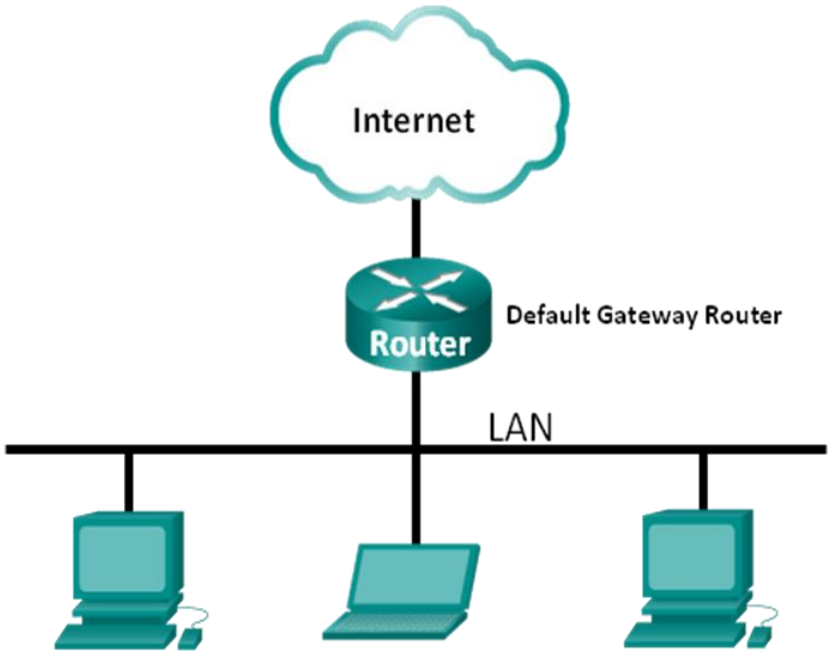
Laboratorium - Używanie programu Wireshark do badania ruchu sieciowego

Topologia



Cele

Część 1: (Opcjonalna) Pobranie i instalacja programu Wireshark.

Część 2: Użycie programu Wireshark do przechwycenia i analizy lokalnych danych ICMP.

- Przechwycenie danych generowanych w sieci poleceniem ping między hostami lokalnymi.
- Zlokalizowanie adresu IP i MAC w przechwyconych PDU.

Część 3: Użycie programu Wireshark do przechwycenia i analizy zdalnych danych ICMP.

- Przechwycenie danych generowanych w sieci poleceniem ping między hostami zdalnymi.
- Zlokalizowanie adresu IP i MAC w przechwyconych PDU.
- Wyjaśnienie dlaczego adresy MAC zdalnych hostów są inne, niż adresy MAC lokalnych hostów.

Scenariusz

Wireshark jest programowym analizatorem protokołów sieciowych, czasem zwany bywa snifferem pakietów. Używany jest do analizy sieci, diagnozowania problemów, wspierania rozwoju różnego rodzaju oprogramowania i nowych protokołów. Jego głównym zastosowaniem jest również edukacja. W momencie gdy strumienie danych podróżują poprzez sieć, analizator przechwytuje i zapamiętuje każdą jednostkę PDU. Następnie dekoduje informacje w nich zawarte do postaci przejrzystej struktury odzwierciedlającej zalecenia RFC i umożliwiającej obserwatorowi bardzo wygodną ich analizę.

Wireshark jest bardzo użytecznym narzędziem dla każdego, kto w swej pracy ma do czynienia z sieciami komputerowymi. Może być z powodzeniem wykorzystywany w większości laboratoriów kursu CCNA w celu analizy przesyłanych danych oraz rozwiązywania napotkanych problemów. To laboratorium zawiera instrukcję dotyczącą pobierania i instalacji programu Wireshark, aczkolwiek może on już być zainstalowany.

W tym laboratorium użyjesz programu Wireshark do przechwytywania danych ICMP w celu wyłuskiwania z nich adresów IP i adresów MAC.

Wymagane wyposażenie

- 1 PC (Windows 7, Vista lub XP z dostępem do Internetu)
- Dodatkowy komputer(y) PC w sieci lokalnej (LAN), którego zadaniem będzie odpowiadać na przychodzące żądania ping.

Część 1: (Opcjonalnie) Ściągnięcie i instalacja programu Wireshark.

Wireshark stał się podstawowym programem w branży, używanym do analizy pakietów przez inżynierów sieciowych. Jest to oprogramowanie "open source", dostępne na wiele różnych systemów operacyjnych z Windows, Mac i Linux włącznie. W części 1 tego laboratorium, ściągniesz i zainstalujesz aplikację Wireshark na swoim komputerze.

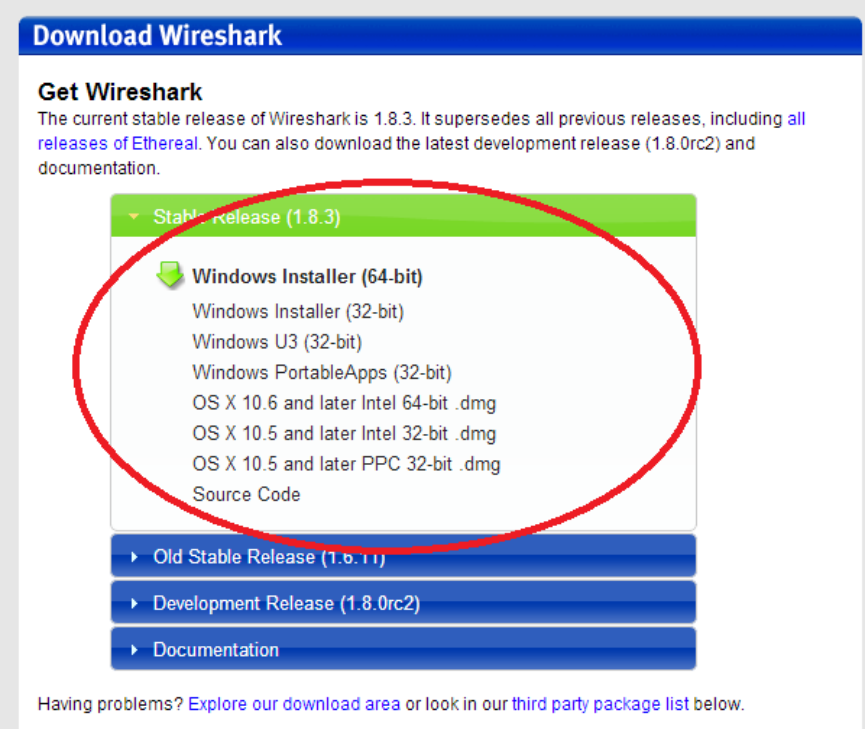
Uwaga: Jeżeli Wireshark jest już zainstalowany na twoim komputerze, możesz pominąć część 1 niniejszego laboratorium i od razu przejść do części 2. Jeżeli Wireshark nie jest zainstalowany na twoim komputerze, wraz z instruktorem sprawdź politykę bezpieczeństwa twojej uczelni odnośnie pobierania oprogramowania.

Krok 1: Pobranie aplikacji Wireshark.

a. Wireshark można pobrać ze strony www.wireshark.org.

b. Kliknij **Download Wireshark**.

c. Wybierz wersję programu dopasowaną do architektury i systemu operacyjnego twojego komputera. Na przykład, jeżeli posiadasz 64-bitowy komputer PC pracujący pod kontrolą systemu Windows, wybierz **Windows Installer (64-bit)**.

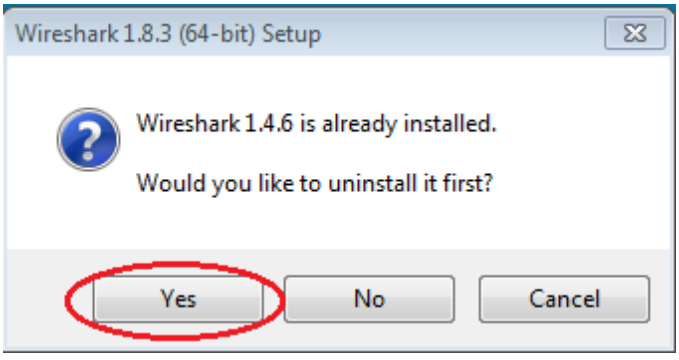


Po dokonaniu wyboru, proces pobierania powinien się rozpocząć. Miejsce zapisania pliku na twardym dysku zależy od tego, jakiej przeglądarki internetowej i systemu operacyjnego używasz. Dla użytkowników systemu Windows domyślna lokalizacja to katalog **Downloads**.

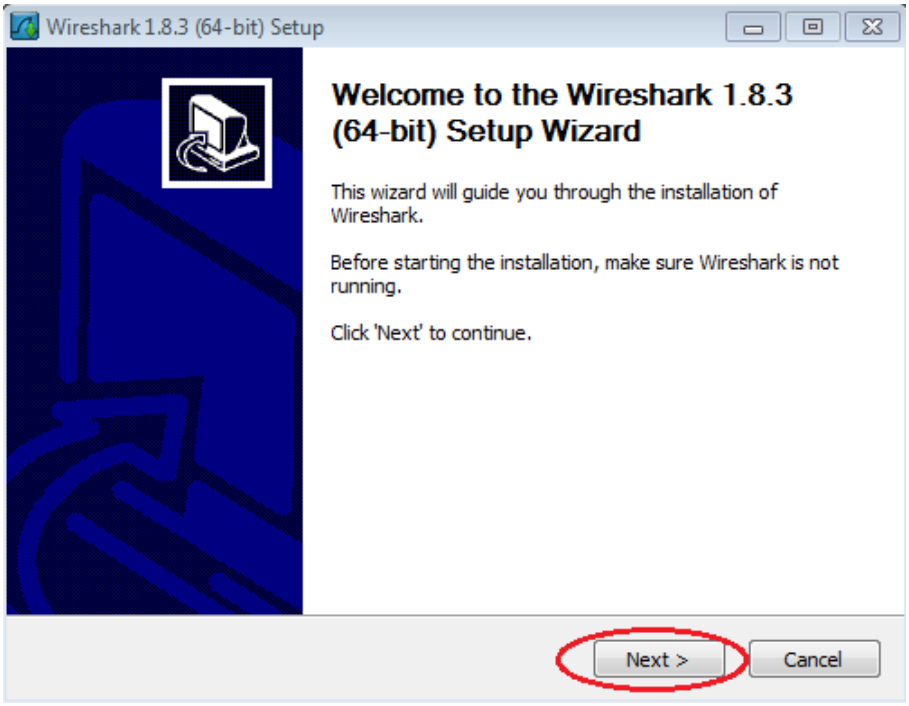
Krok 2: Instalacja programu Wireshark.

a. Pobrany plik ma nazwę **Wireshark-win64-x.x.x.exe**, gdzie **x** oznacza numer wersji. Kliknij dwa razy na plik by rozpocząć proces instalacji.

