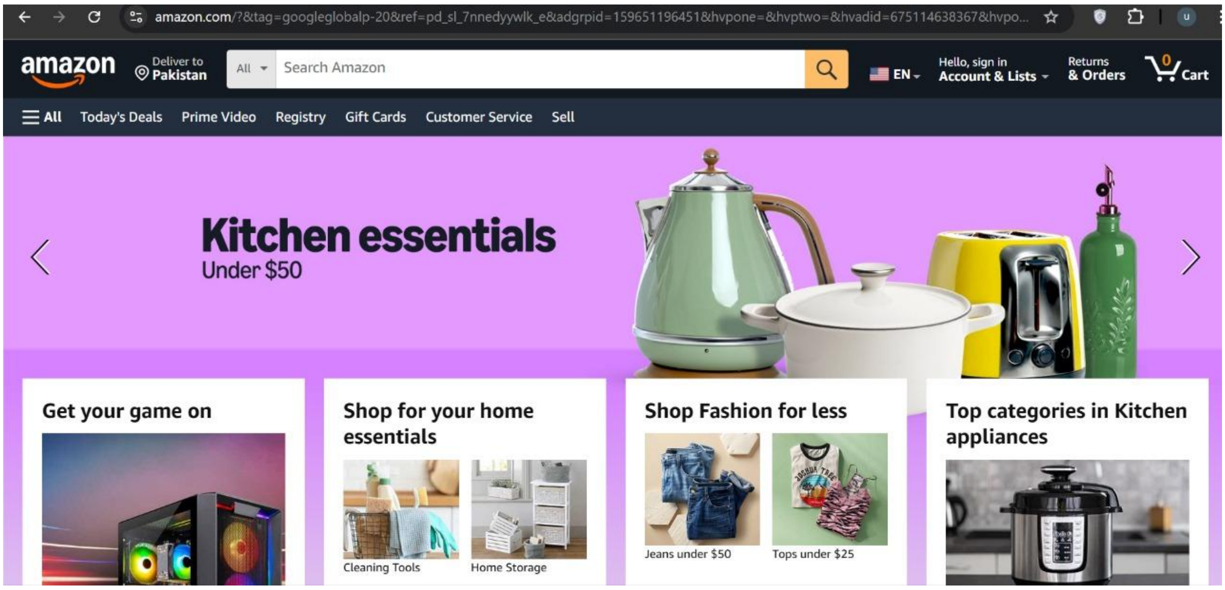
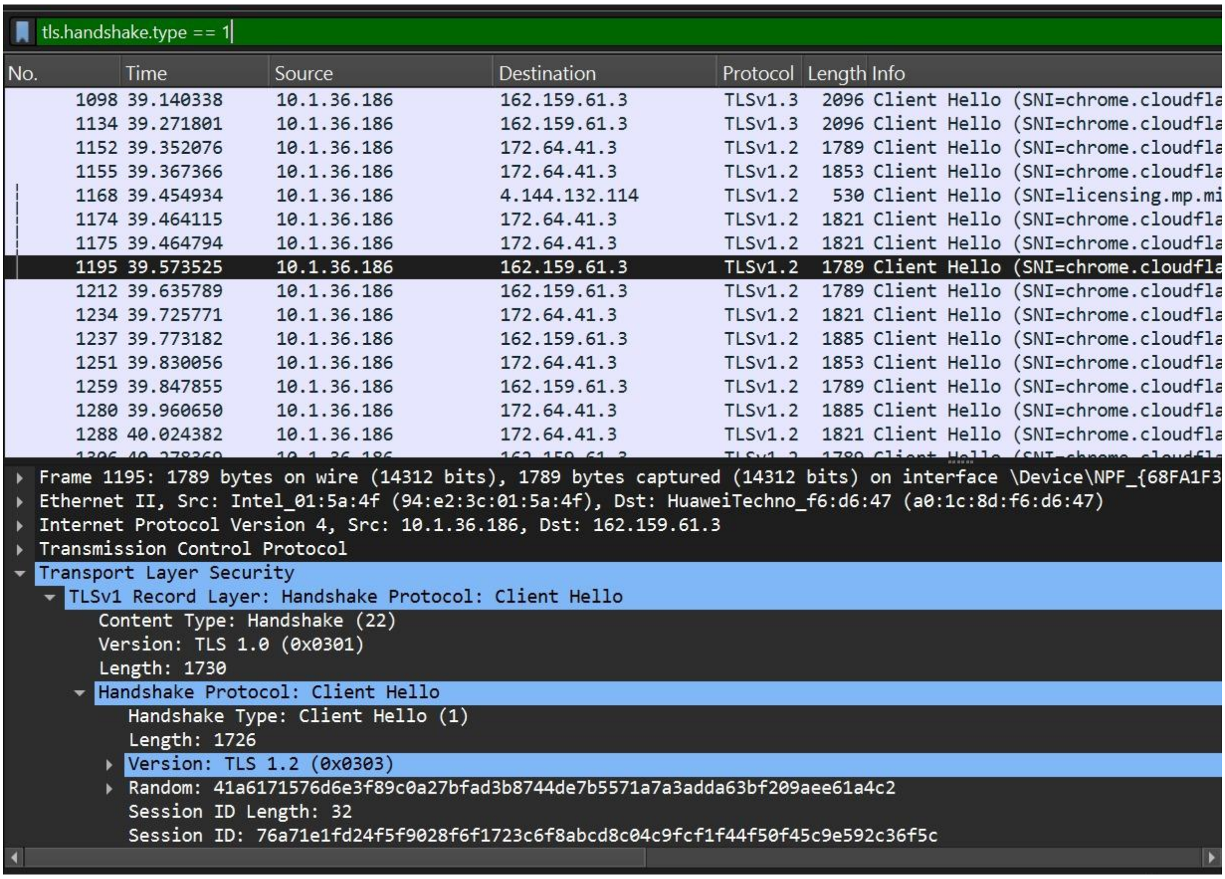
Assignment task No 02	Computer Networking
Name	Omair Ahmad Sudais Aziz M.Azhan
Reg No	B23F0001AI058 B23F0344Ai084 B23F0001AI059
Instructor	Dr Adnan Iqbal
Date	27/09/2025

