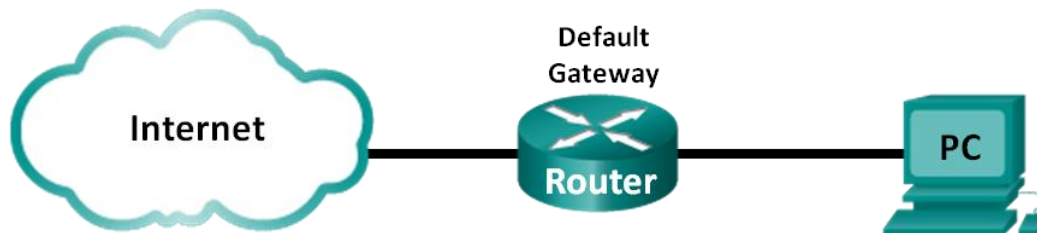


Laboratorium - Przechwytywanie i badanie datagramów DNS w programie Wireshark

Topologia



Cele

Część 1: Zapisanie informacji dotyczących konfiguracji IP komputerów

Część 2: Użycie programu Wireshark do przechwycenia żądań i odpowiedzi DNS

Część 3: Analiza przechwyconych pakietów DNS lub UDP

Scenariusz

Jeżeli kiedykolwiek korzystałeś z Internetu, to musiałeś używać systemu Domain Name System (DNS). DNS to rozproszona sieć serwerów, które tłumaczą przyjazne dla użytkownika nazwy domen, takie jak np. www.google.com, na adresy IP. Po wpisaniu adresu URL witryny, w przeglądarce twój komputer wykonuje zapytanie do serwera DNS, aby uzyskać odpowiedni adres IP. Zapytanie o serwer DNS wykonane z komputera PC oraz odpowiedź z serwera DNS używają protokołu UDP (User Datagram Protocol) w warstwie transportowej. UDP jest protokołem bezpołączeniowym i nie wymaga konfiguracji sesji. Zapytania i odpowiedzi DNS mają bardzo mały rozmiar i nie wymagają protokołu TCP.

W tym laboratorium będziesz komunikować się z serwerem DNS, wysyłając zapytanie DNS za pomocą protokołu transportowego UDP. Będziesz używać programu Wireshark do badania zapytań i odpowiedzi DNS do i z serwera nazw.

Uwaga: To ćwiczenie nie może być przeprowadzone przy użyciu 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: Zapisanie informacji dotyczących konfiguracji IP komputerów

W części 1 można użyć polecenia `ipconfig /all` na komputerze lokalnym, aby znaleźć i zapisać adresy MAC i IP karty sieciowej komputera, adres IP bramy domyślnej oraz adres IP serwera DNS. Zapisz te informacje w tabeli. Informacje te zostaną wykorzystane w dalszej części tego ćwiczenia w analizie pakietów.

AdresIP	
Adres MAC	
Adres IP bramy domyślnej	
Adres IP serwera DNS	

Część 2: Użycie programu Wireshark do przechwytywania żądań i odpowiedzi DNS

W części 2 należy skonfigurować Wireshark do przechwytywania pakietów zapytań i odpowiedzi DNS aby zademonstrować zastosowanie protokołu transportowego UDP podczas komunikacji z serwerem DNS.

- a. Kliknij przycisk Windows **Start** i przejdź do programu Wireshark.

Uwaga: Jeżeli program Wireshark nie jest jeszcze zainstalowany, to możesz go pobrać ze strony <http://www.wireshark.org/download.html>.

- b. Wybierz interfejs sieciowy dla Wireshark w celu przechwytywania pakietów. Użyj **Interface List** aby wybrać interfejs, który odpowiada adresom IP i MAC (Media Access Control) określonym w części 1.
- c. Po wybraniu konkretnego interfejsu kliknij **Start** aby przechwycić pakiety.
- d. Uruchom przeglądarkę internetową i wpisz adres **www.google.com**. Naciśnij klawisz Enter, aby kontynuować.
- e. Gdy zobaczysz stronę domową Google, kliknij **Stop** aby zakończyć przechwytywanie.