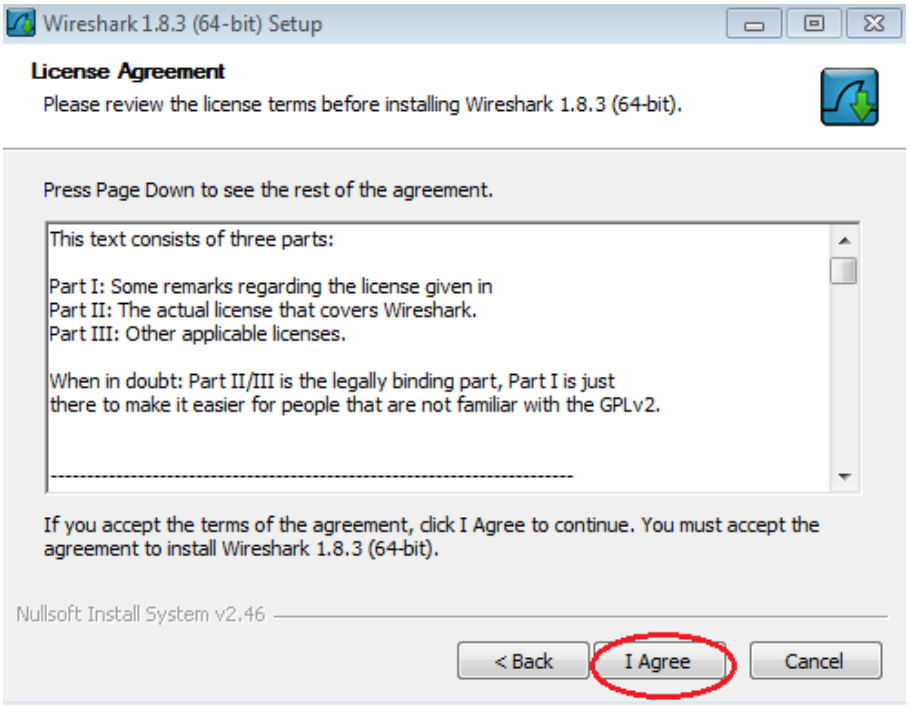
b. Odpowiedz na wszelkie komunikaty bezpieczeństwa, które mogą pojawić się na ekranie. Jeżeli masz już zainstalowany program Wireshark na swoim komputerze, przed instalacją nowej wersji będziesz poproszony o jego odinstalowanie. Zaleca się, abyś najpierw usunął starą wersję Wiresharka, a dopiero potem zainstalował jego nową wersję. Kliknij **Yes** by odinstalować poprzednią wersję programu Wireshark.



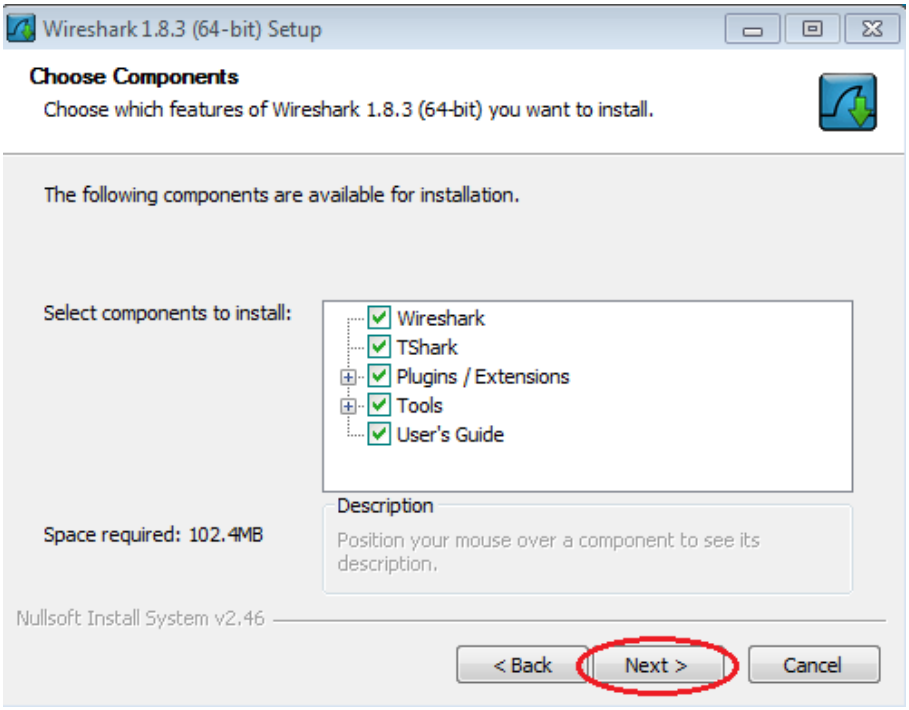
c. Jeżeli instalujesz aplikację Wireshark po raz pierwszy, lub instalujesz ją po odinstalowaniu poprzedniej wersji, zostaniesz od razu przeniesiony do kreatora instalacji (Wireshark Setup Wizard). Kliknij **Next**.



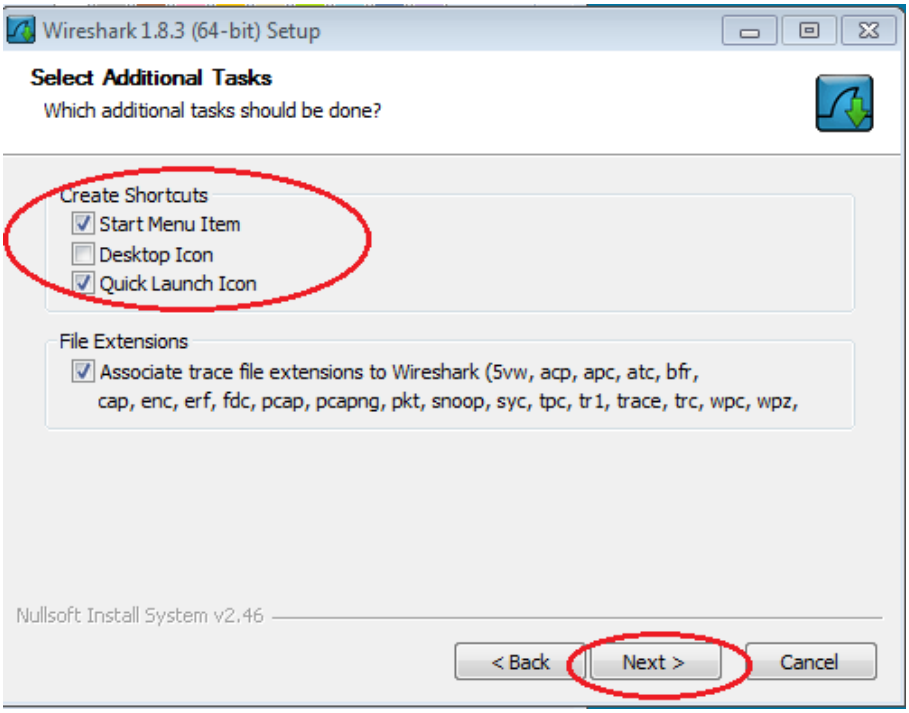
d. Kontynuuj proces instalacji. Kliknij **I Agree,** gdy wyświetli się okno zawierające umowę licencyjną (License Agreement).



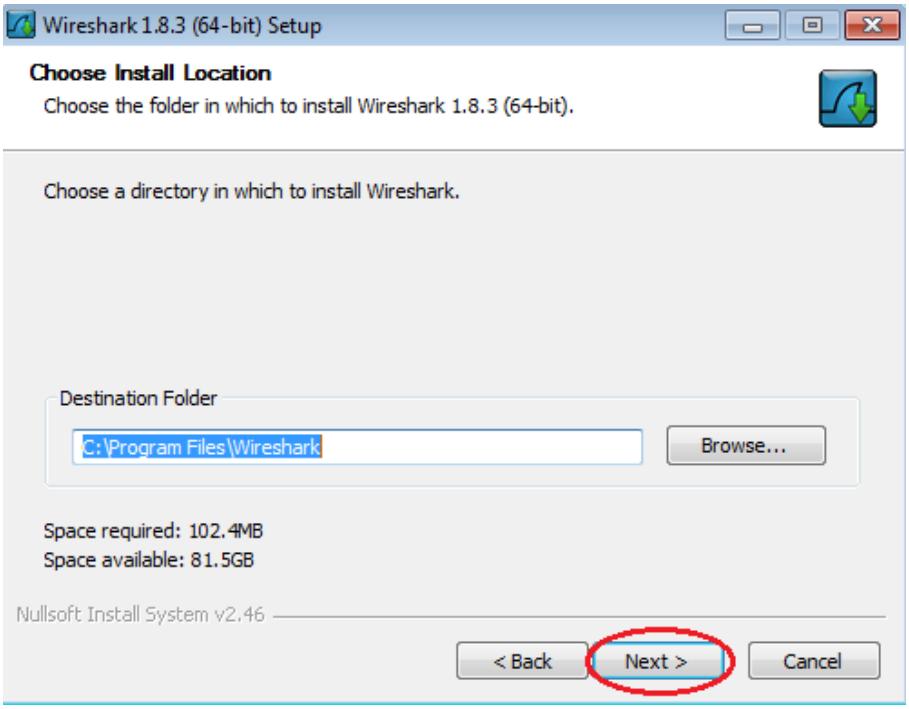
e. W oknie wyboru komponentów do zainstalowania (Choose Components) zachowaj ustawienia domyślne i kliknij **Next**.



f. Wybierz skróty które chcesz utworzyć i kliknij **Next**.

