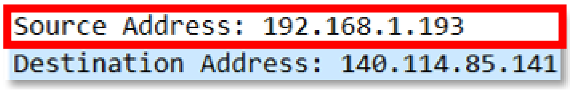
(1) HTTP

(a) What is your computer's IP address?

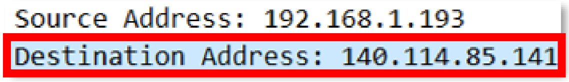
A: 192.168.1.193



```
Source Address: 192.168.1.193
Destination Address: 140.114.85.141
```

(b) What is the IP address of the domain can.cs.nthu.edu.tw?

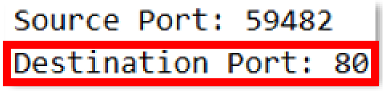
A: 140.114.85.141



```
Source Address: 192.168.1.193
Destination Address: 140.114.85.141
```

(c) Which port number is used by the web server?

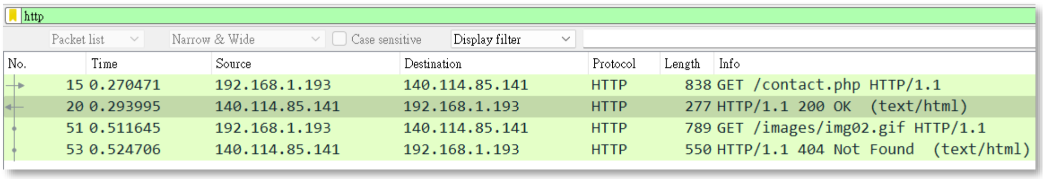
A: 80



```
Source Port: 59482
Destination Port: 80
```

(d) What is the HTTP status code (a 3-digit integer) returned from the web server? Briefly explain what does it mean?

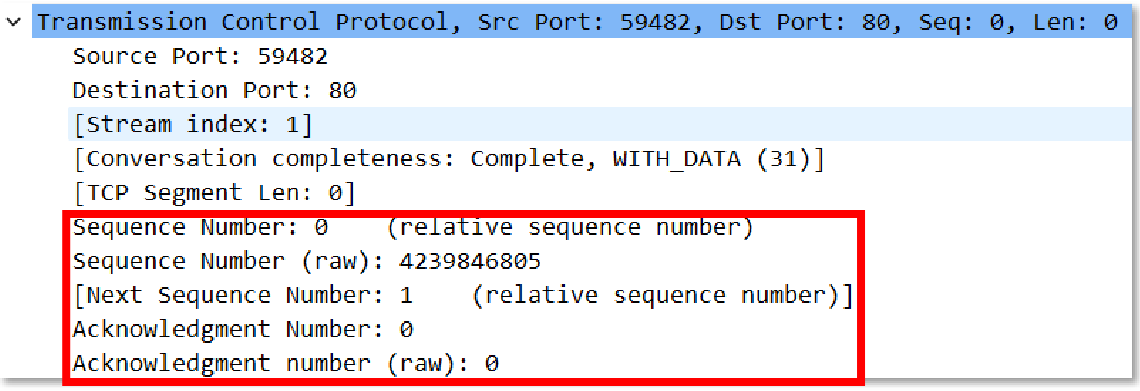
A: 200. It indicates that the request has succeeded.



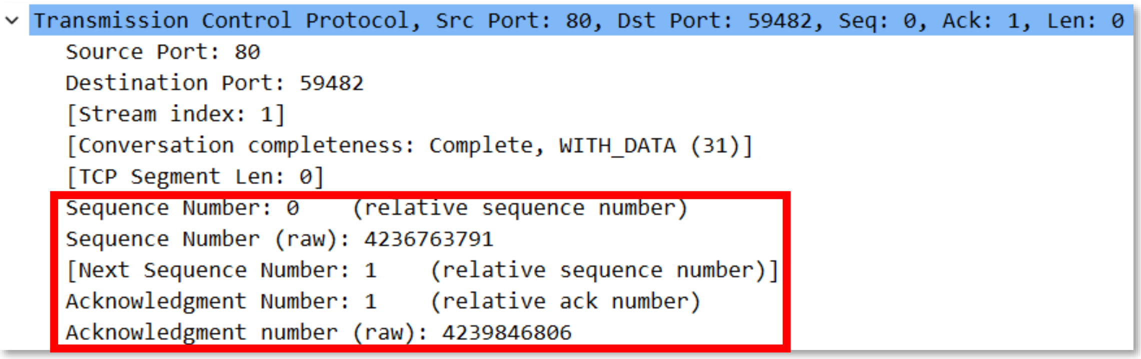
No.	Time	Source	Destination	Protocol	Length	Info
15	0.270471	192.168.1.193	140.114.85.141	HTTP	838	GET /contact.php HTTP/1.1
20	0.293995	140.114.85.141	192.168.1.193	HTTP	277	HTTP/1.1 200 OK (text/html)
51	0.511645	192.168.1.193	140.114.85.141	HTTP	789	GET /images/img02.gif HTTP/1.1
53	0.524706	140.114.85.141	192.168.1.193	HTTP	550	HTTP/1.1 404 Not Found (text/html)

(e) Observe the sequence numbers and acknowledgment numbers in the three packets of the Three-way Handshake, and please provide the raw values rather than the relative values.

