Instrukcja laboratoryjna dla „Sieci komputerowe i Internet” – Moduł 2, Zadanie 1 *– Radosław Terelak*

1. Cele zadania laboratoryjnego:

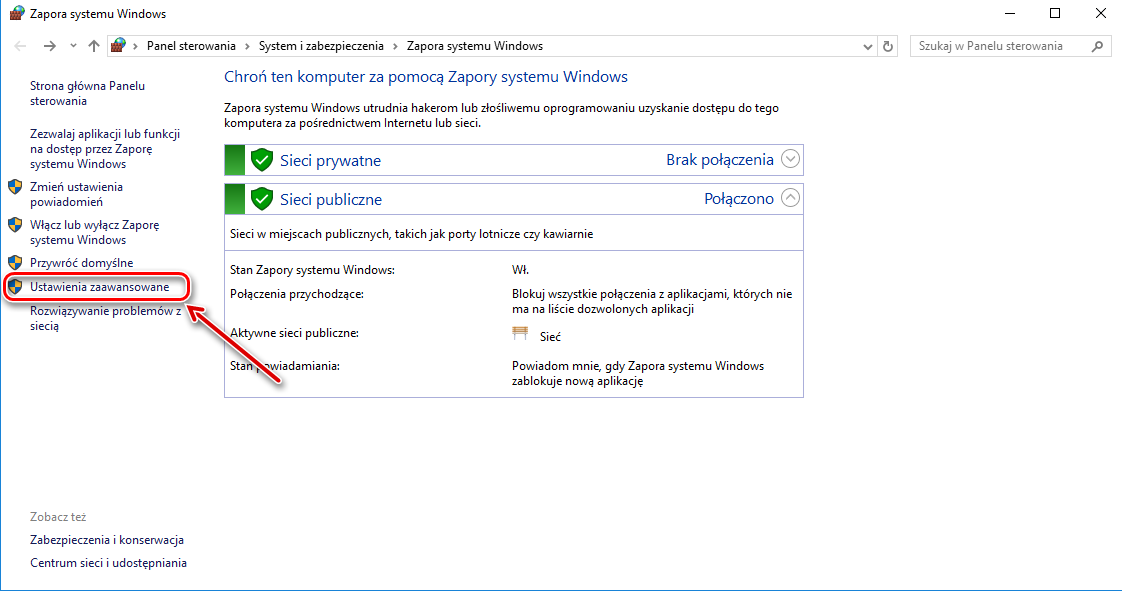
Celem zadania laboratoryjnego jest zaznajomienie się z przykładem oprogramowania typu „sniffer pakietów”, umożliwiającego przechwytywanie i przeglądanie pakietów na wybranym interfejsie sieciowym, na przykładzie aplikacji „Wireshark”.

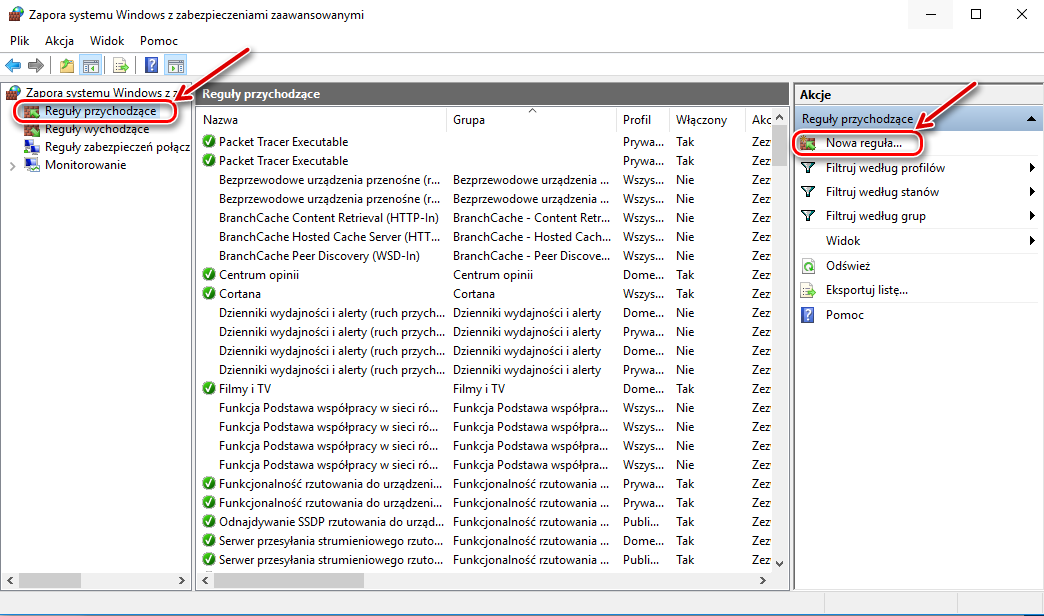
W ramach zadania aplikacja Wireshark zostanie użyta do przechwycenia i analizy transmisji protokołu ICMP, z wykorzystaniem aplikacji „ping”, skierowanej najpierw do urządzenia znajdującego się w lokalnej sieci komputerowej, a następnie w zdalnej sieci komputerowej. Analiza ta ma udowodnić, iż urządzenia komunikując się przez sieć komputerową z innym urządzeniem w tej samej sieci lokalnej realizuje tą komunikację bezpośrednio, bez potrzeby użycia urządzenia jakim jest ruter, natomiast podczas komunikacji z urządzeniem w sieci zdalnej, komunikacja ta odbywa się za pośrednictwem urządzenia jakim jest ruter.

