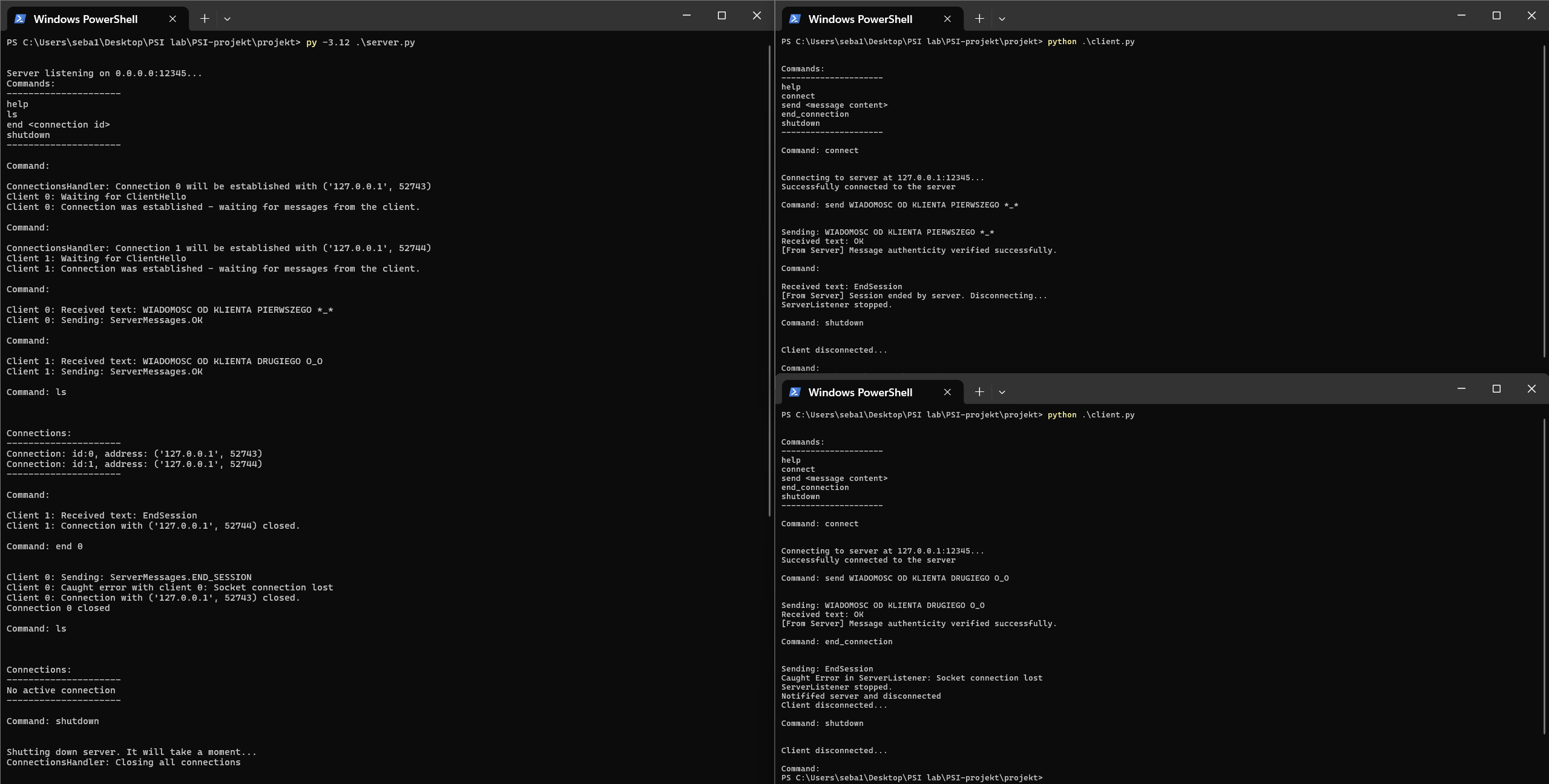
**PSI 24Z - Mini TLS**

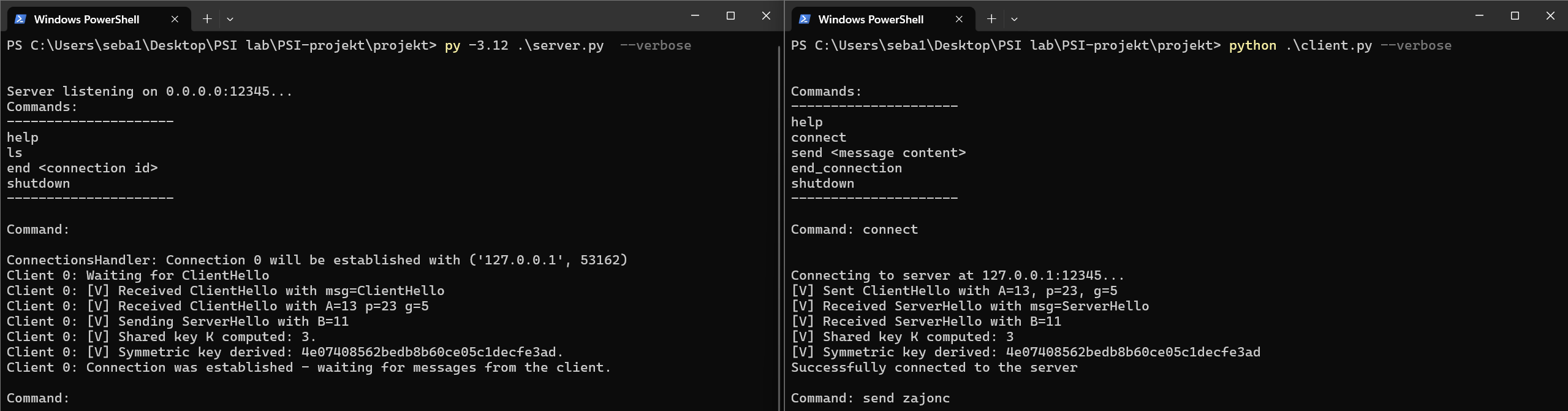
**Kompleksowe przedstawienie funkcjonalności klienta