

哈尔滨工业大学(深圳)

《网络与系统安全》 实验报告

实验五

TLS 实验

学 院: 计算机科学与技术学院

姓 名: 梁鑫嵘

学 号: 200110619

专 业: 计算机科学与技术学院

日 期: 2023 年 4 月

1.在客户端容器中执行如下命令 `./handshake.py www.baidu.com` 根据执行结果回答下面三个问题。

(1) 客户端和服务端使用的加密算法有哪些，分别起什么作用？

从 Client Hello 包得知，客户端支持的加密算法有：

No.	Time	Source	Destination	Protocol	Length	Info
10	2023-05-27 09:2...	192.168.122.245	14.119.104.189	TLSv1.2	571	Client Hello
11	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TCP	54	443 → 40418 [ACK] Seq=2579742065 Ack=268058582 Win=30208 Len=0
12	2023-05-27 09:2...	192.168.122.245	192.168.122.245	TLSv1.2	5280	Server Hello, Certificate, Server Key Exchange, Server Hello ...

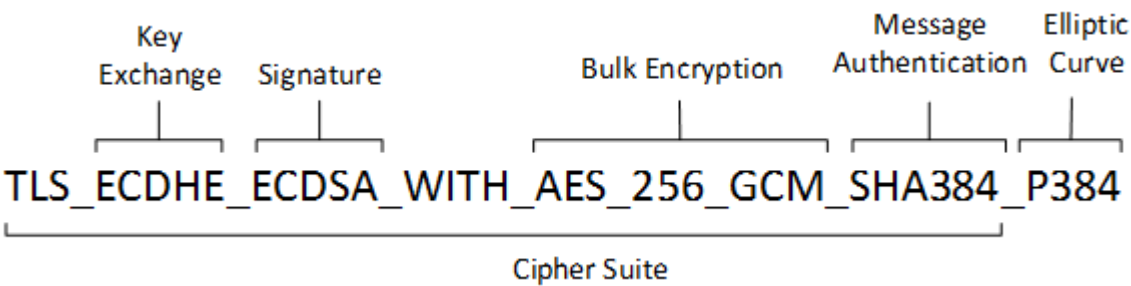
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: d1149f2c6b4b55e4856680f8f298855aa903813146b5aa44...
Session ID Length: 32
Session ID: cbb691cd055f72ad116af2b55948f9cd800ded0856dd43d2...
Cipher Suites Length: 62
Cipher Suites (31 suites)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03a)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03b)
Cipher Suite: TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x008d)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x008c)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 373
Extension: server_name (len=18)
Extension: ec_point_formats (len=4)
Extension: supported_groups (len=12)
Extension: session_ticket (len=0)
Extension: encrypt_then_mac (len=0)
Extension: extended_master_secret (len=0)
Extension: signature_algorithms (len=42)
Extension: supported_versions (len=5)
Type: supported_versions (43)
Length: 5
Supported Versions Length: 4
Supported Version: TLS 1.3 (0x0304)
Supported Version: TLS 1.2 (0x0303)
Extension: psk_key_exchange_modes (len=2)
Extension: key_share (len=38)
Extension: padding (len=208)

主要为 AES、ECDSA、CHACHA20、RSA 等。

从 Server Hello 包中得知，服务端使用的是

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

```
11 2023-05-27 09:27:14.119.104.109 192.168.122.245 TCP 5843 -> 40410 [ACK] Seq=2379742003 Win=30700 Len=0
12 2023-05-27 09:27:14.119.104.109 192.168.122.245 TLSv1.2 5280 Server Hello, Certificate, Server Key Exchange, Server Hello
13 2023-05-27 09:27:14.119.104.109 192.168.122.245 TLSv1.2 5280 Server Hello, Certificate, Server Key Exchange, Server Hello
> Frame 12: 5280 bytes on wire (42240 bits), 5280 bytes captured (42240 bits) on interface enp1s0, id 0
> Ethernet II, Src: RealtekU_3d:ce:f3 (52:54:00:3d:ce:f3), Dst: RealtekU_ed:8d:74 (52:54:00:ed:8d:74)
> Internet Protocol Version 4, Src: 14.119.104.109, Dst: 192.168.122.245
> Transmission Control Protocol, Src Port: 443, Dst Port: 40418, Seq: 2579742065, Ack: 268058582, Len: 5226
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    > Content Type: Handshake (22)
      > Version: TLS 1.2 (0x0303)
        > Length: 59
      > Handshake Protocol: Server Hello
        > Handshake Type: Server Hello (2)
          > Length: 55
          > Version: TLS 1.2 (0x0303)
            > Random: 6472050667689fee2d9efc86ebb65161024949c13cf052a0...
              > Session ID Length: 0
            > Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
              > Compression Method: null (0)
                > Extensions Length: 15
```