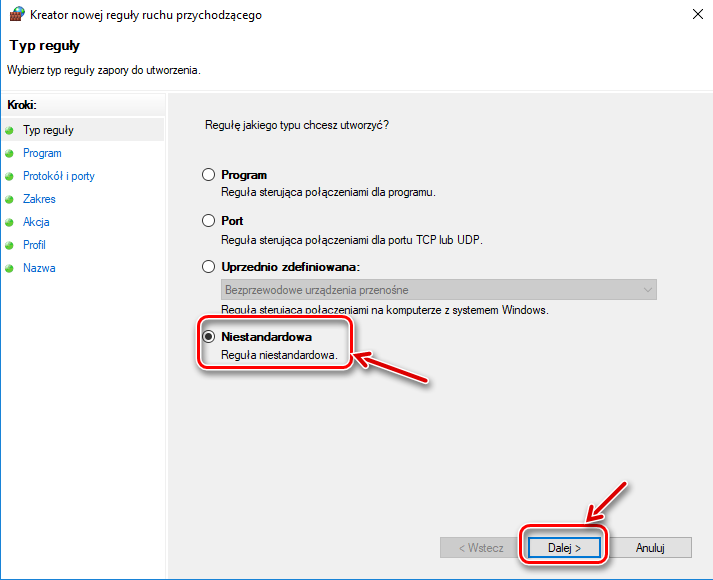
1. Przygotowanie środowiska do zajęć:

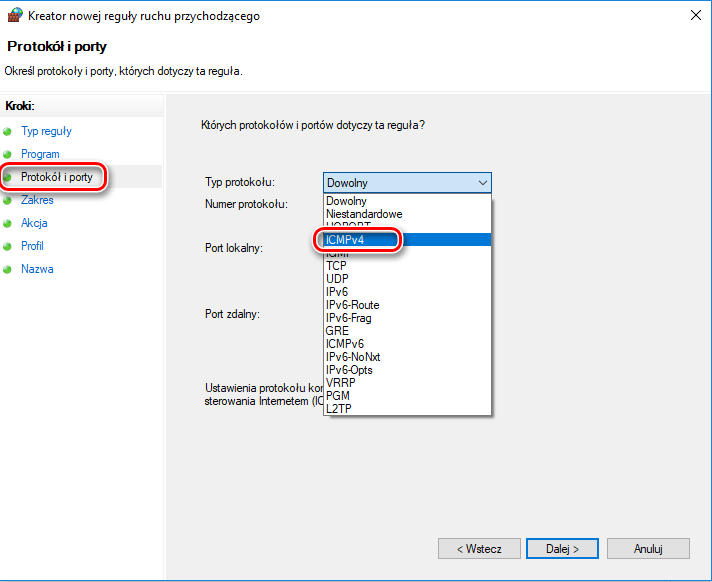
W ramach przygotowania środowiska do wykonania zadania laboratoryjnego, należy uruchomić aplikację Wireshark (jeżeli nie jest zainstalowana, to najpierw należy ją zainstalować z witryny <https://www.wireshark.org/download.html>).  
  
