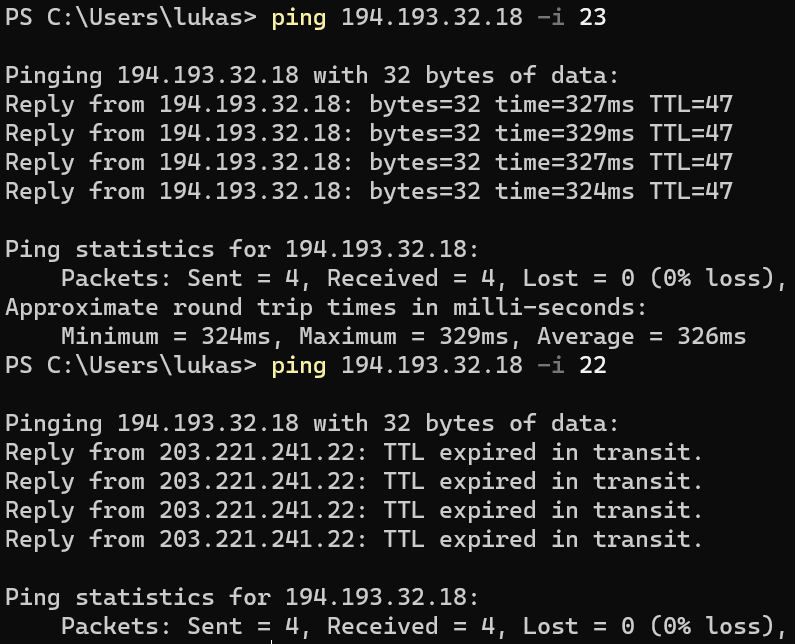
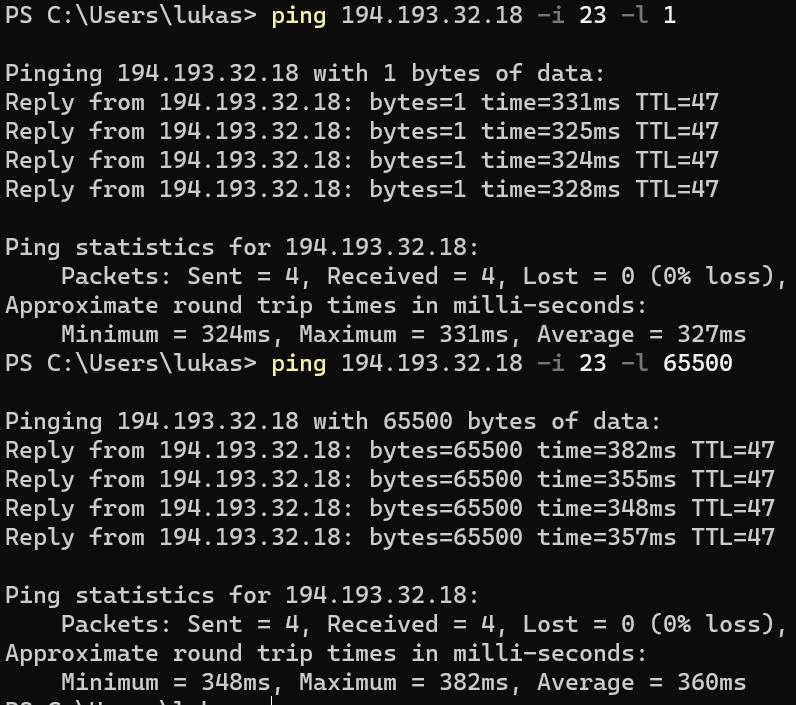
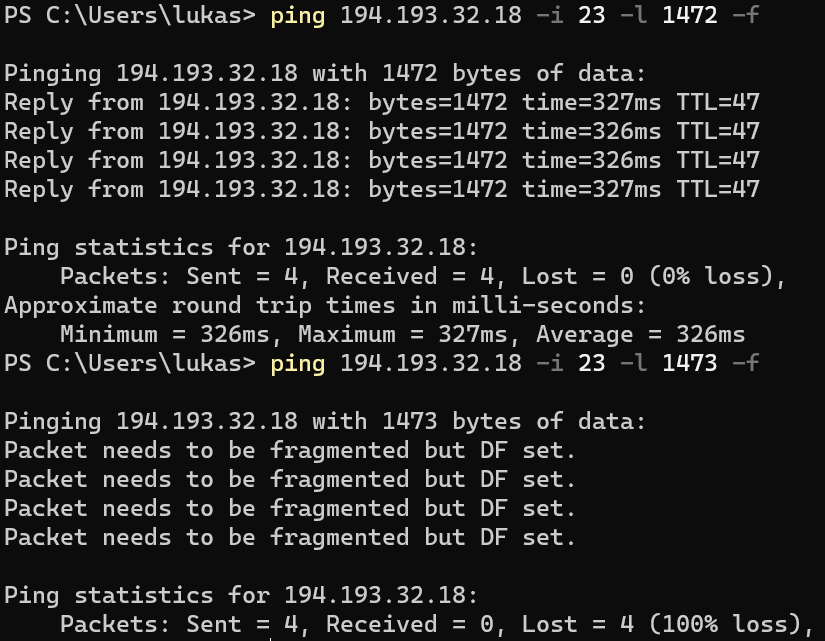
Lista nr 1