(2) 分析打印出来的服务器端证书

```

After making TCP connection. Press any key to continue ...
=== Cipher used: ('ECDHE-RSA-AES128-GCM-SHA256', 'TLSv1.2', 128)
=== Server hostname: www.baidu.com
=== Server certificate:
{'OCSP': ('http://ocsp.globalsign.com/gsrsoavsslca2018',),
'caIssuers': ('http://secure.globalsign.com/cacert/gsrsoavsslca2018.crt',),
'crlDistributionPoints': ('http://crl.globalsign.com/gsrsoavsslca2018.crl',),
'issuer': (((('countryName', 'BE'),),
              (('organizationName', 'GlobalSign nv-sa'),),
              (('commonName', 'GlobalSign RSA OV SSL CA 2018'),)),
'notAfter': 'Aug  6 05:16:01 2023 GMT',
'notBefore': 'Jul  5 05:16:02 2022 GMT',
'serialNumber': '4417CE86EF82EC6921CC6F68',
'subject': (((('countryName', 'CN'),),
              (('stateOrProvinceName', 'beijing'),),
              (('localityName', 'beijing'),),
              (('organizationalUnitName', 'service operation department'),),
              (('organizationName',
                'Beijing Baidu Netcom Science Technology Co., Ltd'),),
              (('commonName', 'baidu.com'),)),
'subjectAltName': (('DNS', 'baidu.com'),
                  ('DNS', 'baifubao.com'),
                  ('DNS', 'www.baidu.cn'),
                  ('DNS', 'www.baidu.com.cn'),
                  ('DNS', 'mct.y.nuomi.com'),
                  ('DNS', 'apollo.auto'),
                  ('DNS', 'dwz.cn'),
                  ('DNS', '*.baidu.com'),
                  ('DNS', '*.baifubao.com'),
                  ('DNS', '*.baidustatic.com'),
                  ('DNS', '*.bdstatic.com'),
                  ('DNS', '*.bding.com'),
                  ('DNS', '*.hao123.com'),
                  ('DNS', '*.nuomi.com'),
                  ('DNS', '*.chuanke.com'),
                  ('DNS', '*.trustgo.com'),
                  ('DNS', '*.bce.baidu.com'),
                  ('DNS', '*.eyun.baidu.com'),
                  ('DNS', '*.map.baidu.com'),
                  ('DNS', '*.mbd.baidu.com'),
                  ('DNS', '*.fanyi.baidu.com'),
                  ('DNS', '*.baidubce.com'),
                  ('DNS', '*.mipcdn.com'),
                  ('DNS', '*.news.baidu.com'),
                  ('DNS', '*.baidupcs.com'),
                  ('DNS', '*.aipage.com'),
                  ('DNS', '*.aipage.cn'),
                  ('DNS', '*.bcehost.com'),
                  ('DNS', '*.safe.baidu.com'),
                  ('DNS', '*.im.baidu.com'),
                  ('DNS', '*.baiducontent.com'),
                  ('DNS', '*.dlnel.com'),
                  ('DNS', '*.dlnel.org'),
                  ('DNS', '*.dueros.baidu.com'),

```

证书分析:

1. 颁发者是 BE（比利时）的 GlobalSign
2. 持有者是 CN（中国）的 Beijing Baidu Netcom Science

Technology

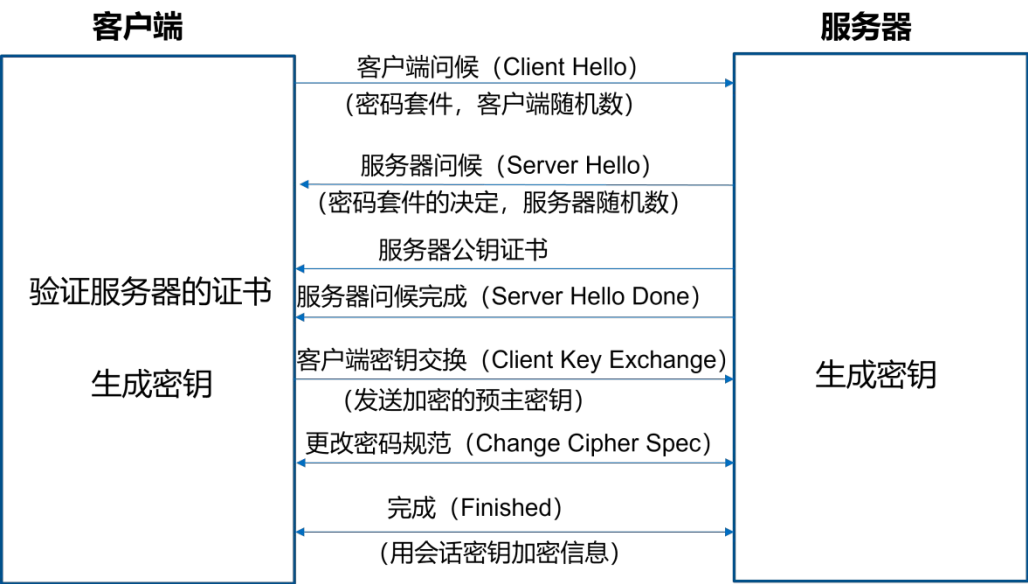
3. 此证书对下列域名都有效

(3) 抓包分析 TLS 握手协议

对脚本运行过程抓包：

No.	Time	Source	Destination	Protocol	Length	Info
10	2023-05-27 09:2...	192.168.122.245	14.119.104.189	TLSv1.2	571	Client Hello
12	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	5280	Server Hello, Certificate, Server Key Exchange, Server Hello ...
14	2023-05-27 09:2...	192.168.122.245	14.119.104.189	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake ...
15	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	924	[TCP Spurious Retransmission], Ignored Unknown Record
18	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	280	New Session Ticket, Change Cipher Spec, Encrypted Handshake M...

运行结束后有 4 个 TLSv1.2 导书的 TLS 握手过程：



Client Hello:

tls						
No.	Time	Source	Destination	Protocol	Length	Info
10	2023-05-27 09:2...	192.168.122.245	14.119.104.189	TLSv1.2	571	Client Hello
12	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	5280	Server Hello, Certificate, Server Key Exchange, Server Hello ...
14	2023-05-27 09:2...	192.168.122.245	14.119.104.189	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake ...
15	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	924	[TCP Spurious Retransmission] , Ignored Unknown Record
18	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	280	New Session Ticket, Change Cipher Spec, Encrypted Handshake M...

Frame 10: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface enp1s0, id 0
Ethernet II, Src: RealtekU_ed:8d:74 (52:54:00:ed:8d:74), Dst: RealtekU_3d:ce:f3 (52:54:00:3d:ce:f3)
Internet Protocol Version 4, Src: 192.168.122.245, Dst: 14.119.104.189
Transmission Control Protocol, Src Port: 40418, Dst Port: 443, Seq: 268058065, Ack: 2579742065, Len: 517

Transport Layer Security

- TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 512
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 508
 - Version: TLS 1.2 (0x0303)
 - Random: d1149f2c6b4b55e4056680f8f298855aa903813146b5aa44...
 - Session ID Length: 32
 - Session ID: cbb691cd055f72ad116af2b55948f9cd800ded0856dd43d2...
 - Cipher Suites Length: 62
 - Cipher Suites (31 suites)
 - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
 - Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
 - Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)
 - Cipher Suite: TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)

Server Hello:

tls					
No.	Time	Source	Destination	Protocol	Length Info
10	2023-05-27 09:2	192.168.122.245	14.119.104.189	TLSv1.2	571 Client Hello
12	2023-05-27 09:2	14.119.104.189	192.168.122.245	TLSv1.2	5280 Server Hello, Certificate, Server Key Exchange, Server Hello
14	2023-05-27 09:2	192.168.122.245	14.119.104.189	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
15	2023-05-27 09:2	14.119.104.189	192.168.122.245	TLSv1.2	924 [TCP Spurious Retransmission] , Ignored Unknown Record
18	2023-05-27 09:2	14.119.104.189	192.168.122.245	TLSv1.2	280 New Session Ticket, Change Cipher Spec, Encrypted Handshake M

