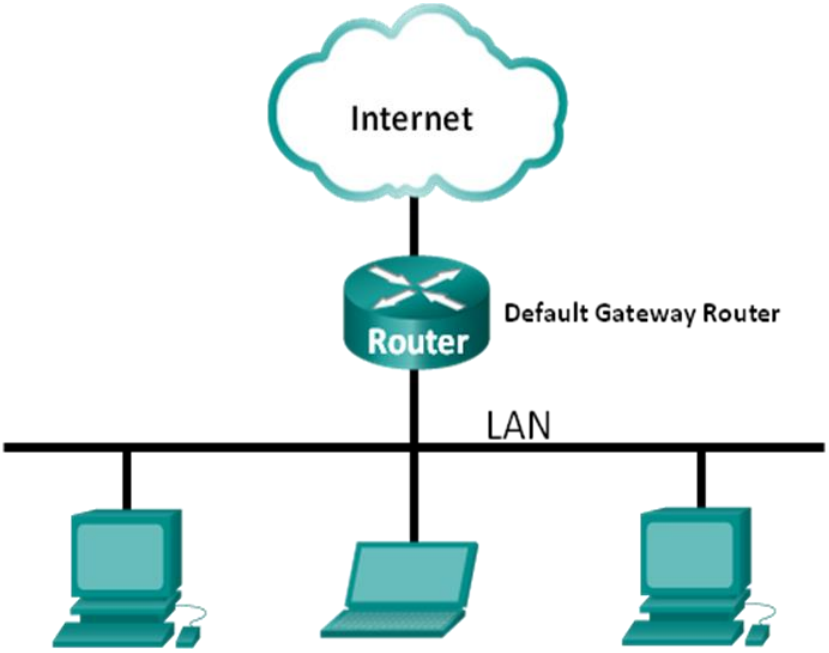
Laboratorium - Używanie programu Wireshark do badania ruchu sieciowego

Topologia



Cele

Część 1: 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 2: 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: Użycie programu Wireshark do przechwycenia i analizy lokalnych danych ICMP.

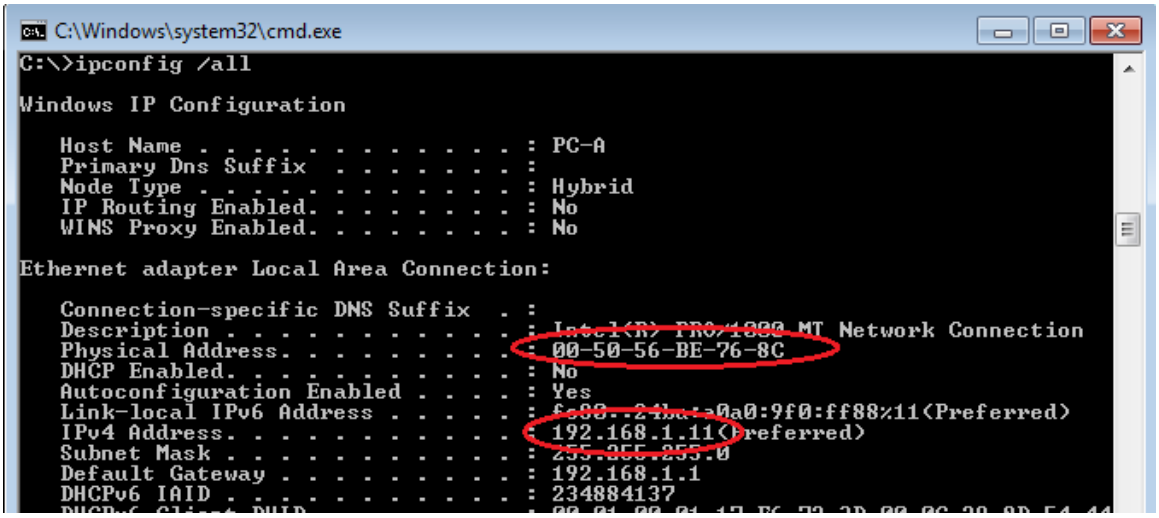
W 2 części tego ćwiczenia będziesz wysyłać pakiety ping do innego komputera w sieci lokalnej i przechwycisz żądania i odpowiedzi ICMP w programie Wireshark. Ponadto zajrzysz do wnętrza przechwyconych ramek w celu znalezienia konkretnych informacji. Analiza ta powinna przyczynić się do wyjaśnienia, w 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.