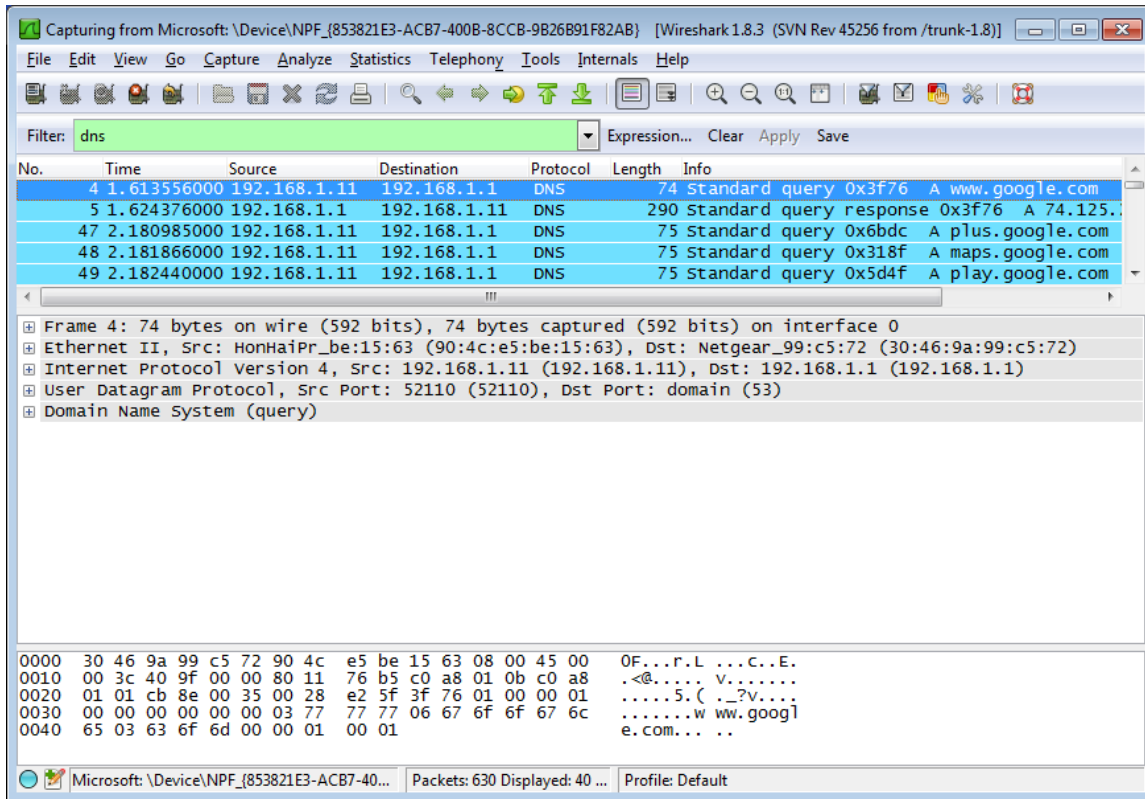
Część 3: Analiza przechwyconych pakietów DNS lub datagramów UDP

W części 3 będziesz badał pakiety UDP, które zostały wygenerowane podczas komunikowania się z serwerem DNS dla adresów IP dotyczących witryny www.google.com.

Krok 1: Filtrowanie pakietów DNS.

- f. W oknie głównym programu Wireshark wpisz **dns** w pasku **Filter** . Kliknij **Apply** lub naciśnij Enter.

