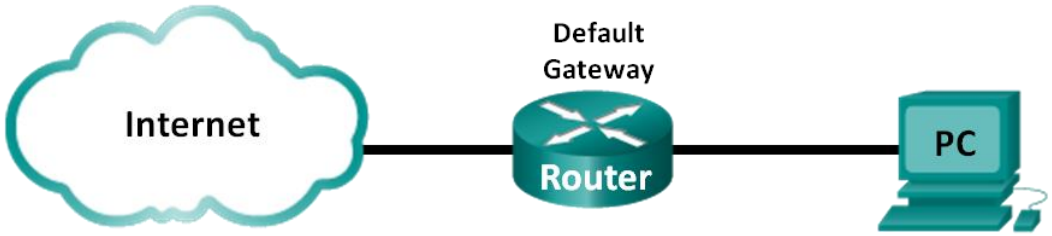
Laboratorium - Używanie programu Wireshark do obserwacji mechanizmu uzgodnienia trójetapowego TCP

Topologia



Cele

Część 1: Przygotowanie Wireshark do przechwytywania pakietów

- Wybór odpowiedniego interfejsu karty sieciowej do przechwytywania pakietów.

Część 2: Przechwytywanie, lokalizowanie i badanie pakietów

- Przechwytywanie sesji internetowej dla adresu www.google.com.
- Znajdowanie odpowiednich pakietów dla sesji internetowej.
- Sprawdzanie informacji zawartych w pakietach: adresy IP, numery portów TCP oraz flagi TCP.

Scenariusz

W tym laboratorium używany jest program Wireshark w celu przechwytywania i sprawdzania pakietów generowanych pomiędzy przeglądarką PC używającą protokołu HyperText Transfer Protocol (HTTP) i serwerem www, takim jak www.google.com. Jeżeli aplikacja, taka jak HTTP lub File Transfer Protocol (FTP) zostanie uruchomiona, to protokół TCP użyje mechanizmu uzgodnienia trójetapowego w celu ustanowienia wiarygodnej sesji TCP pomiędzy dwoma hostami. Na przykład, gdy komputer korzysta z przeglądarki internetowej, aby przeglądać Internet, uzgadnianie trójetapowe jest inicjowane i sesja jest ustalona pomiędzy hostem PC i serwerem WWW. Komputer PC może obsługiwać wiele równoczesnych aktywnych sesji TCP do różnych stron internetowych.

Uwaga: To ćwiczenie nie może być przeprowadzone przy użyciu środowiska Netlab. To ćwiczenie zakłada, że masz dostęp do Internetu.

Wymagane wyposażenie

1 PC (Windows 7, Vista, lub XP z dostępem do wiersza poleceń, dostępem do Internetu i zainstalowanym programem Wireshark)

Część 1. Przygotowanie Wireshark do przechwytywania pakietów

W części 1 należy uruchomić program Wireshark i wybrać odpowiedni interfejs, aby rozpocząć przechwytywanie pakietów.

Krok 1. Pobieranie adresów interfejsu PC.

W tym laboratorium, musisz znać adres IP twojego komputera oraz adres fizyczny karty sieciowej(NIC), nazywany adresem MAC.