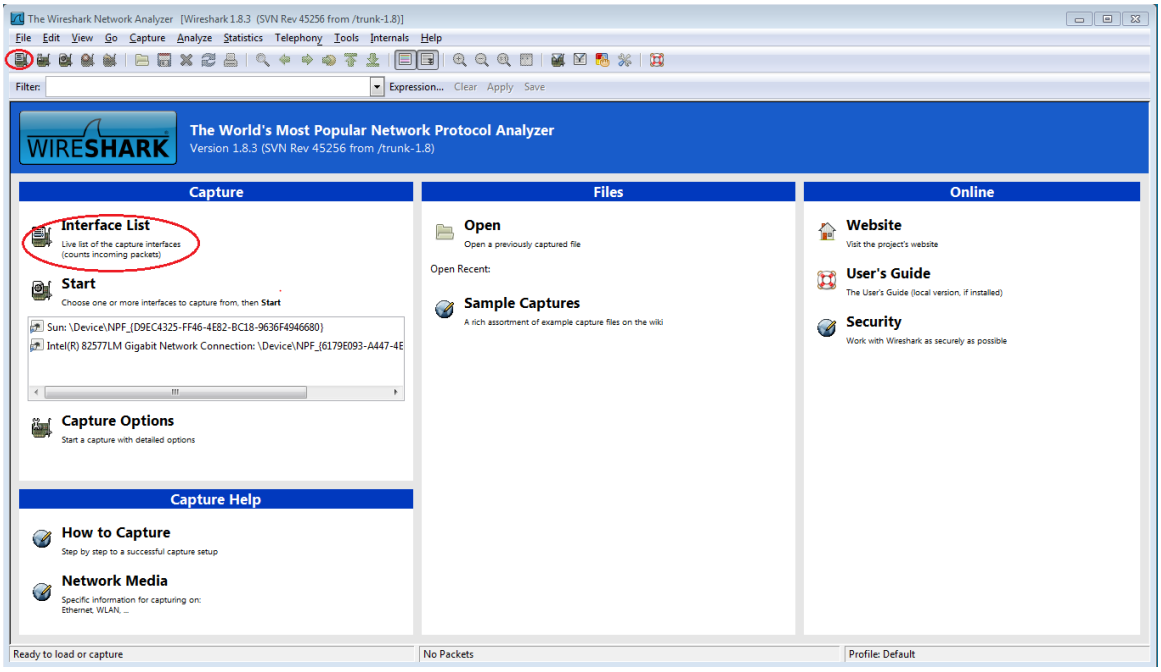


c. Poproś innych uczestników o ich adresy IP oraz przekaż im swój. Nie podawaj im swojego adresu MAC.

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

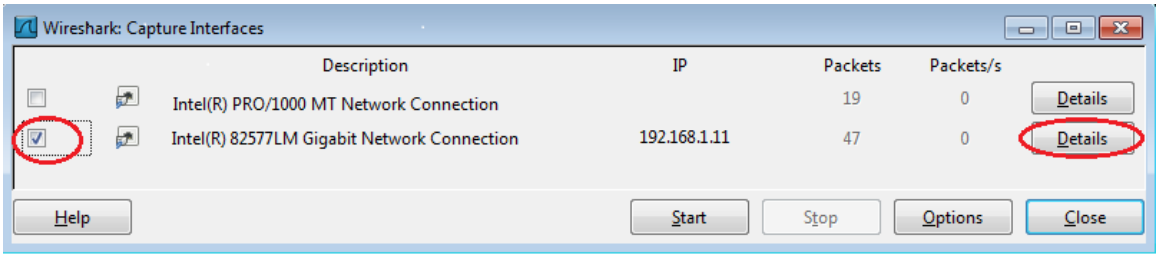
a. Na swoim komputerze, kliknij przycisk **Start** systemu Windows i w menu podręcznym znajdź program Wireshark. Kliknij dwukrotnie **Wireshark**.