▶ Frame 12: 5280 bytes on wire (42240 bits), 5280 bytes captured (42240 bits) on interface enp1s0, id 0
▶ Ethernet II, Src: RealtekU_3d:ce:f3 (52:54:00:3d:ce:f3), Dst: RealtekU_ed:8d:74 (52:54:00:ed:8d:74)
▶ Internet Protocol Version 4, Src: 14.119.104.189, Dst: 192.168.122.245
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 40418, Seq: 2579742065, Ack: 268058582, Len: 5226
▶ Transport Layer Security
▶ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 59
▶ Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 55
Version: TLS 1.2 (0x0303)
▶ Random: 6472050667689fee2d9efc86ebb65161024949c13cf052a0...
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Compression Method: null (0)
Extensions Length: 15
▶ Extension: session_ticket (len=0)
Type: session_ticket (35)
Length: 0
Data (0 bytes)
▶ Extension: renegotiation_info (len=1)
Type: renegotiation_info (65281)
Length: 1
▶ Renegotiation Info extension
▶ Extension: ec_point_formats (len=2)
Type: ec_point_formats (11)
Length: 2
EC point formats Length: 1
▶ Elliptic curves point formats (1)
▶ TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4810
▶ Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 4806
Certificates Length: 4803
▶ Certificates (4803 bytes)
▶ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 333
▶ Handshake Protocol: Server Key Exchange
Handshake Type: Server Key Exchange (12)
Length: 329
▶ EC Diffie-Hellman Server Params
▶ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 4
▶ Handshake Protocol: Server Hello Done
Handshake Type: Server Hello Done (14)

▶ Frame 12: 5280 bytes on wire (42240 bits), 5280 bytes captured (42240 bits) on interface enp1s0, id 0
▶ Ethernet II, Src: RealtekU_3d:ce:f3 (52:54:00:3d:ce:f3), Dst: RealtekU_ed:8d:74 (52:54:00:ed:8d:74)
▶ Internet Protocol Version 4, Src: 14.119.104.189, Dst: 192.168.122.245
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 40418, Seq: 2579742065, Ack: 268058582, Len: 5226
▶ Transport Layer Security
▶ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
▶ TLSv1.2 Record Layer: Handshake Protocol: Certificate
▶ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
▶ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done

此时一次传输了 Server Hello、服务器证书、服务器密钥交换、服务器问候完成。

客户端密钥交换、更改密码规范、传递加密信息：

10	2023-05-27 09:2...	192.168.122.245	14.119.104.189	TLSv1.2	571 Client Hello
12	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	5280 Server Hello, Certificate, Server Key Exchange, Server Hello ...
14	2023-05-27 09:2...	192.168.122.245	14.119.104.189	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake ...
15	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	924 [TCP Spurious Retransmission] , Ignored Unknown Record
18	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	280 New Session Ticket, Change Cipher Spec, Encrypted Handshake M...

»	Frame 14: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface enp1s0, id 0
»	Ethernet II, Src: RealtekU_ed:8d:74 (52:54:00:ed:8d:74), Dst: RealtekU_3d:ce:f3 (52:54:00:3d:ce:f3)
»	Internet Protocol Version 4, Src: 192.168.122.245, Dst: 14.119.104.189
»	Transmission Control Protocol, Src Port: 40418, Dst Port: 443, Seq: 268058582, Ack: 2579747291, Len: 126
»	Transport Layer Security
»	TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
»	TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
»	TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

12	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	5280 Server Hello, Certificate, Server Key Exchange, Server Hello ...
14	2023-05-27 09:2...	192.168.122.245	14.119.104.189	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake ...
15	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	924 [TCP Spurious Retransmission] , Ignored Unknown Record
18	2023-05-27 09:2...	14.119.104.189	192.168.122.245	TLSv1.2	280 New Session Ticket, Change Cipher Spec, Encrypted Handshake M...

»	Frame 18: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface enp1s0, id 0
»	Ethernet II, Src: RealtekU_3d:ce:f3 (52:54:00:3d:ce:f3), Dst: RealtekU_ed:8d:74 (52:54:00:ed:8d:74)
»	Internet Protocol Version 4, Src: 14.119.104.189, Dst: 192.168.122.245
»	Transmission Control Protocol, Src Port: 443, Dst Port: 40418, Seq: 2579747291, Ack: 268058708, Len: 226
»	Transport Layer Security
»	TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
»	TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
»	TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

2. 更改证书文件路径，请同学们将 www.baidu.com 网站的测试过程截图保存（如果不将证书拷贝过来应该有报错信息，拷贝过来之后应该正常），也可选用其他网站做测试。