What is the name of website?

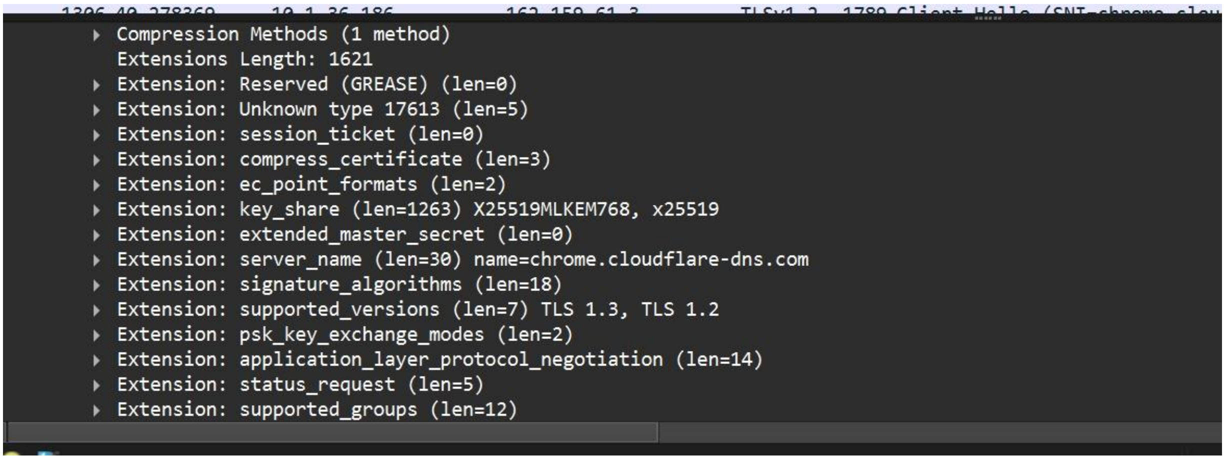


1 Find the packet that contains the **ClientHello** message for the website you are accessing.



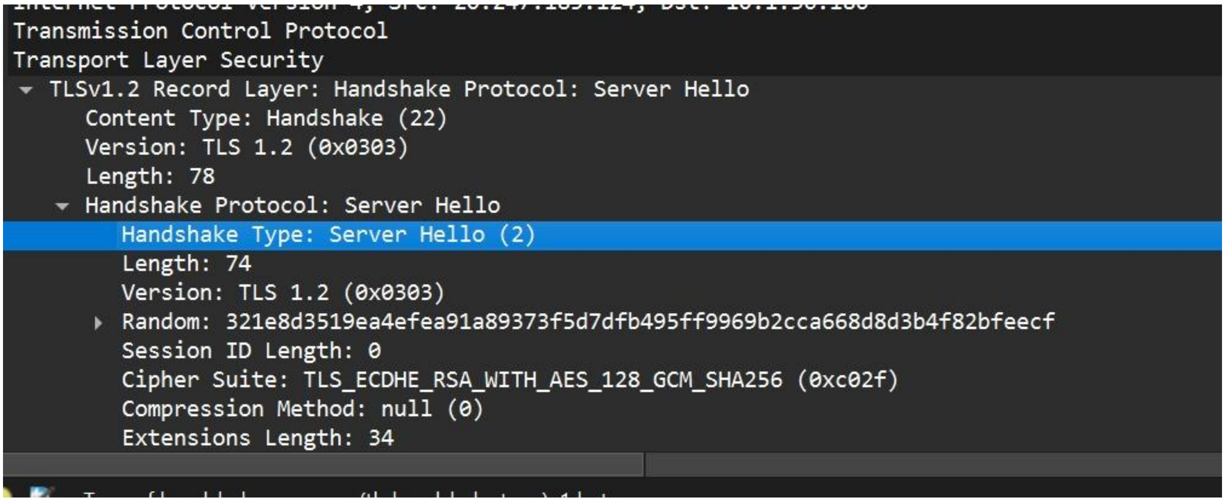
```
tls.handshake.type == 1

No.   Time       Source        Destination    Protocol Length Info
 1098 39.140338  10.1.36.186   162.159.61.3   TLSv1.3  2096 Client Hello (SNI=chrome.cloudfla
 1134 39.271801  10.1.36.186   162.159.61.3   TLSv1.3  2096 Client Hello (SNI=chrome.cloudfla
 1152 39.352076  10.1.36.186   172.64.41.3    TLSv1.2  1789 Client Hello (SNI=chrome.cloudfla
 1155 39.367366  10.1.36.186   172.64.41.3    TLSv1.2  1853 Client Hello (SNI=chrome.cloudfla
 1168 39.454934  10.1.36.186   4.144.132.114  TLSv1.2   530 Client Hello (SNI=licensing.mp.mi
 1174 39.464115  10.1.36.186   172.64.41.3    TLSv1.2  1821 Client Hello (SNI=chrome.cloudfla
 1175 39.464794  10.1.36.186   172.64.41.3    TLSv1.2  1821 Client Hello (SNI=chrome.cloudfla
 1195 39.573525  10.1.36.186   162.159.61.3   TLSv1.2  1789 Client Hello (SNI=chrome.cloudfla
 1212 39.635789  10.1.36.186   162.159.61.3   TLSv1.2  1789 Client Hello (SNI=chrome.cloudfla
 1234 39.725771  10.1.36.186   172.64.41.3    TLSv1.2  1821 Client Hello (SNI=chrome.cloudfla