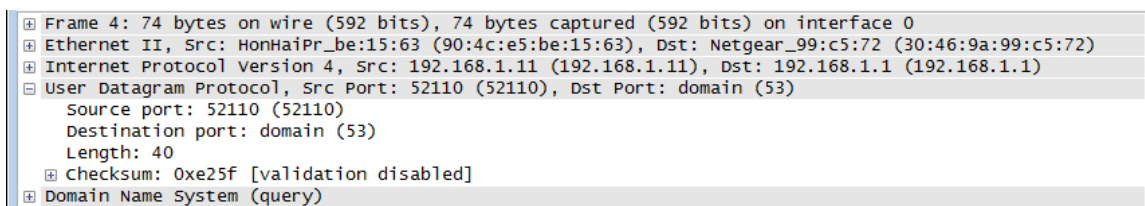
Uwaga: Jeżeli nie widzisz żadnych wyników po zastosowaniu filtru DNS, to zamknij przeglądarkę i w oknie wiersza polecenia wpisz polecenie **ipconfig /flushdns** aby usunąć wszystkie poprzednie wyniki DNS. Ponownie uruchom przechwytywanie w Wireshark i powtórz instrukcje zawarte w części 2b –2e. Jeżeli to nie rozwiąże problemu, to w oknie wiersza poleceń wpisz **nslookup www.google.com** (jako alternatywa dla przeglądarki internetowej).



- g. W panelu listy pakietów (górną sekcją) w oknie głównym znajdź pakiet, który zawiera frazy "standard query" i "www.google.com". Obejrzyj ramkę 4 jako przykład.

Krok 2: Zbadaj segment UDP używając zapytania DNS.

Zbadaj UDP używając zapytania DNS www.google.com przechwyconego przez program Wireshark. W tym przykładzie Wireshark ma zaznaczoną do analizy ramkę 4 znajdującą się w panelu listy pakietów. Protokoły tego zapytania są wyświetlane w panelu szczegółów pakietów (sekcja środkowa). Pozycje protokołu są podświetlone na szaro.



- h. Ramka 4 ma 74 bajty danych i jest wyświetlana w pierwszej linii w panelu szczegółów pakietów. Jest to liczba bajtów do wysłania jako zapytanie do serwera DNS w celu uzyskania adresu IP strony www.google.com.
- i. Linia Ethernet II wyświetla adresy: źródłowy MAC oraz docelowy MAC. Adres źródłowy MAC dotyczy lokalnego komputera, ponieważ lokalny komputer wysłał zapytanie do DNS. Docelowy adres MAC dotyczy bramy domyślnej, ponieważ jest to miejsce przez które zapytanie DNS może wyjść z sieci lokalnej.

Czy źródłowy adres MAC dla komputera lokalnego jest taki sam jak w części 1? _____

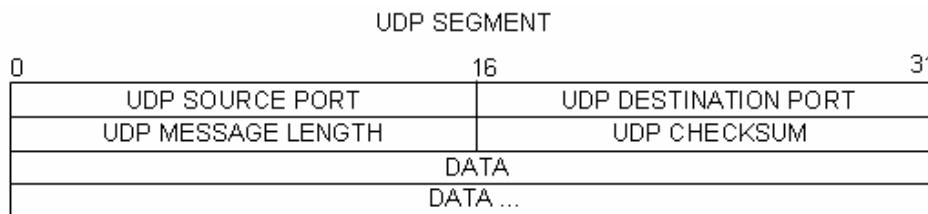
- j. W linii Internet Protocol Version 4 Wireshark przechwycony pakiet IP wskazujące na to, że adres źródłowy IP zapytania DNS to 192.168.1.11 a adres docelowy IP to 192.168.1.1. W tym przykładzie adres docelowy jest bramą domyślną. Router jest bramą domyślną w tej sieci.

Czy możesz skojarzyć pary adresów IP i MAC dla urządzeń źródłowych i docelowych?