Ponadto konieczne będzie skonfigurowanie wbudowanej w system Windows zapory ogniowej, w taki sposób, aby system odpowiadał na przesyłane do niego żądania ping (domyślnie zapora ogniowa wbudowana w system Windows blokuje przychodzące żądania ***ping request***). W tym celu należy:

Przejść do ***Panel sterowania\System i zabezpieczenia\Zapora systemu Windows*** a następnie kliknąć na pozycję ***Ustawienia zaawansowane***:

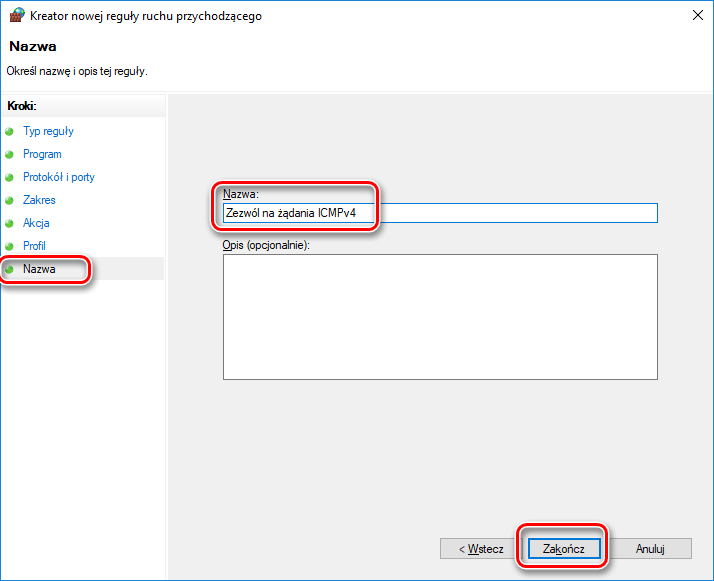


W lewym panelu okna ***Zapora systemu Windows z ustawieniami zaawansowanymi***, należy wybrać opcję ***Reguły przychodzące***, a następnie w prawym panelu kliknąć pozycję ***Nowa reguła…***:  


Nastąpi uruchomienie kreatora nowej reguły ruchu przychodzącego. Na ekranie Typ reguły, zaznaczyć opcję ***Niestandardowa***, a następnie kliknąć przycisk ***Dalej***:  


W oknie kreatora, w lewym panelu, kliknąć opcję ***Protokół i porty***, i używając rozwijanego menu, wybrać opcję ***ICMPv4***, a następnie kliknąć ***Dalej***:  


Następnie w lewym panelu, kliknąć opcję ***Nazwa*** i w polu ***Nazwa*** wpisać jako nazwę ***Zezwól na żądania OCMPv4***. Kliknąć ***Zakończ***:



Ta nowa reguła powinna umożliwić koledze/koleżance z zajęć otrzymanie odpowiedzi ping z twojego PC w ramach jednego z kroków zadania.

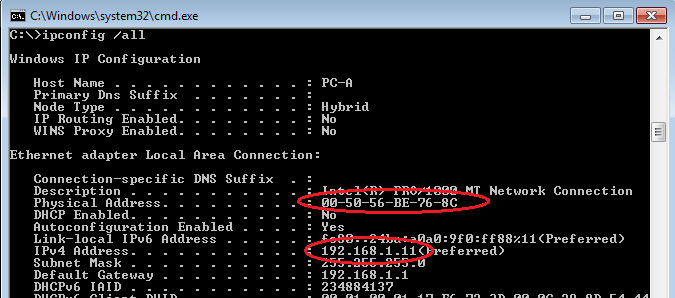
Zadania do realizacji

Krok 1:

Należy odczytać przypisane do interfejsu aktualnie dane adresowe TCP/IP, w tym celu należy:

Otworzyć okno wiersza poleceń w systemie operacyjnym, następnie wpisać polecenie   
***ipconfig /all*** i nacisnąć ***Enter***

Odczytać adres IPv4 oraz adres MAC (tzw. adres fizyczny interfejsu sieciowego) przydzielony dla interfejsu sieciowego, który jest wykorzystywany aktualnie do komunikacji z siecią Internet (w systemie Windows od 8 wzwyż, najczęściej to będzie interfejs o nazwie „Ethernet”):



Zanotuj odczytane ustawienia konfiguracyjne wykorzystywane przez interfejs sieciowy (adres IP, oraz adres MAC):