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

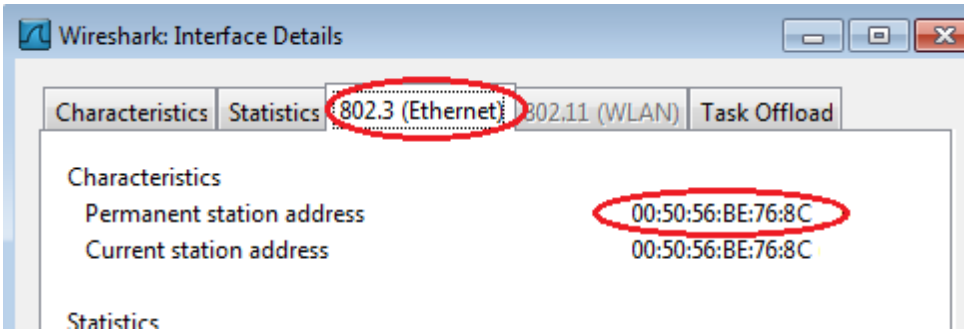


Uwaga: Kliknięcie na pierwszą ikonę z lewej strony w pasku narzędzi również otworzy Interface List.

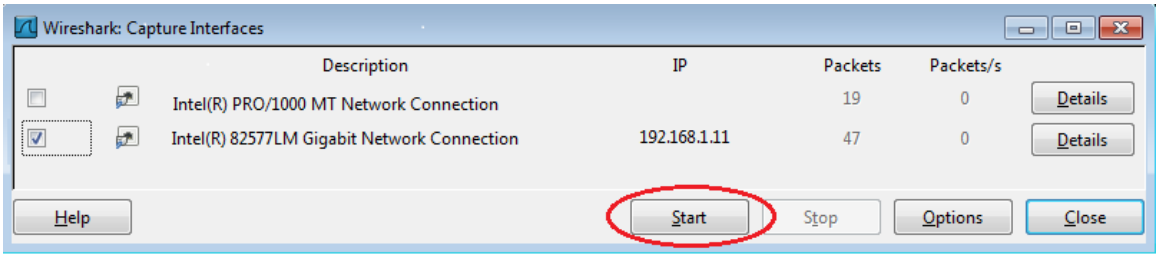
c. W oknie Wireshark: Capture Interfaces, kliknij pole wyboru (zaznacz je) odpowiadające interfejsowi podłączonemu do twojej sieci LAN.



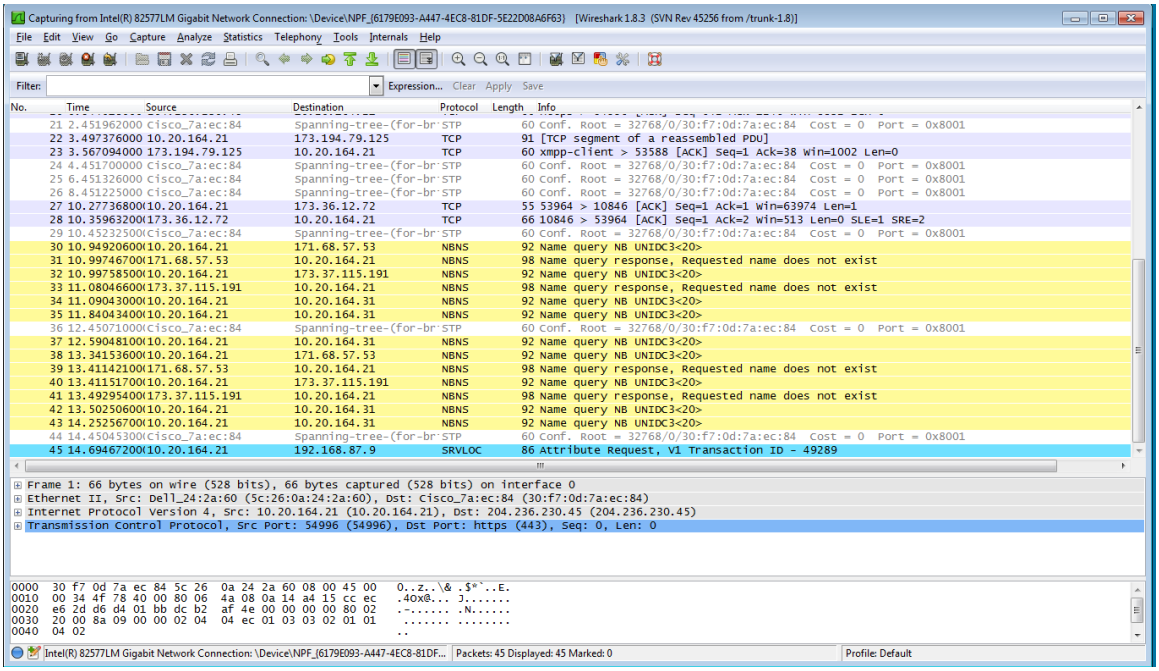
Uwaga: Jeżeli w wykazie znajduje się wiele interfejsów, a nie jesteś pewien, który z nich zaznaczyć, kliknij przycisk **Details** oraz otwórz zakładkę **802.3 (Ethernet)**. Sprawdź czy adres MAC jest taki sam jak ten, który zapisałeś w kroku 1b. Po pomyślnej weryfikacji zamknij okno Interface Details.