3.


```

root@413c996b044c:/volumes# ./handshake.py www.baidu.com
After making TCP connection. Press any key to continue ...
=== Cipher used: ('ECDHE-RSA-AES128-GCM-SHA256', 'TLSv1.2', 128)
=== Server hostname: www.baidu.com
=== Server certificate:
{'OCSP': ('http://ocsp.globalsign.com/gsrsoavsslca2018',),
'caIssuers': ('http://secure.globalsign.com/cacert/gsrsoavsslca2018.crt',),
'crlDistributionPoints': ('http://crl.globalsign.com/gsrsoavsslca2018.crl',),
'issuer': (((('countryName', 'BE'),),
              (('organizationName', 'GlobalSign nv-sa'),),
              (('commonName', 'GlobalSign RSA OV SSL CA 2018'),)),
'notAfter': 'Aug  6 05:16:01 2023 GMT',
'notBefore': 'Jul  5 05:16:02 2022 GMT',
'serialNumber': '4417CE86EF82EC6921CC6F68',
'subject': (((('countryName', 'CN'),),
              (('stateOrProvinceName', 'beijing'),),
              (('localityName', 'beijing'),),
              (('organizationalUnitName', 'service operation department'),),
              (('organizationName',
                'Beijing Baidu Netcom Science Technology Co., Ltd'),),
              (('commonName', 'baidu.com'),)),
'subjectAltName': (('DNS', 'baidu.com'),
                  ('DNS', 'baifubao.com'),
                  ('DNS', 'www.baidu.cn'),
                  ('DNS', 'www.baidu.com.cn'),
                  ('DNS', 'mct.y.nuomi.com'),
                  ('DNS', 'apollo.auto'),
                  ('DNS', 'dwz.cn'),
                  ('DNS', '*.baidu.com'),
                  ('DNS', '*.baifubao.com'),
                  ('DNS', '*.baidustatic.com'),
                  ('DNS', '*.bdstatic.com'),
                  ('DNS', '*.bdimg.com'),
                  ('DNS', '*.haol23.com'),
                  ('DNS', '*.nuomi.com'),
                  ('DNS', '*.chuanke.com'),
                  ('DNS', '*.trustgo.com'),
                  ('DNS', '*.bce.baidu.com'),
                  ('DNS', '*.eyun.baidu.com'),
                  ('DNS', '*.map.baidu.com'),
                  ('DNS', '*.mbd.baidu.com'),
                  ('DNS', '*.fanyi.baidu.com'),
                  ('DNS', '*.baidubce.com'),
                  ('DNS', '*.mipcdn.com'),
                  ('DNS', '*.news.baidu.com'),
                  ('DNS', '*.baidupcs.com'),
                  ('DNS', '*.aipage.com'),
                  ('DNS', '*.aipage.cn'),
                  ('DNS', '*.bcehost.com'),
                  ('DNS', '*.safe.baidu.com'),
                  ('DNS', '*.im.baidu.com'),
                  ('DNS', '*.baiducontent.com'),
                  ('DNS', '*.dlnel.com'),
                  ('DNS', '*.dlnel.org')),

```

[36/36]

[01] 0:docker-compose 1:tmux1*7

"VM" 12:18 27 May 23

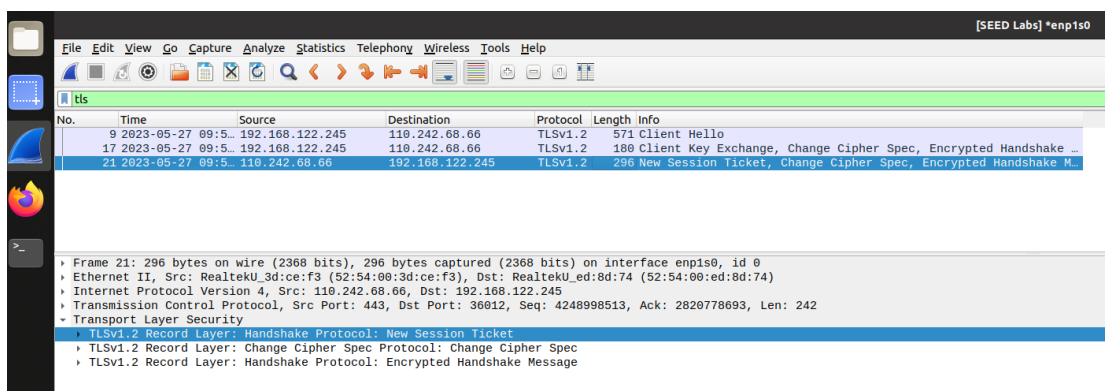
3. 请同学们将修改 `www.baidu.com` 网站主机名的测试过程截图保存在报告里并分析执行的结果，也可选用其他网站做测试。

