Name: Asmita Suresh Shinde

PRN: 21510012

CNS LA2

List of experiments

7. Implementation of RSA Algorithm

8. Implement the Diffie-Hellman Key Exchange algorithm for a given problem

9. Calculate the message digest of a text using the SHA-1 algorithm

10. Implement the SIGNATURE SCHEME – Digital Signature Standard

11. Demonstration of SSL using Wireshark

**7. Implementation of RSA Algorithm**

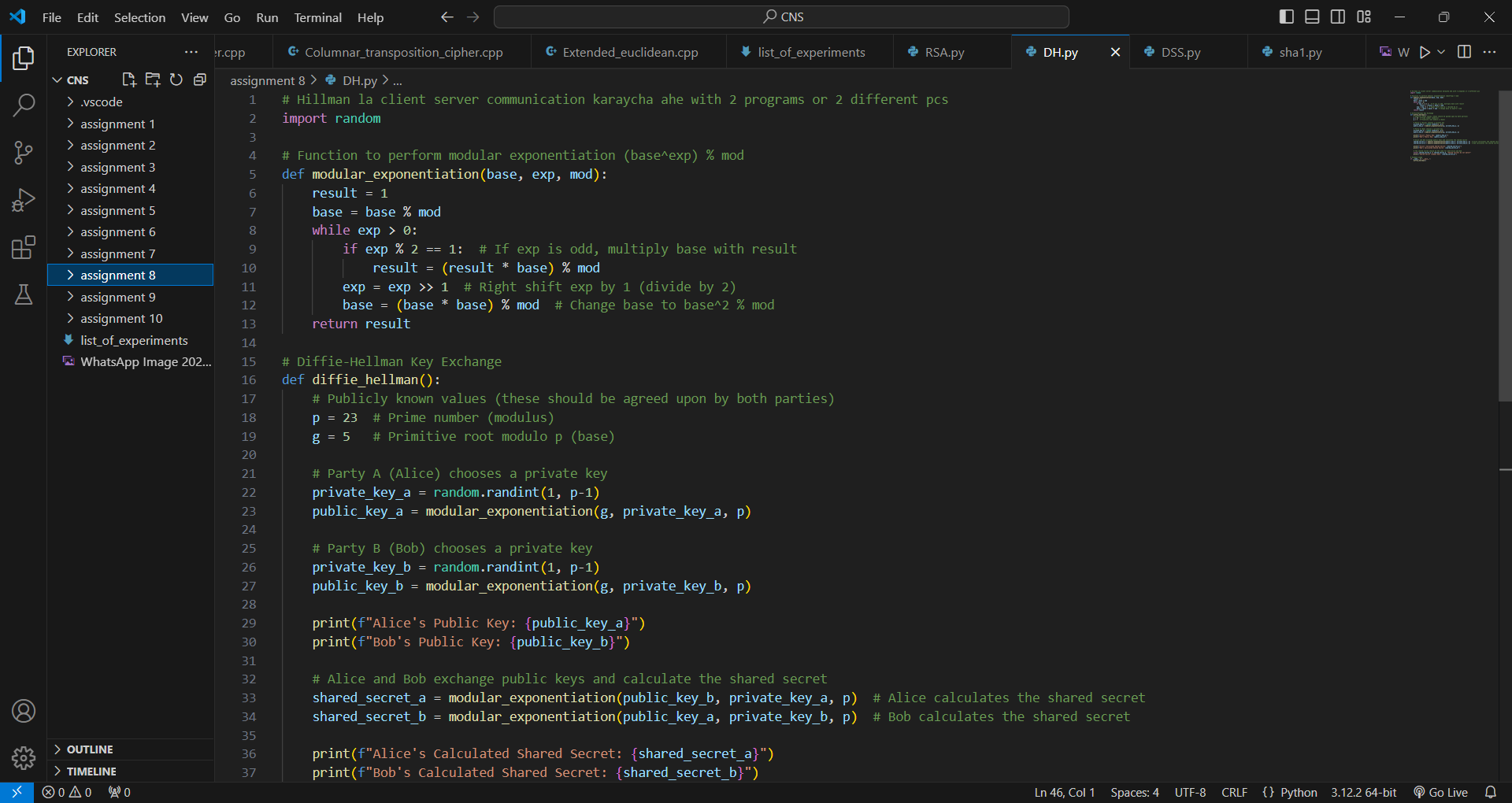
A screen shot of a computer program

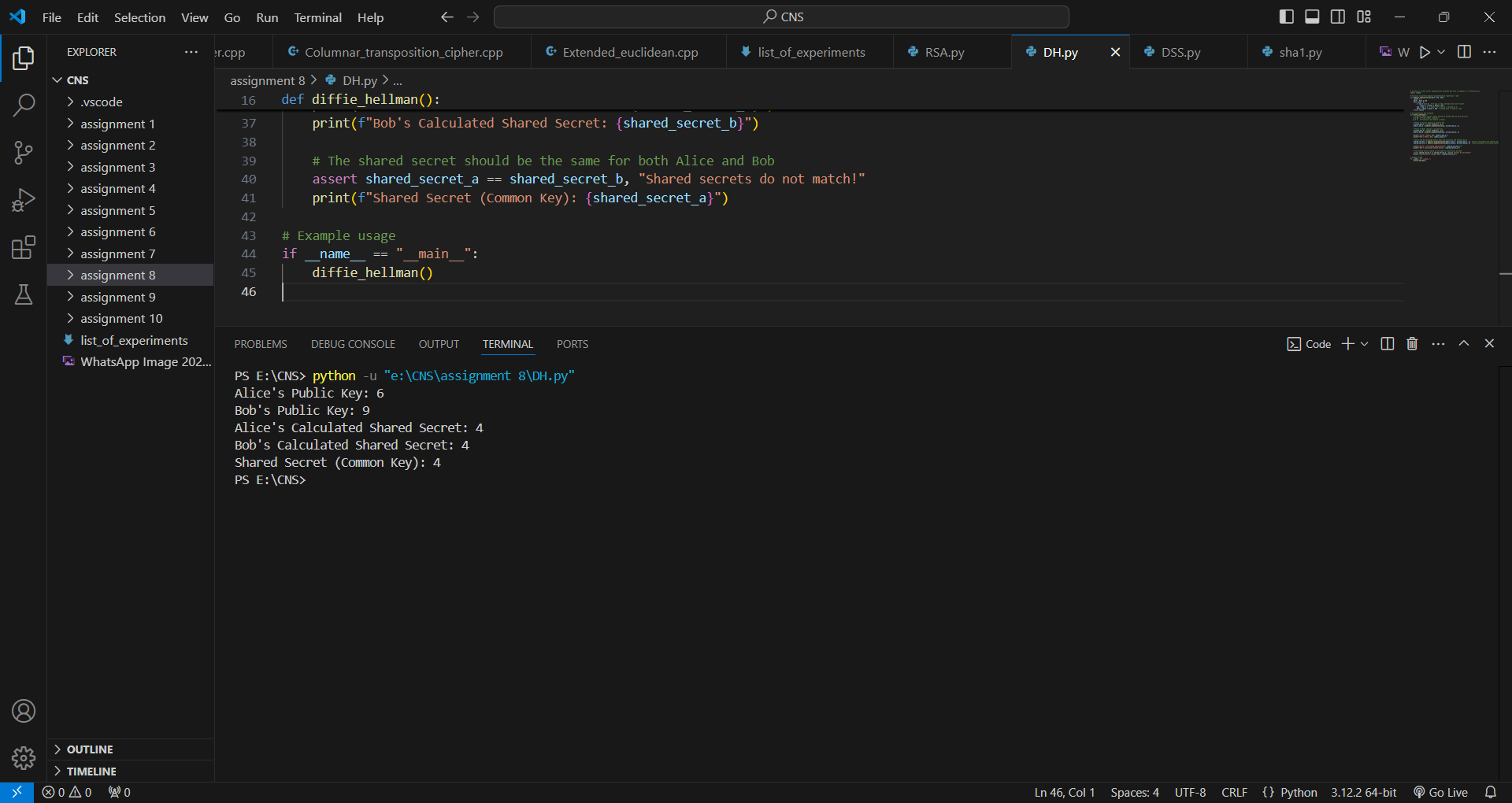
Description automatically generated

A screenshot of a computer program