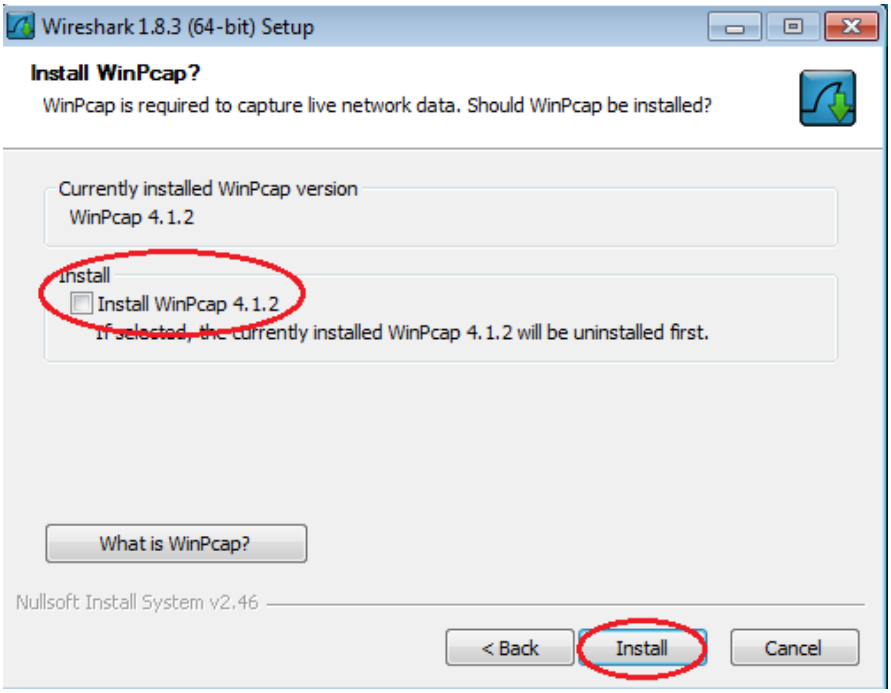


g. Możesz zmienić lokalizację instalacji programu Wireshark, ale jeżeli nie masz ograniczonego miejsca na dysku, najlepiej jak zainstalujesz aplikację w domyślnej lokalizacji.

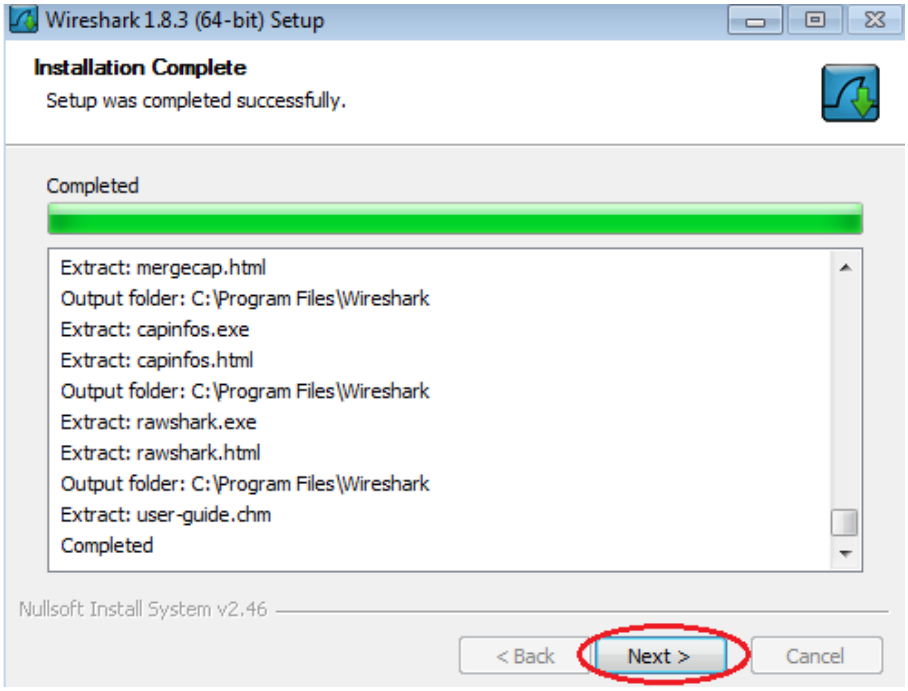


h. Aby móc przechwytywać na żywo dane z sieci, na twoim komputerze musi być zainstalowany program WinPcap. Jeżeli WinPcap jest już zainstalowany, pole wyboru umożliwiające jego instalację będzie niezaznaczone. Jeśli zainstalowana wersja WinPcap jest starsza niż wersja pochodząca z instalatora Wireshark, zaleca się abyś zezwolił na instalację jego nowszej wersji, poprzez zaznaczenie pola wyboru **Install WinPcap x.x.x** (numer wersji).

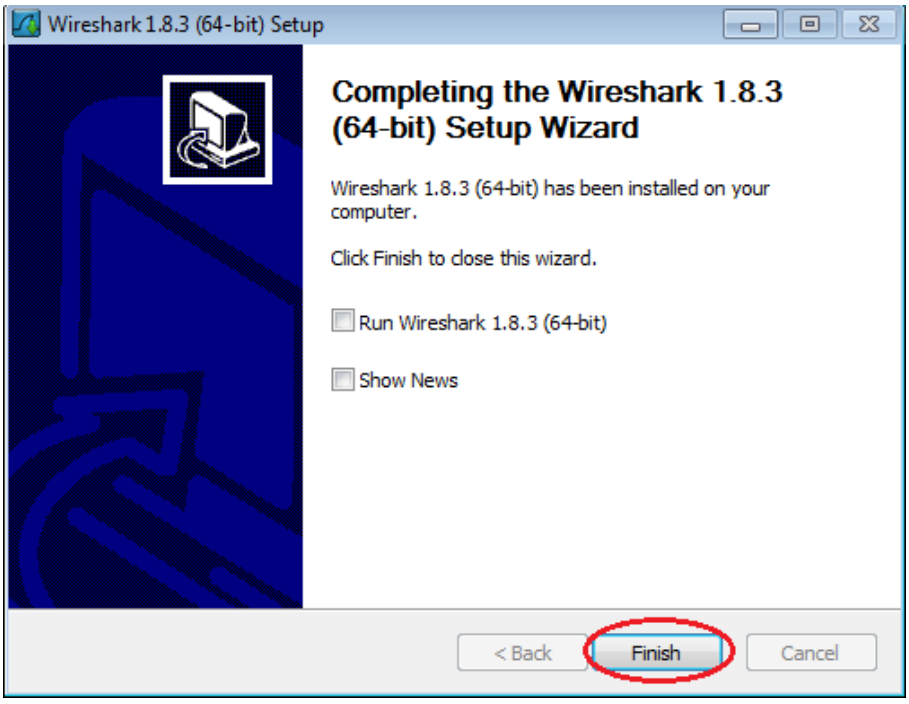
i. Zakończ pracę kreatora instalacji programu WinPcap - jeżeli WinPcap jest instalowany.



j. Rozpoczyna się instalacja programu Wireshark, a jej postępy można śledzić w osobnym oknie. Po zakończeniu instalacji kliknij przycisk **Next**.



k. Kliknij **Finish** by zakończyć proces instalacji programu Wireshark.



Część 2: Użycie programu Wireshark do przechwycenia i analizy lokalnych danych ICMP.

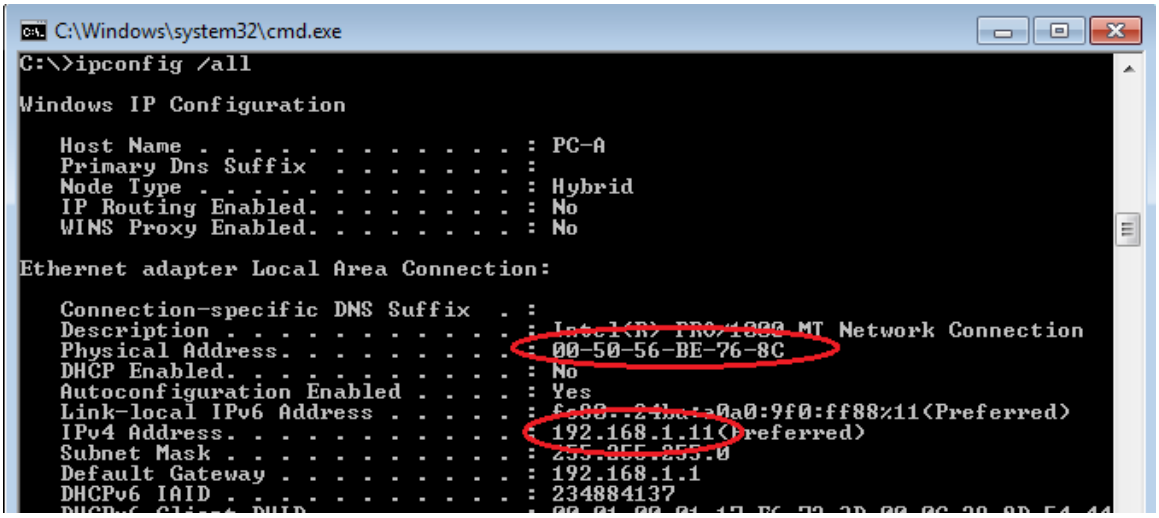
W 2 części tego ćwiczenia będziesz wysyłać pakiety ping do innego komputera w sieci lokalnej i przechwycisz żądania i odpowiedzi ICMP w programie Wireshark. Ponadto zajrzysz do wnętrza przechwyconych ramek w celu znalezienia konkretnych informacji. Analiza ta powinna przyczynić się do wyjaśnienia, w jaki sposób nagłówki pakietów są używane do transportu danych w miejsce przeznaczenia.