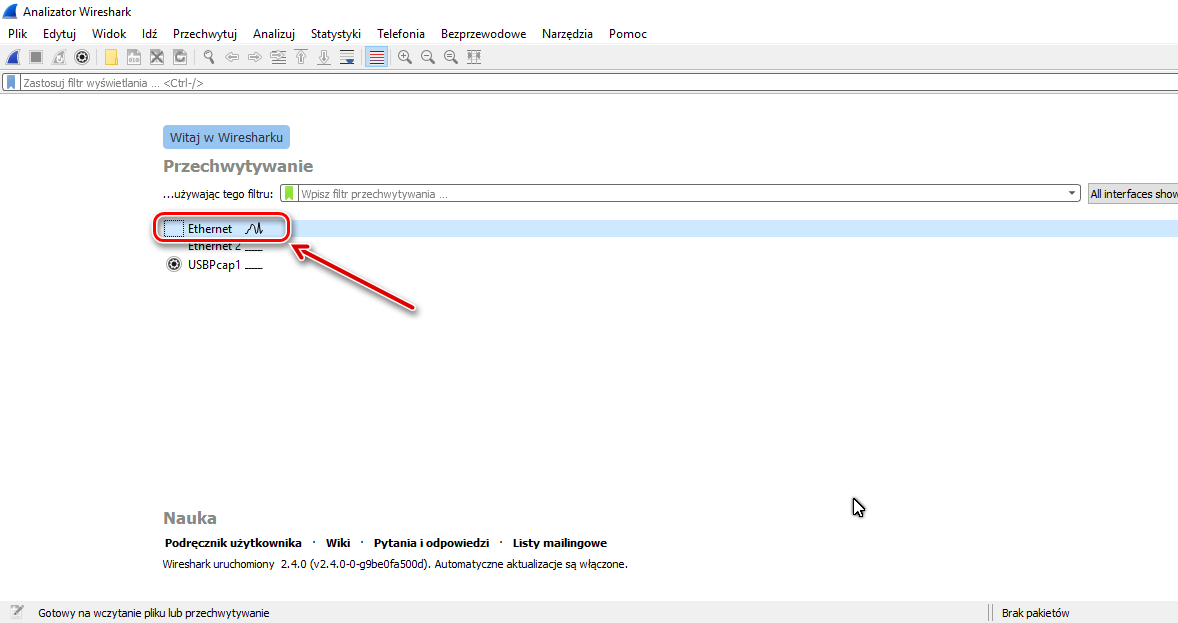
***IP: 192.168.1.101***

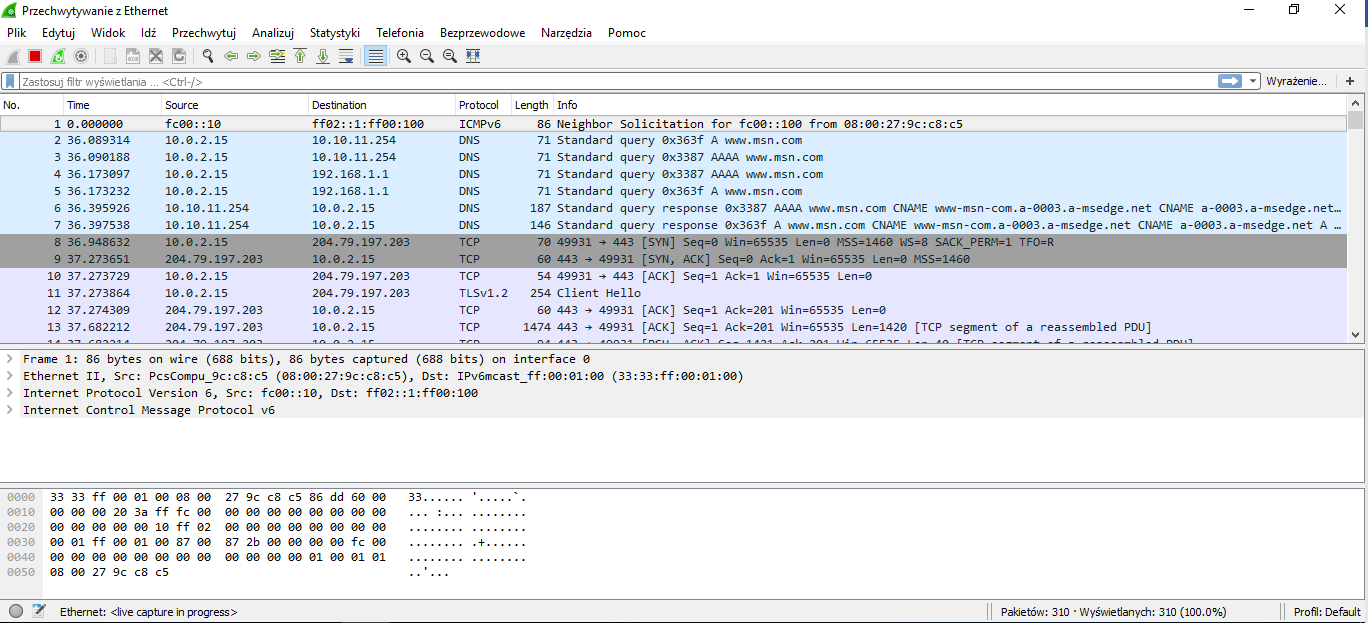
***MAC: 08-D4-0C-1B-AE-9F***

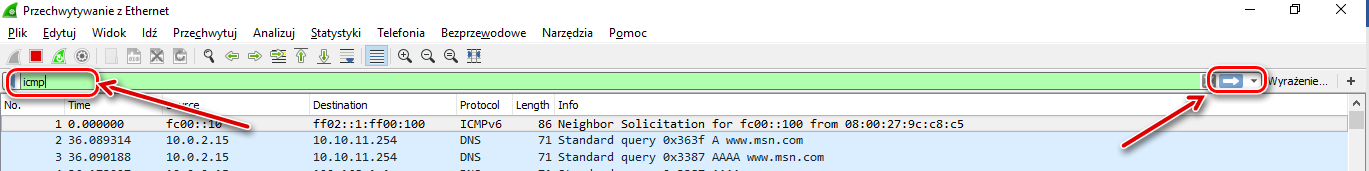
c. Dobierz się w parę z kolegą/koleżanką obok i poproś go/ją o podanie adresu IPv4 jej/jego komputera, oraz przekaż swój. Nie podawaj bynajmniej swojego adresu MAC.

Zanotuj adres IPv4 komputera kolegi/koleżanki: ***192.168.1.14 (mój drugi komputer)***

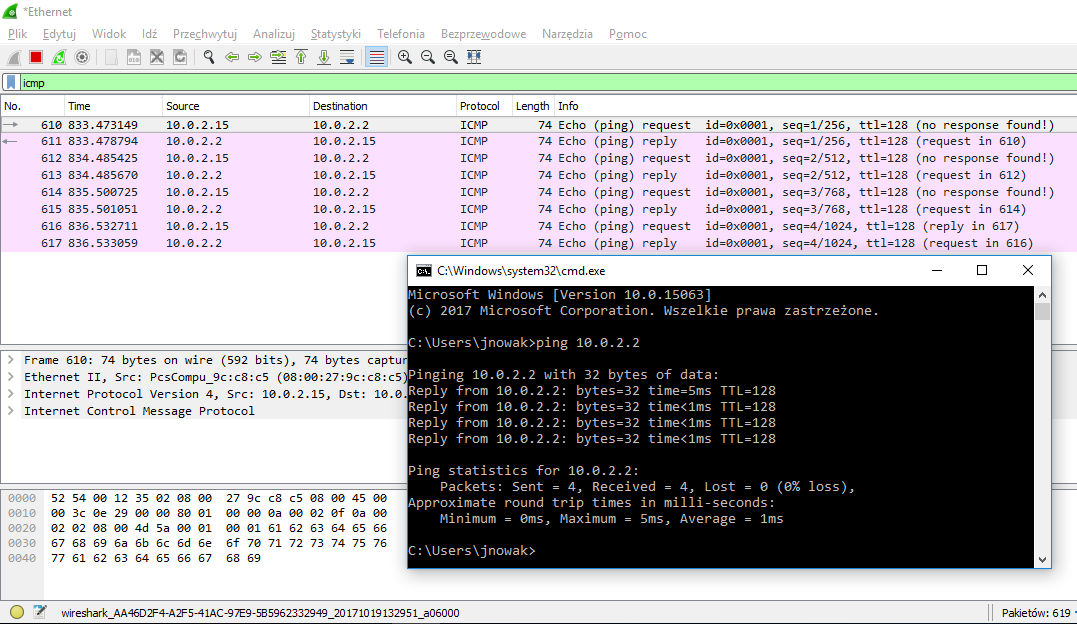
Krok 2:

Uruchomić na swoim komputerze aplikację Wireshark (jeżeli nie jest jeszcze uruchomiona)  
Następnie należy uruchomić przechwytywanie pakietów na interfejsie, który jest aktualnie wykorzystywane przez system operacyjny do komunikacji z lokalną siecią komputerową, odnajdując na liście tenże interfejs sieciowy (aby się wspomóc w wyszukiwaniu tegoż interfejsu, można się zasugerować linią wskazującą aktualną wielkość ruchu sieciowego na danym interfejsie, tj. jak jest jakiś ruch, to „może” to jest ten właściwy interfejs, który łączy się z siecią lokalną, inną możliwością jest odnalezienie nazwy interfejsu w *Panel sterowania\Sieć i Internet\Połączenia sieciowe,* najczęściej dla systemów od Windows 8 wzwyż będzie to zapewne interfejs o nazwie „*Ethernet*”), i dwa razy klikając na niego:  


