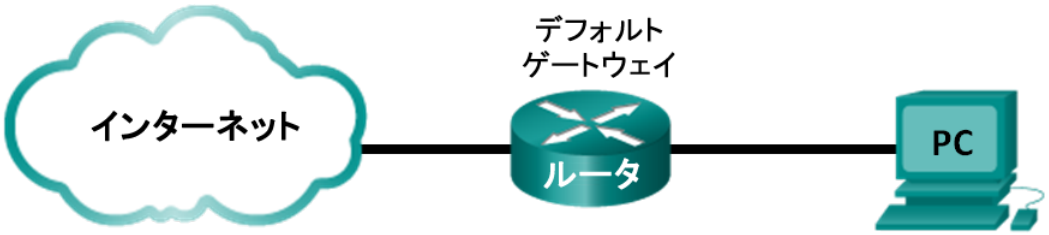
実習 - Wireshark を使用して UDP DNS キャプチャを調べる

トポロジ



目的

パート 1：PC の IP 構成情報の記録

パート 2：Wireshark を使用して DNS クエリーおよび応答をキャプチャする

パート 3：キャプチャされた DNS または UDP パケットを分析する

背景/シナリオ

インターネットを使用したことがあれば、DNS（Domain Name System）も使用していることになります。DNS は、www.google.com などのユーザ フレンドリなドメイン名を IP アドレスに変換するサーバの分散ネットワークです。Web サイトの URL をブラウザに入力すると、ローカル PC が DNS サーバの IP アドレスに向けて DNS クエリーを実行します。ローカル PC の DNS サーバ クエリーと DNS サーバの応答には、トランスポート層プロトコルとして UDP（User Datagram Protocol）が使用されます。UDP はコネクションレス型なので、TCP で行われるようなセッションの確立を必要としません。DNS クエリーと DNS 応答は、サイズが非常に小さいので、TCP のようなオーバーヘッドを必要としません。

この実習では、UDP トランスポート プロトコルを使用して DNS クエリーを送信することにより、DNS サーバと通信します。そして、Wireshark を使用してネーム サーバとの間での DNS クエリーと DNS 応答のやり取りを調べます。

注：この実習は Netlab では完了できません。この実習は、インターネットにアクセスできることを前提としています。

実習に必要なリソースや機器

PC 1 台（インターネットとコマンド プロンプトを利用できて Wireshark がインストールされている Windows 7、Vista、または XP 搭載 PC）

パート 1:　PC の IP 設定情報の記録

パート 1 では、ローカル PC で **ipconfig /all** コマンドを使用して、その PC のネットワーク インターフェイス カード（NIC）の MAC アドレスと IP アドレス、指定のデフォルト ゲートウェイの IP アドレス、およびその PC に対して指定された DNS サーバの IP アドレスを調べ、それらを記録します。この情報を下の表に記録してください。情報は、この実習の後続のパートでパケット分析に使用します。

IP アドレス	
MAC アドレス	
デフォルト ゲートウェイの IP アドレス	
DNS サーバの IP アドレス	

パート 2:　Wireshark を使用した DNS クエリーおよび応答のキャプチャ

パート 2 では、DNS サーバとの通信時に UDP トランスポート プロトコルがどのように使用されるのかを明らかにするため、DNS クエリーと DNS 応答のパケットをキャプチャするように Wireshark をセットアップします。

a. Windows の [**スタート**] ボタンをクリックし、Wireshark プログラムに移動します。

注：Wireshark がまだインストールされていない場合は、http://www.wireshark.org/download.html からダウンロードできます。

b. パケットをキャプチャするための Wireshark のインターフェイスを選択します。[**Interface List**] を使用して、パート 1 で記録した PC の IP アドレスとメディア アクセス制御（MAC）アドレスに関連付けられたインターフェイスを選択します。