Krok 1: Pobieranie adresów interfejsu twojego PC.

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

a. Otwórz okno wiersza poleceń, wpisz **ipconfig /all** i naciśnij Enter.

b. Zanotuj adres IP i adres MAC (fizyczny) twojego komputera.

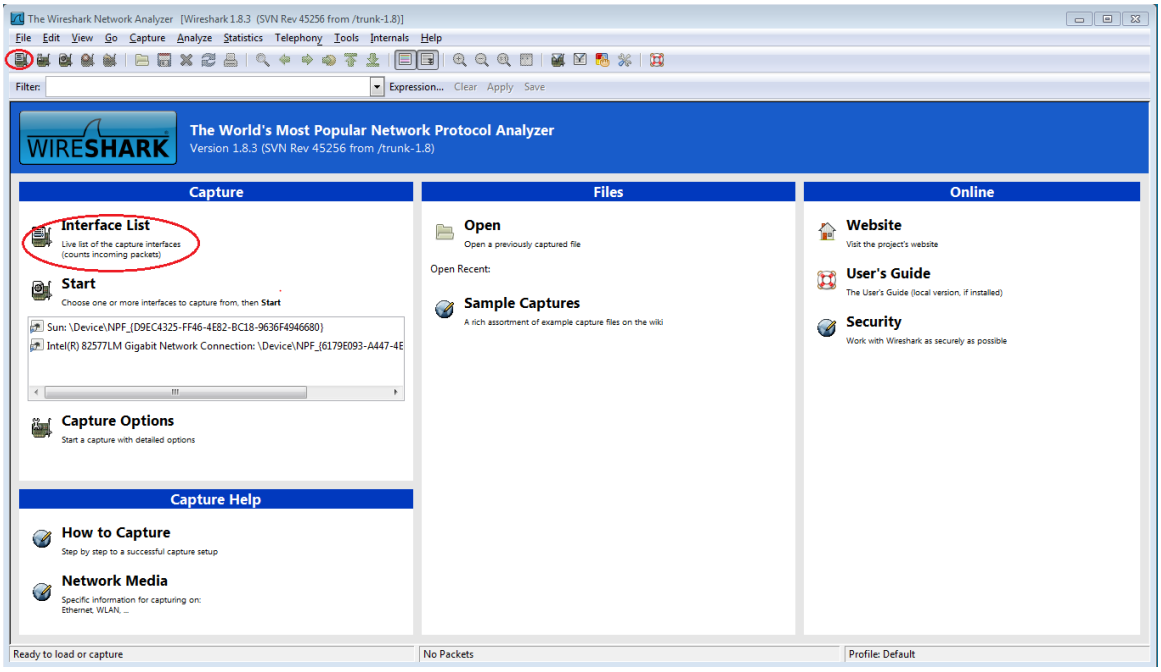


c. Poproś innych uczestników o ich adresy IP oraz przekaż im swój. Nie podawaj im swojego adresu MAC.

Krok 2: Uruchomienie programu Wireshark i rozpoczęcie przechwytywania pakietów danych.

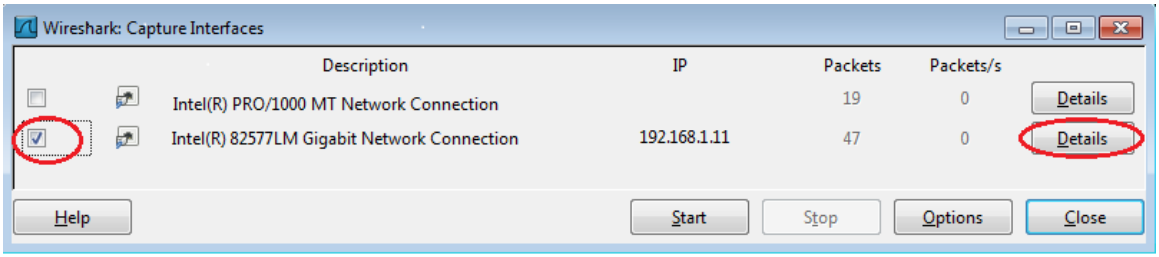
a. Na swoim komputerze, kliknij przycisk **Start** systemu Windows i w menu podręcznym znajdź program Wireshark. Kliknij dwukrotnie **Wireshark**.

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

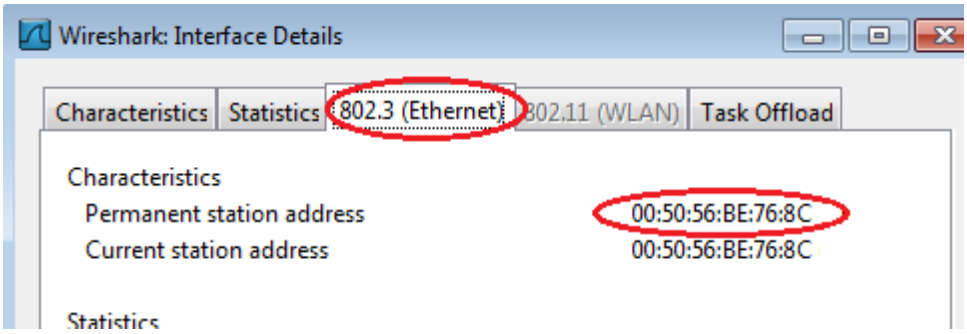


Uwaga: Kliknięcie na pierwszą ikonę z lewej strony w pasku narzędzi również otworzy Interface List.

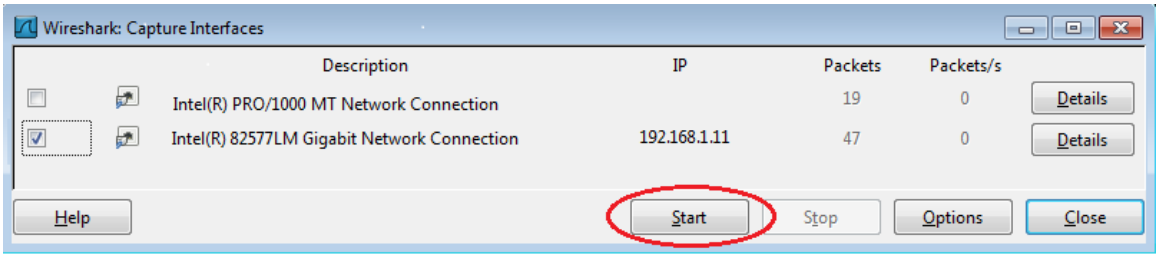
c. W oknie Wireshark: Capture Interfaces, kliknij pole wyboru (zaznacz je) odpowiadające interfejsowi podłączonemu do twojej sieci LAN.



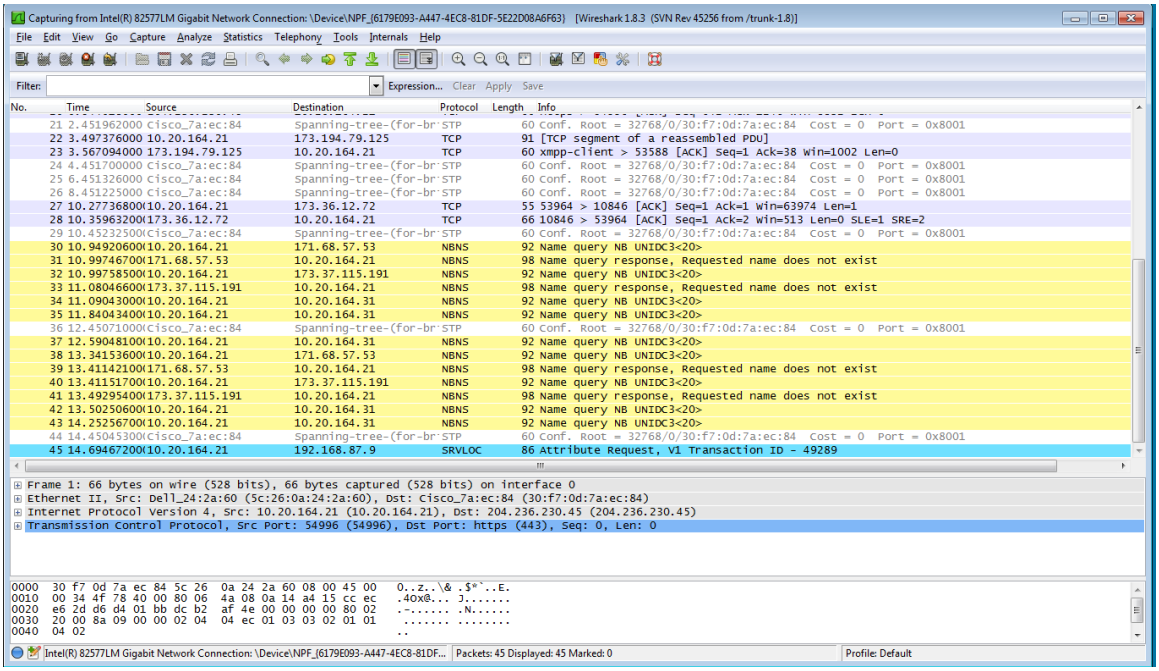
Uwaga: Jeżeli w wykazie znajduje się wiele interfejsów, a nie jesteś pewien, który z nich zaznaczyć, kliknij przycisk **Details** oraz otwórz zakładkę **802.3 (Ethernet)**. Sprawdź czy adres MAC jest taki sam jak ten, który zapisałeś w kroku 1b. Po pomyślnej weryfikacji zamknij okno Interface Details.



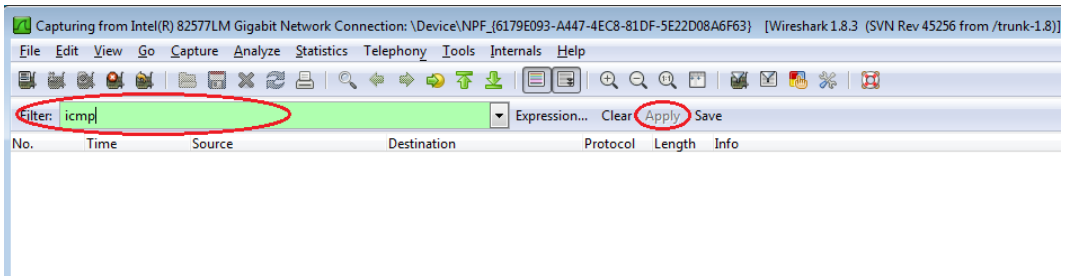
d. Po wybraniu właściwego interfejsu, kliknij **Start** by rozpocząć przechwytywanie danych.