 1237 39.773182  10.1.36.186   162.159.61.3   TLSv1.2  1885 Client Hello (SNI=chrome.cloudfla
 1251 39.830056  10.1.36.186   172.64.41.3    TLSv1.2  1853 Client Hello (SNI=chrome.cloudfla
 1259 39.847855  10.1.36.186   162.159.61.3   TLSv1.2  1789 Client Hello (SNI=chrome.cloudfla
 1280 39.960650  10.1.36.186   172.64.41.3    TLSv1.2  1885 Client Hello (SNI=chrome.cloudfla
 1288 40.024382  10.1.36.186   172.64.41.3    TLSv1.2  1821 Client Hello (SNI=chrome.cloudfla

▸ Frame 1195: 1789 bytes on wire (14312 bits), 1789 bytes captured (14312 bits) on interface \Device\NPF_{68FA1F3
▸ Ethernet II, Src: Intel_01:5a:4f (94:e2:3c:01:5a:4f), Dst: HuaweiTechno_f6:d6:47 (a0:1c:8d:f6:d6:47)
▸ Internet Protocol Version 4, Src: 10.1.36.186, Dst: 162.159.61.3
▸ Transmission Control Protocol
▾ Transport Layer Security
  ▾ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1730
    ▾ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 1726
      ▸ Version: TLS 1.2 (0x0303)
      ▸ Random: 41a6171576d6e3f89c0a27bfad3b8744de7b5571a7a3adda63bf209aee61a4c2
        Session ID Length: 32
        Session ID: 76a71e1fd24f5f9028f6f1723c6f8abcd8c04c9fcf1f44f50f45c9e592c36f5c
```

