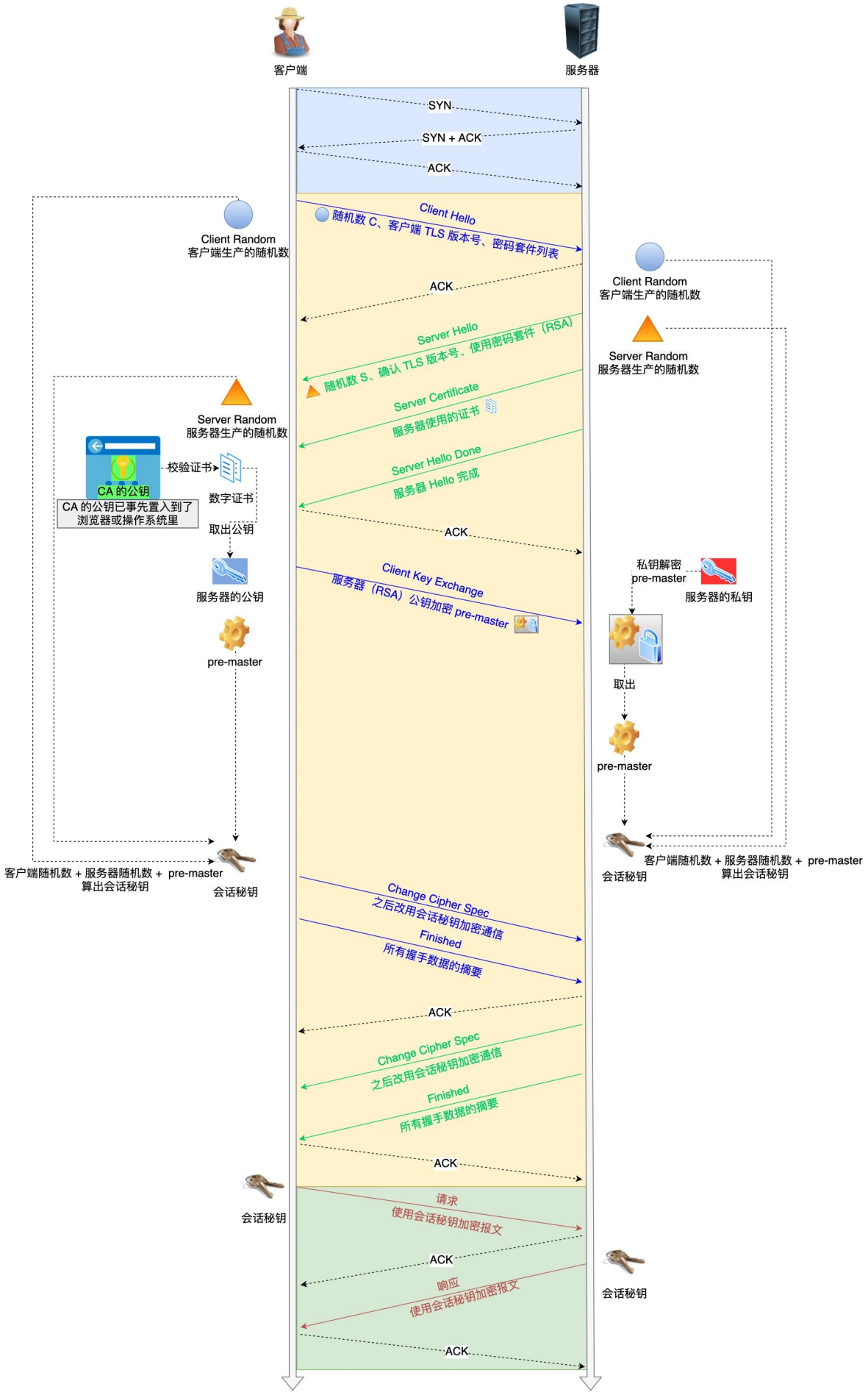
4.第四次

Server端进行第二次握手。当它使用私钥解密之前的Encryed Handshake Message时，得到一个随机数。将前面的三个随机数以及他们协商的加密方式，计算生成一个会话密钥 session secrect。服务端也会使用 Session Secret 加密一段 Finish 消息发送给客户端，以验证之前通过握手建立起来的加解密通道是否成功。然后返回一个报文，其中包含两个主要Message：Change Cipher Spec和Encryed Handshake Message。

```
Transport Layer Security
  TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

VPN主要通过通过TLSv1.2，以上四次握手过程完成客户端和VPN服务器之间的连接建立。

总体流程图：


客户端
服务器
SYN
SYN + ACK
ACK
Client Random
客户端生产的随机数
Client Hello
随机数 C、客户端 TLS 版本号、密码套件列表
ACK
Client Random
客户端生产的随机数
Server Hello
随机数 S、确认 TLS 版本号、使用密码套件（RSA）
Server Random
服务器生产的随机数
Server Random
服务器生产的随机数
Server Certificate
服务器使用的证书
校验证书
CA 的公钥
CA 的公钥已事先置入到了
浏览器或操作系统里
数字证书
取出公钥
Server Hello Done
服务器 Hello 完成
ACK
服务器的公钥
Client Key Exchange
服务器（RSA）公钥加密 pre-master
私钥解密
pre-master
服务器的私钥
pre-master
取出
pre-master
客户端随机数 + 服务器随机数 + pre-master
算出会话秘钥
会话秘钥
客户端随机数 + 服务器随机数 + pre-master
算出会话秘钥
会话秘钥
Change Cipher Spec
之后改用会话秘钥加密通信
Finished
所有握手数据的摘要
ACK
Change Cipher Spec
之后改用会话秘钥加密通信
Finished
所有握手数据的摘要
ACK
会话秘钥
请求
使用会话秘钥加密报文
ACK
响应
使用会话秘钥加密报文
会话秘钥
ACK

访问资源：

在访问校内资源时走的是vpn流量，即报文发给与其建立vpn连接的服务器，而不是直接发给资源对应的服务器；

访问校外资源则与未连接东大vpn时一样，即直接将报文发送给资源对应的服务器。

访问校外资源：

访问Bing进行搜索，通过Wireshark对流量进行抓包，连接与未连接时情况相同，直接访问外部服务器。

连接VPN

7357	185.796039	202.89.233.100	192.168.121.52	TLSv1.2	285	Application Data
7358	185.796094	192.168.121.52	202.89.233.100	TCP	54	7169 → 443 [ACK] Seq=350533 Ack=241781 Win=133120 Len
7359	185.796335	202.89.233.100	192.168.121.52	TCP	1414	443 → 7169 [ACK] Seq=241781 Ack=350533 Win=4194304 Le
7360	185.796376	192.168.121.52	202.89.233.100	TCP	54	7169 → 443 [ACK] Seq=350533 Ack=243141 Win=133120 Len
7361	185.796569	202.89.233.100	192.168.121.52	TLSv1.2	1158	Application Data
7362	185.801539	202.89.233.100	192.168.121.52	TLSv1.2	92	Application Data
7363	185.801615	192.168.121.52	202.89.233.100	TCP	54	7169 → 443 [ACK] Seq=350533 Ack=244283 Win=132096 Len