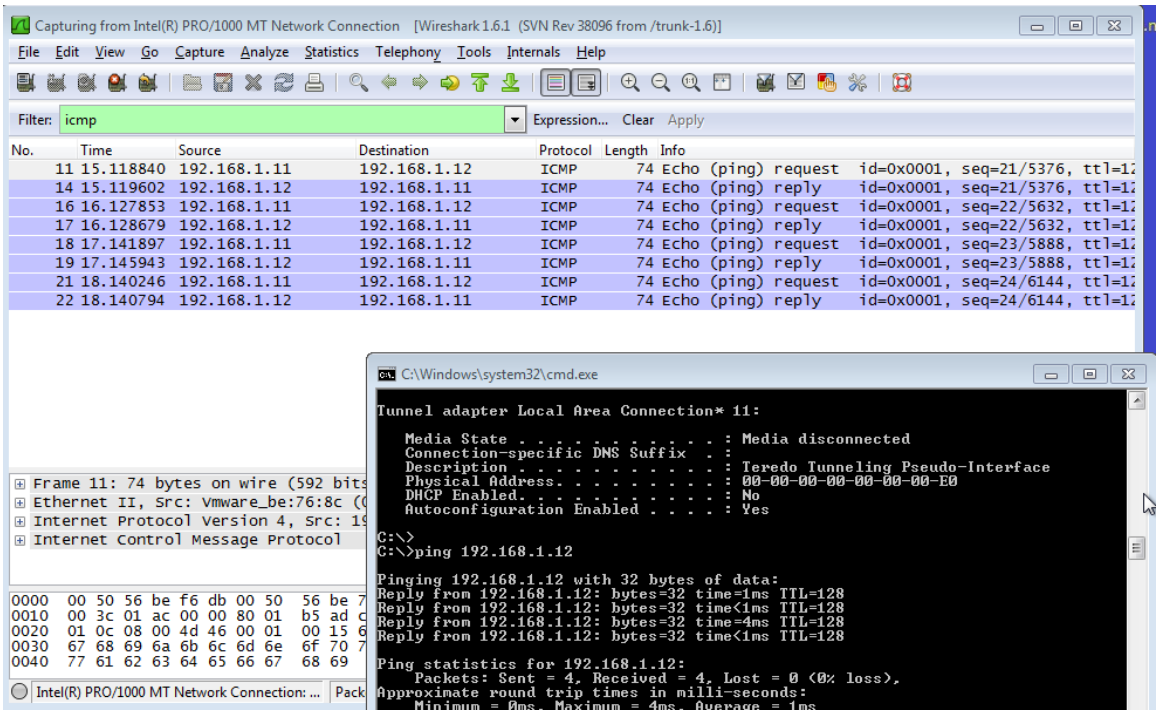
Informacje zaczną pojawiać się w górnej sekcji programu Wireshark. W zależności od typu protokołu, linie z danymi będą pojawiać się w różnych kolorach.



e. Ilość napływających danych może być bardzo duża i zależy od intensywności komunikacji między twoim PC a siecią LAN. Możemy nałożyć filtr, by ułatwić przeglądanie i pracę z danymi przechwytywanymi przez Wireshark. Dla celów tego laboratorium interesują nas tylko PDU typu ICMP (ping). By przeglądać tylko PDU typu ICMP (ping), w polu Filter, znajdującym się w górnej części programu Wireshark wpisz **icmp** i kliknij przycisk **Apply** lub naciśnij Enter.

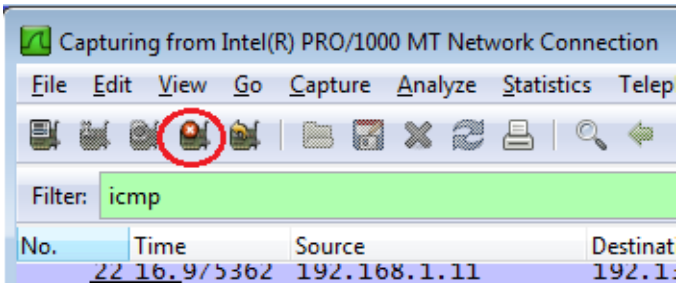


f. Ten filtr spowoduje zniknięcie wszystkich danych w głównym oknie aplikacji, jednak nadal są one przechwytywane na interfejsie. Przywróć okno wiersza poleceń, które wcześniej otworzyłeś i wyślij test ping na adres IP otrzymany od twojego kolegi z zajęć. Zauważ, że w głównym oknie programu Wireshark, ponownie pojawią się dane.



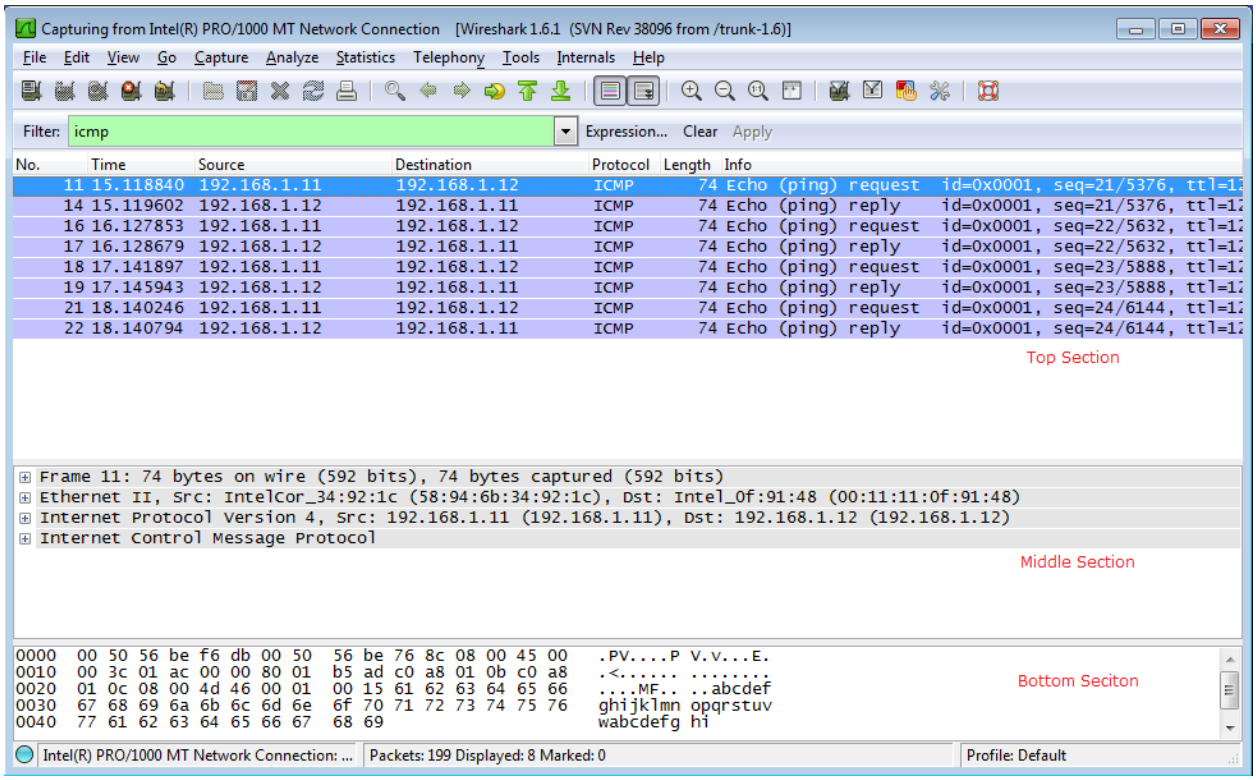
Uwaga: Jeżeli komputer twojego kolegi z zajęć nie odpowiada na test ping, możliwe, że jego firewall blokuje twoje zapytania. Zobacz Dodatek A: Umożliwienie ruchu ICMP przez zaporę ogniową by uzyskać więcej informacji na temat odblokowania ruchu ICMP w zaporze ogniowej systemu Windows 7.

g. Zatrzymaj proces przechwytywania danych klikając ikonę **Stop Capture**.

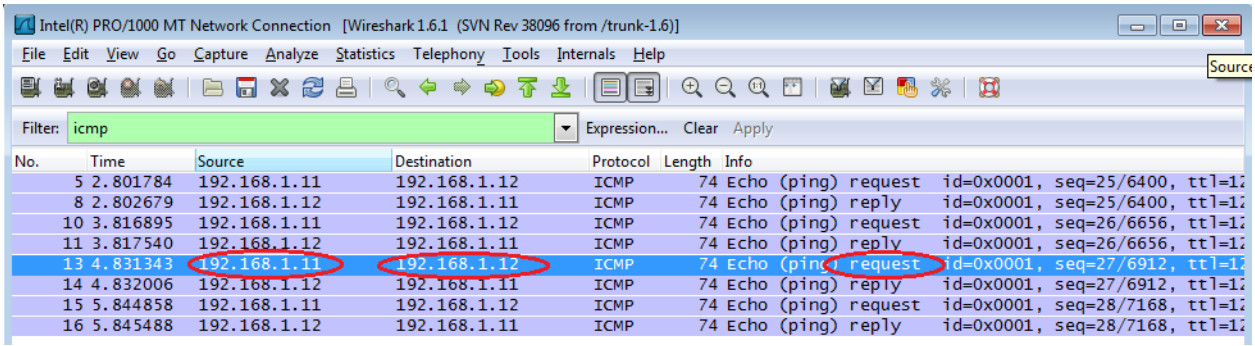


Krok 3: Analiza przechwyconych danych.