修改 `hosts` 后，由于没有校验域名正确性，所以整个流程可以顺利进行。

```

root@413c996b044c:/volumes# ./handshake.py www.baidu.com
After making TCP connection. Press any key to continue ...
=== Cipher used: ('ECDHE-RSA-AES128-GCM-SHA256', 'TLSv1.2', 128)
=== Server hostname: www.baidu.com
=== Server certificate:
{'OCSP': ('http://ocsp.digicert.cn',),
'caIssuers': ('http://cacerts.digicert.cn/DigiCertSecureSiteProCNCAG3.crt',),
'crlDistributionPoints': ('http://crl.digicert.cn/DigiCertSecureSiteProCNCAG3.crl',),
'issuer': (((('countryName', 'US'),),
              (('organizationName', 'DigiCert Inc'),),
              (('commonName', 'DigiCert Secure Site Pro CN CA G3'))),),
'notAfter': 'Feb 27 23:59:59 2024 GMT',
'notBefore': 'Jan 30 00:00:00 2023 GMT',
'serialNumber': '07C632B21329FD68B7B760DD87D15F20',
'subject': (((('countryName', 'CN'),),
               (('stateOrProvinceName', '北京市'),),
               (('organizationName',
                 'Beijing Baidu Netcom Science Technology Co., Ltd'),),
               (('commonName', 'www.baidu.cn'))),),
'subjectAltName': (('DNS', 'www.baidu.cn'),
                  ('DNS', 'baidu.cn'),
                  ('DNS', 'baidu.com'),
                  ('DNS', 'baidu.com.cn'),
                  ('DNS', 'w.baidu.com'),
                  ('DNS', 'ww.baidu.com'),
                  ('DNS', 'www.baidu.com.cn'),
                  ('DNS', 'www.baidu.com.hk'),
                  ('DNS', 'www.baidu.hk'),
                  ('DNS', 'www.baidu.net.au'),
                  ('DNS', 'www.baidu.net.ph'),
                  ('DNS', 'www.baidu.net.tw'),
                  ('DNS', 'www.baidu.net.vn'),
                  ('DNS', 'www.baidu.com'),
                  ('DNS', 'www.baidu.com.cn')),
'version': 3}
[{'issuer': (((('countryName', 'US'),),
               (('organizationName', 'DigiCert Inc'),),
               (('organizationalUnitName', 'www.digicert.com'),),
               (('commonName', 'DigiCert Global Root CA'))),),
'notAfter': 'Nov 10 00:00:00 2031 GMT',
'notBefore': 'Nov 10 00:00:00 2006 GMT',
'serialNumber': '083BE056904246B1A1756AC95991C74A',
'subject': (((('countryName', 'US'),),
               (('organizationName', 'DigiCert Inc'),),
               (('organizationalUnitName', 'www.digicert.com'),),
               (('commonName', 'DigiCert Global Root CA'))),),
'version': 3}]
After TLS handshake. Press any key to continue ...
root@413c996b044c:/volumes# 110.242.68.66^C
root@413c996b044c:/volumes# █