a. W oknie poleceń wpisz **ipconfig /all** i naciśnij **Enter**.

```
   Physical Address. . . . . . . . . : C8-0A-A9-FA-DE-0D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.130(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, December 01, 2012 1:43:35 PM
   Lease Expires . . . . . . . . . . : Sunday, December 02, 2012 1:43:35 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

b. Zapisz adres IP i adres MAC dla wybranej karty Ethernet, ponieważ te adresy źródłowy będą używane do przechwytywania pakietów.

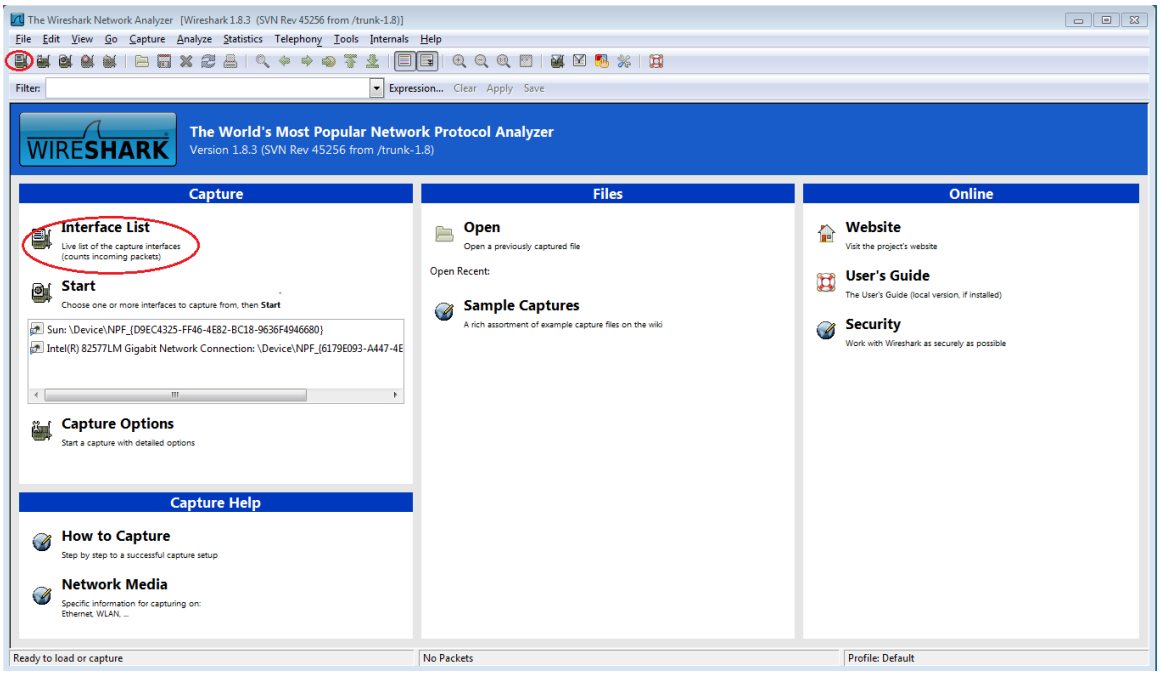
Adres hosta PC: _____

Adres MAC dla hosta: _____

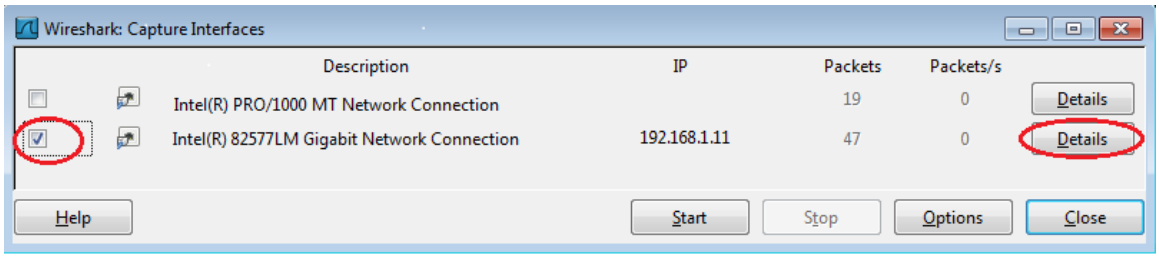
Krok 2. Uruchom program Wireshark i wybierz odpowiedni interfejs.

a. Kliknij przycisk Windows **Start** i rozwiń menu za pomocą podwójnego kliknięcia **Wireshark**.

b. Po uruchomieniu Wireshark kliknij **Interface List**.



c. W oknie **Wireshark: Capture Interfaces** kliknij opcję (zaznacz ją) odpowiadającą Twojemu interfejsowi podłączonego do sieci LAN.



Uwaga: W przypadku wielu interfejsów gdy nie masz pewności, który interfejs sprawdzić, to kliknij przycisk **Details**. Kliknij zakładkę **802.3 (Ethernet)** i sprawdź czy adres MAC zgadza się z adresem zapisanym w kroku 1b. Zamknij okno Interface Details.