2. List all the TLS extensions included in the ClientHello.



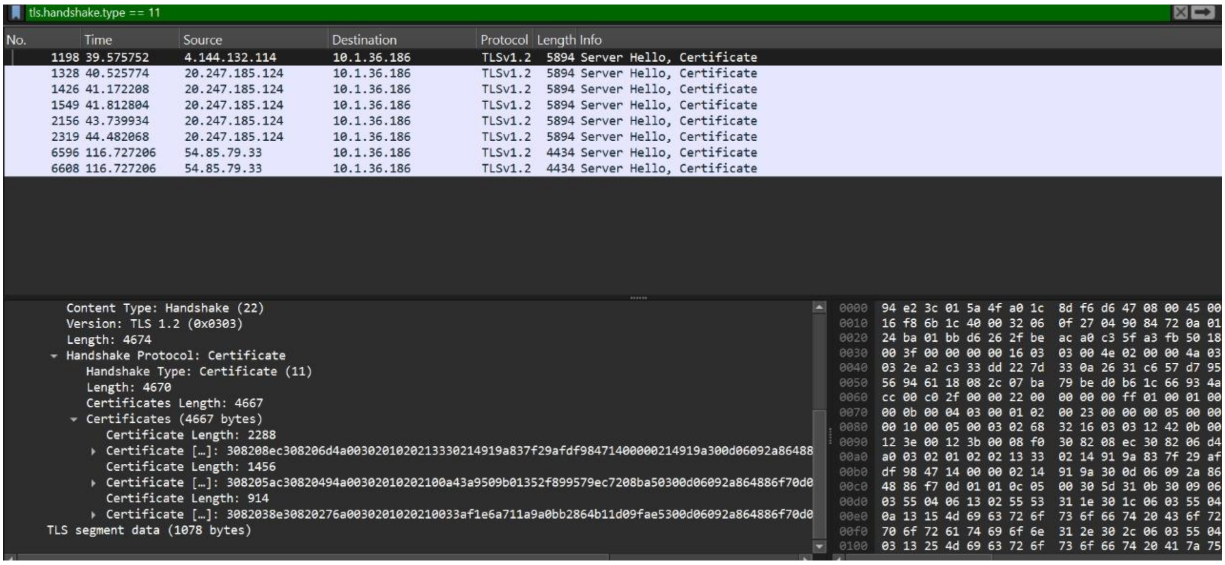
```
▸ Compression Methods (1 method)
  Extensions Length: 1621
▸ Extension: Reserved (GREASE) (len=0)
▸ Extension: Unknown type 17613 (len=5)
▸ Extension: session_ticket (len=0)
▸ Extension: compress_certificate (len=3)
▸ Extension: ec_point_formats (len=2)
▸ Extension: key_share (len=1263) X25519MLKEM768, x25519
▸ Extension: extended_master_secret (len=0)
▸ Extension: server_name (len=30) name=chrome.cloudflare-dns.com
▸ Extension: signature_algorithms (len=18)
▸ Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
▸ Extension: psk_key_exchange_modes (len=2)
▸ Extension: application_layer_protocol_negotiation (len=14)
▸ Extension: status_request (len=5)
▸ Extension: supported_groups (len=12)
```

3. Identify the ServerHello message. What cipher suite is chosen by the server?



```
Internet Protocol Version 4, Src: 20.247.185.124, Dst: 10.1.36.186
Transmission Control Protocol
Transport Layer Security
 ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
     Content Type: Handshake (22)
     Version: TLS 1.2 (0x0303)
     Length: 78
   ▾ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 74
        Version: TLS 1.2 (0x0303)
      ▸ Random: 321e8d3519ea4efea91a89373f5d7dfb495ff9969b2cca668d8d3b4f82bfeecf
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 34
```