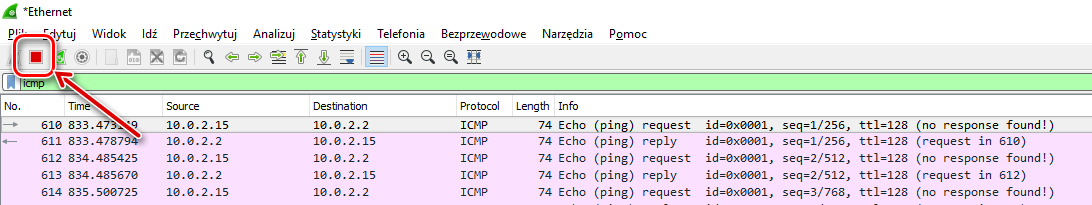
Informacje zaczną pojawiać się w górnej sekcji programu Wireshark. W zależności od typu protokołu, linie z danymi będą pojawiać się w różnych kolorach.  
  


Ilość napływających danych może być bardzo duża (co zależy od intensywności komunikacji między naszym komputerem a lokalną siecią komputerową). Aby sobie z taką sytuacją poradzić, można nałożyć filtr na dane przechwytywane przez Wireshark. Dla celów tego zadania laboratoryjnego interesować nas będą tylko komunikaty protokołu ICMP (ping). By przeglądać więc tylko komunikaty protokołu ICMP (ping), w polu ***Filter***, znajdującym się w górnej części programu Wireshark należy wpisać ***icmp*** i kliknąć przycisk ***Zastosuj filtr*** lub nacisnąć ***Enter***:  
  


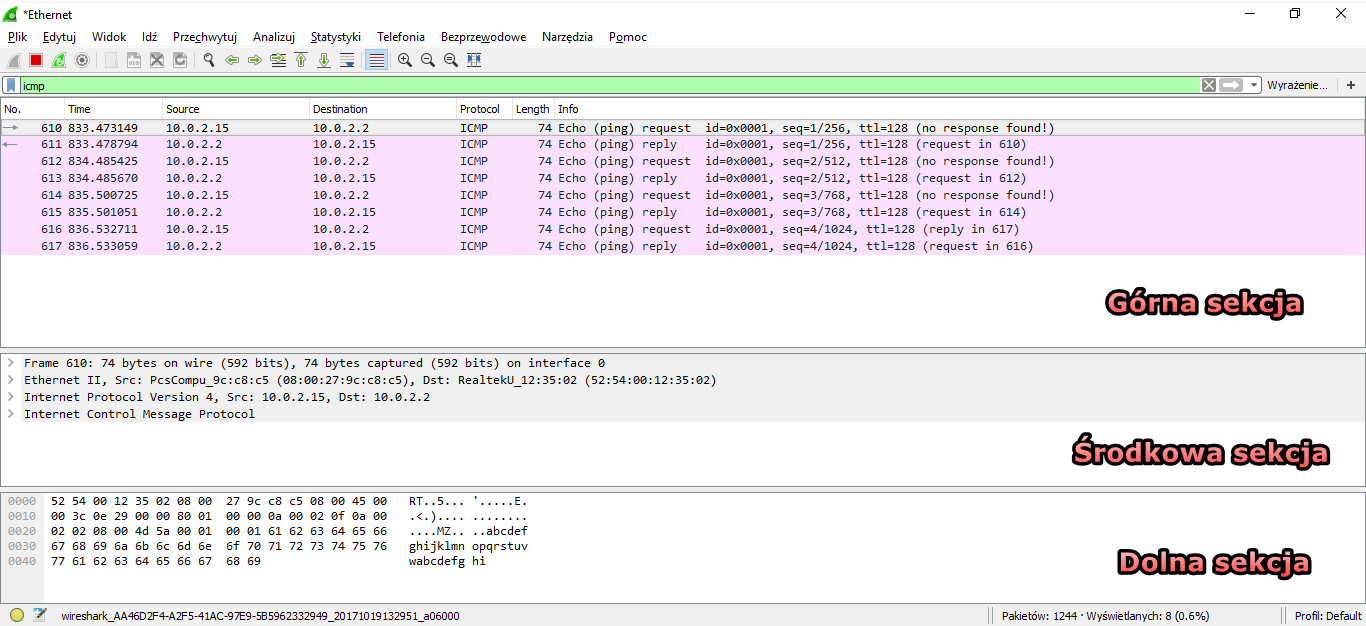
Następnie należy uruchomić wiersz poleceń, i wykorzystując narzędzie wiersza poleceń jakim jest ***ping***, wysłać test ***ping*** na adres IP otrzymany od kolegi/koleżanki z zajęć. Warto zauważyć, że w tym momencie w głównym oknie programu Wireshark, ponownie pojawią się przechwycone dane:

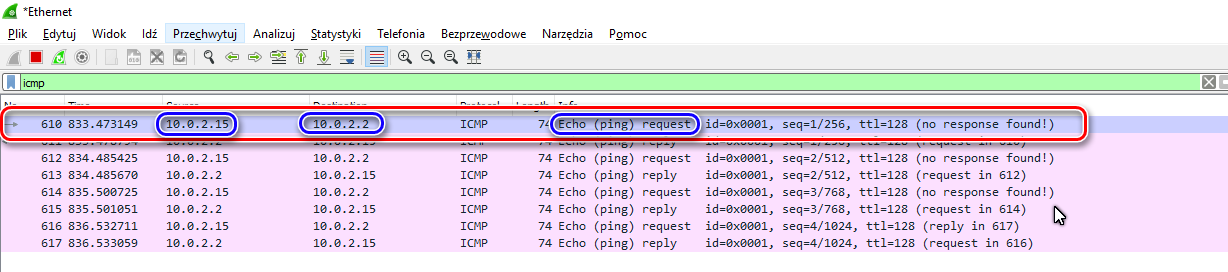


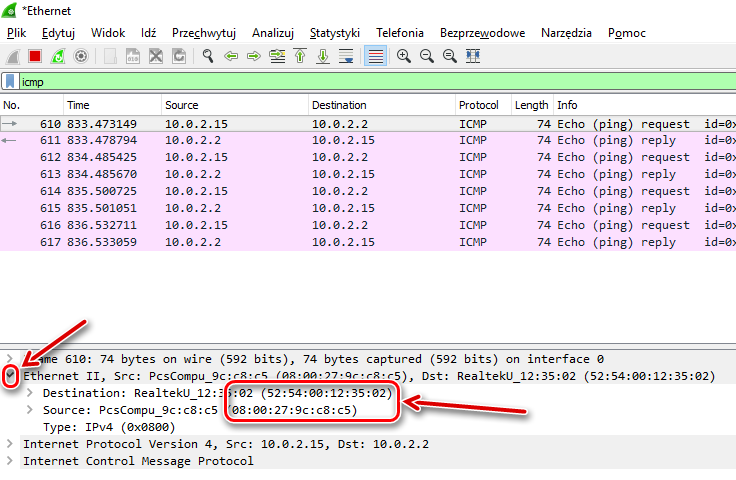
**Uwaga**: Jeżeli komputer kolegi/koleżanki z zajęć nie odpowiada na test ping, możliwe, że wbudowany w system operacyjny firewall blokuje takowe zapytania, i należy skonfigurować odpowiednie wyjątki, które pozwolą na takową transmisję (co było wskazane jako element przygotowania środowiska do niniejszego zadania laboratoryjnego).

Po wykonanym teście ***ping*** zatrzymać proces przechwytywania danych klikając ikonę **Zatrzymaj przechwytywanie**:  


1. Krok 3:

W tym kroku przeanalizujemy przechwycone dane przez aplikację Wireshark, tj. dane wygenerowane przez żądanie ping, wysłane do komputera koleżanki/kolegi z zajęć.   
Można zauważyć, że w programie Wireshark, dane są wyświetlane w trzech sekcjach:   
1) Górna sekcja wyświetla listę ramek wraz z podsumowaniem informacji o tejże ramce   
2) Środkowa sekcja wyświetla informacje na temat ramki (przy czym, tej, która została zaznaczona myszką w górnej części ekranu), umożliwiając przeglądnięcie nagłówków poszczególnych warstw protokołów,   
3) Dolna sekcja wyświetla nieprzetworzone dane dla poszczególnej warstwy. Nieprzetworzone dane są wyświetlane w trybie szesnastkowym (heksadecymalnym) oraz dziesiętnym.  


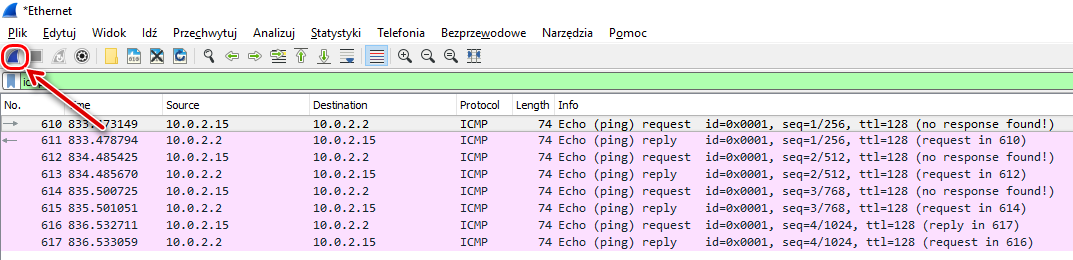
Należy kliknąć na pierwsze żądanie ICMP z listy ramek w górnej sekcji programu Wireshark. Warto zwrócić uwagę, że w kolumnie ***Source*** zapisany jest adres IP twojego komputera, a w kolumnie ***Destination*** adres IP komputera kolegi/koleżanki z zajęć, na który zostało wysłane żądanie ping.  