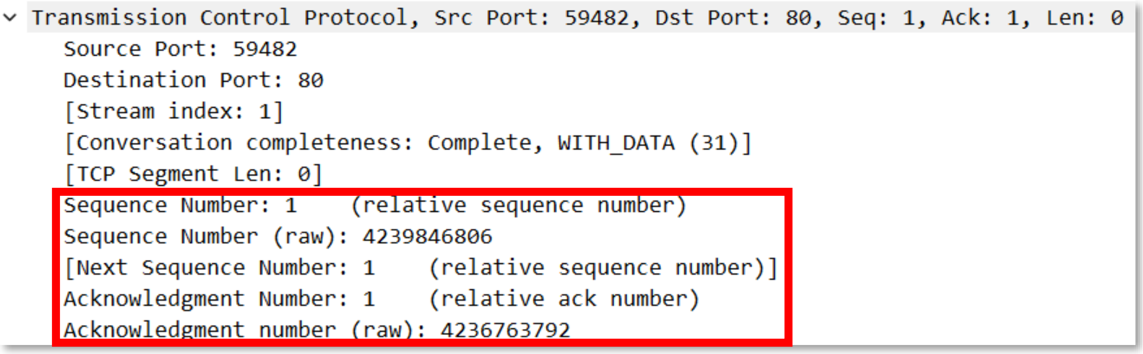
1: Client → Server	SEQ number (raw) = 4239846805	
2: Server → Client	SEQ number (raw) = 4236763791	ACK number (raw) = 4239846806
3: Client → Server	SEQ number (raw) = 4239846806	ACK number (raw) = 4236763792



```
Transmission Control Protocol, Src Port: 59482, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 59482
    Destination Port: 80
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4239846805
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
```



```
Transmission Control Protocol, Src Port: 80, Dst Port: 59482, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 59482
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4236763791
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4239846806
```



```
Transmission Control Protocol, Src Port: 59482, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 59482
    Destination Port: 80
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4239846806
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4236763792
```

(f) Continuing from the previous question, observe the changes in the values and express the relationship between them using given x and y.

A:

1: Client → Server	SEQ number (raw) = x	
2: Server → Client	SEQ number (raw) = y	ACK number (raw) = x + 1
3: Client → Server	SEQ number (raw) = x + 1	ACK number (raw) = y + 1

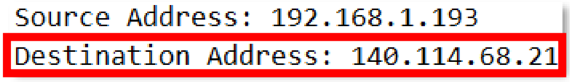
(2) HTTPS

(a) Briefly explain why HTTPS is more secure than HTTP.

A: HTTPS uses encryption to protect information (ex: TSL) sending between clients and servers.

(b) What is the IP address of the domain www.ccxp.nthu.edu.tw?

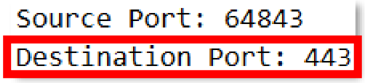
A: 140.114.68.21



```
Source Address: 192.168.1.193
Destination Address: 140.114.68.21
```

(c) Which port number is used by the HTTPS web server?

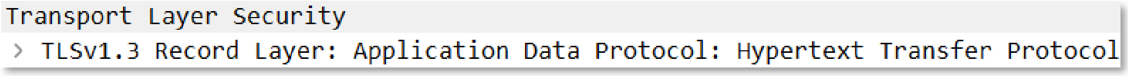
A: 443



```
Source Port: 64843
Destination Port: 443
```

(d) Which security protocol is used, TLS or SSL?

