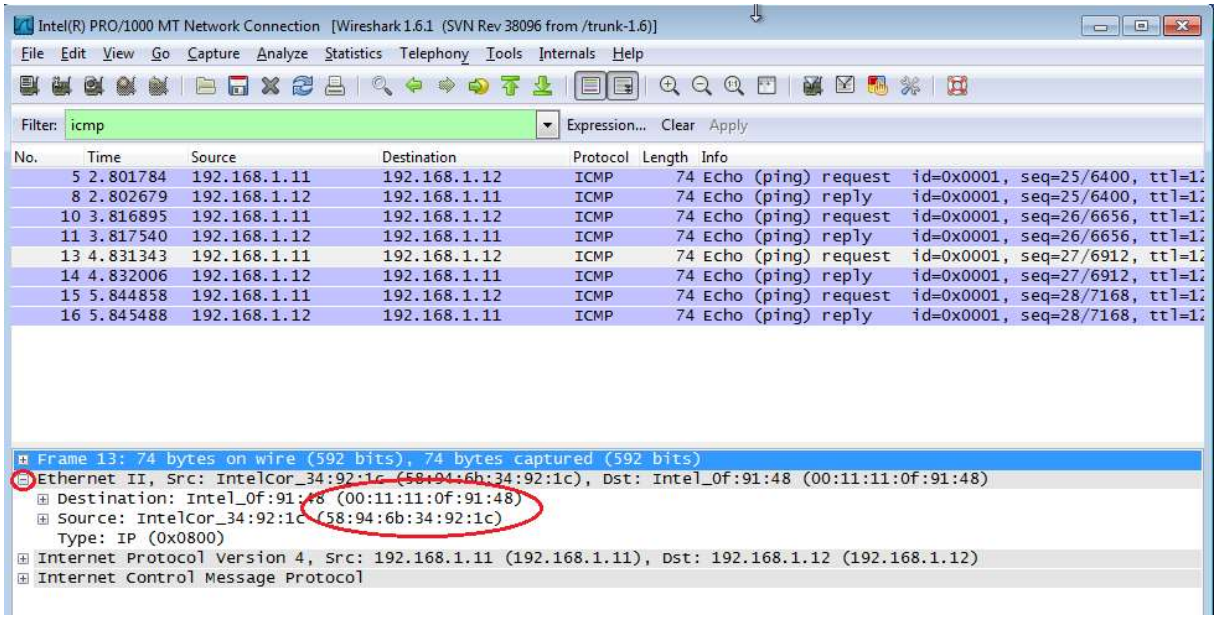
b. Przejdź do środkowej sekcji programu, ramka PDU w sekcji górnej nadal musi być zaznaczona. Kliknij znak plusa znajdujący się po lewej stronie wiersza Ethernet II, by zobaczyć adresy MAC urządzenia źródłowego i docelowego.



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

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

W jaki sposób twój PC uzyskał MAC adres komputera PC, na który wysyłałeś żądania ping?
za pomocą protokołu ARP(adres IP na MAC)

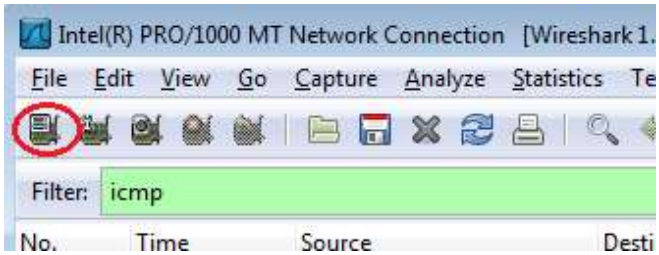
Uwaga: W powyższym przykładzie ilustrującym przechwytywanie żądania ICMP, dane ICMP enkapsulowane są wewnątrz PDU pakietu IPv4 (nagłówek IPv4), który następnie enkapsulowany jest w PDU ramki Ethernet II (nagłówek Ethernet II) i przygotowany do transmisji w sieci LAN.

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.

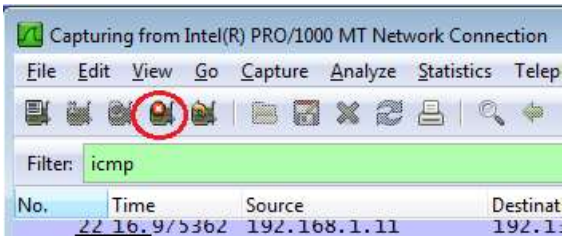
Krok 1: Rozpoczęcie przechwytywania danych z interfejsu.

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



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: 87.248.119.252 MAC: 9c:9d:7e:16:a7:a5

2nd Lokalizacja: IP: 2.19.218.95 MAC: 9c:9d:7e:16:a7:a5

3rd Lokalizacja: IP: 142.251.141.164 MAC: 9c:9d:7e:16:a7:a5

b. Co jest istotne w tej informacji?

Otrzymaliśmy adresy IP poszczególnych serwisów www, ale nie mamy właściwego adresu MAC.

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

W tym przypadku do tłumaczenia adresu www na adres IP używany jest inny protokół (DNS zamiast ARP), który posługuje się adresami IP a nie MAC. Zdobyty wyżej adres MAC to adres routera, przez który przechodzi cała komunikacja z Internetem.

Do przemyślenia

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

jak wyżej (pkt c)