Łukasz Machnik – 268456

# Zadanie 1

1. Działanie programu Ping  
   Program Ping służy przede wszystkim do sprawdzenia czy istnieje trasa między naszym komputerem a dowolnym innym urządzeniem w sieci.   
   Składnia: ping [opcje] [adres do którego chcemy się połączyć]  
   Użyte przeze mnie opcje:  
   -i [t] => ustawia wartość flagi TTL pakietu ping na wartość [t]  
   -l [s] => ustawia rozmiar pojedynczego pakietu ping na wartość [s] bajtów (przyjmowane wartości: od 0 do 65500)  
   -f => wymusza aby pakiet nie był fragmentowany (większe pakiety mogą się nie wysyłać)  
     
   Żeby sprawdzić średnicę sieci znalazłem adres serwera DNS znajdującego się w Australii i ustawiając różne wartości flagi TTL wywnioskowałem że między moim komputerem a serwerem są 24 routery (jeśli ustawiłem TTL na 23 to ping dochodził do celu a jeśli ustawiłem na 22 to już nie a zatem pakiet pokonał dokładnie 23 krawędzie – „odwiedził” 24 routery), a w drodze powrotnej najprawdopodobniej 17 krawędzi (18 routerów), bo wartość flagi po powrocie to 47 więc serwer zapewne ustawił ją na 64. 64 – 47 = 17 => tyle krawędzi pokonał pakiet.  
     
   Z moich obserwacji wynika że na ilość skoków nie ma wpływu rozmiar pakietu co widać na poniższych screenach gdzie wysyłałem pakiety o różnych skrajnych rozmiarach a liczba skoków była niezmienna. Wydaje się jednak że rozmiar pakietu wpłynął na czas propagacji. Pakietowi o rozmiarze 65500 B dotarcie do celu zajęło ok 20-30 ms dłużej niż pakietowi 1 B.  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   Największy niepofragmentowany pakiet jaki udało mi się wysłać miał 1472 B (screen poniżej)   
   Wydaje się też że pakiet niefragmentowany (z opcją „-f”) ma minimalnie mniejszy czas propagacji (różnica kilku ms): Obraz zawierający kalendarz