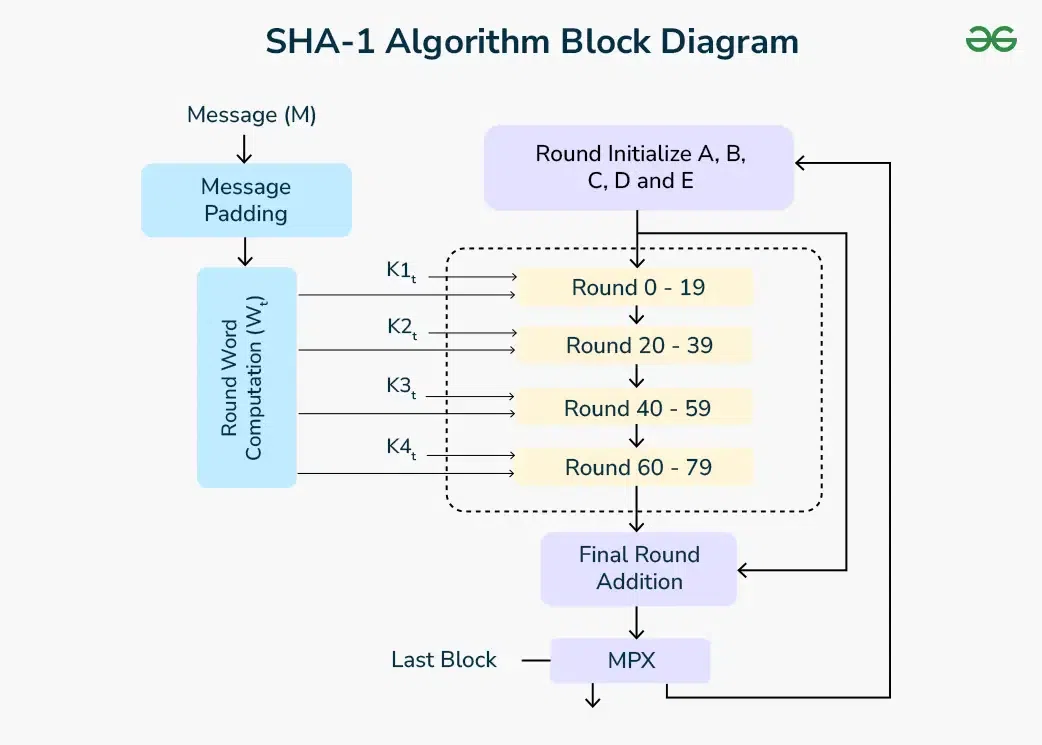
Description automatically generated

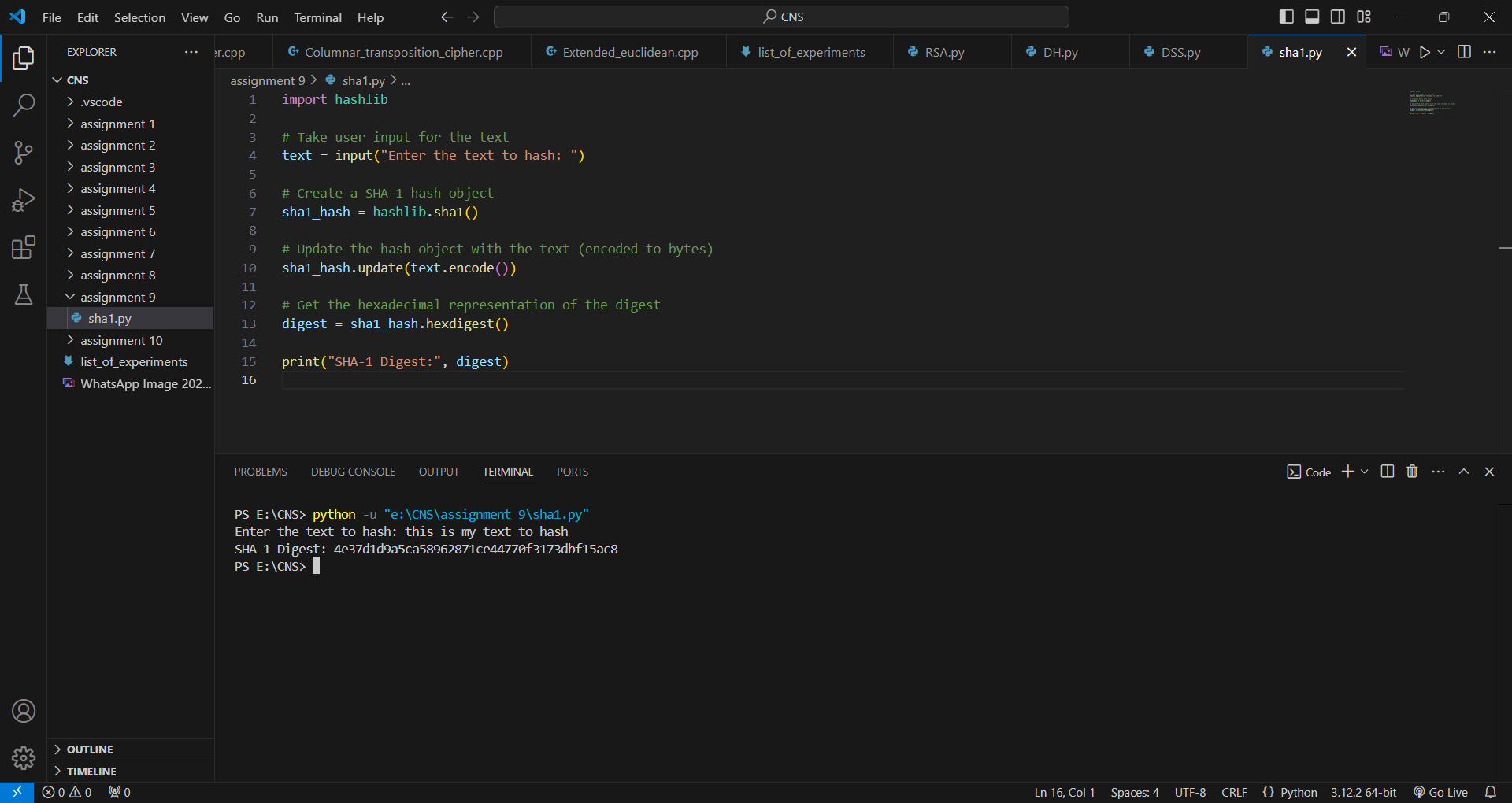
**8. Implement the Diffie-Hellman Key Exchange algorithm for a given problem**