Część 2. Przechwytywanie, lokalizowanie i badanie pakietów

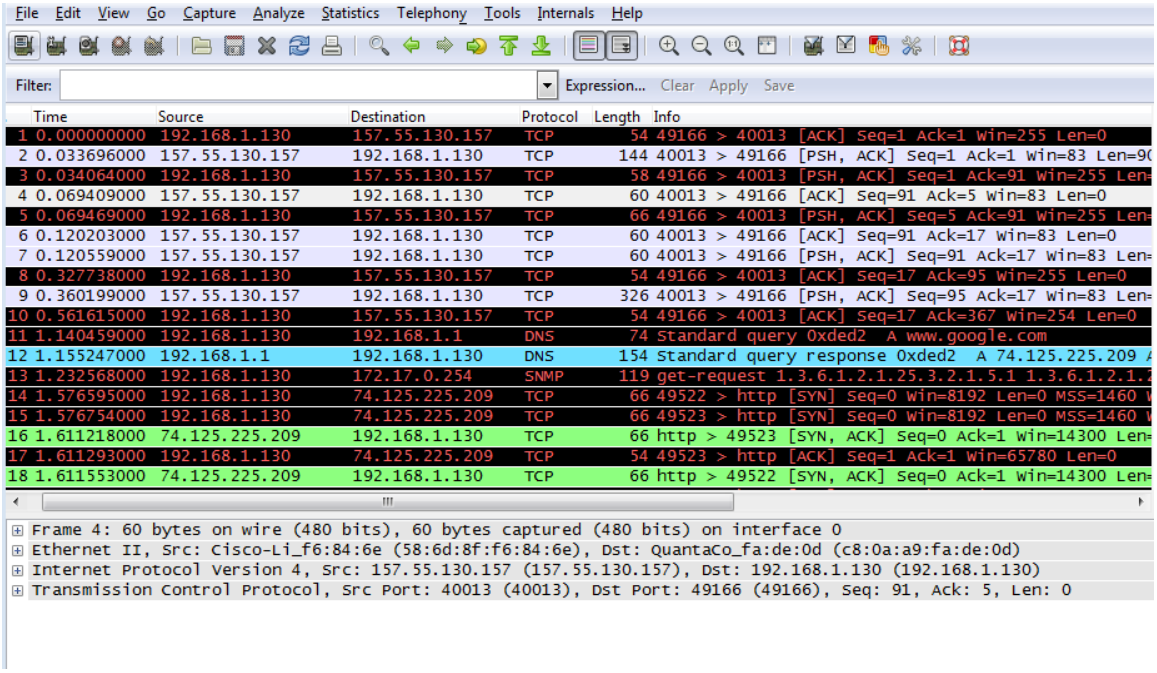
Krok 1. Kliknij przycisk Start aby rozpocząć przechwytywanie.

a. Wybierz www.google.com Zminimalizuj okno przeglądarki i wróć do Wireshark. Zatrzymaj proces przechwytywania. Powinieneś zobaczyć przechwycony ruch podobny do tego poniżej w kroku b.

Uwaga: Twój instruktor może podać Ci inną stronę. Jeżeli tak, to wpisz nazwę lub adres strony tutaj:

_____

b. Mając aktywne okno Capture, znajdź kolumny: **Source**, **Destination**,**Protocol** .



Krok 2. Znajdź odpowiednie pakiety dla sesji internetowej.

Jeżeli komputer został dopiero dołączony do sieci i nie było żadnej jego aktywności dotyczącej dostępu do Internetu, to możesz zobaczyć cały proces przechwytywanych komunikatów: Address Resolution Protocol (ARP),Domain Name System (DNS) i uzgadnianie 3-etapowe TCP. Ekran przechwytywania w kroku 1 w części 2 pokazuje wszystkie pakiety wymagane, aby komputer musiał pobrać stronę www.google.com. W tym przypadku komputer PC ma już wpis w tabeli ARP dla bramy domyślnej; w związku z tym, komputer żąda odwzorowania adresu DNS www.google.com.