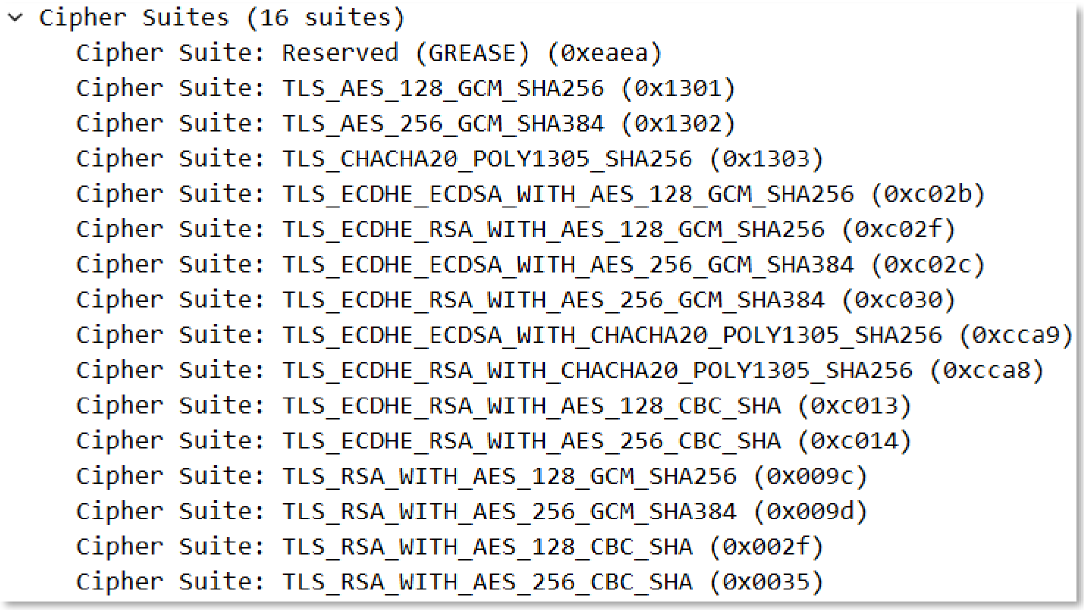
A: TLS



```
Transport Layer Security
 > TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
```

(e) How many cipher suites does your browser offer for the server to choose from?

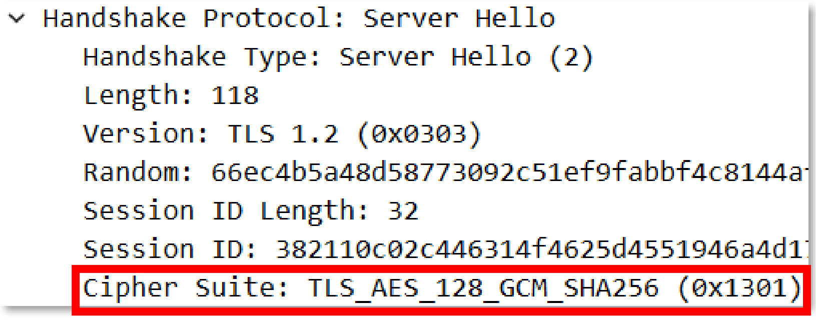
A: 16



```
 v Cipher Suites (16 suites)
     Cipher Suite: Reserved (GREASE) (0xeaea)
     Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
     Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
     Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
     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_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
     Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
     Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
     Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
     Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
     Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
     Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
     Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
     Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
     Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
```

(f) Which cipher suite has the server selected to use?

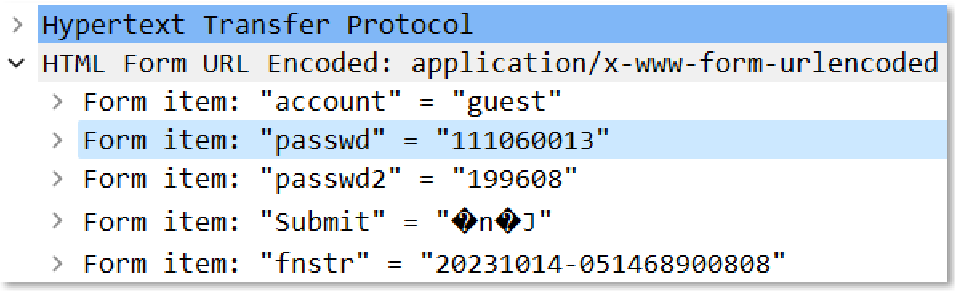
A: TLS_AES_128_GCM_SHA256 (0x1301)



```
⌄ Handshake Protocol: Server Hello
     Handshake Type: Server Hello (2)
     Length: 118
     Version: TLS 1.2 (0x0303)
     Random: 66ec4b5a48d58773092c51ef9fabbf4c8144a
     Session ID Length: 32
     Session ID: 382110c02c446314f4625d4551946a4d1
     Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
```

(g) Locate the HTTP POST request packet with the form data and provide a clear screenshot while highlighting your student ID.

A:



```
› Hypertext Transfer Protocol
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
   › Form item: "account" = "guest"
   › Form item: "passwd" = "111060013"
   › Form item: "passwd2" = "199608"
   › Form item: "Submit" = "�n�J"
   › Form item: "fnstr" = "20231014-051468900808"
```