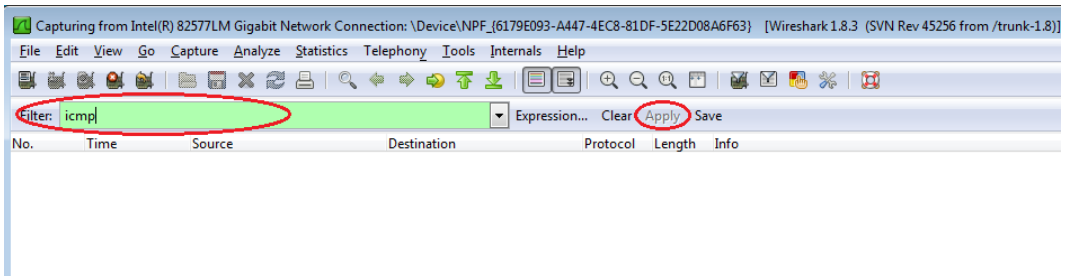
d. Po wybraniu właściwego interfejsu, kliknij **Start** by rozpocząć przechwytywanie danych.



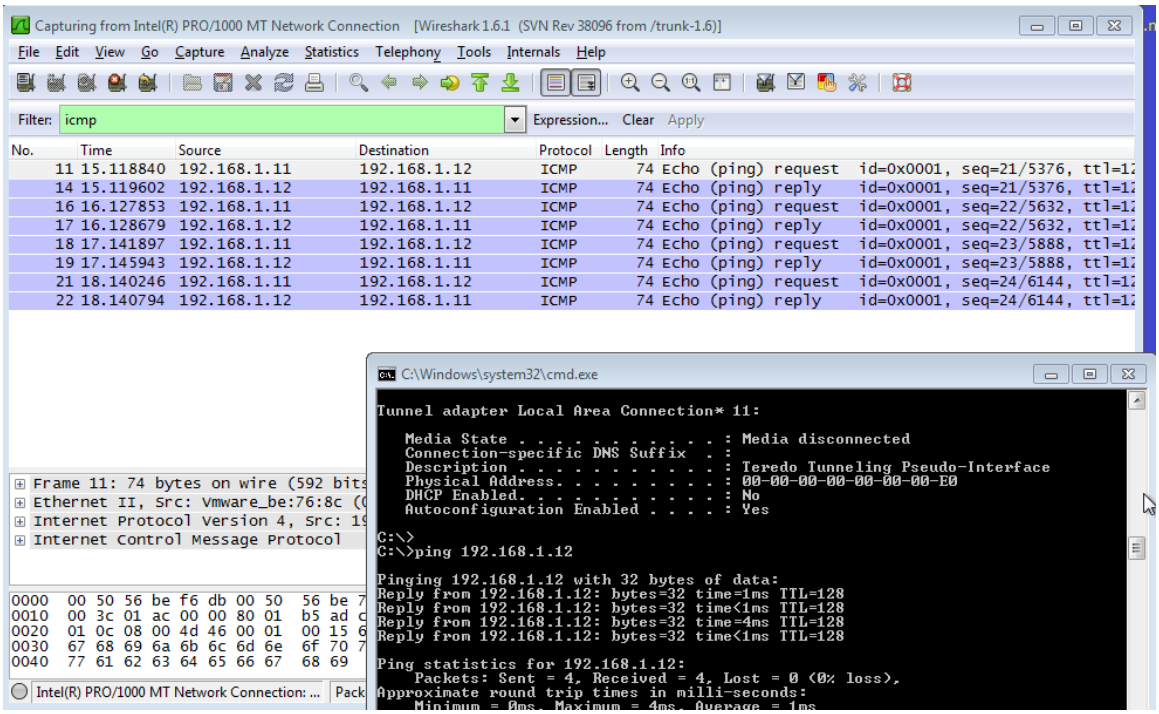
Informacje zaczną pojawiać się w górnej sekcji programu Wireshark. W zależności od typu protokołu, linie z danymi będą pojawiać się w różnych kolorach.