7364	185.804737	192.168.121.52	202.89.233.100	TCP	1414	7169 → 443 [ACK] Seq=350533 Ack=244283 Win=132096 Len
7365	185.804737	192.168.121.52	202.89.233.100	TLSv1.2	1219	Application Data
7366	185.805802	192.168.121.52	202.89.233.100	TCP	1414	7169 → 443 [ACK] Seq=353058 Ack=244283 Win=132096 Len
7367	185.805802	192.168.121.52	202.89.233.100	TLSv1.2	1219	Application Data
7368	185.806335	192.168.121.52	202.89.233.100	TCP	1414	7169 → 443 [ACK] Seq=355583 Ack=244283 Win=132096 Len
7369	185.806335	192.168.121.52	202.89.233.100	TLSv1.2	1201	Application Data
7370	185.806845	192.168.121.52	202.89.233.100	TCP	1414	7169 → 443 [ACK] Seq=358090 Ack=244283 Win=132096 Len
7371	185.806845	192.168.121.52	202.89.233.100	TLSv1.2	1219	Application Data
7372	185.807780	192.168.121.52	202.89.233.100	TCP	1414	7169 → 443 [ACK] Seq=360615 Ack=244283 Win=132096 Len
7373	185.807780	192.168.121.52	202.89.233.100	TLSv1.2	1218	Application Data
7374	185.807880	192.168.121.52	202.89.233.100	TCP	1414	7169 → 443 [ACK] Seq=363139 Ack=244283 Win=132096 Len
7375	185.807880	192.168.121.52	202.89.233.100	TLSv1.2	1201	Application Data
7376	185.808775	192.168.121.52	202.89.233.100	TCP	1414	7169 → 443 [ACK] Seq=365646 Ack=244283 Win=132096 Len

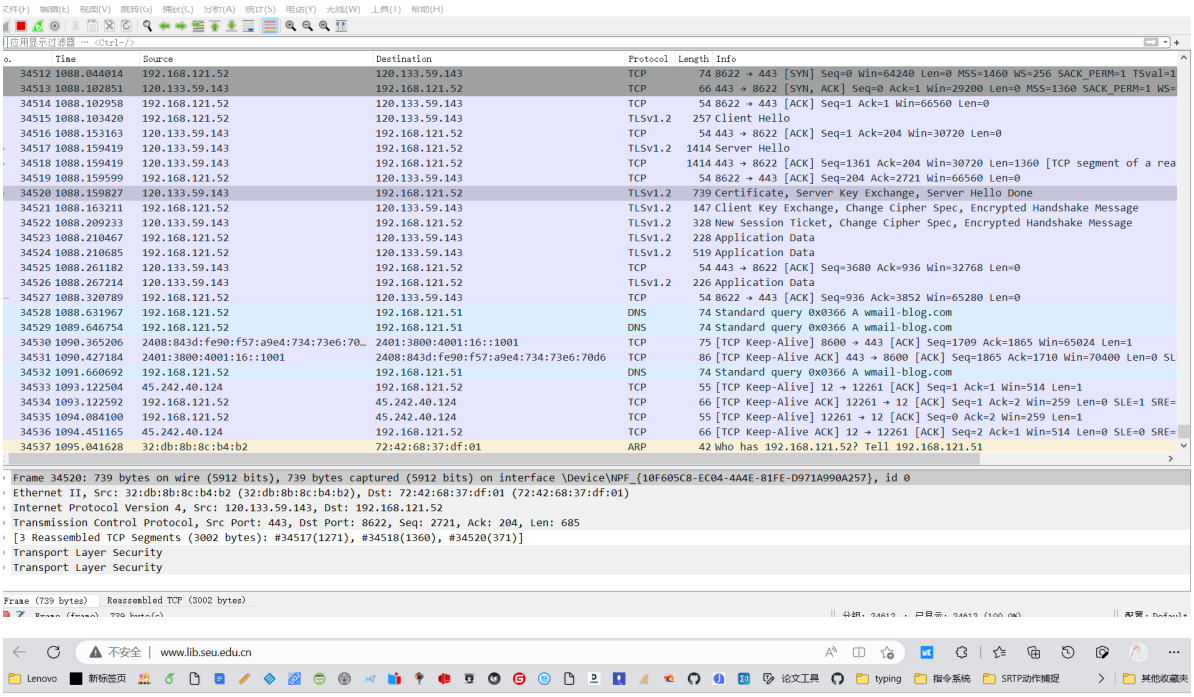
断开VPN

9333	232.975979	192.168.121.52	202.89.233.101	TCP	1414	2989 → 443 [ACK] Seq=179589 Ack=206492 Win=266496 Len=1
9334	232.975979	192.168.121.52	202.89.233.101	TLSv1.2	1383	Application Data
9335	233.031030	202.89.233.101	192.168.121.52	TCP	54	443 → 2989 [ACK] Seq=206492 Ack=182278 Win=4195584 Len=
9336	233.058709	202.89.233.101	192.168.121.52	TCP	1414	443 → 2989 [ACK] Seq=206492 Ack=182278 Win=4195584 Len=
9337	233.058709	202.89.233.101	192.168.121.52	TCP	1414	443 → 2989 [ACK] Seq=207852 Ack=182278 Win=4195584 Len=