4. Locate the Certificate message. Extract the server's certificate information (issuer, subject, validity dates).



```
tls.handshake.type == 11

No.   Time        Source          Destination  Protocol Length Info
 1198 39.575752   4.144.132.114   10.1.36.186  TLSv1.2  5894 Server Hello, Certificate
 1328 40.525774   20.247.185.124  10.1.36.186  TLSv1.2  5894 Server Hello, Certificate
 1426 41.172208   20.247.185.124  10.1.36.186  TLSv1.2  5894 Server Hello, Certificate
 1549 41.812804   20.247.185.124  10.1.36.186  TLSv1.2  5894 Server Hello, Certificate
 2156 43.739934   20.247.185.124  10.1.36.186  TLSv1.2  5894 Server Hello, Certificate
 2319 44.482068   20.247.185.124  10.1.36.186  TLSv1.2  5894 Server Hello, Certificate
 6596 116.727206  54.85.79.33     10.1.36.186  TLSv1.2  4434 Server Hello, Certificate
 6608 116.727206  54.85.79.33     10.1.36.186  TLSv1.2  4434 Server Hello, Certificate
```

```
     Content Type: Handshake (22)
     Version: TLS 1.2 (0x0303)
     Length: 4674
   ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 4670
        Certificates Length: 4667
      ▾ Certificates (4667 bytes)
           Certificate Length: 2288
         ▸ Certificate […]: 308208ec308206d4a003020102021333021491 9a837f29afdf98471400000214919a300d06092a86488
           Certificate Length: 1456
         ▸ Certificate […]: 308205ac30820494a00302010202100a43a9509b01352f899579ec7208ba50300d06092a864886f70d0
           Certificate Length: 914
         ▸ Certificate […]: 3082038e30820276a0030201020210033af1e6a711a9a0bb2864b11d09fae5300d06092a864886f70d0
   TLS segment data (1078 bytes)
```

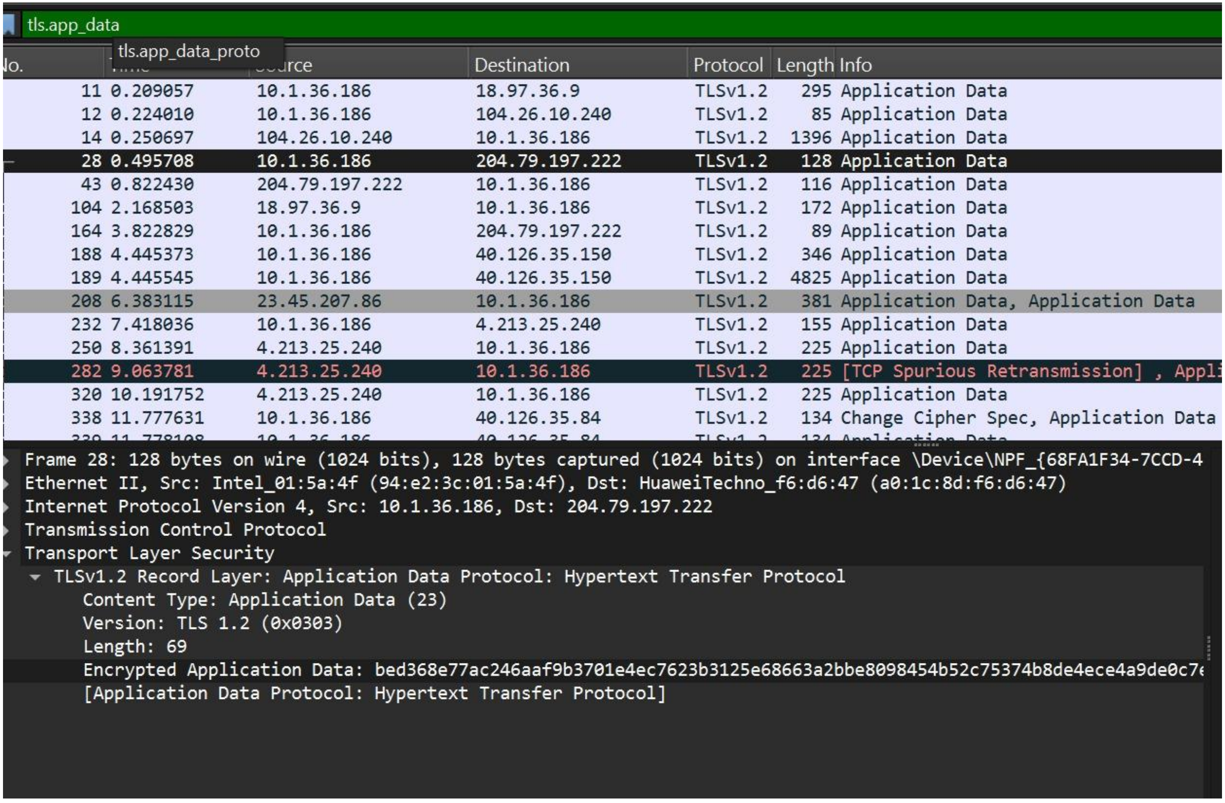
```
0000  94 e2 3c 01 5a 4f a0 1c  8d f6 d6 47 08 00 45 00
0010  16 f8 6b 1c 40 00 32 06  0f 27 04 90 84 72 0a 01
0020  24 ba 01 bb d6 26 2f be  ac a0 c3 5f a3 fb 50 18
0030  00 3f 00 00 00 00 16 03  03 00 4e 02 00 00 4a 03
0040  03 2e a2 c3 33 dd 22 7d  33 0a 26 31 c6 57 d7 95
0050  56 94 61 18 08 2c 07 ba  79 be d0 b6 1c 66 93 4a
0060  cc 00 c0 2f 00 00 22 00  00 00 00 ff 01 00 01 00
0070  00 0b 00 04 03 00 01 02  00 23 00 00 00 05 00 00
0080  00 10 00 05 00 03 02 68  32 16 03 03 12 42 0b 00
0090  12 3e 00 12 3b 00 08 f0  30 82 08 ec 30 82 06 d4
00a0  a0 03 02 01 02 02 13 33  02 14 91 9a 83 7f 29 af
00b0  df 98 47 14 00 00 02 14  91 9a 30 0d 06 09 2a 86
00c0  48 86 f7 0d 01 01 0c 05  00 30 5d 31 0b 30 09 06
00d0  03 55 04 06 13 02 55 53  31 1e 30 1c 06 03 55 04
00e0  0a 13 15 4d 69 63 72 6f  73 6f 66 74 20 43 6f 72
00f0  70 6f 72 61 74 69 6f 6e  31 2e 30 2c 06 03 55 04
0100  03 13 25 4d 69 63 72 6f  73 6f 66 74 20 41 7a 75
```