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.

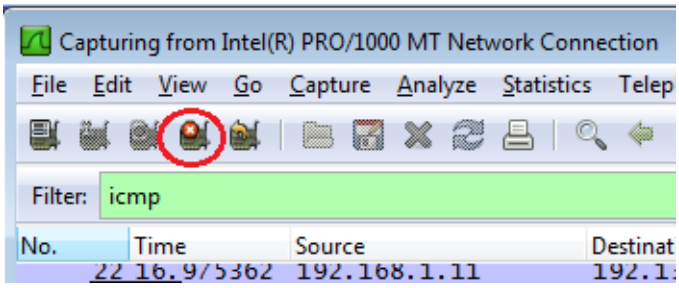


f. Ten filtr spowoduje zniknięcie wszystkich danych w głównym oknie aplikacji, jednak nadal są one przechwytywane na interfejsie. Przywróć okno wiersza poleceń, które wcześniej otworzyłeś i wyślij test ping na adres IP otrzymany od twojego kolegi z zajęć. Zauważ, że w głównym oknie programu Wireshark,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



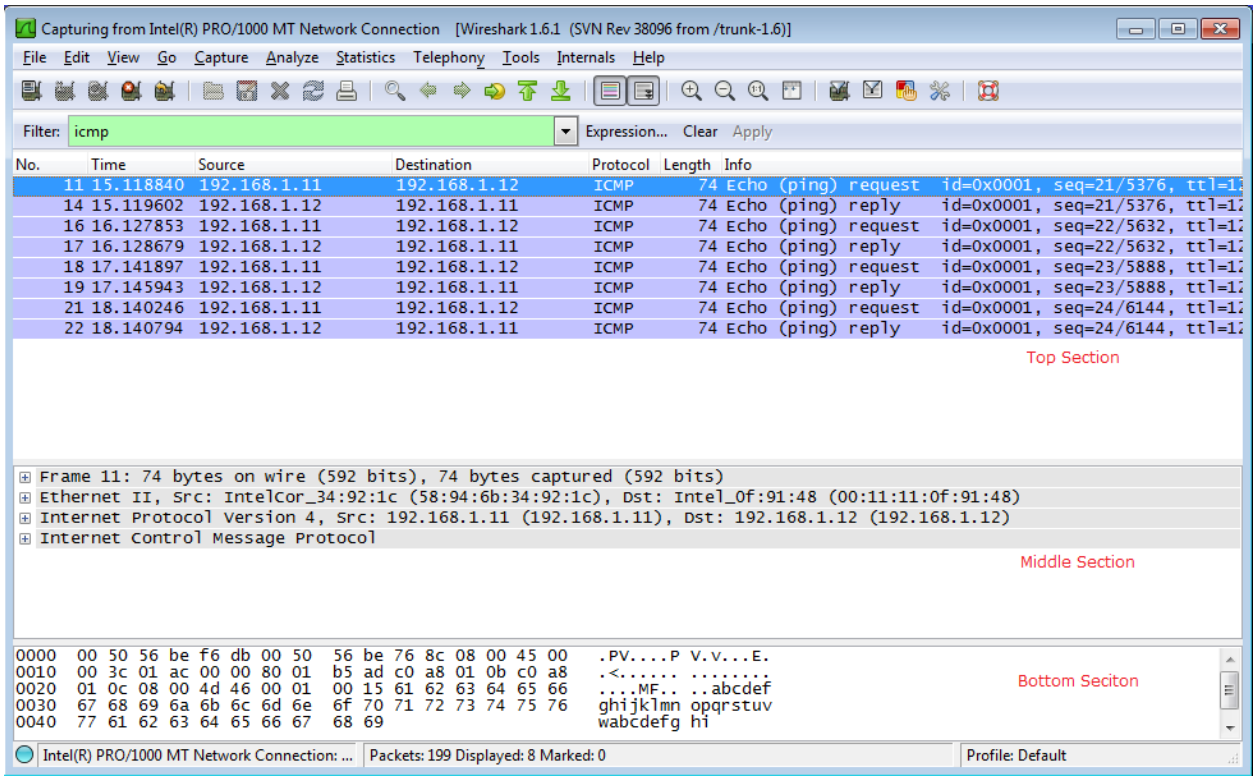
Uwaga: Jeżeli komputer twojego kolegi z zajęć nie odpowiada na test ping, możliwe, że jego firewall blokuje twoje zapytania. Zobacz **Błąd! Nie można odnaleźć źródła odwołania.** by uzyskać więcej informacji na temat odblokowania ruchu ICMP w zaporze ogniowej systemu Windows 7.