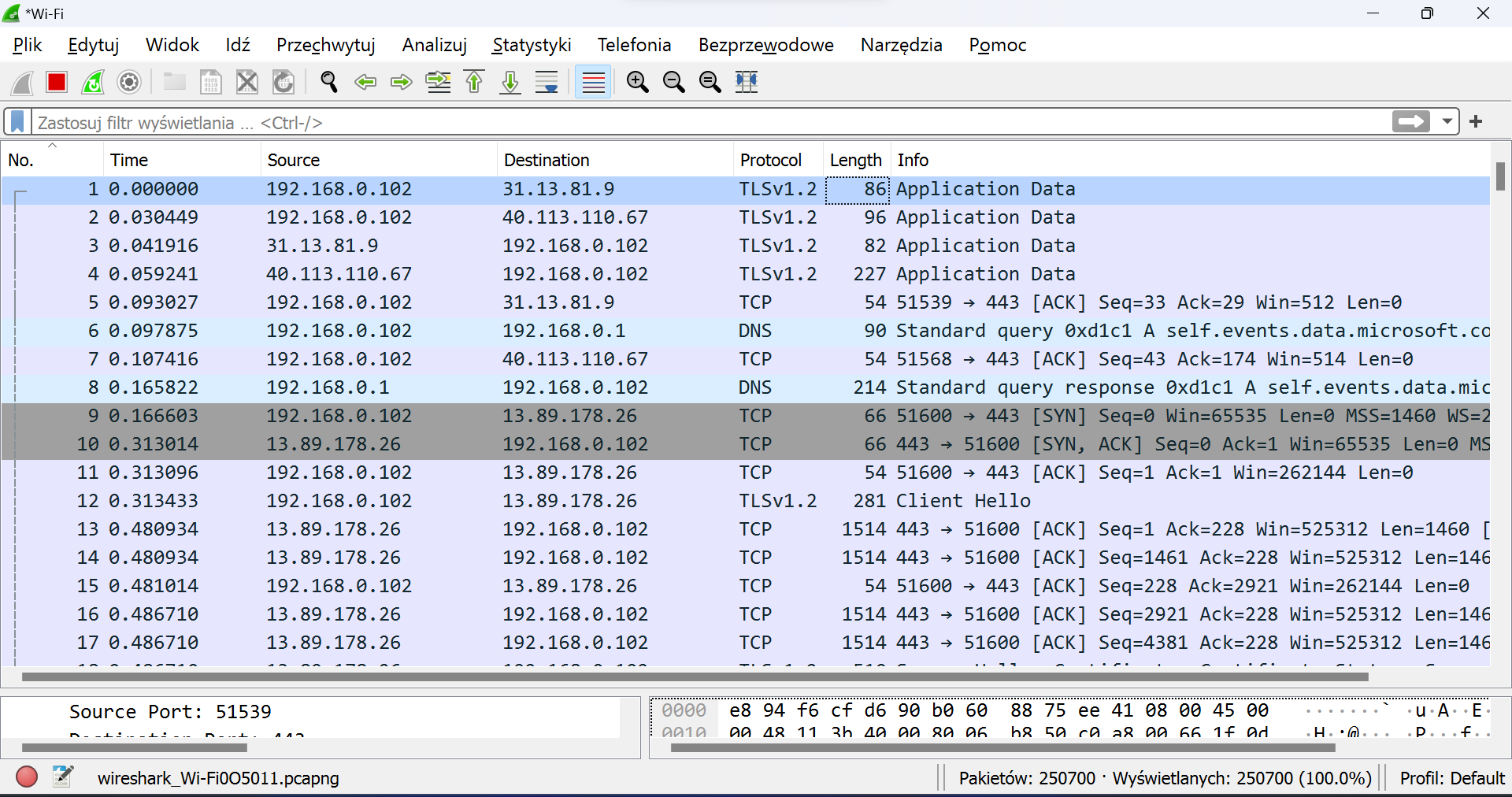
   Opis wygenerowany automatycznie  
   Drugim adresem który testowałem był adres Uniwersytetu Wrocławskiego. Z analogicznych jak wcześniej eksperymentów wywnioskowałem że do serwera pakiet pokonuje 12 krawędzi a w drodze powrotnej „odwiedza” 11 węzłów (TTL ustawiony przez serwer to najprawdopodobniej 64). Obraz zawierający tekst