**9. Calculate the message digest of a text using the SHA-1 algorithm**

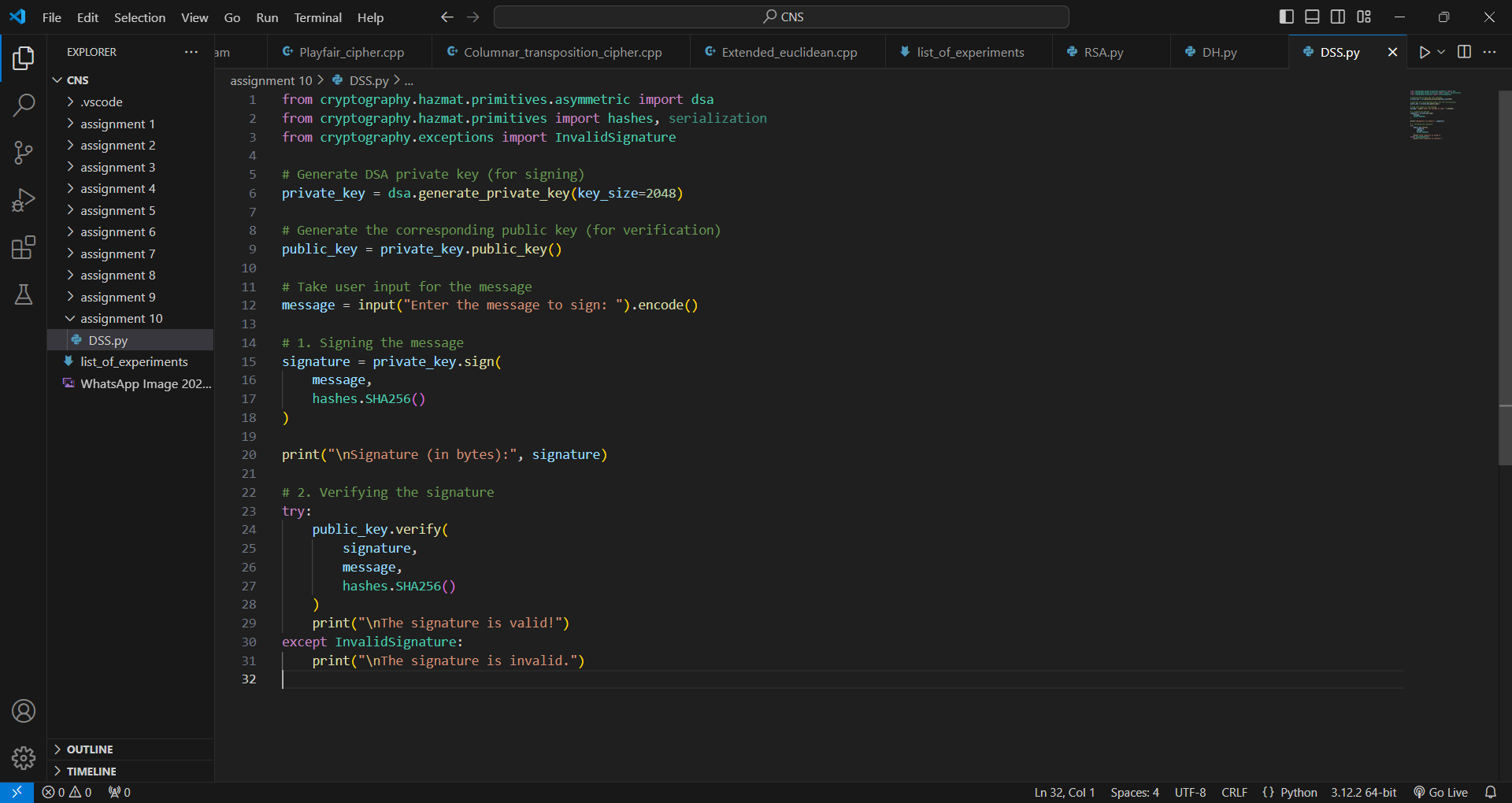
****

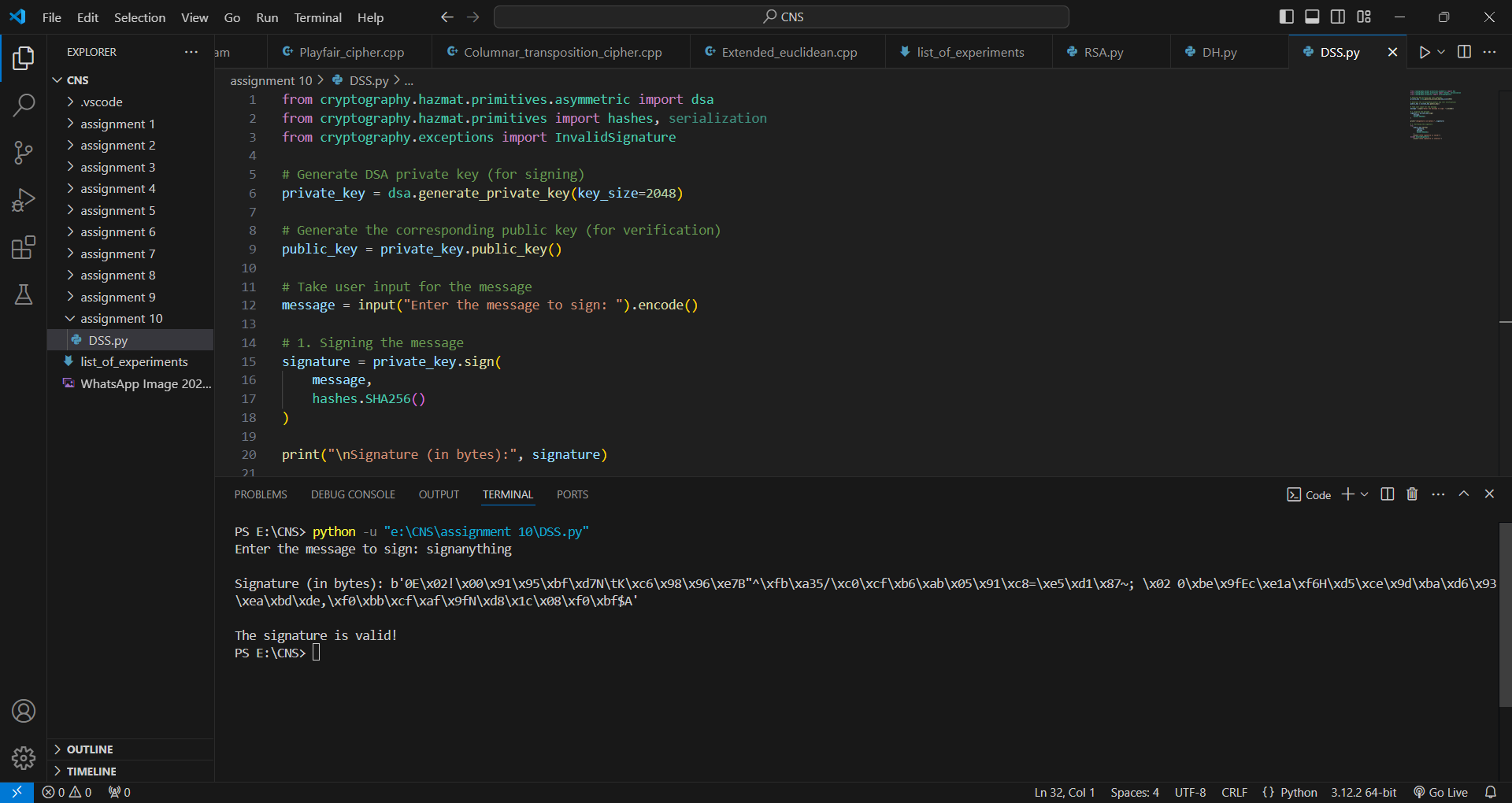
****

**10. Implement the SIGNATURE SCHEME – Digital