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

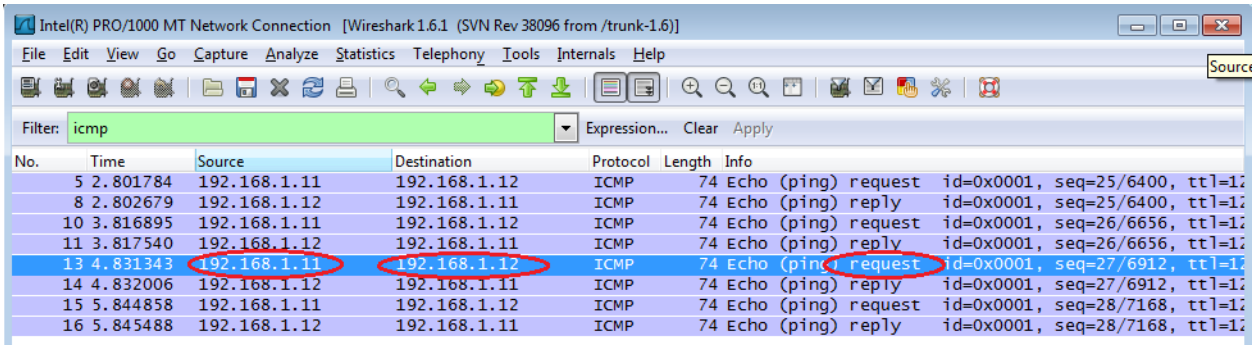


Krok 3: Analiza przechwyconych danych.