9338	233.058794	192.168.121.52	202.89.233.101	TCP	54	2989 → 443 [ACK] Seq=182278 Ack=209212 Win=266496 Len=0
9339	233.058876	202.89.233.101	192.168.121.52	TLSv1.2	252	Application Data
9340	233.058876	202.89.233.101	192.168.121.52	TLSv1.2	140	Application Data
9341	233.058902	192.168.121.52	202.89.233.101	TCP	54	2989 → 443 [ACK] Seq=182278 Ack=209496 Win=266240 Len=0
9342	233.060170	202.89.233.101	192.168.121.52	TCP	1414	443 → 2989 [ACK] Seq=209496 Ack=182278 Win=4195584 Len=
9343	233.060406	202.89.233.101	192.168.121.52	TLSv1.2	1159	Application Data
9344	233.060429	192.168.121.52	202.89.233.101	TCP	54	2989 → 443 [ACK] Seq=182278 Ack=211961 Win=266496 Len=0
9345	233.064313	202.89.233.101	192.168.121.52	TLSv1.2	92	Application Data
9346	233.100126	202.89.233.101	192.168.121.52	TLSv1.2	201	Application Data
9347	233.100267	192.168.121.52	202.89.233.101	TCP	54	2989 → 443 [ACK] Seq=182278 Ack=212146 Win=266240 Len=0
9348	236.542582	2600:1406:4400::687…	2408:843d:fe90:f57:…	TLSv1.3	739	Application Data
9349	236.594562	2408:843d:fe90:f57:…	2600:1406:4400::687…	TCP	74	2996 → 443 [ACK] Seq=1178 Ack=1223 Win=64256 Len=0
9350	236.625709	192.168.121.52	139.196.217.115	TLSv1.2	102	Application Data
9351	236.652085	139.196.217.115	192.168.121.52	TLSv1.2	98	Application Data
9352	236.702735	192.168.121.52	139.196.217.115	TCP	66	6944 → 443 [ACK] Seq=433 Ack=385 Win=254 Len=0 TSval=17

访问校内资源：

访问图书馆资源时，未连VPN，直接对服务器120.133.59.143进行访问，结果被防火墙拒绝，错误代码504。连接VPN时，访问校内资源均通过222.190.112.125进行转发，可以绕过防火墙，正常使用。

断开VPN：

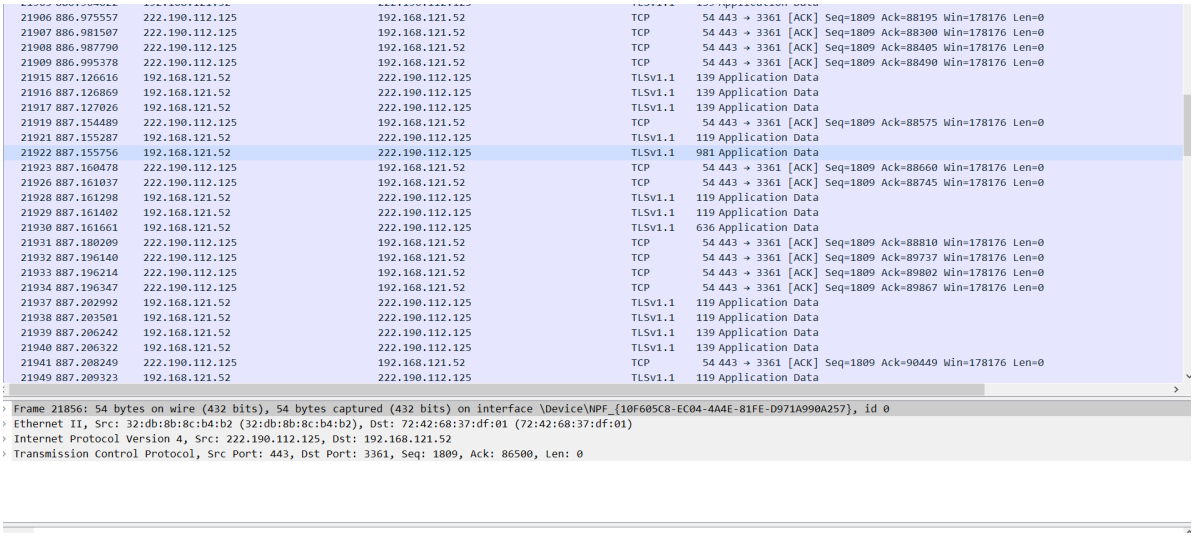


No.	Time	Source	Destination	Protocol	Length	Info
34512	1088.044014	192.168.121.52	120.133.59.143	TCP	74	8622 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=1
34513	1088.102851	120.133.59.143	192.168.121.52	TCP	66	443 → 8622 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM=1 WS=
34514	1088.102958	192.168.121.52	120.133.59.143	TCP	54	8622 → 443 [ACK] Seq=1 Ack=1 Win=66560 Len=0