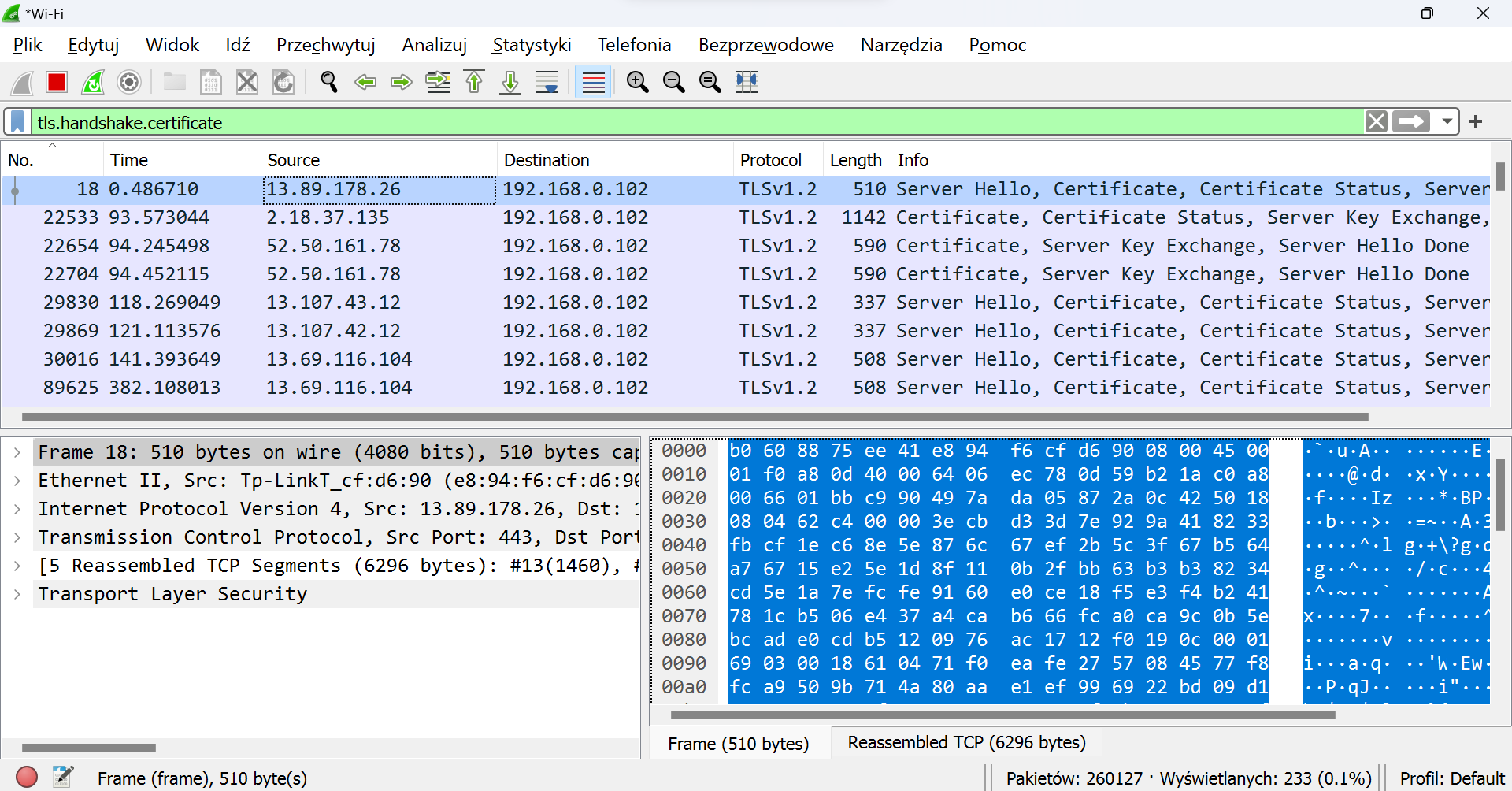
   Opis wygenerowany automatycznie  
   W przypadku tego serwera największy ping który przetworzy serwer docelowy to 996 B. Na tak niewielkiej różnicy rozmiarów również widać jednak sporą różnicę w czasie propagacji pakietów o rozmiarze 996 B i 1 B.   
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   W tym przykładzie wymuszenie niefragmentowania pakietów sprawia że czas propagacji jeszcze bardziej się wydłuża  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   W celu znalezienia sieci wirtualnej pingowałem wielokrotnie ten sam adres oczekując różnych ścieżek za każdym razem jednak nie znalazłem takiego przypadku.
2. Działanie programu Traceroute  
   Program Traceroute służy do sprawdzania trasy jaką pokonuje pakiet z naszego komputera do dowolnego urządzenia w sieci. W systemie Windows składnia jest następująca:  
   tracert [opcje] [adres do którego chcemy się dostać]. Traceroute w przeciwieństwie do programu Ping wypisuje adresy węzłów mijanych w drodze do celu (nie wszystkich co jest związane z polityką i ustawieniami tych urządzeń). W pierwszej kolumnie wyświetla się numer węzła, kolejne 3 kolumny to czas jaki zajęło dotarcie do węzła i z powrotem (traceroute wysyła 3 pakiety żeby pojedyncza anomalia nie zepsuła ogólnego obrazu; \* pojawia się jeśli przekroczono limit czasu oczekiwania na odpowiedź) a ostatnia kolumna to adres węzła. Na poniższych screenach widać na przykład że jeśli łączę się z akademika to pierwszym węzłem jest router w moim pokoju, następnie jakiś serwer zbiorczy dla całego akademika (T4), następnie jakieś 2 serwery Politechniki – z czego pierwszy sądząc po nazwie domenowej na ul. Wittiga w akademiku T19. Następnie są już różne kolejne adresy które po kolei doprowadzają mnie w końcu do adresu docelowego.   
   Przykłady użycia dla adresów z poprzedniego zadania:  
   Serwer DNS w Australii:  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   Serwer Uniwersytetu Wrocławskiego:  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie
3. Działanie programu Wireshark  
   Wireshark to potężne narzędzie służące analizie ruchu sieciowego. Program przechwytuje wszystkie pakiety wchodzące i wychodzące z komputera i prezentuje ich zawartość we w miarę przystępnej formie.  
   Po uruchomieniu programu można wybrać konkretny interfejs na którym program ma nasłuchiwać. Po tym od razu dostajemy widok ze wszystkimi przechwyconymi pakietami – jeśli komputer podłączony jest do internetu to będzie ich przybywać dosyć szybko. Każdy wyświetlony rząd odpowiada jednemu pakietowi: w pierwszej kolumnie jego numer (Wireshark numeruje wszystkie przechwycone pakiety od 1) następnie czas między uruchomieniem programu a przechwyceniem danego pakietu, adres źródłowy i adres docelowy pakietu (w każdym rzędzie pojawia się mój adres – albo jako źródło albo jako cel), protokół przy użyciu jakiego wysłano pakiet, jego długość oraz dodatkowe informacje dot. zawartości pakietu.  
     