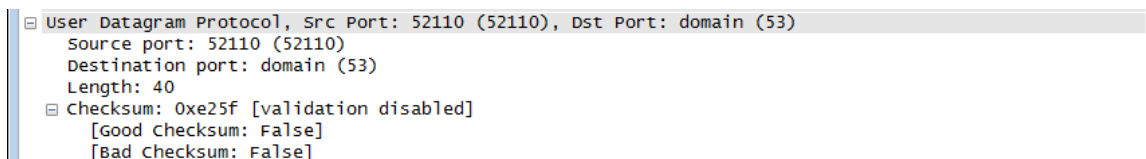
Urządzenie	Adres IP	Adres MAC
Lokalny komputer PC		
Brama domyślna		

Pakiet i nagłówek IP zawiera w sobie segment UDP. Segment UDP w polu danych zawiera zapytanie DNS.

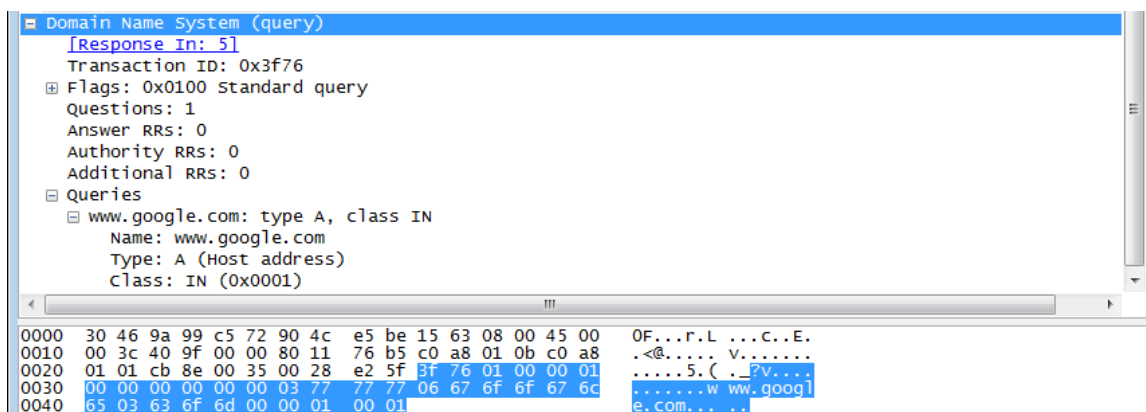
- k. Nagłówek UDP składa się tylko z portu źródłowego, portu docelowego, długości oraz pola sumy kontrolnej. Każde pole w nagłówku UDP ma tylko 16 bitów, co przedstawiono poniżej.



Kliknij znak plus (+), aby rozwinąć User Datagram Protocol w panelu szczegółów pakietów. Zauważ, że tutaj są tylko cztery pola. Numer portu źródłowego w tym przykładzie to 52110. Port źródłowy został losowo wygenerowany przez lokalny komputer używając numerów portów, które nie są zarezerwowane. Port docelowy to 53. Port 53 jest tzw. dobrze znanym portem, zastrzeżonym dla DNS. Serwery DNS nasłuchują (oczekują) zapytań DNS od klientów na porcie 53.



W tym przykładzie długość segmentu UDP wynosi 40 bajtów. W 40 bajtach, 8 bajtów zajmuje nagłówek. Pozostałe 32 bajty danych są używane przez zapytanie DNS. W poniższej ilustracji te 32 bajty danych zapytania DNS są wyróżnione w panelu bajtów pakietów (dolna sekcja) w oknie głównym Wireshark.



Suma kontrolna jest wykorzystywana do ustalenia integralności pakietu po jego wysłaniu do Internetu.

Nagłówek UDP ma mały rozmiar, ponieważ protokół UDP nie posiada pól związanych z 3-etapowym uzgadnianiem, jak to jest w przypadku protokołu TCP. Wszelkie problemy związane z niezawodnością transmisji danych muszą być obsługiwane przez warstwę aplikacji.

