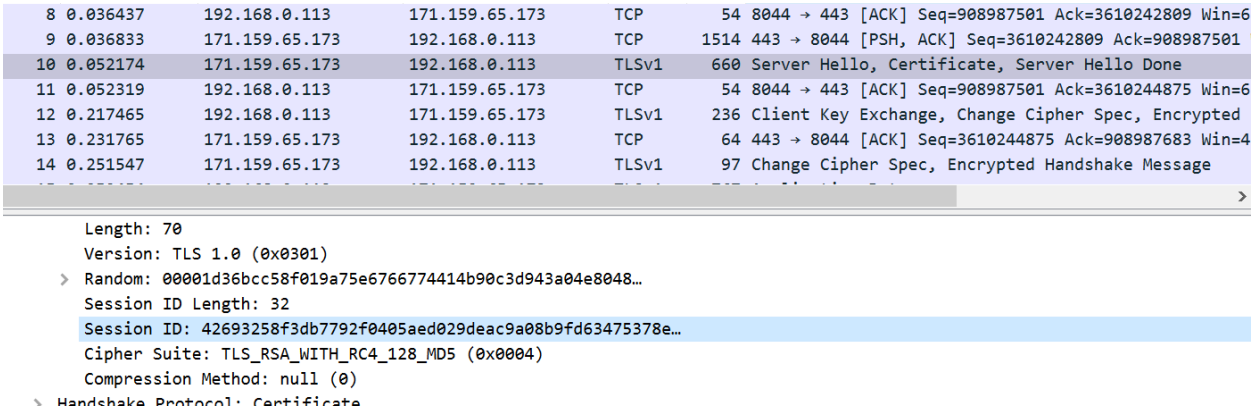
SSL/TLS Assignment

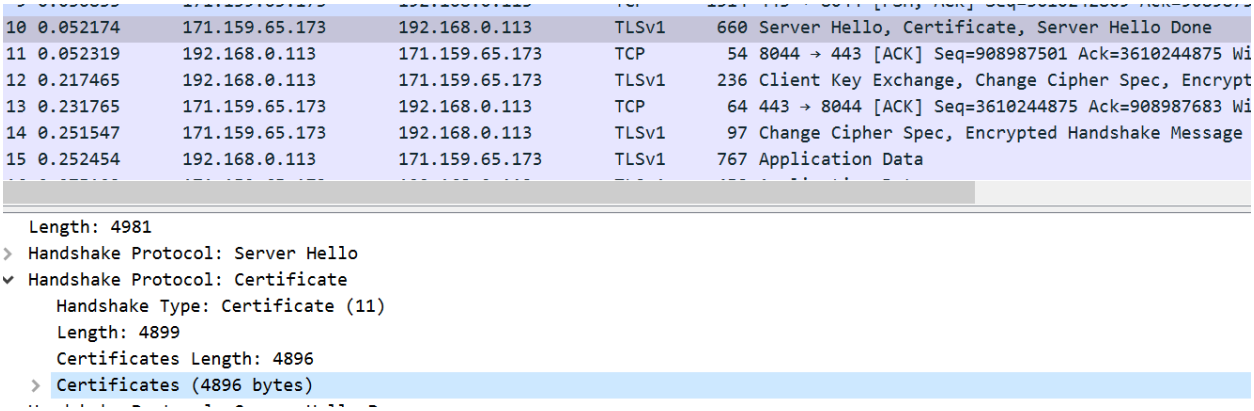
- This is an individual lab assignment.
- The due date is Wednesday, November 18.
- For this assignment, you will need to use Wireshark and the attached “https-justlaunchpage”.
- Please make the solutions readable and highlight the answers.
- Follow the usual naming convention.

Note: Provide screenshots for each answer.

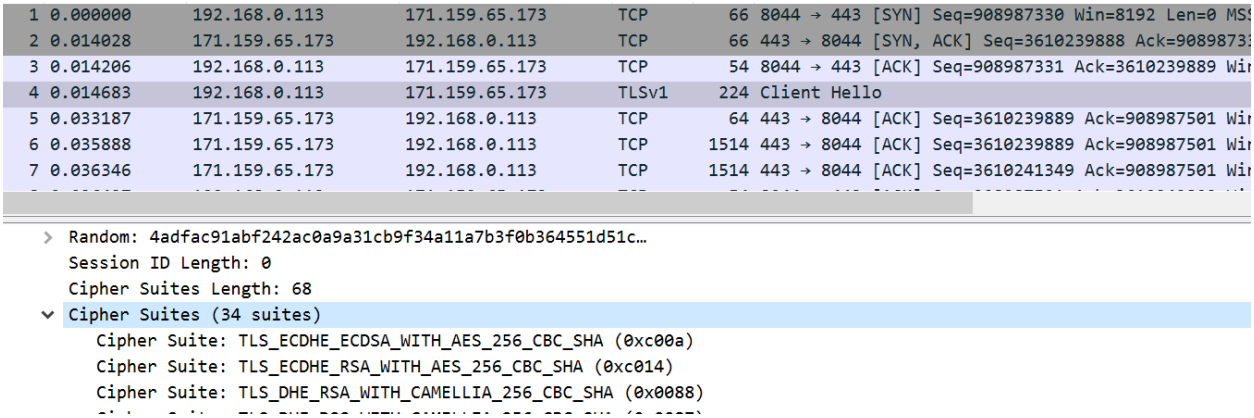
1. What is the session ID of the SSL/TLS handshaking?