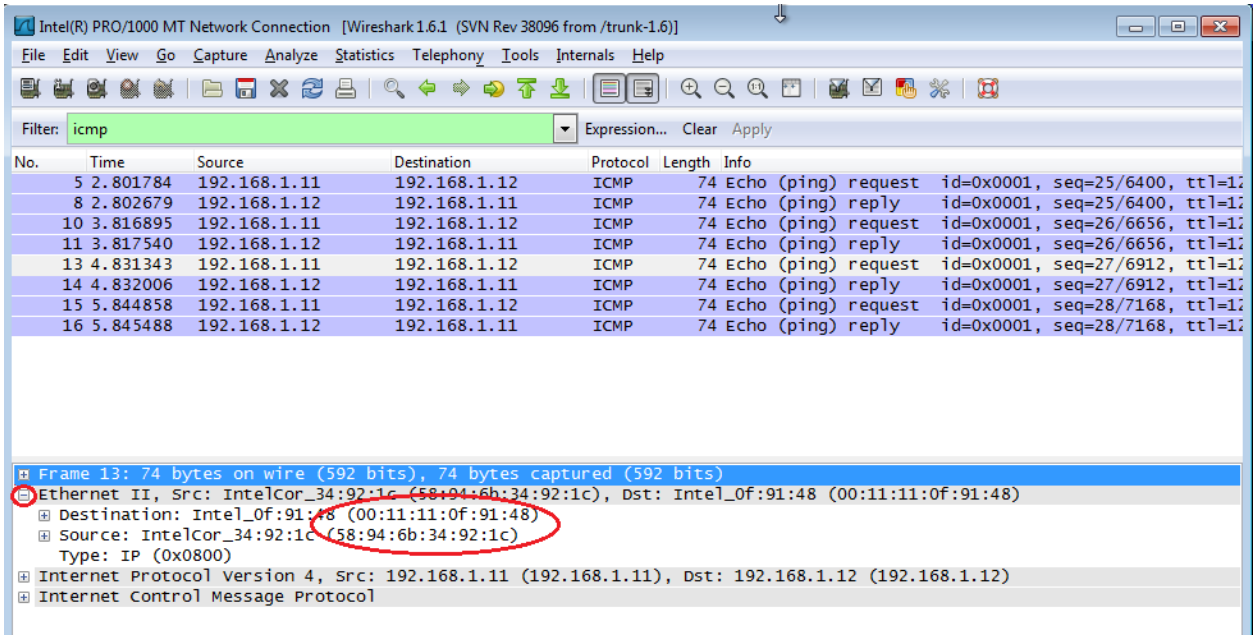
W 3 Kroku przeanalizuj dane, wygenerowane przez żądania ping, wysyłane do komputera twojego kolegi z zajęć. W programie Wireshark, dane te są wyświetlane w trzech sekcjach: 1) Górna sekcja wyświetla listę ramek PDU wraz z podsumowaniem informacji o danym pakiecie IP, 2) środkowa sekcja wyświetla informacje 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?

_____

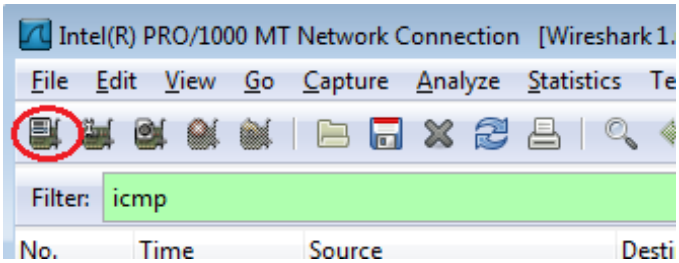
Uwaga: W powyższym przykładzie ilustrującym przechwytywanie żądania ICMP, dane ICMP enkapsulowane są wewnątrz PDU pakietu IPv4 (nagłówek IPv4), który następnie enkapsulowany jest w PDU ramki Ethernet II (nagłówek Ethernet II) i przygotowany do transmisji w sieci LAN.

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

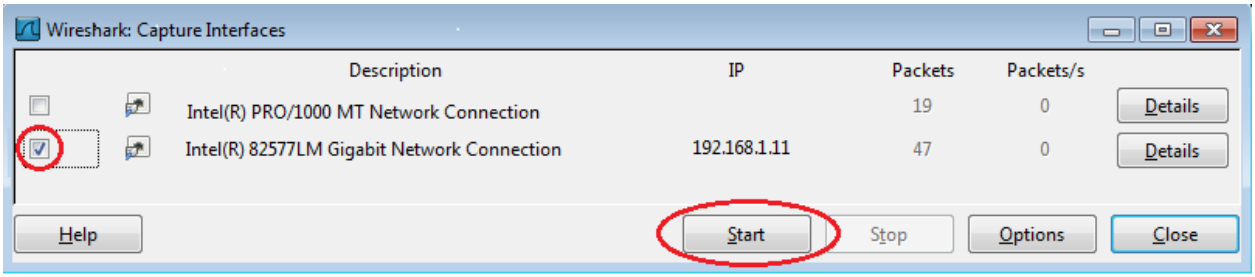
W części 3, wykonasz test ping do zdalnych komputerów (komputerów nie będących w sieci LAN) oraz zbadasz dane wygenerowane przez test ping. Następnie ustalisz, jaka jest różnica między tymi danymi, a danymi zbadanymi w Części 2.