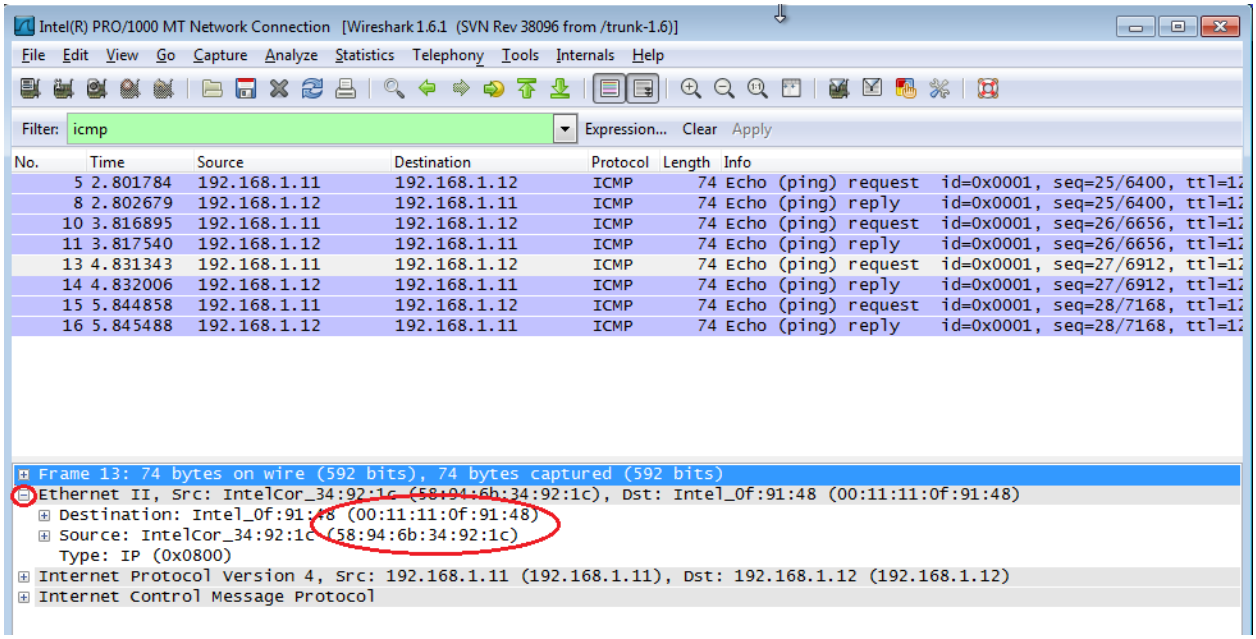
W 3 Kroku przeanalizuj dane, wygenerowane przez żądania ping, wysyłane do komputera twojego kolegi z zajęć. W programie Wireshark, dane te są wyświetlane w trzech sekcjach: 1) Górna sekcja wyświetla listę ramek PDU wraz z podsumowaniem informacji o danym pakiecie IP, 2) środkowa sekcja wyświetla informacje na temat ramki PDU zaznaczonej w górnej części ekranu oraz dzieli ją na bazie poszczególnych warstw protokołów, i 3) dolna sekcja wyświetla nieprzetworzone dane dla poszczególnej warstwy. Nieprzetworzone dane są wyświetlane w trybie szesnastkowym (heksadecymalnym) oraz dziesiętnym.



a. Kliknij na pierwsze żądanie ICMP z listy ramek PDU w górnej sekcji programu Wireshark. Zwróć uwagę, że w kolumnie Source zapisany jest adres IP twojego komputera, a w kolumnie Destination adres IP komputera kolegi z zajęć, na który wysyłałeś żądania ping.



b. Przejdź do środkowej sekcji programu, ramka PDU w sekcji górnej nadal musi być zaznaczona. Kliknij znak plusa znajdujący się po lewej stronie wiersza Ethernet II, by zobaczyć adresy MAC urządzenia źródłowego i docelowego.



Czy adres MAC urządzenia źródłowego pasuje do interfejsu twojego PC? _____

Czy adres MAC urządzenia docelowego w programie Wireshark, pasuje do adresu MAC komputera twojego kolegi z zajęć?_____

W jaki sposób twój PC uzyskał MAC adres komputera PC, na który wysyłałeś żądania ping?

_____

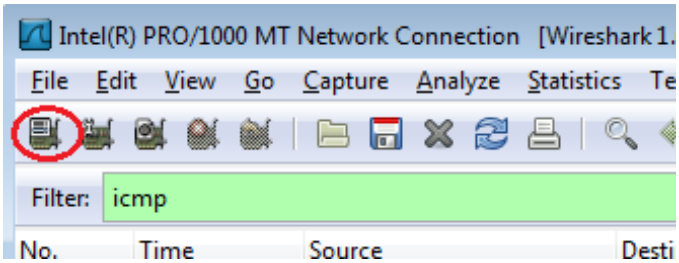
Uwaga: W powyższym przykładzie ilustrującym przechwytywanie żądania ICMP, dane ICMP enkapsulowane są wewnątrz PDU pakietu IPv4 (nagłówek IPv4), który następnie enkapsulowany jest w PDU ramki Ethernet II (nagłówek Ethernet II) i przygotowany do transmisji w sieci LAN.

Część 3: Użycie programu Wireshark do przechwycenia i analizy zdalnych danych ICMP.

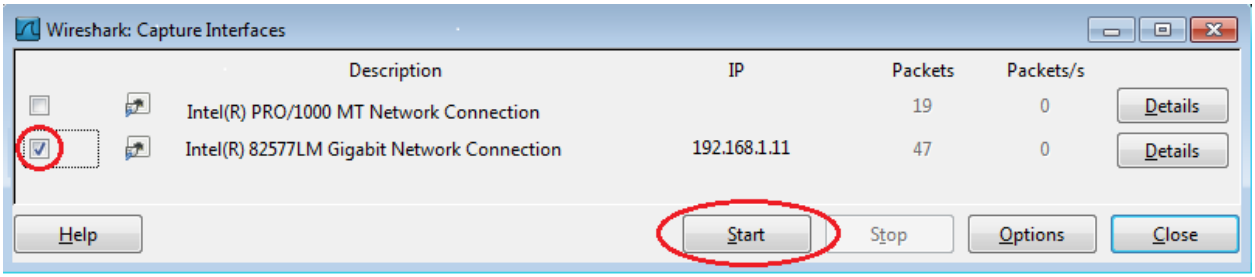
W części 3, wykonasz test ping do zdalnych komputerów (komputerów nie będących w sieci LAN) oraz zbadasz dane wygenerowane przez test ping. Następnie ustalisz, jaka jest różnica między tymi danymi, a danymi zbadanymi w Części 2.

Krok 1: Rozpoczęcie przechwytywania danych z interfejsu.

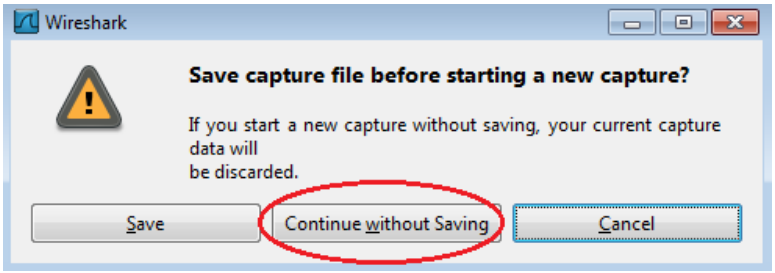
a. Kliknij ikonę **Interface List**, by ponownie przywołać listę interfejsów twojego PC.



b. Upewnij się, że pole wyboru obok interfejsu LAN jest zaznaczone, a następnie kliknij **Start**.

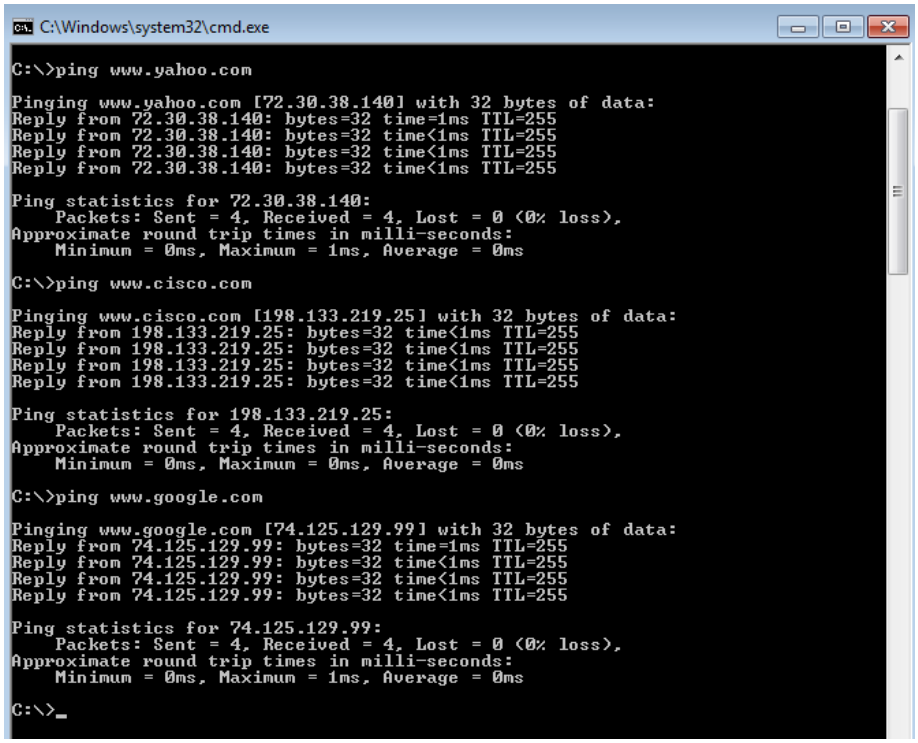


c. Przed rozpoczęciem nowego procesu przechwytywania, pojawi się okno informujące o możliwości zapisania wcześniej przechwyconych danych. Nie ma potrzeby ich zapisywać. Kliknij **Continue without Saving**.