Zapisz wyniki swoich badań w programie Wireshark w poniższej tabeli:

Rozmiar ramki	
Źródłowy adres MAC	
Docelowy adres MAC	
Źródłowy adres IP	
Docelowy adres IP	
Port źródłowy	
Port docelowy	

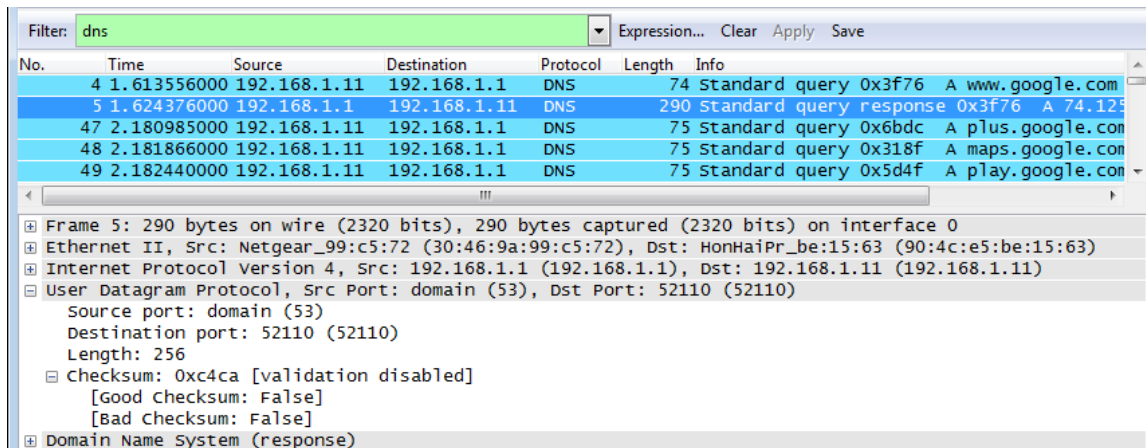
Czy źródłowy adres IP jest taki sam jak adres IP komputera lokalnego w części 1? _____

Czy docelowy adres IP jest taki sam jak brama domyślna w części 1? _____

Krok 3: Zbadaj protokół UDP używając odpowiedzi DNS.

W tym kroku będziesz badał pakiet odpowiedzi DNS i sprawdzał, czy pakiet odpowiedzi DNS korzysta z protokołu UDP.

- i. W tym przykładzie ramka 5 jest przyporządkowana do pakietu odpowiedzi DNS. Zauważ, że liczba bajtów wynosi 290. Jest to większy pakiet w stosunku do pakietu zawierającego zapytanie DNS.



- m. Na podstawie analizy ramki Ethernet II w odpowiedzi DNS, odpowiedz na pytanie: z jakiego urządzenia pochodzi źródłowy adres MAC i docelowy adres MAC?
- n. Zwróć uwagę na źródłowy i docelowy adres IP w pakiecie. Jaki jest docelowy adres IP? Jaki jest źródłowy adres IP?