   Jeśli klikniemy dowolny rząd to na dole w dwóch kolumnach wyświetli się zawartość pakietu – po lewej w wersji sformatowanej na łatwą do odczytania dla człowieka, po prawej bezpośrednią zawartość pakietu w hexie.  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   U góry okna programu możemy wpisywać filtry tak aby ograniczyć liczbę wyświetlanych rekordów. Np. wpisując tls.handshake.certificate wyświetlę tylko te pakiety w których doszło do wymiany certyfikatu:   
   Z pakietu możemy odczytać np. klucz publiczny tego certyfikatu albo jego wystawcę: rozwijamy ostatni wiersz, i szukamy certyfikatu:  
   Obraz zawierający tekst

   Opis wygenerowany automatycznie  
   Jeśli klikniemy na wartość w lewej sekcji przeglądania pakietu to podświetli się jej reprezentacja w hexie i vice versa. Jeżeli znajdziemy odpowiednie pole to podświetli nam się klucz publiczny certyfikatu:   
   Obraz zawierający tekst

   Opis wygenerowany automatycznie

# Wnioski:

Programy Ping i Traceroute to programy bardzo proste ale bardzo przydatne do diagnostyki sieci. Mogą pomóc wykryć awarie lub pozwolić upewnić się że wszystko działa jak powinno.

Program Wireshark jest większym narzędziem i pozwala zajrzeć od środka do tego jak działa przesyłanie danych. Wireshark pokazuje również jak ważne jest szyfrowanie danych gdyż bez niego każdy nasłuchujący przepływu pakietów w sieci mógłby z nich bezpośrednio odczytać wszystkie przesyłane dane (np. hasła).