a. Ramka 11 przedstawia zapytanie DNS z komputera do serwera DNS, próbując odwzorować nazwę domeny www.google.com na adres IP serwera www. Komputer musi mieć adres IP, zanim wyśle pierwszy pakiet do serwera www.

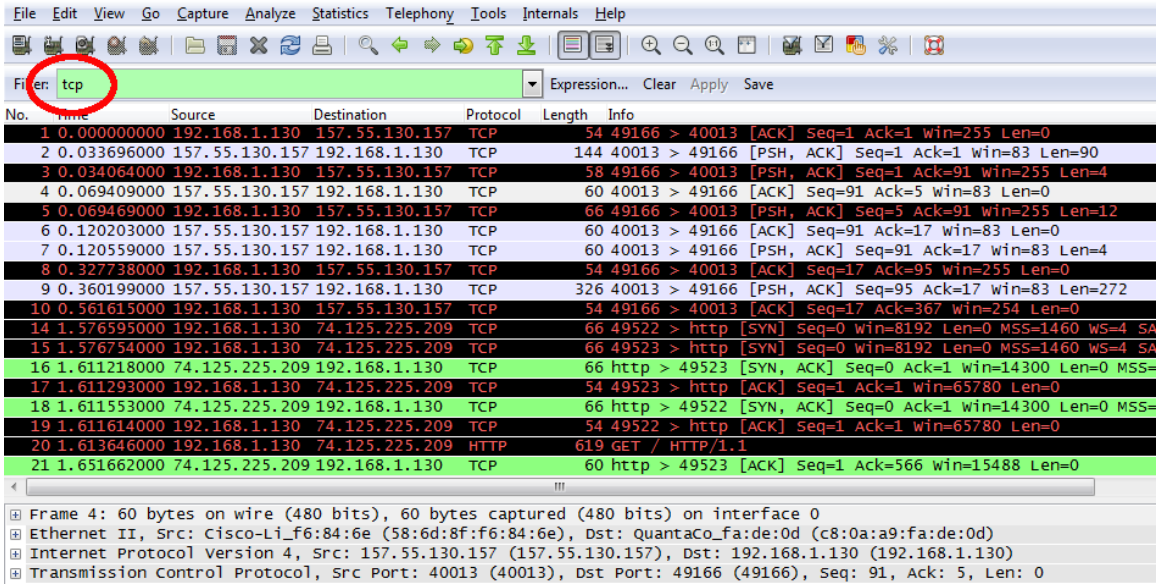
   Jaki jest adres IP serwera DNS? _____

b. Ramka 12 to odpowiedź z serwera DNS (zawiera adres IP strony www.google.com).

c. Znajdź odpowiedni pakiet w początkowej fazie procesu uzgadniania trójetapowego. W tym przykładzie ramka 15 jest początkiem procesu uzgadniania trójetapowego TCP.

   Jaki jest adres serwera Google?_____

d. Jeżeli masz dużo pakietów, które nie są powiązane z sesją TCP to może być konieczne aby użyć opcji filtrowania. W programie Wireshark wpisz **tcp** w obszarze filtru i naciśnij Enter.



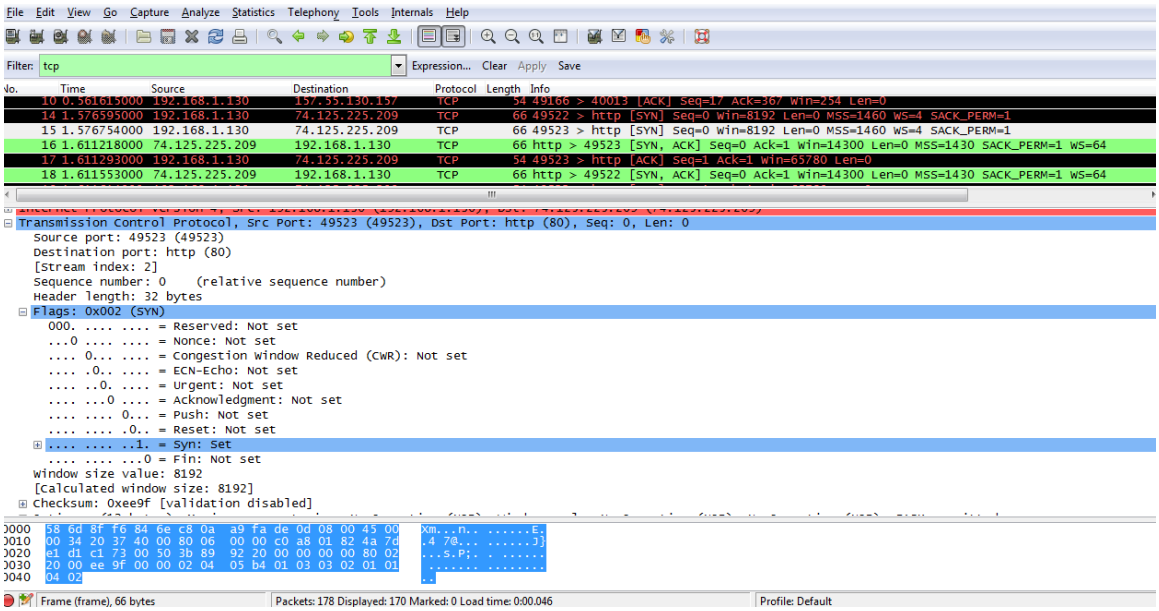
Krok 3. Sprawdź informacje zawarte w pakietach: adresy IP, numery portów TCP oraz flagi TCP.