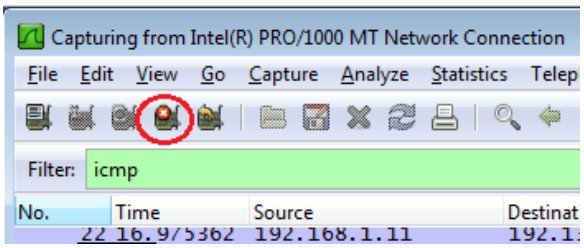
d. Kiedy już proces przechwytywania jest aktywny, wykonaj test ping dla trzech poniższych stron internetowych:

1. www.yahoo.com
2. www.cisco.com
3. www.google.com



Uwaga: Kiedy wykonujesz test ping kolejnych URL zwróć uwagę, że DNS (ang. Domain Name Server) tłumaczy URL na adres IP. Zanotuj adres IP dla każdego URL.

e. Zatrzymaj proces przechwytywania danych klikając ikonę **Stop Capture**.



Krok 2: Badanie i analiza danych otrzymanych z hostów zdalnych.

a. Przejrzyj przechwycone dane w programie Wireshark, sprawdź adresy IP i MAC trzech stron internetowych dla których wykonałeś polecenie ping. Poniżej wpisz, docelowy adres IP i MAC dla wszystkich trzech stron internetowych.

1st Lokalizacja: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

2nd Lokalizacja: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

3rd Lokalizacja: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

b. Co jest istotne w tej informacji?

_____

c. Czym różni się ta informacja od informacji uzyskanej w części 2, dotyczącej używania polecenia ping w sieci lokalnej?

_____

_____

Do przemyślenia

Dlaczego Wireshark pokazuje aktualny adres MAC dla hostów lokalnych, ale już nie pokazuje aktualnego MAC dla hostów zdalnych?

_____

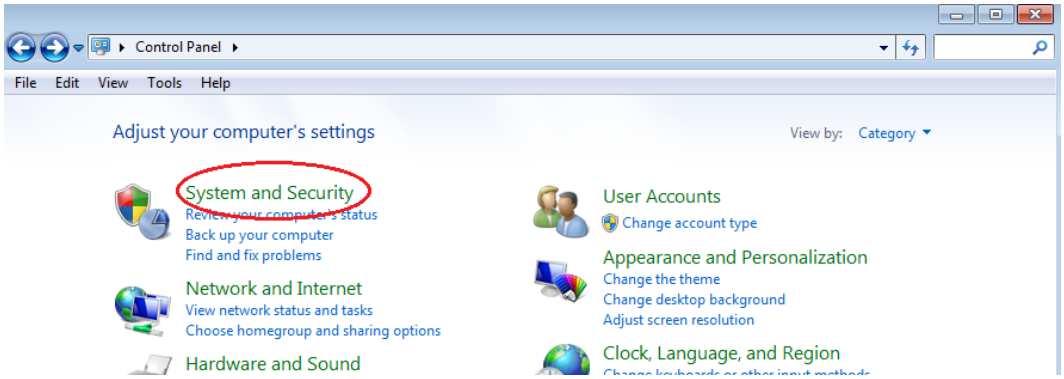
_____

Dodatek A: Umożliwienie ruchu ICMP przez zaporę ogniową

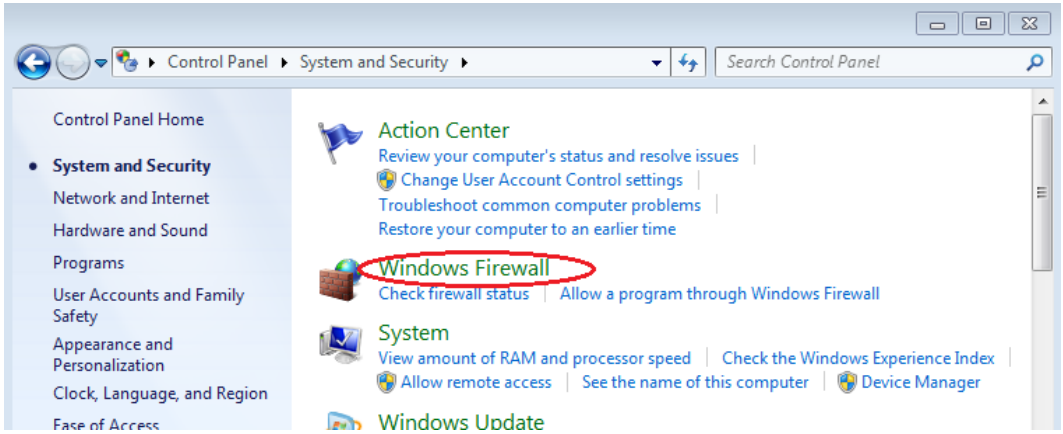
Jeżeli koledzy z zajęć nie otrzymują odpowiedzi z twojego PC na wysyłane żądania ping, prawdopodobnie zapora ogniowa blokuje te prośby. Niniejszy dodatek opisuje w jaki sposób stworzyć regułę w zaporze ogniowej, umożliwiającą przesyłanie żądań ping. Ponadto opisuje jak wyłączyć stworzoną regułę ICMP, gdy już ukończysz laboratorium.

Krok 1: Utworzenie nowej reguły przychodzącej, zezwalającej na ruch ICMP przez zaporę ogniową.

a. W Panelu Sterowania, kliknij opcję **System and Security (System i zabezpieczenia)**.

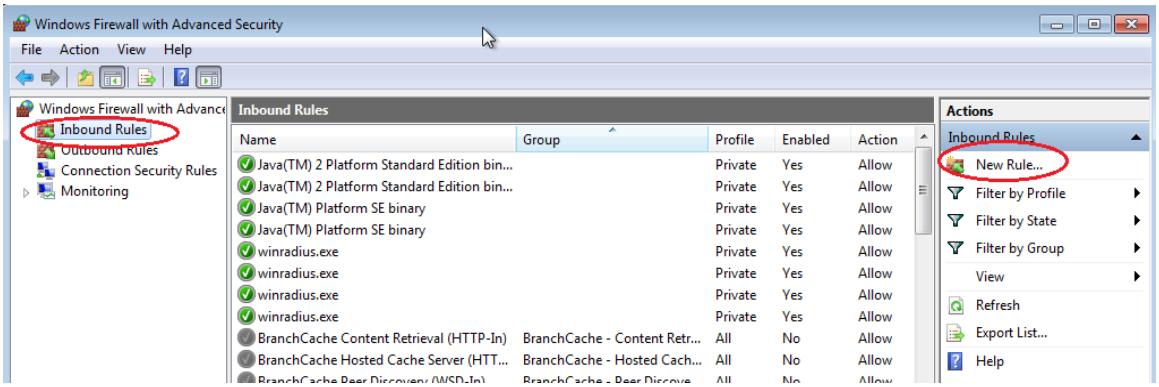


b. W oknie System i zabezpieczenia, kliknij **Windows Firewall (Zapora systemu Windows)**.

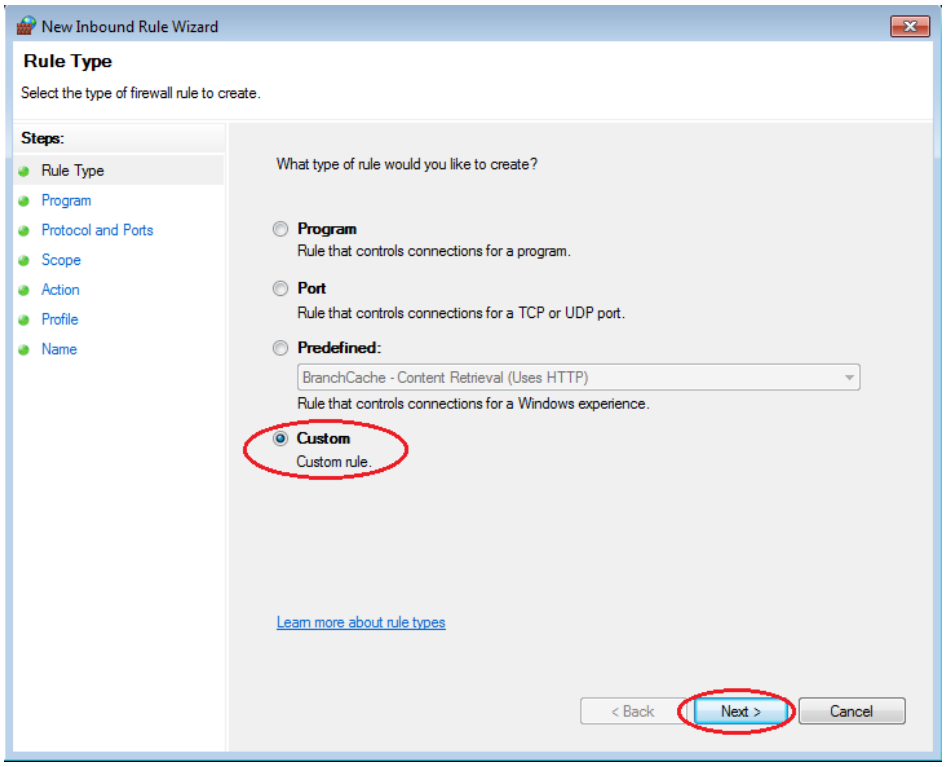


c. W lewym panelu okna Zapora systemu Windows, kliknij **Advanced settings (Ustawienia zaawansowane)**.