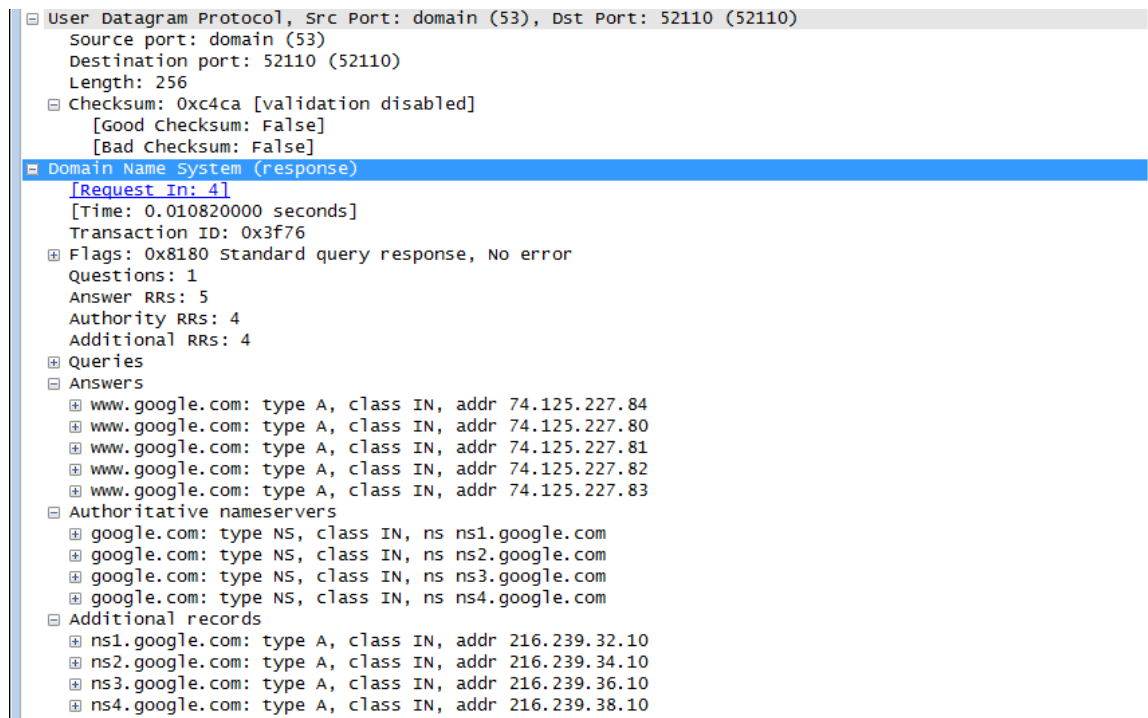
Docelowy adres IP: _____ Źródłowy adres IP: _____

Co stało się z adresem źródłowym i docelowym dla lokalnego hosta oraz bramą domyślną?

- o. W segmencie UDP numery portów także zostały odwrócone. Docelowy numer portu to 52110. Numer portu 52110 to ten sam port, który został wygenerowany przez lokalny komputer, podczas wysłania zapytania DNS do serwera DNS. Twój lokalny komputer nasłuchuje odpowiedzi DNS na tym porcie.

Numer portu źródłowego 53. Serwer DNS nasłuchuje zapytań DNS na porcie 53, a następnie wysłała odpowiedź DNS z numeru portu źródłowego 53 do tego hosta, który wysłał zapytanie DNS.

Aby zobaczyć odpowiedź DNS (adres IP odpowiadający www.google.com), przejdź do sekcji **Answers**.



```

User Datagram Protocol, Src Port: domain (53), Dst Port: 52110 (52110)
  Source port: domain (53)
  Destination port: 52110 (52110)
  Length: 256
  Checksum: 0xc4ca [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Domain Name System (response)
    [Request In: 4]
    [Time: 0.010820000 seconds]
    Transaction ID: 0x3f76
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 4
    Additional RRs: 4
  Queries
  Answers
    www.google.com: type A, class IN, addr 74.125.227.84
    www.google.com: type A, class IN, addr 74.125.227.80
    www.google.com: type A, class IN, addr 74.125.227.81
    www.google.com: type A, class IN, addr 74.125.227.82
    www.google.com: type A, class IN, addr 74.125.227.83
  Authoritative nameservers
    google.com: type NS, class IN, ns ns1.google.com
    google.com: type NS, class IN, ns ns2.google.com
    google.com: type NS, class IN, ns ns3.google.com
    google.com: type NS, class IN, ns ns4.google.com
  Additional records
    ns1.google.com: type A, class IN, addr 216.239.32.10
    ns2.google.com: type A, class IN, addr 216.239.34.10
    ns3.google.com: type A, class IN, addr 216.239.36.10
    ns4.google.com: type A, class IN, addr 216.239.38.10

```

Do przemyślenia

Jakie są zalety korzystania z protokołu UDP zamiast protokołu TCP w warstwie transportowej dla DNS?