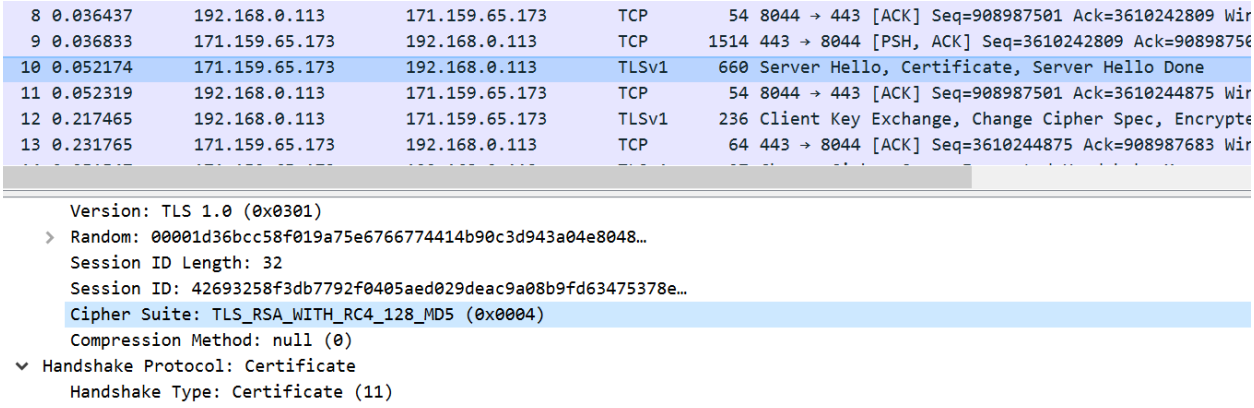
2. What is the length (bytes) of the certificate that the server shared with the client?



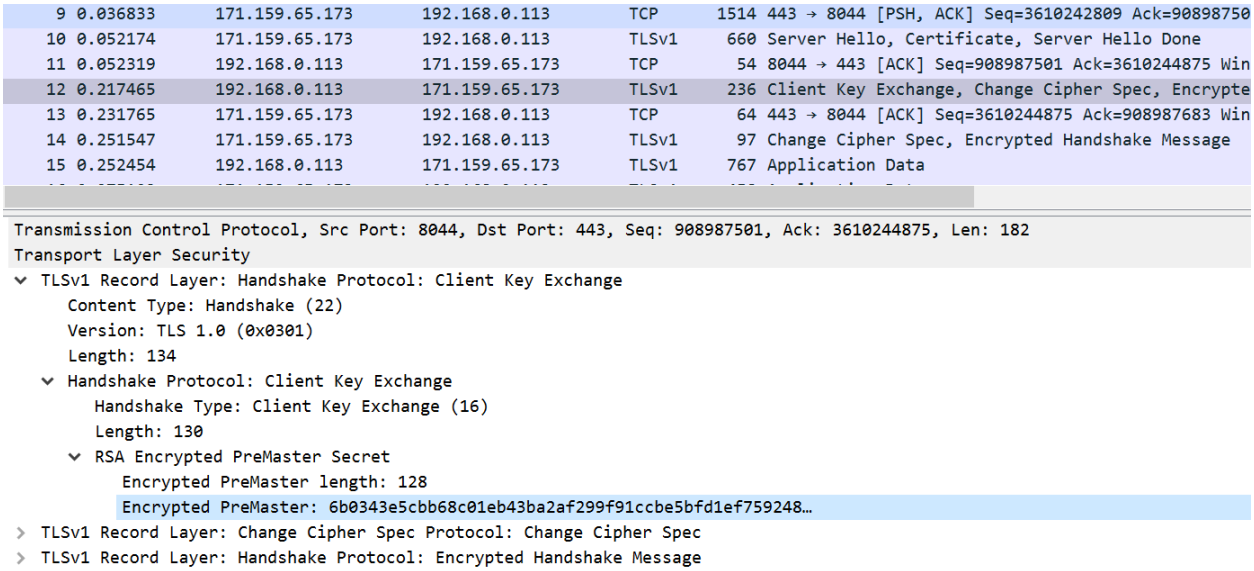
3A. How many cipher suites are supported by the client's browser?