i serwera**

****

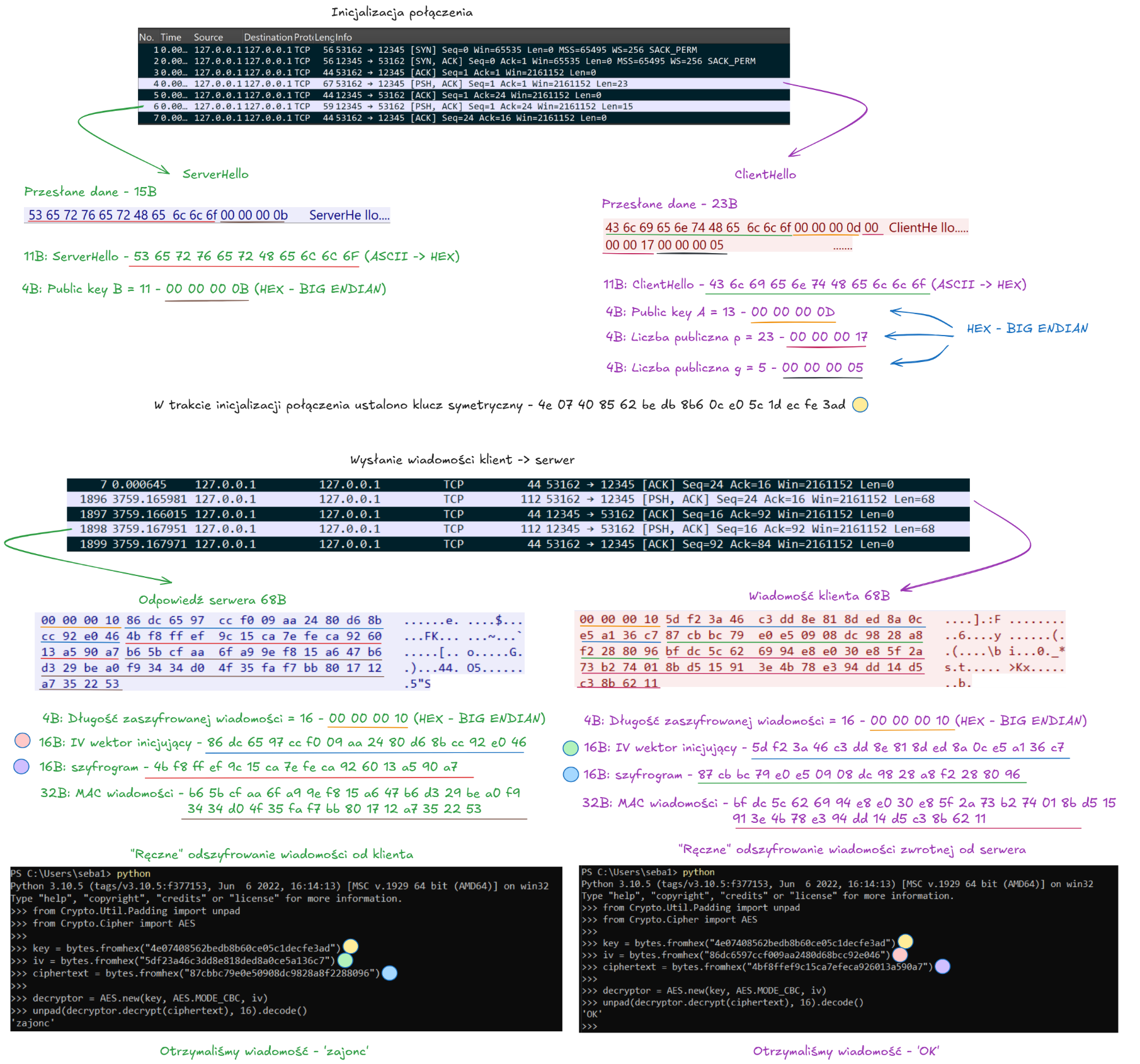
Serwer oferuje możliwość wyświetlenia pomocy, zakończenia połączenia z danym klientem, wyłączenia

