(1)

(a) 192.168.1.86

(b) 140.114.85.141

```
> Frame 369: 996 bytes on wire (7968 bits), 996 bytes captured (7968 bits) on interface \Devi
> Ethernet II, Src: IntelCor_eb:d1:d3 (88:d8:2e:eb:d1:d3), Dst: ASUSTekC_d6:54:dc (1c:b7:2c:d
v Internet Protocol Version 4, Src: 192.168.1.86, Dst: 140.114.85.141
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 982
    Identification: 0x0f70 (3952)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.86
    Destination Address: 140.114.85.141
v Transmission Control Protocol, Src Port: 10815, Dst Port: 80, Seq: 1, Ack: 1, Len: 942
```

(c) 80

```
v Transmission Control Protocol, Src Port: 10815, Dst Port: 80, Seq: 1, Ack: 1, Len: 942
    Source Port: 10815
    Destination Port: 80
    [Stream index: 10]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 942]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 591479597
    [Next Sequence Number: 943    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3425785577
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
```

(d) 200

```
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 24 Oct 2023 18:40:58 GMT\r\n
    Server: Apache/2.4.56 (Ubuntu)\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
```

The HTTP 200 OK success status response code indicates that the request has succeeded.

(e)

1:Client→Server SEQ number (raw) = 591479596

2:Server→Client SEQ number (raw) = 3425785576　ACK number (raw) = 591479597

3:Client→Server SEQ number (raw) = 591479597　ACK number (raw) =3425785577

```
Transmission Control Protocol, Src Port: 10815, Dst Port: 80, Seq: 0, Len: 0
   Source Port: 10815
   Destination Port: 80
   [Stream index: 10]
   [Conversation completeness: Complete, WITH_DATA (31)]
   [TCP Segment Len: 0]
   Sequence Number: 0    (relative sequence number)
   Sequence Number (raw): 591479596
   [Next Sequence Number: 1    (relative sequence number)]
   Acknowledgment Number: 0
   Acknowledgment number (raw): 0
   1000 .... = Header Length: 32 bytes (8)
 > Flags: 0x002 (SYN)
   Window: 64240
   [Calculated window size: 64240]
   Checksum: 0xa424 [unverified]
   [Checksum Status: Unverified]
```

```
Transmission Control Protocol, Src Port: 80, Dst Port: 10815, Seq: 0, Ack: 1, Len: 0
   Source Port: 80
   Destination Port: 10815
   [Stream index: 10]
   [Conversation completeness: Complete, WITH_DATA (31)]
   [TCP Segment Len: 0]
   Sequence Number: 0    (relative sequence number)
   Sequence Number (raw): 3425785576
   [Next Sequence Number: 1    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 591479597
   1000 .... = Header Length: 32 bytes (8)
 > Flags: 0x012 (SYN, ACK)
   Window: 64240
   [Calculated window size: 64240]
   Checksum: 0x1c03 [unverified]
   [Checksum Status: Unverified]
```

```
Transmission Control Protocol, Src Port: 10815, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
   Source Port: 10815
   Destination Port: 80
   [Stream index: 10]
   [Conversation completeness: Complete, WITH_DATA (31)]
   [TCP Segment Len: 0]
   Sequence Number: 1    (relative sequence number)
   Sequence Number (raw): 591479597
   [Next Sequence Number: 1    (relative sequence number)]
   Acknowledgment Number: 1    (relative ack number)
   Acknowledgment number (raw): 3425785577
   0101 .... = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)
   Window: 516
   [Calculated window size: 132096]
   [Window size scaling factor: 256]
   Checksum: 0xa418 [unverified]
```

(f)

1:Client→Server　SEQ number = x

2:Server→Client　SEQ number = y　ACK number = x+1

3:Client→Server　SEQ number = x+1　ACK number = y+1

(2)

(a)

HTTPS encrypts the data exchanged between a user's web browser and the server. This means that even if a third party intercepts the data, they won't be able to read it without the SSL key.

(b) 140.114.68.21

```
Internet Protocol Version 4, Src: 192.168.1.86, Dst: 140.114.68.21
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 1237
   Identification: 0xa79e (42910)
 > 010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 128
   Protocol: TCP (6)
   Header Checksum: 0x0000 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.1.86
   Destination Address: 140.114.68.21
Transmission Control Protocol, Src Port: 5876, Dst Port: 443, Seq:
Transport Layer Security
Hypertext Transfer Protocol
```

(c) 443

```
Transmission Control Protocol, Src Port: 5876, Dst Port: 443,
   Source Port: 5876
   Destination Port: 443
   [Stream index: 19]
   [Conversation completeness: Complete, WITH_DATA (31)]
   [TCP Segment Len: 1197]
   Sequence Number: 637    (relative sequence number)
   Sequence Number (raw): 3097939037
   [Next Sequence Number: 1834    (relative sequence number)]
   Acknowledgment Number: 5110    (relative ack number)
   Acknowledgment number (raw): 1938625742
   0101 .... = Header Length: 20 bytes (5)
 > Flags: 0x018 (PSH, ACK)
   Window: 65340
```

(d) TLS

```
Transport Layer Security
 v TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
     Opaque Type: Application Data (23)
     Version: TLS 1.2 (0x0303)
     Length: 1192
     [Content Type: Application Data (23)]
     Encrypted Application Data: b45d428a478a152fb94b4bdeb679b98686ed18088c191f4bb88566386e3
     [Application Data Protocol: Hypertext Transfer Protocol]
```

(e) 16

```
Transport Layer Security
 v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
     Content Type: Handshake (22)
     Version: TLS 1.0 (0x0301)
     Length: 567
   v Handshake Protocol: Client Hello
       Handshake Type: Client Hello (1)
       Length: 563
       Version: TLS 1.2 (0x0303)
       Random: cbedcf72dfddd4f5fc1146d96181ffcf67876dfbec19a434df26ddcc0b4ac934
       Session ID Length: 32
       Session ID: cf4394406a2549acf1aca7d56c318f052215997cffba9e348277dd41ee781b58
       Cipher Suites Length: 32
     > Cipher Suites (16 suites)
       Compression Methods Length: 1
     > Compression Methods (1 method)
       Extensions Length: 458
```

(f) TLS_AES_128_GCM_SHA256

```
Transport Layer Security
▾ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 122
  ▾ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 118
      Version: TLS 1.2 (0x0303)
      Random: f1afacda58f76ad92ae1589d2c76f76994b3e86c6c571d3c450e8798ced6937a
      Session ID Length: 32
      Session ID: cf4394406a2549acf1aca7d56c318f052215997cffba9e348277dd41ee781b58
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Compression Method: null (0)
      Extensions Length: 46
    ▸ Extension: key_share (len=36)
```

(g)

```
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "account" = "guest"
  ▸ Form item: "passwd" = "109021115"
  ▸ Form item: "passwd2" = "198276"
  ▸ Form item: "Submit" = "n J"
  ▸ Form item: "fnstr" = "20231025-849191324649"
```