c. 目的のインターフェイスを選択したら、[**Start**] をクリックして、パケットをキャプチャします。

d. Web ブラウザを開き、「**www.google.com**」と入力します。Enter キーを押して処理を続行します。

e. Google のホームページが表示されたら、[**Stop**] をクリックして、Wireshark のキャプチャを停止します。

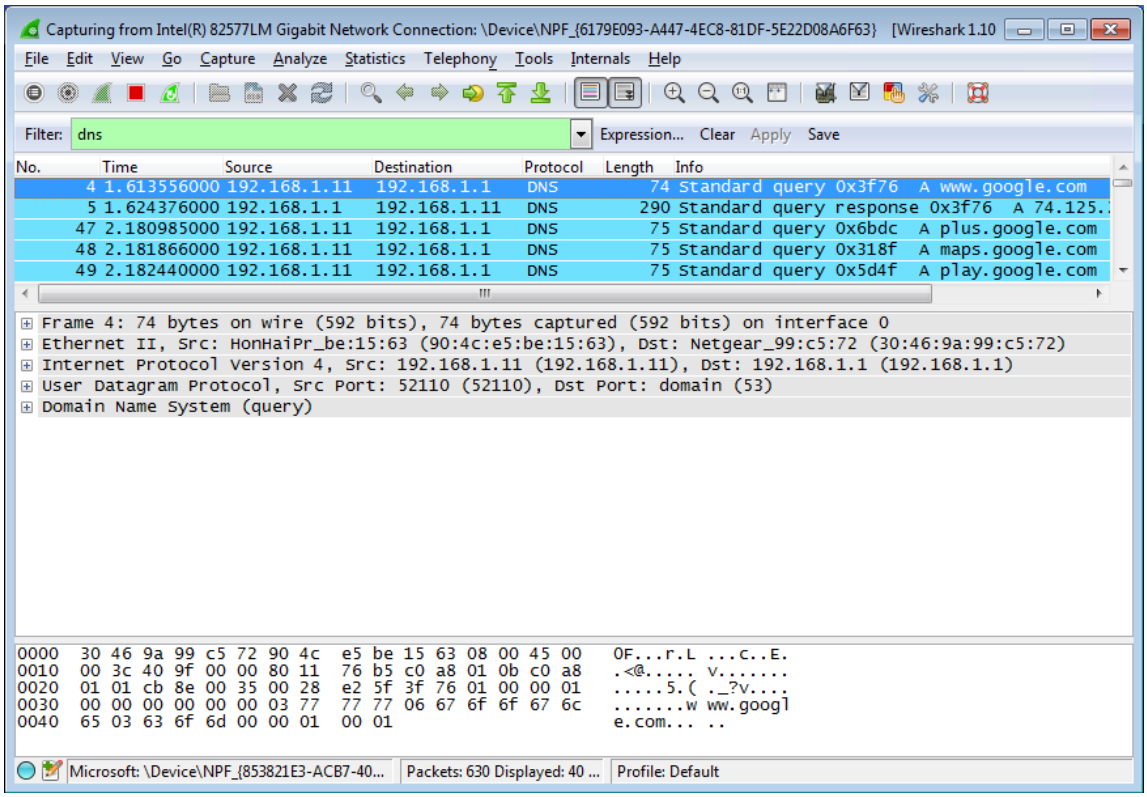
パート 3:　キャプチャされた DNS または UDP パケットの分析

パート 3 では、DNS サーバとの通信時に生成された UDP パケットを調べて、www.google.com の IP アドレスを突き止めます。

手順 1:　DNS パケットをフィルタリングします。

a. Wireshark のメイン ウィンドウで、[**Filter**] ツールバーの入力領域に「**dns**」と入力します。[**Apply**] をクリックするか、Enter キーを押します。