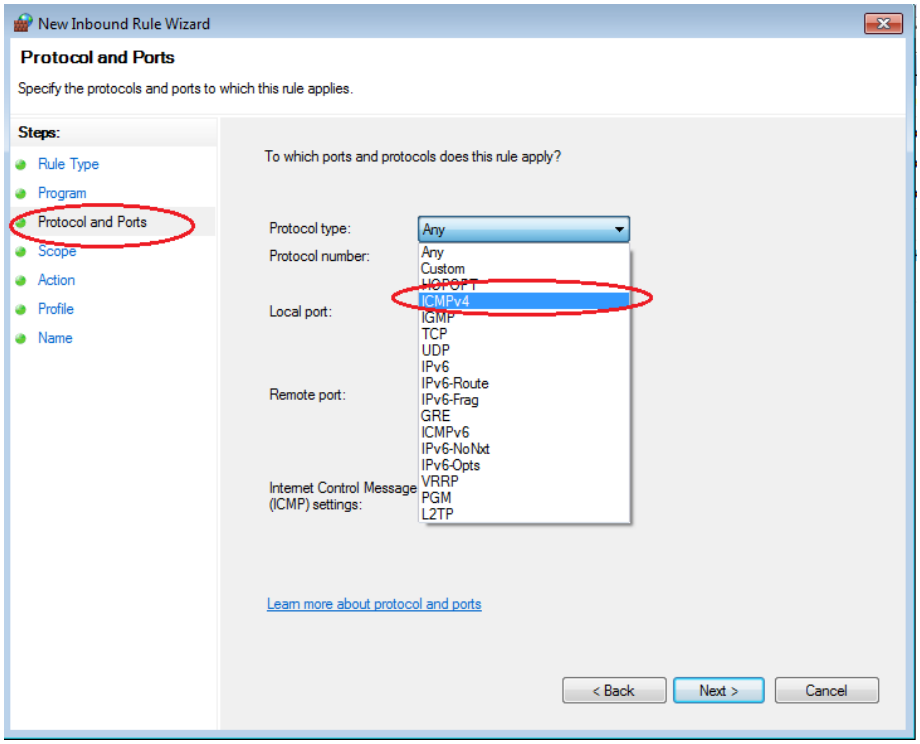
d. W lewym panelu okna Ustawienia zaawansowane, wybierz opcję **Inbound Rules** (**Reguły przychodzące)**, a następnie w prawym panelu kliknij **New Rule…** (**Nowa reguła…)**.



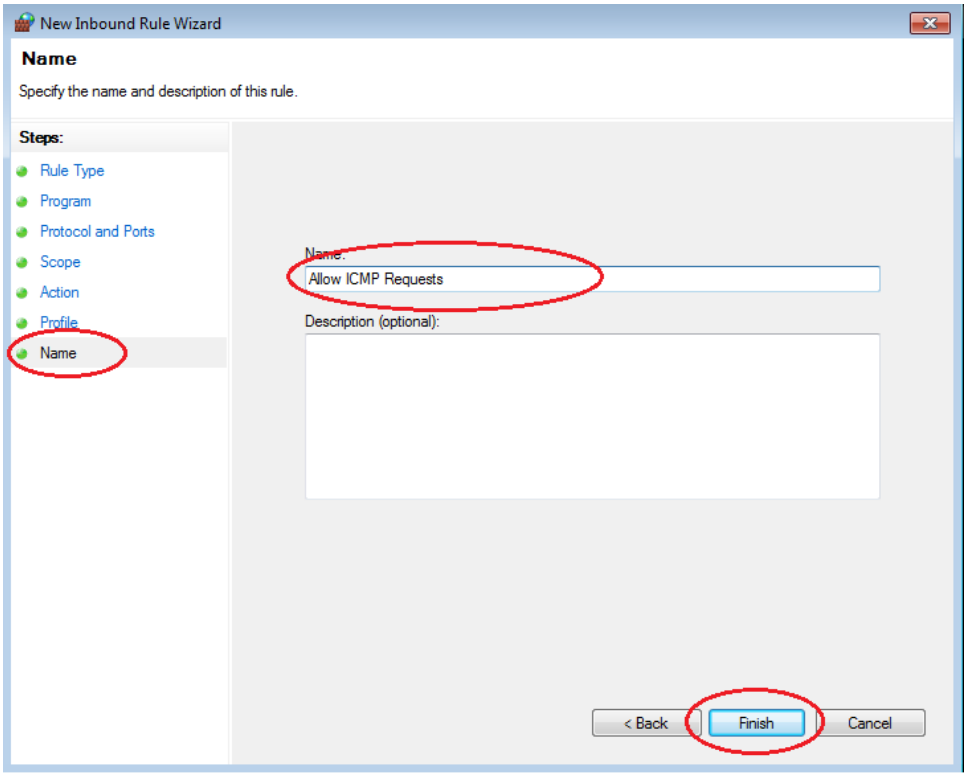
e. Spowoduje to uruchomienie Kreatora nowej reguły ruchu przychodzącego. Na ekranie Typ reguły, zaznacz opcję **Custom (Niestandardowa)**, a następnie kliknij przycisk **Next (Dalej)**



f. W lewym panelu, kliknij opcję **Protocol and Ports** (**Protokół i porty)** i używając rozwijanego menu, wybierz **ICMPv4**, a następnie kliknij **Next (Dalej)**.



g. W lewym panelu, kliknij opcję **Name (Nazwa)** i w polu Name (Nazwa) wpisz **Allow ICMP Requests**. Kliknij **Finish (Zakończ)**.

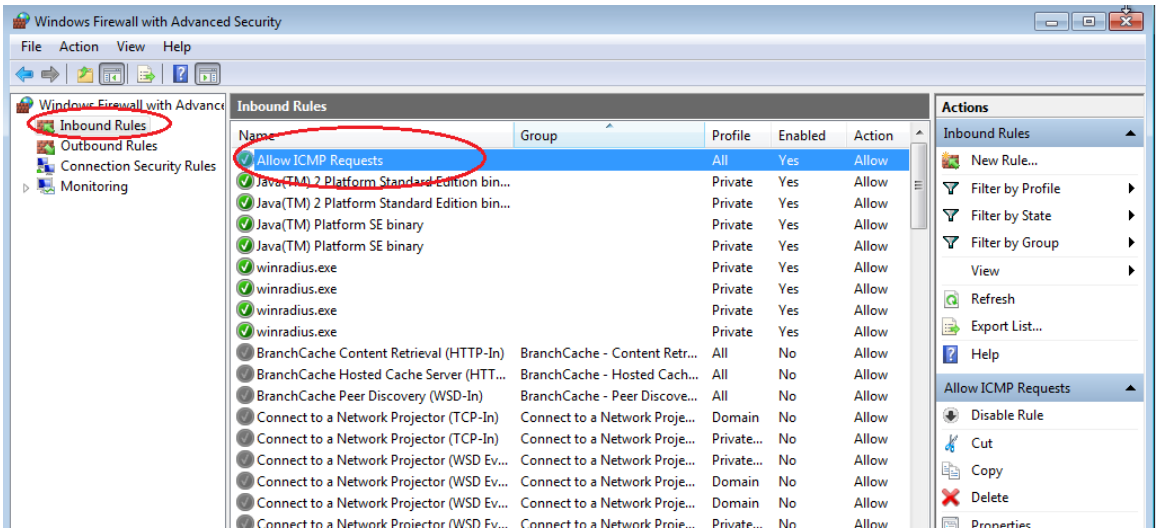


Ta nowa reguła powinna umożliwić twoim kolegom z zajęć otrzymanie odpowiedzi ping z twojego PC.

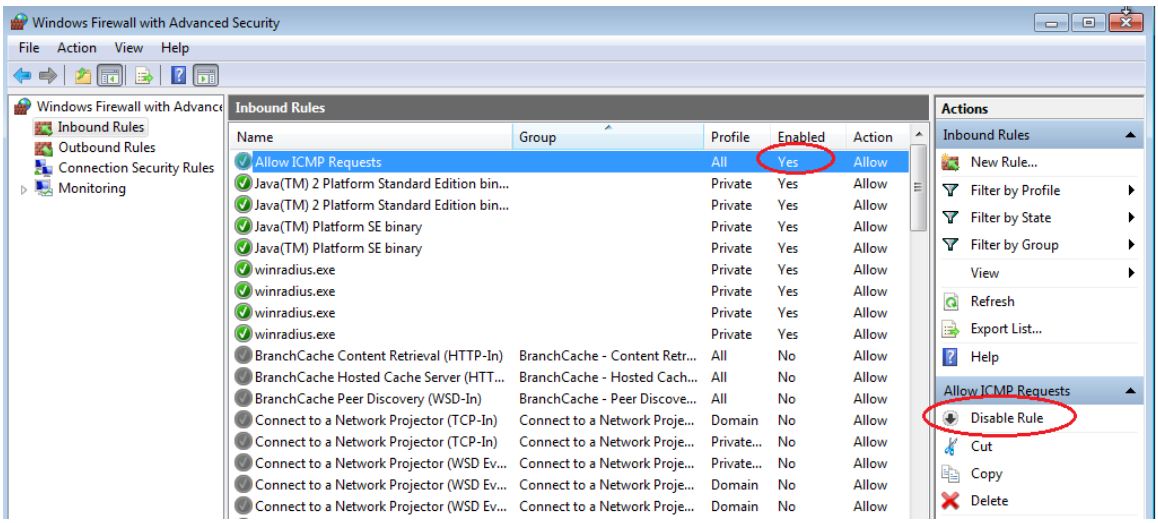
Krok 2: Wyłączenie lub usunięcie nowej reguły ICMP.

Po zakończeniu laboratorium możesz chcieć wyłączyć lub nawet usunąć, regułę którą stworzyłeś w kroku 1. Użycie opcji **Disable Rule (Wyłącz regułę)** umożliwi ci jej ponowne włączenie w późniejszym czasie. Skasowanie reguły, permanentnie usuwa ją z listy Inbound Rules (Reguły przychodzące).

a. W lewym panelu okna Ustawienia zaawansowane, kliknij **Inbound Rules (Reguły przychodzące)**, a następnie znajdź regułę, którą utworzyłeś w kroku 1.



b. Aby wyłączyć regułę, kliknij opcję **Disable Rule (Wyłącz regułę)**. Gdy już wybierzesz tą opcję, zauważysz, że przemieni się ona na **Enable Rule (Włącz regułę)**. W ten sposób możesz aktywować i dezaktywować regułę; stan reguły jest również widoczny w kolumnie Enabled (Włączony) listy Inbound Rules (Reguły przychodzące).



c. Aby na stałe usunąć regułę ICMP, kliknij **Delete (Usuń)**. Jeśli wybierzesz tę opcję, będziesz musiał ponownie utworzyć regułę by umożliwić wysyłanie odpowiedzi ICMP