

**Assignment : 01**

**Submitted by:Umer Khan**

**Registration no:B23F0645AI109**

**Instructor : Sir Adnan**

**Department: BSAI Red**

**Date: 24th Sep ,2025**

**Group members: Rehab Gul, Umer Khan and Abdullah Aslam**

***Part 02 and 05:***

**Task 05:**

For the HTTPS based website access, answer the following:

**Question :01:**

What is the name of website?

**Answer:**

The name of the website is

eu-teams.events.data.microsoft.com

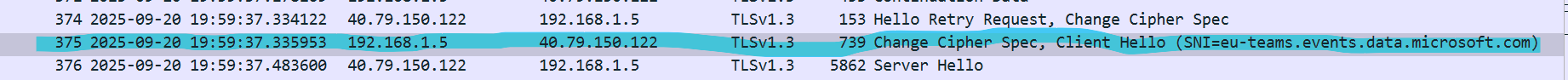
**Question :02:**

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

**Answer:**

The **Packet no. 375** contain the Client Hellow message. Microsoft Teams

Client Hello (SNI=eu-teams.events.data.microsoft.com)



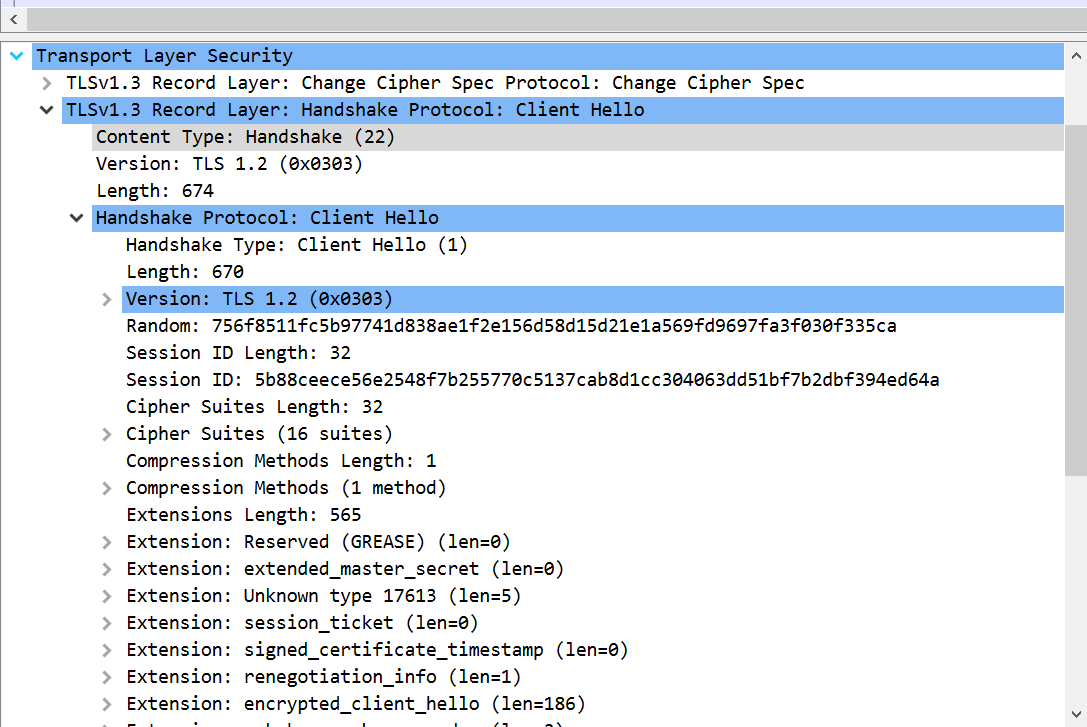
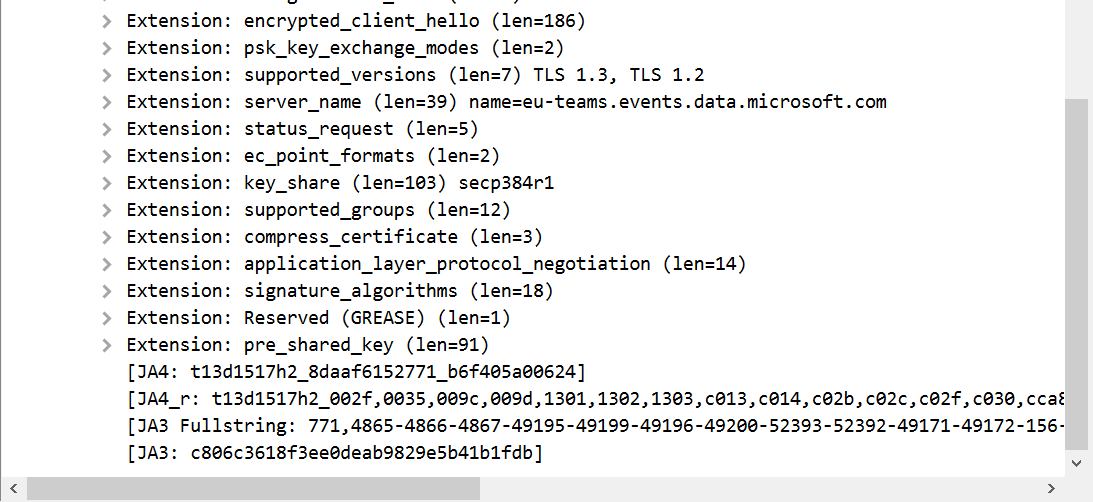
**Question :03:**

List all the TLS extensions included in the ClientHello.