```



4.请分析 TLS 客户端编程和 server.py 的代码，说明客户端和服务端程序的关键步骤。

从客户端访问服务端：

```

seed@VM: ~/../volumes
sssock.close()
[05/31/23]seed@VM:~/../volumes$ dockps
413c996b044c client-10.9.0.5
d91e82627f2e server-10.9.0.43
ca2684fc2a47 mitm-proxy-10.9.0.143
[05/31/23]seed@VM:~/../volumes$ docksh d9
root@d91e82627f2e:/# ls
bin dev home lib32 libx32 mnt proc run srv tmp var
boot etc lib lib64 media opt root sbin sys usr volumes
root@d91e82627f2e:/# cd volumes/
root@d91e82627f2e:/volumes# ls
5ad8a5d6.0 README.txt client-certs client.py handshake.py server-certs server.py
root@d91e82627f2e:/volumes# ./server.py
Traceback (most recent call last):
  File "./server.py", line 18, in <module>
    context.load_cert_chain(SERVER_CERT, SERVER_PRIVATE)
FileNotFoundError: [Errno 2] No such file or directory
root@d91e82627f2e:/volumes# ls
5ad8a5d6.0 README.txt client-certs client.py handshake.py server-certs server.py
root@d91e82627f2e:/volumes# vim server.py
bash: vim: command not found
root@d91e82627f2e:/volumes# nano server.py
root@d91e82627f2e:/volumes# ./server.py
Enter PEM pass phrase:
TLS connection established
"Request: b'GET / HTTP/1.0\r\nHost: www.bank32.com\r\n\r\n'"

{
  'issuer': (
    (('commonName', 'www.modelCA.com'),),
    (('organizationName', 'Model CA LTD.'),),
    (('countryName', 'US'),),
  ),
  'notAfter': 'May 22 06:17:21 2033 GMT',
  'notBefore': 'May 25 06:17:21 2023 GMT',
  'serialNumber': '1000',
  'subject': (
    (('countryName', 'US'),),
    (('organizationName', 'Bank32 Inc.'),),
    (('commonName', 'www.bank32.com'),),
  ),
  'version': 3
}
[
  {
    'issuer': (
      (('commonName', 'www.modelCA.com'),),
      (('organizationName', 'Model CA LTD.'),),
      (('countryName', 'US'),),
    ),
    'notAfter': 'May 22 06:17:09 2033 GMT',
    'notBefore': 'May 25 06:17:09 2023 GMT',
    'serialNumber': '25229E5085C09A445EC412F1F4E026124F1CB722',
    'subject': (
      (('commonName', 'www.modelCA.com'),),
      (('organizationName', 'Model CA LTD.'),),
      (('countryName', 'US'),),
    ),
    'version': 3
  }
]
After TLS handshake. Press any key to continue ...
[b'\nHTTP/1.1 200 OK',
 b'Content-Type: text/html',
 b'',
 b'\n<!DOCTYPE html><html><body><h1>This is Bank32.com!</h1></body></html>\n']
root@413c996b044c:/volumes#
[0] 0:bash- 1:docker-compose 2:docker* "VM" 05:47 31-May-23

```

1. TCP 连接

```

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM, 0)
sock.bind(('10.9.0.43', 443))
sock.listen(5)

while True:
    newsock, fromaddr = sock.accept()
    try:
        ssock = context.wrap_socket(newsock, server_side=True)

```

```

# Create TCP connection
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect((hostname, port))
input("After making TCP connection. Press any key to continue ...")

```

2. 数据传输

a) 服务端 TLS

```

try:
    ssock = context.wrap_socket(newsock, server_side=True)
    print("TLS connection established")
    data = ssock.recv(1024) # Read data over TLS
    pprint.pprint("Request: {}".format(data))
    ssock.sendall(html.encode('utf-8')) # Send data over TLS

    ssock.shutdown(socket.SHUT_RDWR) # Close the TLS connection
    ssock.close()

```

b) 客户端 TLS

```

# Add the TLS
ssock = context.wrap_socket(sock, server_hostname=hostname,
                             do_handshake_on_connect=False)
ssock.do_handshake() # Start the handshake
print("=== Cipher used: {}".format(ssock.cipher()))
print("=== Server hostname: {}".format(ssock.server_hostname))
print("=== Server certificate:")
pprint.pprint(ssock.getpeercert())
pprint.pprint(context.get_ca_certs())
print("After TLS handshake. Press any key to continue ...")

```

3. 客户端 HTTP 请求 Over TLS

```

# Send HTTP Request to Server
request = b"GET / HTTP/1.0\r\nHost: " + hostname.encode('utf-8') + b"\r\n\r\n"
ssock.sendall(request)
# Read HTTP Response from Server
response = ssock.recv(2048)
while response:
    pprint.pprint(response.split(b"\r\n"))
    response = ssock.recv(2048)

