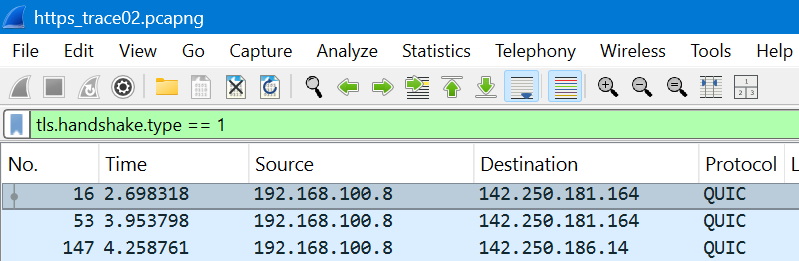
**Task 5**

For the HTTPS based website access, answer the following:

1. **What is the name of website?**

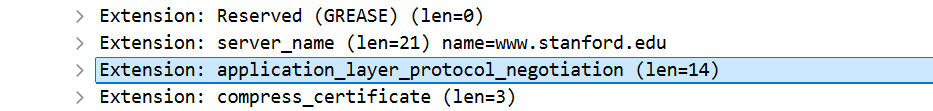


Select the first ClientHello packet.

Expand: Transport Layer Security → Handshake Protocol: Client Hello → Extensions → server name (SNI)

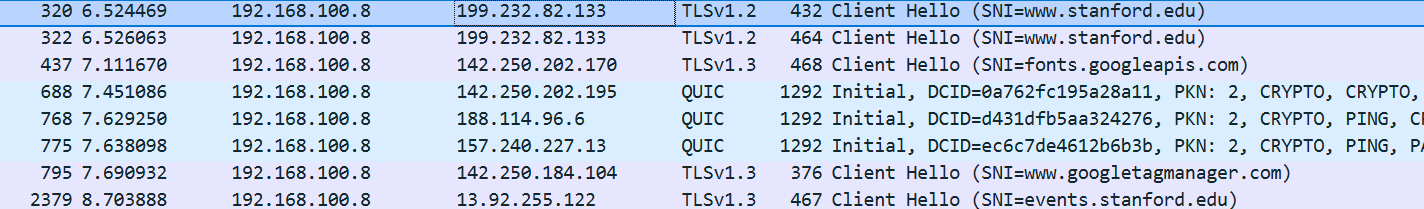
The Server Name Indication (SNI) field shows the website name

**name=www.stanford.edu**

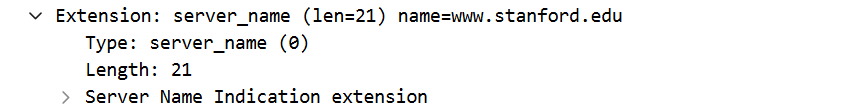


**Find the packet that contains the ClientHello message for the website you are accessing.**

**Frame No:320  
Time:6.524469**



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



A group of black text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

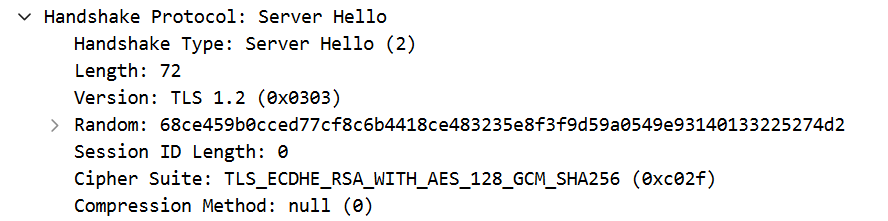
AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

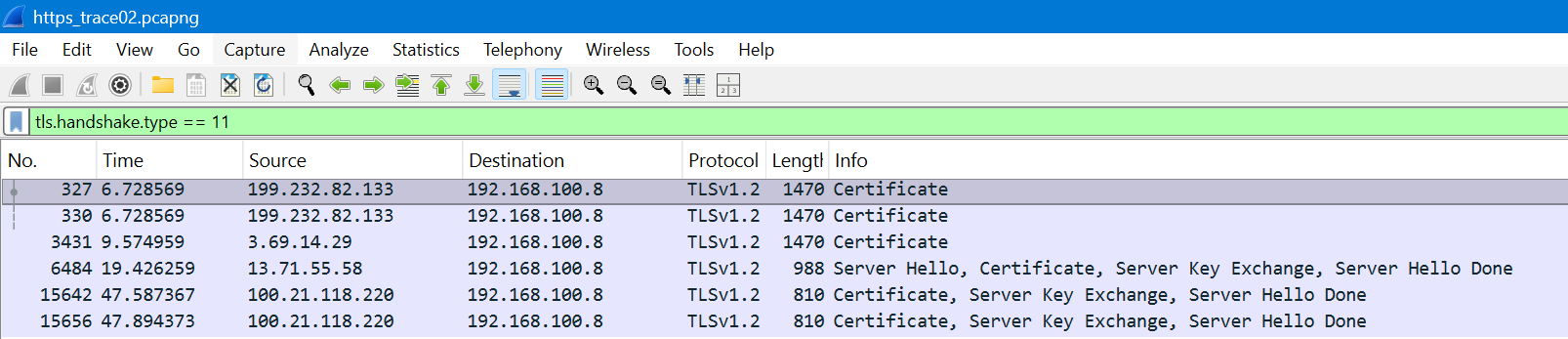
**Identify the ServerHello message. What cipher suite is chosen by the server?**

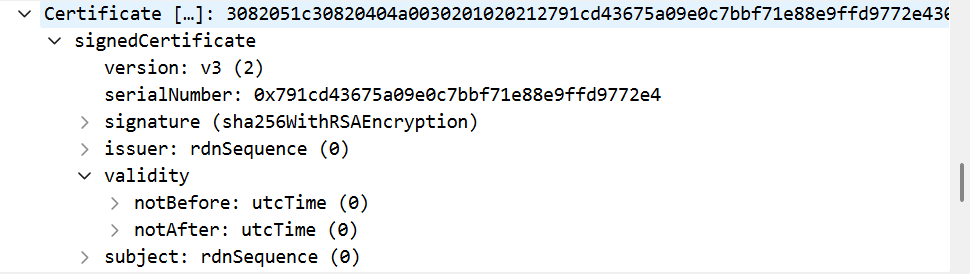
**Cipher Suite:**



**Frame No: 326**

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



A close-up of a computer screen

AI-generated content may be incorrect.

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

**Frame No:1**

A screenshot of a computer

AI-generated content may be incorrect.

**Why you can’t see HTTP headers:**

* Because HTTPS encrypts all HTTP data inside TLS.
* Only TLS records are visible — the actual HTTP headers/body are encrypted and hidden.
* To see them, you would need TLS session keys or the server’s private key to decrypt.

***THE END***