**Answer:**

The TLS extensions included in the ClientHello message are:

* Reserved (GREASE)
* extended\_master\_secret
* Unknown type 17613
* session\_ticket
* signed\_certificate\_timestamp
* renegotiation\_info
* encrypted\_client\_hello
* psk\_key\_exchange\_modes
* supported\_versions
* server\_name
* status\_request
* ec\_point\_formats
* key\_share
* supported\_groups
* compress\_certificate
* application\_layer\_protocol\_negotiation
* signature\_algorithms
* Reserved (GREASE)
* pre\_shared\_key

**Question :04:**

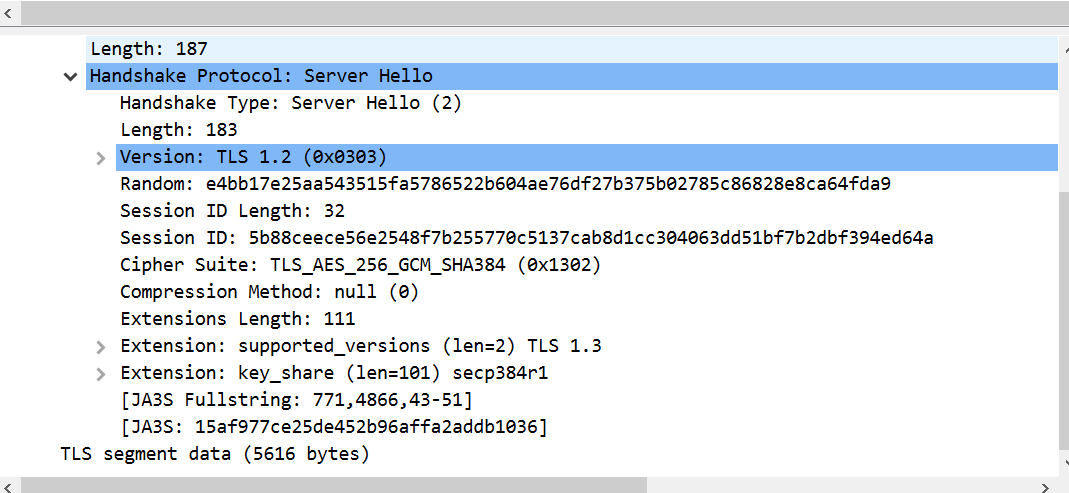
Identify the status code in the first server response.

**Answer:**

The **ServerHello** message is in packet **376**.

The cipher suite chosen by the server is **TLS\_AES\_256\_GCM\_SHA384**.





**Question :05:**

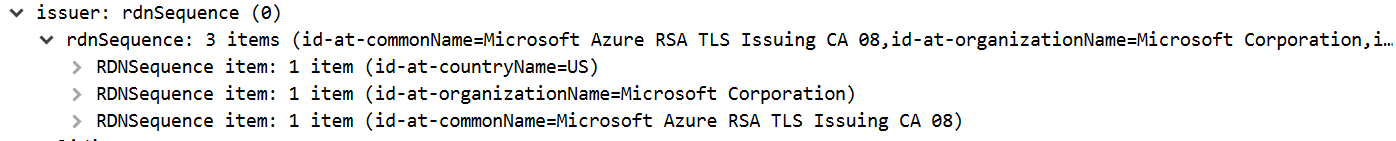
Locate the Certificate message. Extract the server’s certificate information (issuer, subject, validity dates).

**Answer:**

The **Certificate message** is located in packet **961**.

