**­­**

**­­­­­­­**

**ASSIGNMENT # 01**

|  |  |
| --- | --- |
| **SUBMITTED BY** | **­­­M. Ubaidullah**  **Umaima Ghazal**  **Syed Zain Raza Kazmi** |
| **SUBMITTED TO** | **Dr Adnan Iqbal** |
| **REGISTRATION NO.** | **B23F0001AI057**  **B23F0001AI071**  **B23F0045AI085** |

**­**

# **TASK # 05:**

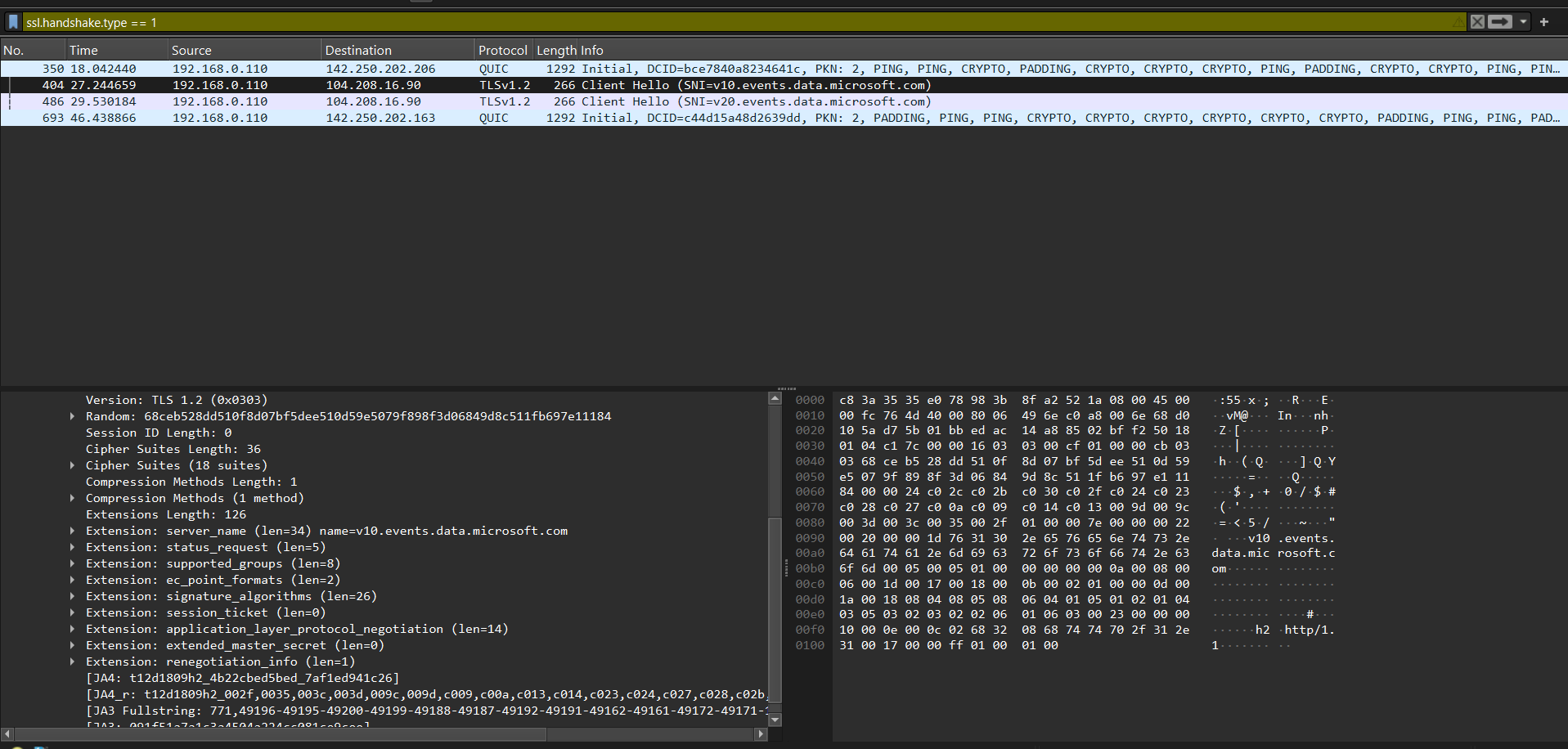
**For HTTPS based Website**

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

The website which we find that is working on https is [**https://www.wikipedia.org**](https://www.wikipedia.org)

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

We have find the clienthello message through this filter **ssl.handshake.type == 1.**