34515	1088.103420	192.168.121.52	120.133.59.143	TLSv1.2	257	Client Hello
34516	1088.153163	120.133.59.143	192.168.121.52	TCP	54	443 → 8622 [ACK] Seq=1 Ack=204 Win=30720 Len=0
34517	1088.159419	120.133.59.143	192.168.121.52	TLSv1.2	1414	Server Hello
34518	1088.159419	120.133.59.143	192.168.121.52	TCP	1414	443 → 8622 [ACK] Seq=1361 Ack=204 Win=30720 Len=1360 [TCP segment of a rea
34519	1088.159599	192.168.121.52	120.133.59.143	TCP	54	8622 → 443 [ACK] Seq=204 Ack=2721 Win=66560 Len=0
34520	1088.159827	120.133.59.143	192.168.121.52	TLSv1.2	739	Certificate, Server Key Exchange, Server Hello Done
34521	1088.163211	192.168.121.52	120.133.59.143	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
34522	1088.209233	120.133.59.143	192.168.121.52	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
34523	1088.210467	192.168.121.52	120.133.59.143	TLSv1.2	228	Application Data
34524	1088.210685	192.168.121.52	120.133.59.143	TLSv1.2	519	Application Data
34525	1088.261182	120.133.59.143	192.168.121.52	TCP	54	443 → 8622 [ACK] Seq=3680 Ack=936 Win=32768 Len=0
34526	1088.267214	120.133.59.143	192.168.121.52	TLSv1.2	226	Application Data
34527	1088.320789	192.168.121.52	120.133.59.143	TCP	54	8622 → 443 [ACK] Seq=936 Ack=3852 Win=65280 Len=0
34528	1088.631967	192.168.121.52	192.168.121.51	DNS	74	Standard query 0x0366 A wmail-blog.com
34529	1089.646754	192.168.121.52	192.168.121.51	DNS	74	Standard query 0x0366 A wmail-blog.com
34530	1090.365206	2408:843d:fe90:f57:a9e4:734:73e6:70…	2401:3800:4001:16::1001	TCP	75	[TCP Keep-Alive] 8600 → 443 [ACK] Seq=1709 Ack=1865 Win=65024 Len=1
34531	1090.427184	2401:3800:4001:16::1001	2408:843d:fe90:f57:a9e4:734:73e6:70d6	TCP	86	[TCP Keep-Alive ACK] 443 → 8600 [ACK] Seq=1865 Ack=1710 Win=70400 Len=0 SL
34532	1091.660692	192.168.121.52	192.168.121.51	DNS	74	Standard query 0x0366 A wmail-blog.com