a. W tym przykładzie ramka 15 jest początkiem procesu uzgadniania trójetapowego pomiędzy komputerem PC i serwerem Google. W panelu listy pakietów (górna część okna głównego), zaznacz ramkę. Po zaznaczeniu linii pokażą się dodatkowe zdekodowane informacje o zawartości pakietu w dwóch dolnych panelach. Sprawdź informacje dotyczące TCP w okienku szczegółów pakietu (środkowa część okna głównego).

b. W panelu dotyczącym szczegółów pakietu kliknij ikonę **+** znajdującą się po lewej stronie pozycji Transmission Control Protocol aby rozwinąć informacje o TCP.

c. Kliknij ikonę **+** znajdującą się po lewej stronie słowa Flags. Przeczytaj numery portów źródłowych i docelowych oraz flagi, które są ustawione.

   Uwaga: Możesz dostosować rozmiary oraz położenie okien programu Wireshark tak aby wyświetlać potrzebne informacje.



Jaki jest numer portu źródłowego TCP? _____

Jak można sklasyfikować port źródłowy? (Jakiego typu jest port źródłowy) _____

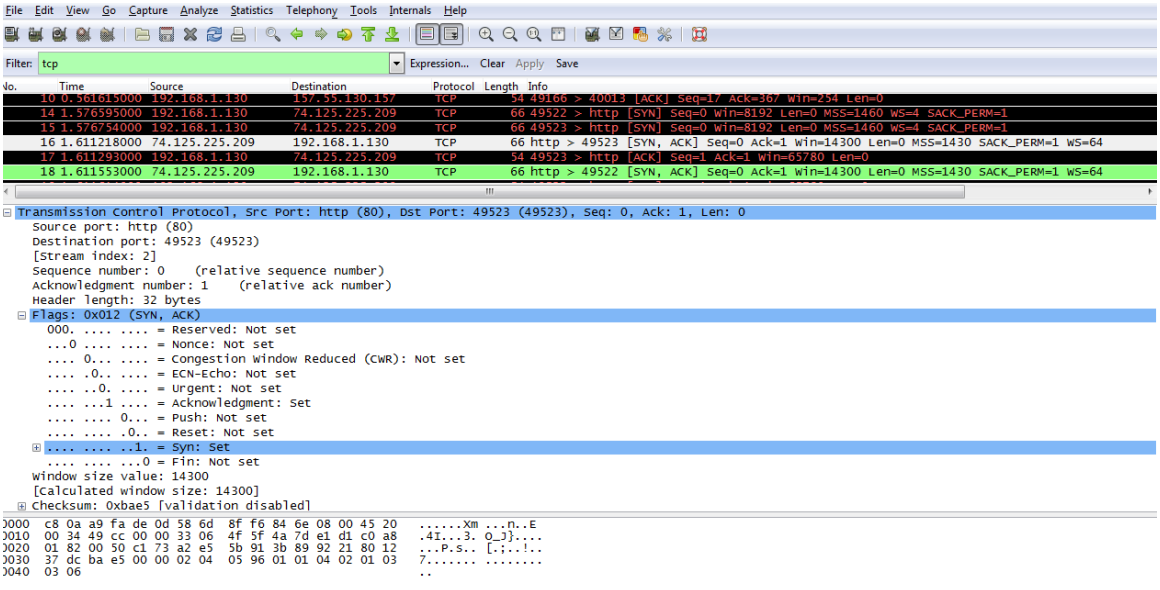
Jaki jest numer portu docelowego TCP? _____

Jak można sklasyfikować port docelowy? (Jakiego typu jest port docelowy) _____

Która flaga (lub flagi) są ustawione (1)? _____

Jaka jest wartość numeru sekwencyjnego? _____