Signature Standard**

A diagram of a communication system

Description automatically generated

****

****

**11. Demonstration of SSL using Wireshark**

Step 1: Open a Trace

A screenshot of a computer

Description automatically generated

Step 2: Inspect the Trace

A screenshot of a computer

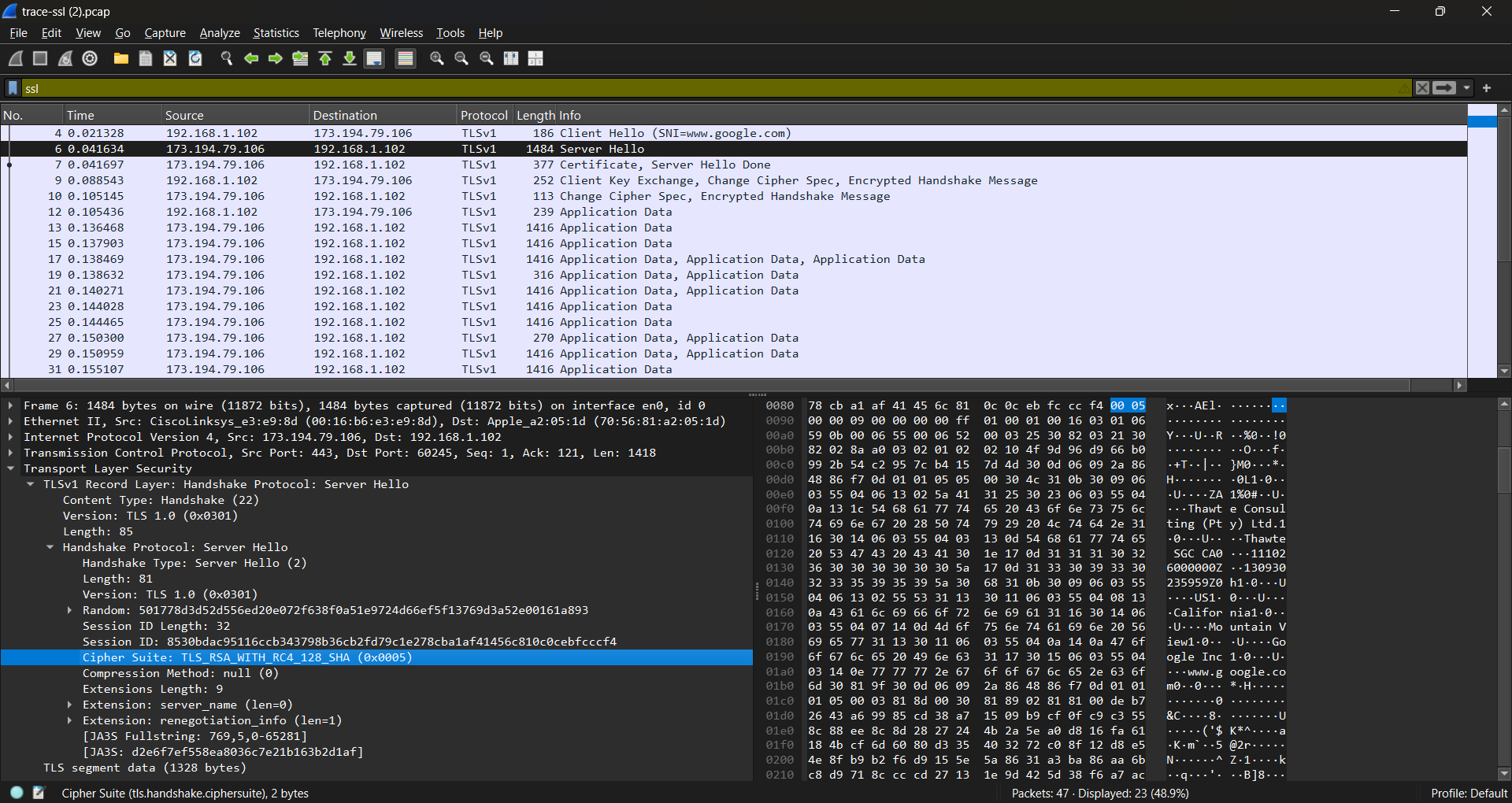
Description automatically generated

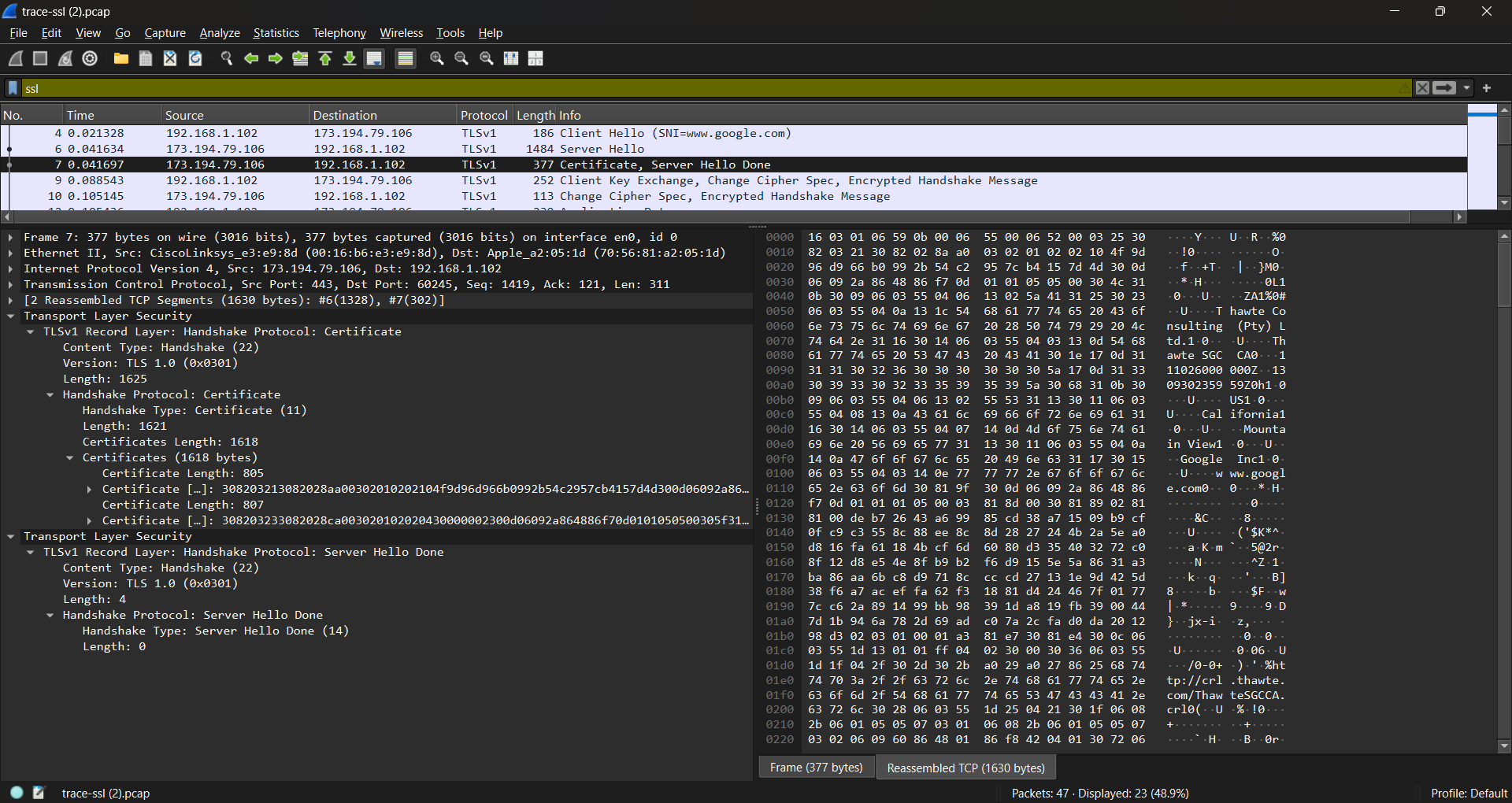
Step 3: The SSL Handshake

**A screenshot of a computer

Description automatically generated**

Hello Messages

****

****

Certificate Messages

**A screenshot of a computer

Description automatically generated**

Alert Message