34533	1093.122504	45.242.40.124	192.168.121.52	TCP	55	[TCP Keep-Alive] 12 → 12261 [ACK] Seq=1 Ack=1 Win=514 Len=1
34534	1093.122592	192.168.121.52	45.242.40.124	TCP	66	[TCP Keep-Alive ACK] 12261 → 12 [ACK] Seq=1 Ack=2 Win=259 Len=0 SLE=1 SRE=
34535	1094.084100	192.168.121.52	45.242.40.124	TCP	55	[TCP Keep-Alive] 12261 → 12 [ACK] Seq=0 Ack=2 Win=259 Len=1
34536	1094.451165	45.242.40.124	192.168.121.52	TCP	66	[TCP Keep-Alive ACK] 12 → 12261 [ACK] Seq=2 Ack=1 Win=514 Len=0 SLE=0 SRE=
34537	1095.041628	32:db:8b:8c:b4:b2	72:42:68:37:df:01	ARP	42	Who has 192.168.121.52? Tell 192.168.121.51

```
Frame 34520: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits) on interface \Device\NPF_{10F605C8-EC04-4A4E-81FE-D971A990A257}, id 0
Ethernet II, Src: 32:db:8b:8c:b4:b2 (32:db:8b:8c:b4:b2), Dst: 72:42:68:37:df:01 (72:42:68:37:df:01)
Internet Protocol Version 4, Src: 120.133.59.143, Dst: 192.168.121.52
Transmission Control Protocol, Src Port: 443, Dst Port: 8622, Seq: 2721, Ack: 204, Len: 685
[3 Reassembled TCP Segments (3002 bytes): #34517(1271), #34518(1360), #34520(371)]
Transport Layer Security
Transport Layer Security
```


504 Gateway Time-out

连接VPN后：



No.	Time	Source	Destination	Protocol	Length	Info
21906	886.975557	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=88195 Win=178176 Len=0
21907	886.981507	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=88300 Win=178176 Len=0
21908	886.987790	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=88405 Win=178176 Len=0
21909	886.995378	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=88490 Win=178176 Len=0
21915	887.126616	192.168.121.52	222.190.112.125	TLSv1.1	139	Application Data
21916	887.126869	192.168.121.52	222.190.112.125	TLSv1.1	139	Application Data
21917	887.127026	192.168.121.52	222.190.112.125	TLSv1.1	139	Application Data