Klient pozwala na wyświetlenie pomocy, połączenie się z serwerem, wysłanie wiadomości, zakończenie połączenia, i wyłączenie

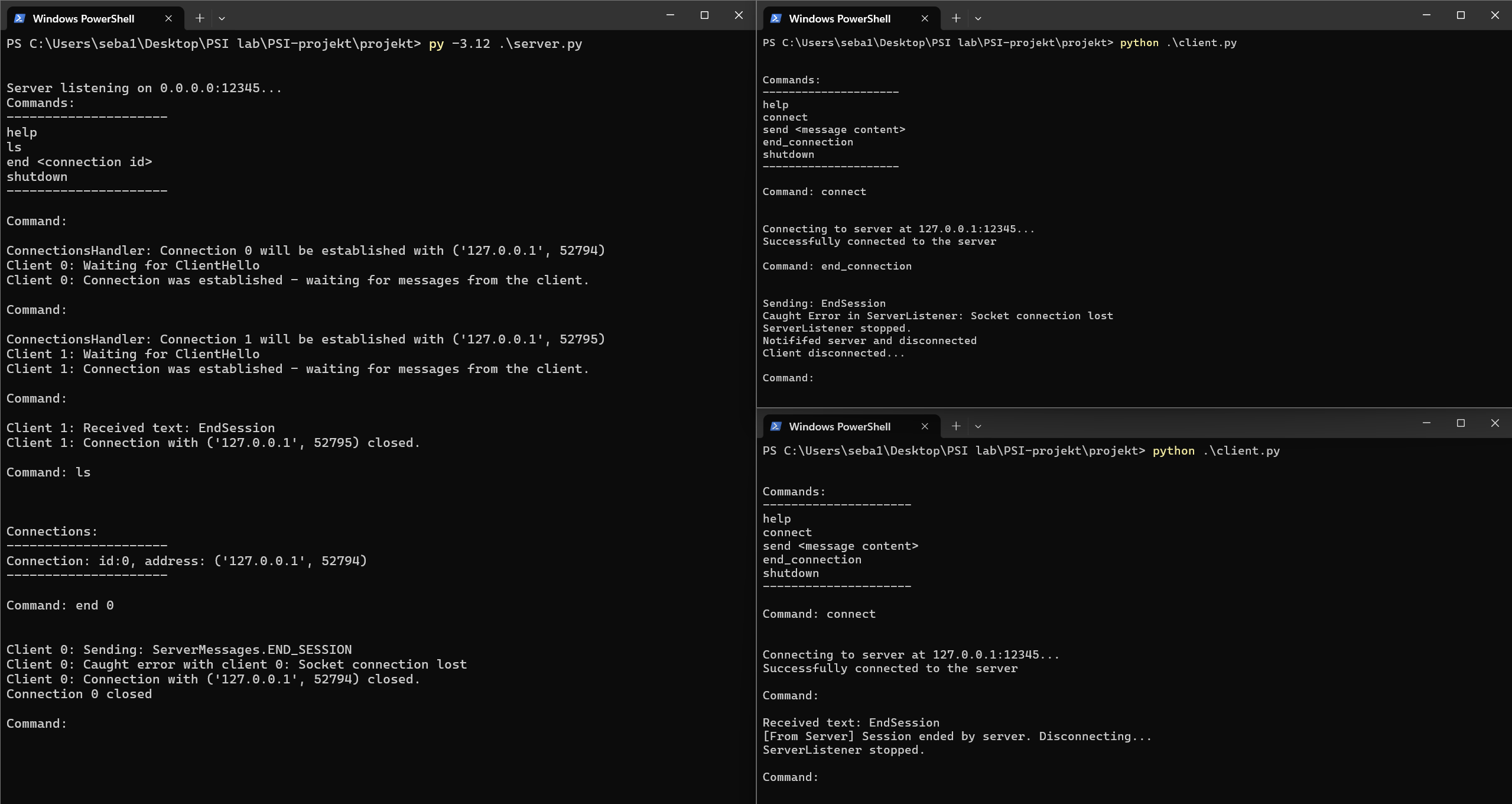
**Zainicjowanie połączenia klienta z serwerem (wiadomości