Krok 1: Rozpoczęcie przechwytywania danych z interfejsu.

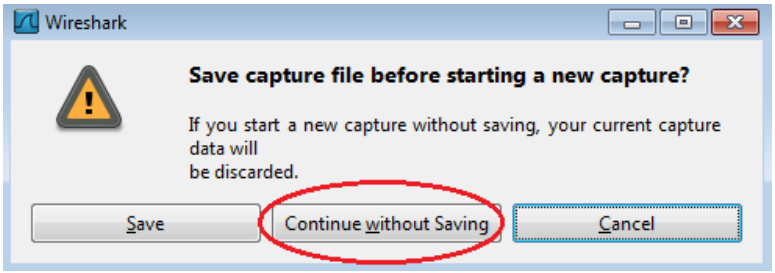
a. Kliknij ikonę **Interface List**, by ponownie przywołać listę interfejsów twojego PC.



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

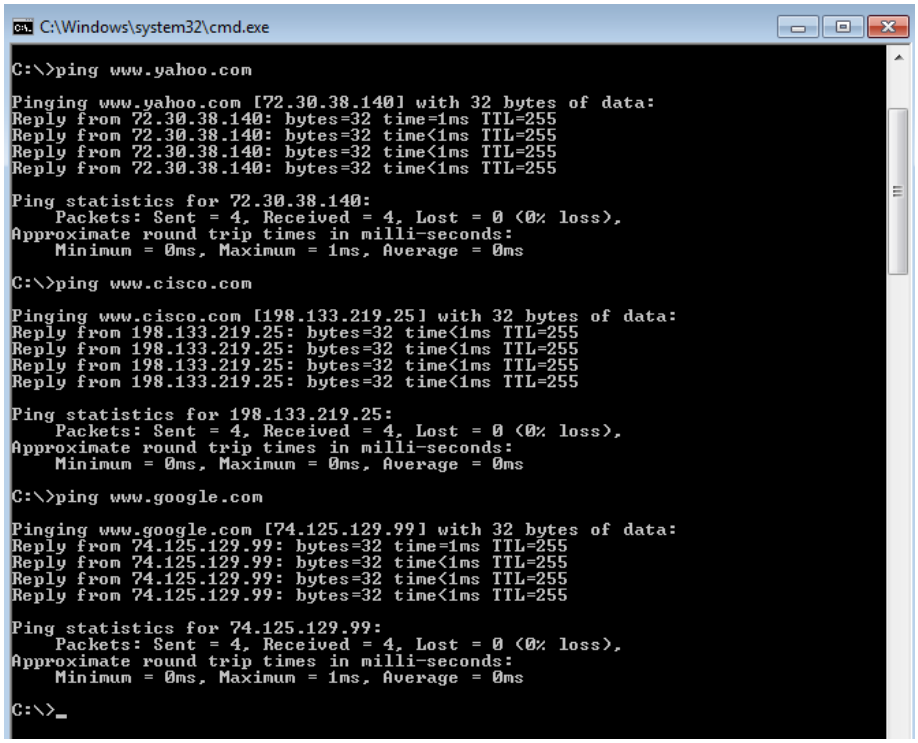


c. Przed rozpoczęciem nowego procesu przechwytywania, pojawi się okno informujące o możliwości zapisania wcześniej przechwyconych danych. Nie ma potrzeby ich zapisywać. Kliknij **Continue without Saving**.



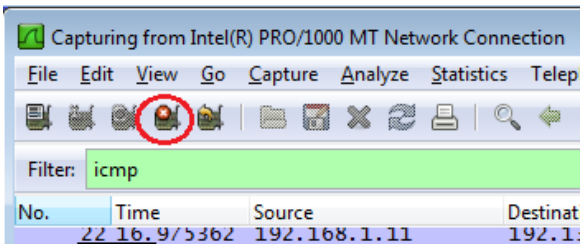
d. Kiedy już proces przechwytywania jest aktywny, wykonaj test ping dla trzech poniższych stron internetowych:

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?

_____

_____