21919	887.154489	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=88575 Win=178176 Len=0
21921	887.155287	192.168.121.52	222.190.112.125	TLSv1.1	119	Application Data
21922	887.155756	192.168.121.52	222.190.112.125	TLSv1.1	981	Application Data
21923	887.160478	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=88660 Win=178176 Len=0
21926	887.161037	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=88745 Win=178176 Len=0
21928	887.161298	192.168.121.52	222.190.112.125	TLSv1.1	119	Application Data
21929	887.161402	192.168.121.52	222.190.112.125	TLSv1.1	119	Application Data
21930	887.161661	192.168.121.52	222.190.112.125	TLSv1.1	636	Application Data
21931	887.180209	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=88810 Win=178176 Len=0
21932	887.196140	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=89737 Win=178176 Len=0
21933	887.196214	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=89802 Win=178176 Len=0
21934	887.196347	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=89867 Win=178176 Len=0
21937	887.202992	192.168.121.52	222.190.112.125	TLSv1.1	119	Application Data
21938	887.203501	192.168.121.52	222.190.112.125	TLSv1.1	119	Application Data
21939	887.206242	192.168.121.52	222.190.112.125	TLSv1.1	139	Application Data
21940	887.206322	192.168.121.52	222.190.112.125	TLSv1.1	139	Application Data
21941	887.208249	222.190.112.125	192.168.121.52	TCP	54	443 → 3361 [ACK] Seq=1809 Ack=90449 Win=178176 Len=0
21949	887.209323	192.168.121.52	222.190.112.125	TLSv1.1	119	Application Data

```
Frame 21856: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{10F605C8-EC04-4A4E-81FE-D971A990A257}, id 0
Ethernet II, Src: 32:db:8b:8c:b4:b2 (32:db:8b:8c:b4:b2), Dst: 72:42:68:37:df:01 (72:42:68:37:df:01)
Internet Protocol Version 4, Src: 222.190.112.125, Dst: 192.168.121.52
Transmission Control Protocol, Src Port: 443, Dst Port: 3361, Seq: 1809, Ack: 86500, Len: 0
```