ClientHello i ServerHello)**

****

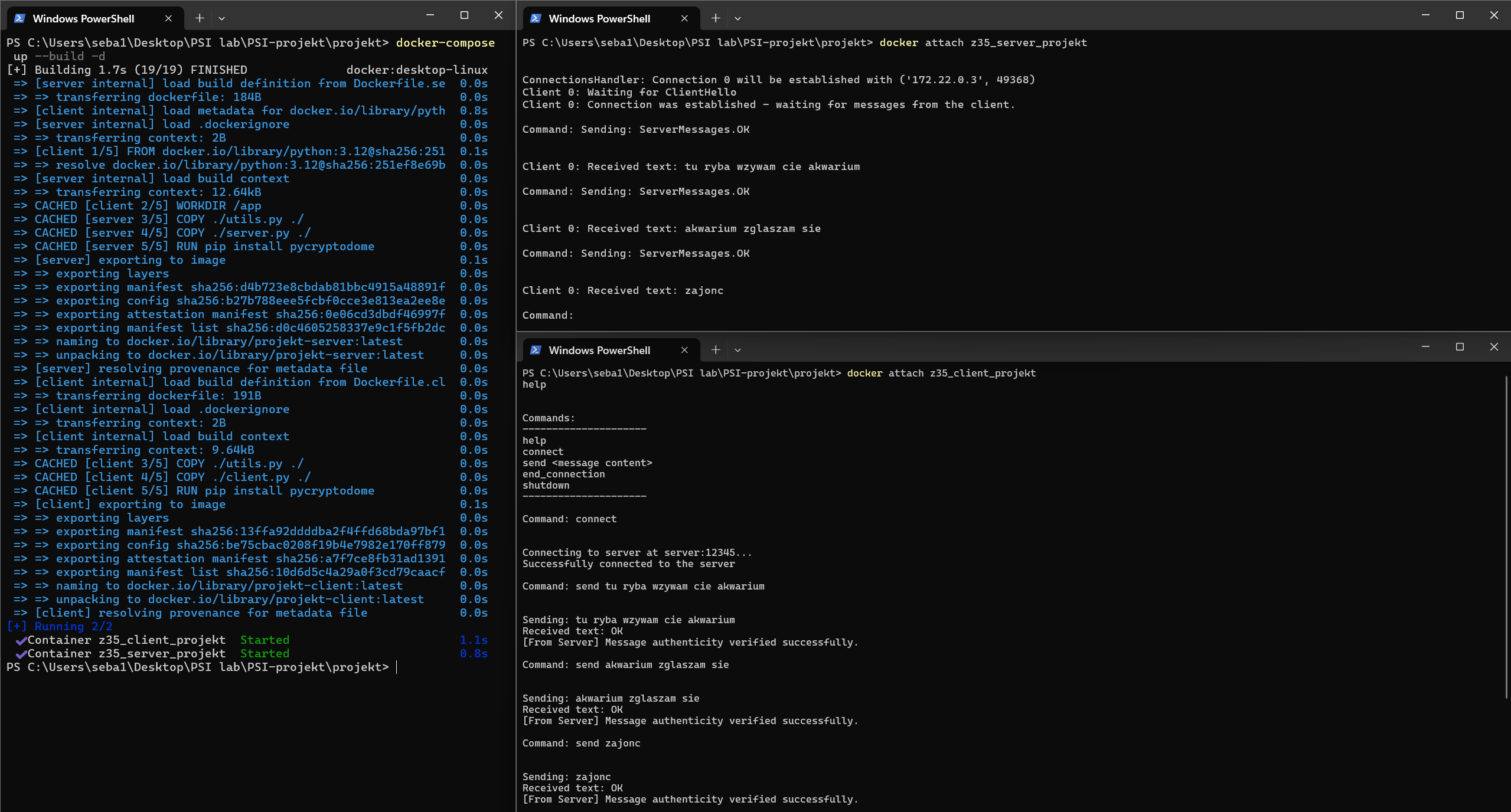
Na załączonych zrzutach ekranu uruchomiono programy z funkcją verbose, żeby pokazać jakie wartości zostały wykorzystane do utworzenia bezpiecznego klucza