5.After the TLS handshake, identify the first encrypted application data packet. Why can't you directly see the HTTP headers in this packet?

The first encrypted application data packet appears right after the TLS handshake completes (use filter: tls.app_data - first packet shown).

You can't see HTTP headers because TLS encryption scrambles all application data (including HTTP headers) into unreadable binary. Only the server has the private key needed to decrypt this data.

This encryption is intentional - it's what makes HTTPS secure by protecting your data from eavesdroppers.



```
tls.app_data
          tls.app_data_proto
lo.                ource          Destination     Protocol Length Info
     11 0.209057   10.1.36.186    18.97.36.9      TLSv1.2   295 Application Data
     12 0.224010   10.1.36.186    104.26.10.240   TLSv1.2    85 Application Data
     14 0.250697   104.26.10.240  10.1.36.186     TLSv1.2  1396 Application Data
     28 0.495708   10.1.36.186    204.79.197.222  TLSv1.2   128 Application Data
     43 0.822430   204.79.197.222 10.1.36.186     TLSv1.2   116 Application Data
    104 2.168503   18.97.36.9     10.1.36.186     TLSv1.2   172 Application Data
    164 3.822829   10.1.36.186    204.79.197.222  TLSv1.2    89 Application Data
    188 4.445373   10.1.36.186    40.126.35.150   TLSv1.2   346 Application Data
    189 4.445545   10.1.36.186    40.126.35.150   TLSv1.2  4825 Application Data
    208 6.383115   23.45.207.86   10.1.36.186     TLSv1.2   381 Application Data, Application Data
    232 7.418036   10.1.36.186    4.213.25.240    TLSv1.2   155 Application Data
    250 8.361391   4.213.25.240   10.1.36.186     TLSv1.2   225 Application Data
    282 9.063781   4.213.25.240   10.1.36.186     TLSv1.2   225 [TCP Spurious Retransmission] , Appli
    320 10.191752  4.213.25.240   10.1.36.186     TLSv1.2   225 Application Data
    338 11.777631  10.1.36.186    40.126.35.84    TLSv1.2   134 Change Cipher Spec, Application Data
    339 11.778108  10.1.36.186    40.126.35.84    TLSv1.2   134 Application Data
```

```
Frame 28: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface \Device\NPF_{68FA1F34-7CCD-4
Ethernet II, Src: Intel_01:5a:4f (94:e2:3c:01:5a:4f), Dst: HuaweiTechno_f6:d6:47 (a0:1c:8d:f6:d6:47)
Internet Protocol Version 4, Src: 10.1.36.186, Dst: 204.79.197.222
Transmission Control Protocol
Transport Layer Security
  TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 69
      Encrypted Application Data: bed368e77ac246aaf9b3701e4ec7623b3125e68663a2bbe8098454b52c75374b8de4ece4a9de0c7e
      [Application Data Protocol: Hypertext Transfer Protocol]
```