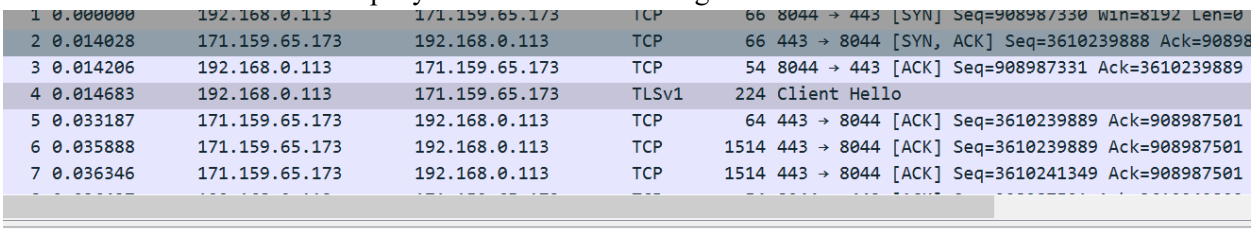
3B. What is the cipher suite that the server selected?



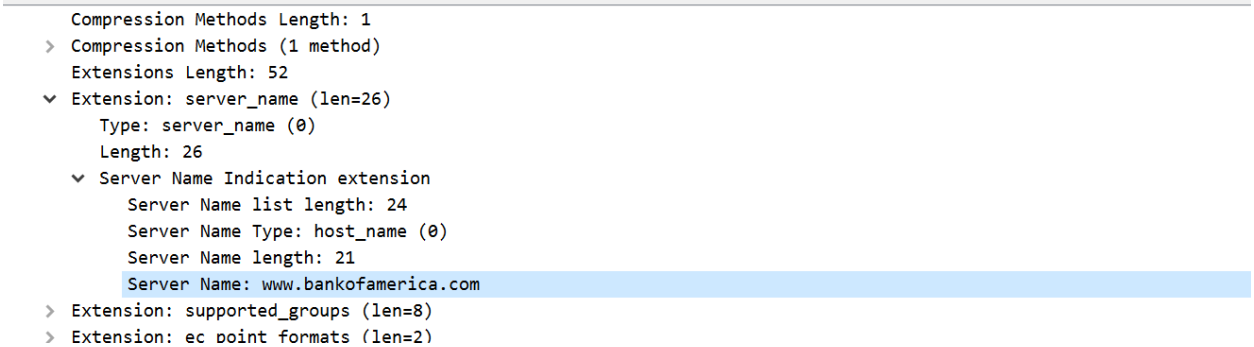
4. What is the length of the RSA Encrypted PreMaster Secret that is used to generate the Master Secret and session keys by the server and client?



5. What is the name of the company that the client is talking with?



1	0.000000	192.168.0.113	171.159.65.173	TCP	66 8044 → 443 [SYN] Seq=908987330 Win=8192 Len=0
2	0.014028	171.159.65.173	192.168.0.113	TCP	66 443 → 8044 [SYN, ACK] Seq=3610239888 Ack=90898
3	0.014206	192.168.0.113	171.159.65.173	TCP	54 8044 → 443 [ACK] Seq=908987331 Ack=3610239889
4	0.014683	192.168.0.113	171.159.65.173	TLSv1	224 Client Hello
5	0.033187	171.159.65.173	192.168.0.113	TCP	64 443 → 8044 [ACK] Seq=3610239889 Ack=908987501
6	0.035888	171.159.65.173	192.168.0.113	TCP	1514 443 → 8044 [ACK] Seq=3610239889 Ack=908987501
7	0.036346	171.159.65.173	192.168.0.113	TCP	1514 443 → 8044 [ACK] Seq=3610241349 Ack=908987501



```
Compression Methods Length: 1
> Compression Methods (1 method)
Extensions Length: 52
v Extension: server_name (len=26)
    Type: server_name (0)
    Length: 26
  v Server Name Indication extension
      Server Name list length: 24
      Server Name Type: host_name (0)
      Server Name length: 21
      Server Name: www.bankofamerica.com
> Extension: supported_groups (len=8)
> Extension: ec point formats (len=2)
```