**Zaobserwowanie wiadomości ClientHello i ServerHello w Wiresharku oraz ‘’ręczne” odczytanie przechwyconych wiadomości**

**Zamykanie połączenia przez klienta i serwer**

****

**Działanie w kontenerze**

****

**Opis użytych algorytmów**

**Wymiana kluczy – Algorytm Diffiego-Hellmana**

* **Klient i serwer ustalają wspólny klucz szyfrujący (K) na podstawie publicznych wartości g i p oraz kluczy publicznych A i B:**
  + **Klient: K = B^a mod p.**
  + **Serwer: K = A^b mod p.**

**Szyfrowanie wiadomości – AES w trybie CBC**

* **Szyfrowanie:**
  + **Wejście: wiadmość plaintext, klucz K, wektor inicjalizacyjny (IV).**
  + **Wyjście: ciphertext (zaszyfrowana treść).**
* **Odszyfrowanie:**
  + **Wejście: ciphertext, K, IV.**
  + **Wyjście: plaintext.**

**Mechanizm Encrypt-then-MAC**

* **Po zaszyfrowaniu wiadomości generowany jest kod HMAC przy użyciu SHA-256.**
* **Wiadomość przesyłana do odbiorcy zawiera:**
  + **Rozmiar**
  + **Ciphertext.**
  + **MAC.**
  + **IV.**
* **Odbiorca weryfikuje integralność i autentyczność wiadomości na podstawie MAC.**

**Napotkane problemy**

Napotkaliśmy drobne trudności z synchronizacją wątków, szczególnie w kontekście poprawnego wypisywania komunikatów na konsolę w środowisku wielowątkowym.

**Wnioski**

1. **Poprawność działania**: Protokół Mini TLS działa zgodnie z założeniami. Każdy etap komunikacji został potwierdzony za pomocą Wireshark i manualnego odszyfrowania wiadomości.
2. **Bezpieczeństwo**: Zastosowanie mechanizmu Encrypt-then-MAC zapewnia integralność i autentyczność wiadomości. Algorytmy Diffiego-Hellmana i AES gwarantują poufność transmisji.