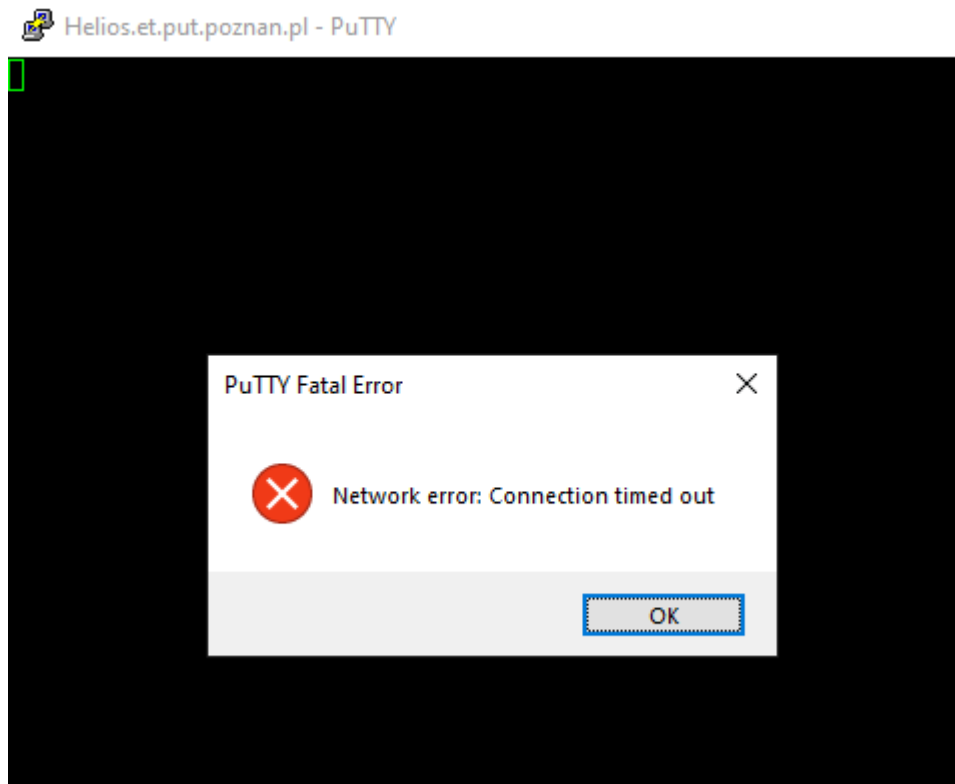


Analiza działania protokołów telnet oraz ssh za pomocą aplikacji Wireshark.

Wireshark to aplikacja służąca do analizy pakietów sieciowych, która pozwala na przechwytywanie i analizowanie ruchu sieciowego. Może ona analizować wiele protokołów sieciowych, takich jak TCP, UDP, HTTP, DNS, DHCP, FTP, SMTP i wiele innych. Może być wykorzystywany do różnych celów, w tym do diagnostyki problemów sieciowych, analizy wydajności sieciowej, wykrywania ataków sieciowych oraz do testowania bezpieczeństwa sieci.

Próba połączenia z helios.et.put.poznan.pl za pomocą programu PuTTY:



Jak widać na załączonym zrzucie ekranu połączenie nie powiodło się, w wyniku czego aplikacja Wireshark nie zarejestrowała żadnych pakietów typu telnet. Zatem nie jest możliwe wykonanie poleceń od a do c dla protokołów telnet i ssh.

d) *Który sposób łączenia z serwerem jest bardziej bezpieczny?*

SSH zapewnia bezpieczne połączenie sieciowe z szyfrowaniem, które chroni poufne dane podczas ich przesyłania między urządzeniami. W przeciwieństwie do Telnet, który przesyła dane w sposób niezaszyfrowany, co oznacza, że dane mogą zostać przechwycone i odczytane przez osoby trzecie. Ponadto, SSH wykorzystuje autentykację klucza, która zapewnia, że użytkownik, który łączy się z urządzeniem,

jest autoryzowany do wykonania operacji na nim. Natomiast Telnet korzysta z prostych metod uwierzytelniania, takich jak nazwa użytkownika i hasło, które są przesyłane w sposób niezaszyfrowany, co umożliwia potencjalnym atakującym przechwycenie tych informacji