****

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

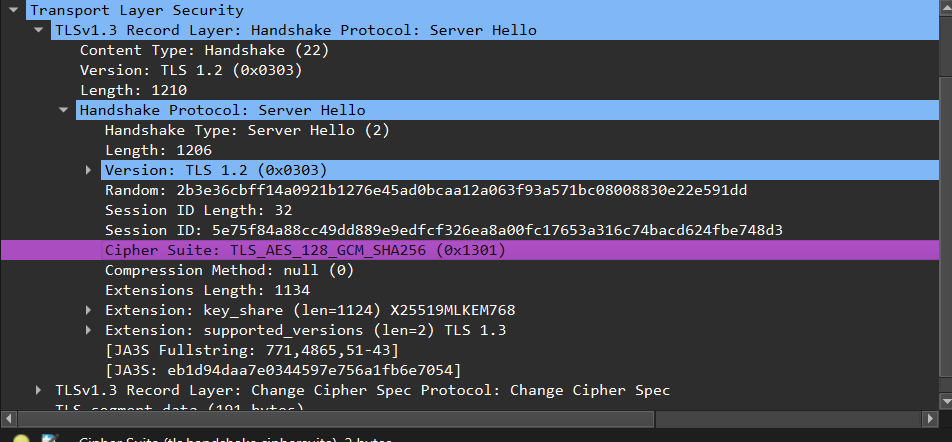
* server\_name
* status\_request
* supported\_groups
* ec\_point\_formats
* signature\_algorithms
* session\_ticket
* application\_layer\_protocol\_negotiation
* extended\_master\_secret
* renegotiation\_info

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

We can identify the ServerHello message by this filter **ssl.handshake.type == 2**

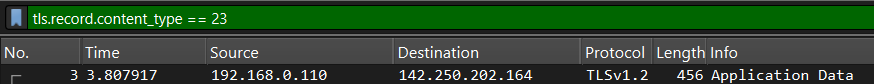
And the Cipher chosen by the Server is

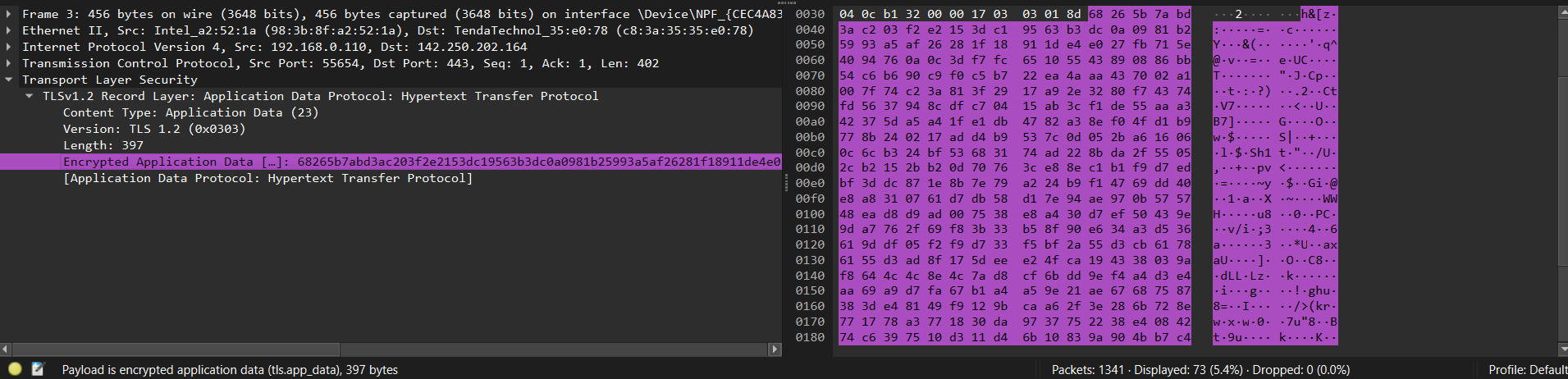
**Cipher Suite:** TLS\_AES\_128\_GCM\_SHA256 (0x1301)



1. **Locate the Certificate message. Extract the server’s certificate information (issuer, subject, validity dates).**
2. **After the TLS handshake, identify the first encrypted application data packet. Why can’t you directly see the HTTP headers in this packet?**

This is the first encrypted application data packet we filter it by **tls.record.content\_type == 23**  and the first packet which appeared is encrypted is this one

****

****

You can’t directly see the HTTP headers in the packet because TLS encrypts all application-layer data, including headers and content, before sending it over the network. As a result, Wireshark only sees “Encrypted Application Data,” and the actual HTTP headers remain hidden unless you provide the session’s encryption keys to decrypt the traffic.

* Internet Society. (n.d.). *TLS basics*. Internet Society. Retrieved September 20, 2025, from [https://www.internetsociety.org/deploy360/tls/basics/](https://www.internetsociety.org/deploy360/tls/basics/?utm_source=chatgpt.com)