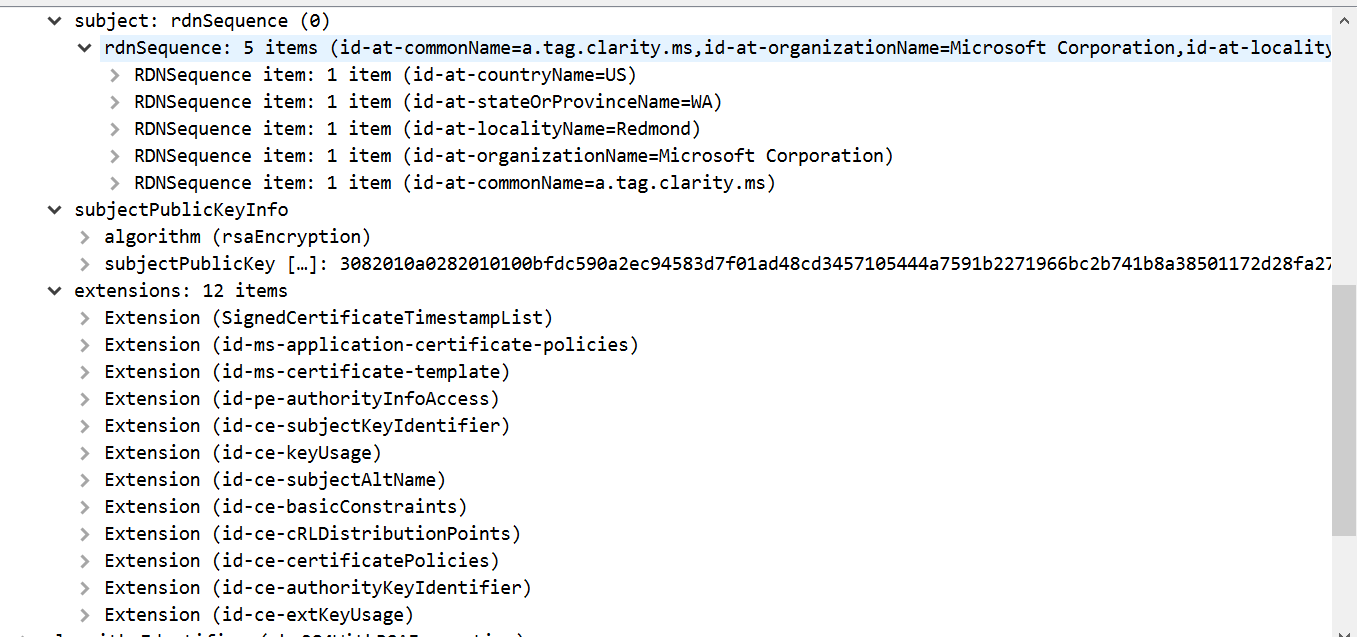
The server’s certificate information is as follows:

* **Issuer:** C=US, O=Microsoft Corporation, CN=Microsoft Azure RSA TLS Issuing CA 08



* **Subject:**

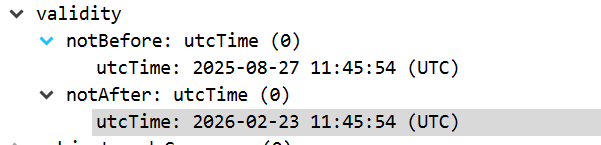
C=US, ST=MA, L=Redmond, O=Microsoft Corporation, CN=a.tag.clarity.ms



* **Validity:**

**Not Before:** utcTime: 2025-08-27 11:45:54 (UTC)

**Not After:** utcTime: 2026-02-23 11:45:54 (UTC)

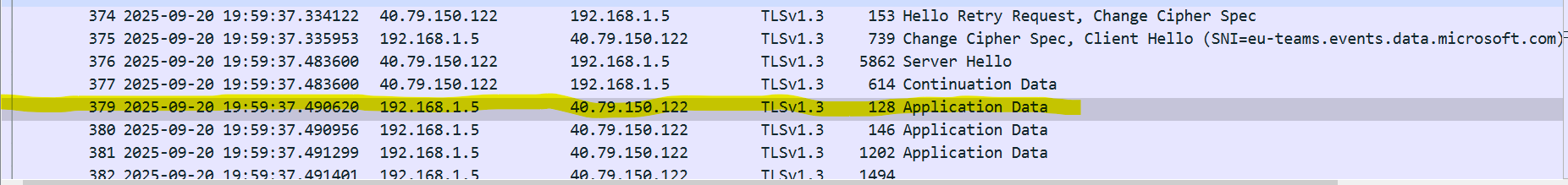


**Question :06:**

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

**Answer:**

The first **encrypted application data packet** after the TLS handshake with 40.79.150.122 is **packet 379**.



You cannot directly see the HTTP headers in this packet because the **application data (including all HTTP headers) is encrypted** by the TLS protocol. This encryption provides confidentiality and security, preventing anyone who intercepts the network traffic from being able to read the sensitive information contained within the HTTP requests and responses.

**Why we use Tls Filter ?**

I used a TLS filter instead of an HTTPS filter because **HTTPS is an application-layer service that is secured using the Transport Layer Security (TLS) protocol**. Wireshark captures the network-level protocols, so it displays the encrypted conversation as TLS packets. The questions specifically asked about the TLS handshake components (ClientHello, ServerHello, Certificate), which are sub-protocols within TLS. Filtering for tls directly isolates these handshake messages, whereas an http filter would show no results because the HTTP data is encrypted inside the TLS "Application Data" packets after the handshake is complete.