Przejść do środkowej sekcji programu (przy czym ramka pierwszego żądania ping w sekcji górnej nadal musi być zaznaczona). Kliknąć 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 adresu MAC wcześniej odczytanego dla interfejsu sieciowego twojego komputera? ***Tak, są identyczne.***

Czy adres MAC urządzenia docelowego w programie Wireshark, pasuje do adresu MAC komputera kolegi/koleżanki z zajęć (należy go/ją o to zapytać)? ***Po zweryfikowaniu poleceniem ipconfig /all na drugim komputerze adresy MAC są takie same.***

1. Krok 3:

W tym kroku wykonamy test ping do zdalnych komputerów (tj. komputerów nie będących w tej samej sieci LAN co nasz komputer), oraz zbadamy dane wygenerowane przez ten test ping. Następnie ustalimy, jaka jest różnica między tymi danymi, a danymi zbadanymi w kroku 2.

Należy na nowo proces przechwytywania pakietów w aplikacji Wireshark, klikając na ikonę ***Uruchom*** ***przechwytywanie pakietów*** - pojawi się też wtedy okno informujące o możliwości zapisania wcześniej przechwyconych danych, w naszym przypadku nie ma potrzeby ich zapisywać, należy więc kliknąć przycisk ***Kontynuuj bez zapisywania***Należy również włączyć filtr ***icmp*** po uruchomieniu nowego przechwytywania pakietów.  


Kiedy już proces przechwytywania jest aktywny, należy wykonać na podobniej zasadzie jak w poprzednim kroku 2, po kolei test ping dla trzech poniższych adresów:

* + - 1. www.google.pl
      2. www.sekurak.pl
      3. www.niebezpiecznik.pl

**Uwaga:** Kiedy wykonuje się test ping dla kolejnych w/w adresów, można zwrócić uwagę, że adres DNS (ang. Domain Name Server) tłumaczony jest na adres IP.

Zanotuj adres IP na jaki został rozwiązany każdy z w/w w punkcie „b” adresów DNS:

www.google.pl: ***216.58.209.3***

www.sekurak.pl: ***51.77.40.125***

www.niebezpiecznik.pl:***104.21.235.124***

Po wykonanym teście ping zatrzymać proces przechwytywania danych klikając ikonę ***Zatrzymaj przechwytywanie***

Przejrzyj przechwycone dane w programie Wireshark, sprawdź adresy IP i adresy MAC przyporządkowane dla transmisji z trzema adresami DNS, dla których wykonane zostało polecenie ping.   
Poniżej wpisz, docelowy adres IP oraz docelowy adres MAC jakie zostały wykorzystane podczas komunikacji dla każdego z trzech adresów DNS:

*www.google.pl:*  IP: ***216.58.209.3***  MAC: ***d0:96:fb:50:3e:3f***

*www.sekurak.pl:* IP: ***51.77.40.125***  MAC: ***d0:96:fb:50:3e:3f***

*www.niebezpiecznik.pl:* IP: ***104.21.235.124*** MAC: ***d0:96:fb:50:3e:3f***

**Uwaga:** jeżeli czasem nie widać w aplikacji Wireshark komunikatów icmp dla którego z trzech użytych adresów zdalnych, może to wynikać z faktu iż transmisja została wykonana z wykorzystaniem protokołu IPv6 oraz ICMPv6, należy więc użyć wtedy filtra ***icmpv6*** aby sprawdzić, czy faktycznie tak czasem nie jest.

Wskaż czym różni się ta powyższa informacja od informacji uzyskanej w kroku 2 (dotyczącej wtedy użycia polecenia ping w sieci lokalnej), gdzie widać zastanawiające różnice, i z czego one wynikają, czego dowodzą informacje jakie uzyskaliśmy?  
***Adresy IP są bardzo zróżnicowane, ale ostatecznie prowadzą do tego samego urządzenia sieciowego. Jest nim nasza brama domyślna, czyli nasz router połączony z internetem. Dzięki routerowi możemy połączyć się z urządzeniami spoza naszej sieci lokalnej.***