d. Aby wybrać następną ramkę w procesie uzgadniania trójetapowego, w menu programu Wireshark wybierz **Go** a potem wybierz **Next Packet In Conversation**. W tym przykładzie jest to ramka 16. To jest odpowiedź serwera Google dla rozpoczęcia sesji.



Jakie są wartości portów źródłowych i docelowych? _____

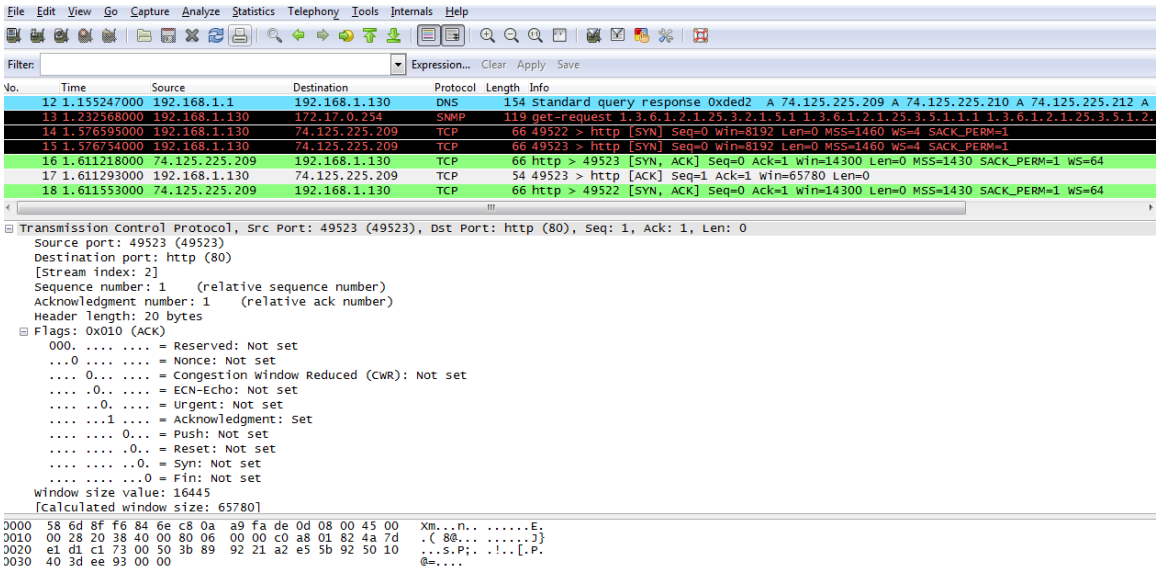
Które flagi są ustawione?

_____

Jakie są względne numery sekwencyjne i potwierdzenia?

_____

e. Na koniec zbadaj trzeci pakiet procesu uzgadniania trójetapowego tego przykładu. Kliknięcie ramki 17 w górnym oknie powoduje wyświetlenie następujących informacji:



Zbadaj trzeciego czyli ostatni pakiet uzgadniania trójetapowego.

Która flaga (lub flagi) jest ustawiona?

_____

Względne numery sekwencyjne oraz potwierdzenie są ustawione na 1. Dopiero teraz jest ustanowione połączenie TCP i możliwa jest komunikacja pomiędzy komputerem a serwerem.

f. Zamknij program Wireshark.

Do przemyślenia

1. W Wireshark wstępnie zdefiniowane jest wiele filtrów. W dużej sieci może być użytych wiele filtrów, które będą pokazywać różnego rodzaju ruch sieciowy. Które trzy filtry z listy mogą być najbardziej przydatne dla administratora sieci?

   _____

2. W jaki inny sposób można użyć programu Wireshark w sieci produkcyjnej?

   _____