**Task 5**

For the HTTPS based website access, answer the following:

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

**A screenshot of a computer

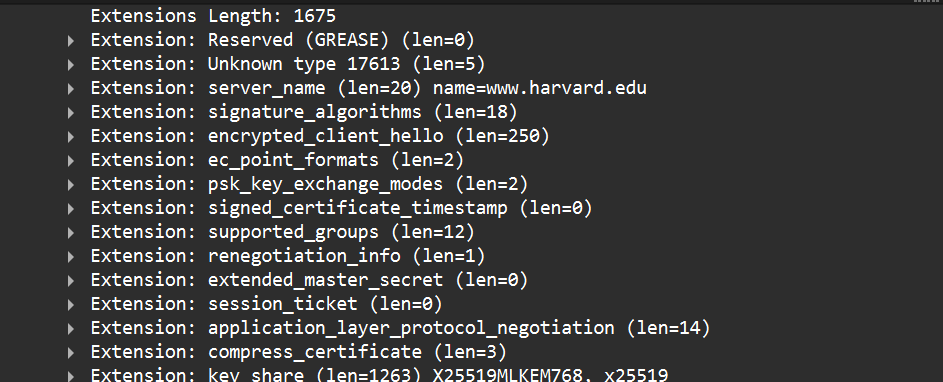
AI-generated content may be incorrect.**

Select the first ClientHello packet.

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

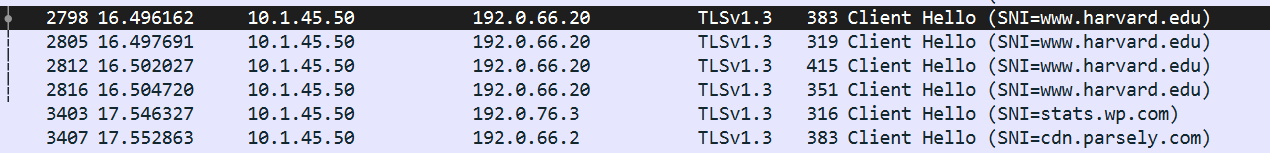
The Server Name Indication (SNI) field shows the website name

**Name=www.harvarduniversity.edu**

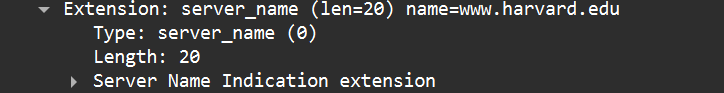
****

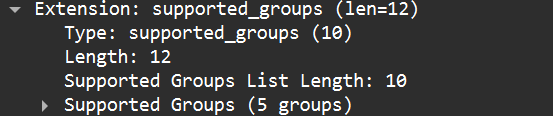
**Frame no :2798**

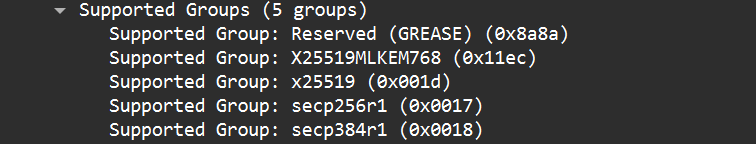
**Time :16.496162**

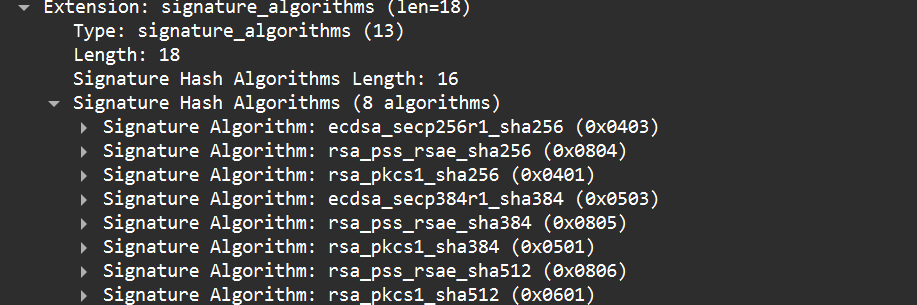
****

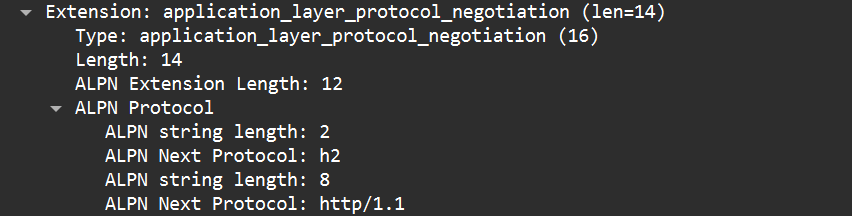
**List all the TLS extensions included in the ClientHello.**

****

****

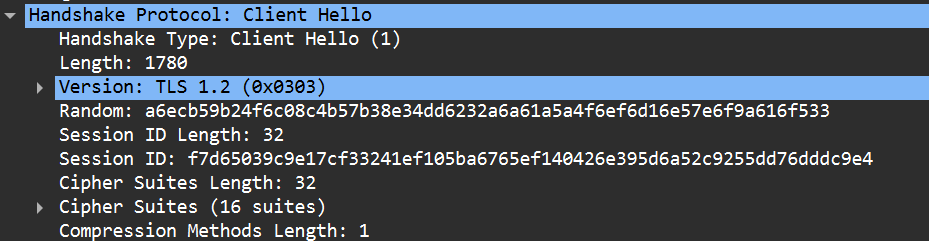
****

****

****

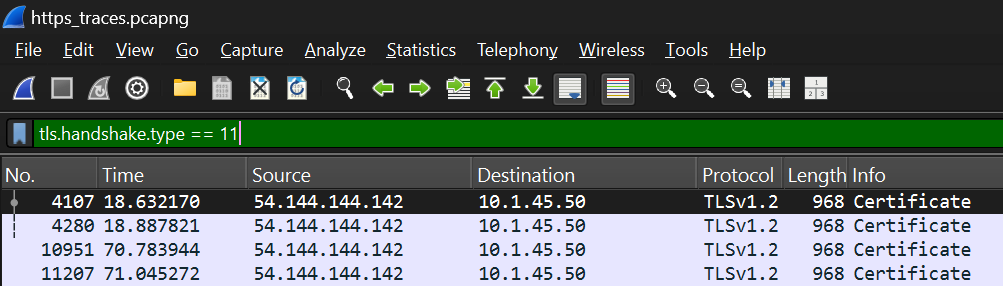
**Identify the ServerHello message. What cipher suite is chosen by the server?**

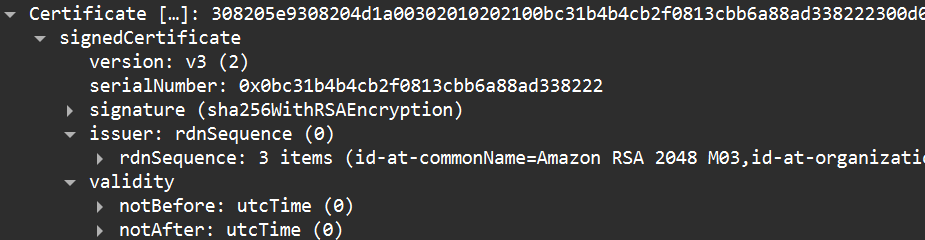
**Cipher Suite:**

****

**FRAME NO:2798**

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

****

****

**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:281**

**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.**