```

5.请分别用 client.py 和浏览器两种方式访问服务器，并记录你观察的结果

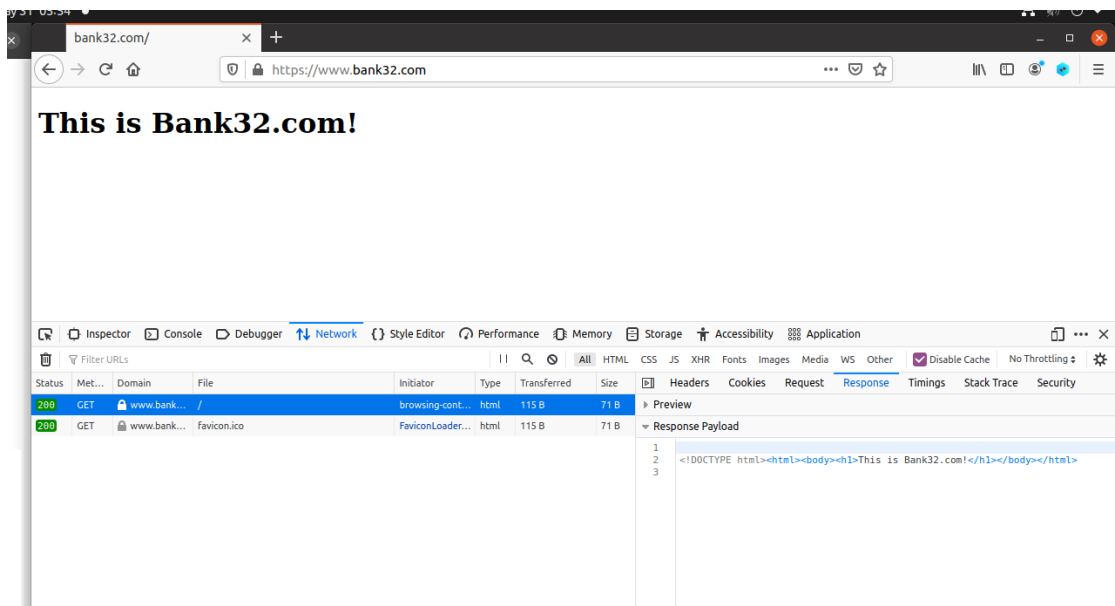
(截图)

```

seed@VM: ~/../volumes
sssock.close()
[05/31/23]seed@VM:~/../volumes$ dockps
413c996b044c  client-10.9.0.5
d91e82627f2e  server-10.9.0.43
ca2684fc2a47  mitm-proxy-10.9.0.143
[05/31/23]seed@VM:~/../volumes$ docksh d9
root@d91e82627f2e:/# ls
bin  dev  home  lib32  libx32  mnt  proc  run  srv  tmp  var
boot  etc  lib  lib64  media  opt  root  sbin  sys  usr  volumes
root@d91e82627f2e:/# cd volumes/
root@d91e82627f2e:/volumes# ls
5ad8a5d6.0  README.txt  client-certs  client.py  handshake.py  server-certs  server.py
root@d91e82627f2e:/volumes# ./server.py
Traceback (most recent call last):
  File "./server.py", line 18, in <module>
    context.load_cert_chain(SERVER_CERT, SERVER_PRIVATE)
FileNotFoundError: [Errno 2] No such file or directory
root@d91e82627f2e:/volumes# ls
5ad8a5d6.0  README.txt  client-certs  client.py  handshake.py  server-certs  server.py
root@d91e82627f2e:/volumes# vim server.py
bash: vim: command not found
root@d91e82627f2e:/volumes# nano server.py
root@d91e82627f2e:/volumes# ./server.py
Enter PEM pass phrase:
TLS connection established
"Request: b'GET / HTTP/1.0\\r\\nHost: www.bank32.com\\r\\n\\r\\n'"

[{'issuer': (((('commonName', 'www.modelCA.com'),),
                (('organizationName', 'Model CA LTD.'),),
                (('countryName', 'US'),)),
  'notAfter': 'May 22 06:17:21 2033 GMT',
  'notBefore': 'May 25 06:17:21 2023 GMT',
  'serialNumber': '1000',
  'subject': (((('countryName', 'US'),),
                (('organizationName', 'Bank32 Inc.'),),
                (('commonName', 'www.bank32.com'),)),
  'version': 3}]
[{'issuer': (((('commonName', 'www.modelCA.com'),),
                (('organizationName', 'Model CA LTD.'),),
                (('countryName', 'US'),)),
  'notAfter': 'May 22 06:17:09 2033 GMT',
  'notBefore': 'May 25 06:17:09 2023 GMT',
  'serialNumber': '25229E5085C09A445EC412F1F4E026124F1CB722',
  'subject': (((('commonName', 'www.modelCA.com'),),
                (('organizationName', 'Model CA LTD.'),),
                (('countryName', 'US'),)),
  'version': 3}]
After TLS handshake. Press any key to continue ...
[b'\nHTTP/1.1 200 OK',
 b'Content-Type: text/html',
 b'',
 b'\n<!DOCTYPE html><html><body><h1>This is Bank32.com!</h1></body></html>\n']
root@413c996b044c:/volumes# 
[0] 0:bash- 1:docker-compose 2:docker* "VM" 05:47 31-May-23

```



现象：

client.py 能够正确获取服务器的网页，

浏览器也能够正常请求服务器网页并显示。