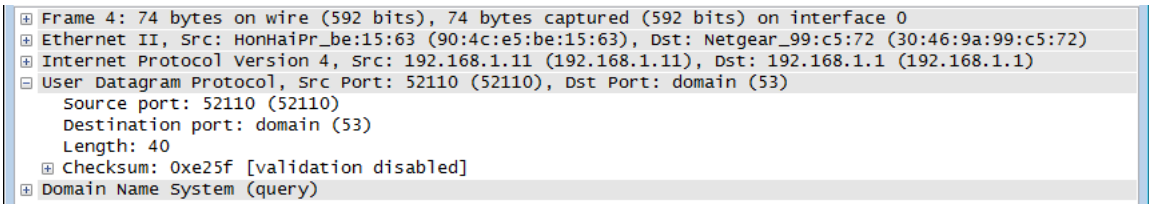
注：DNS フィルタの適用後に結果がまったく表示されない場合は、Web ブラウザを閉じ、コマンド プロンプト ウィンドウで「**ipconfig /flushdns**」と入力して、DNS に関する以前の結果をすべて削除します。それから Wireshark のキャプチャを再開し、パート 2 の b ～ e の手順を繰り返します。それでも問題が解消されない場合は、Web ブラウザの代わりに、コマンド プロンプト ウィンドウで「**nslookup www.google.com**」と入力してください。



b. メイン ウィンドウのパケット リスト ペイン（上部のセクション）で、"standard query" と "A www.google.com" が含まれているパケットを探します。フレーム 4 を例として参照してください。

手順 2: DNS クエリーを使用して UDP セグメントを調べます。

Wireshark によってキャプチャされた www.google.com の DNS クエリーを使用して UDP を調べます。この例では、パケット リスト ペインの Wireshark キャプチャ フレーム 4 が分析用に選択されています。このクエリーのプロトコルがメイン ウィンドウのパケット詳細ペイン（中央のセクション）に表示されています。プロトコルのエントリはグレーで強調表示されています。



a. パケット詳細ペインを見ると、最初の行に表示されているように、フレーム 4 はワイヤ上で 74 バイトのデータを持っていました。これは www.google.com の IP アドレスを要求する DNS クエリーをネーム サーバに送信するためのバイト数です。

b. Ethernet II の行には、送信元と宛先の MAC アドレスが表示されています。送信元の MAC アドレスはローカル PC のものです。DNS クエリーを送信したのはローカル PC だからです。宛先の MAC アドレスはデフォルト ゲートウェイのものです。このクエリーがローカル ネットワークから出る前の最終地点がここだからです。

送信元の MAC アドレスは、パート 1 でローカル PC の MAC アドレスとして記録したものと同じですか。

c. Internet Protocol Version 4 の行は、DNS クエリーの送信元 IP アドレスが 192.168.1.11 で、宛先 IP アドレスが 192.168.1.1 であることを示しています。この例では、宛先アドレスはデフォルト ゲートウェイです。ルータがこのネットワークのデフォルト ゲートウェイです。

送信元デバイスと宛先デバイスのそれぞれの IP アドレスと MAC アドレスを示すことができますか。

デバイス	IP アドレス	MAC アドレス
ローカル PC		
デフォルト ゲートウェイ		

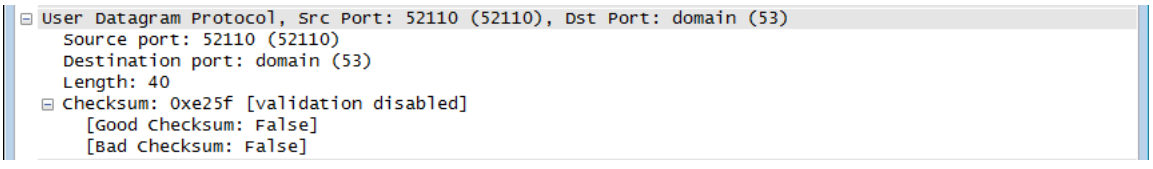
IP パケットとヘッダーは UDP セグメントをカプセル化します。UDP セグメントにはデータとして DNS クエリーが含まれます。

d. UDP ヘッダーには、送信元ポート、宛先ポート、長さ、チェックサムという 4 つのフィールドがあるだけです。UDP ヘッダーの各フィールドは、次に示すように 16 ビットにすぎません。

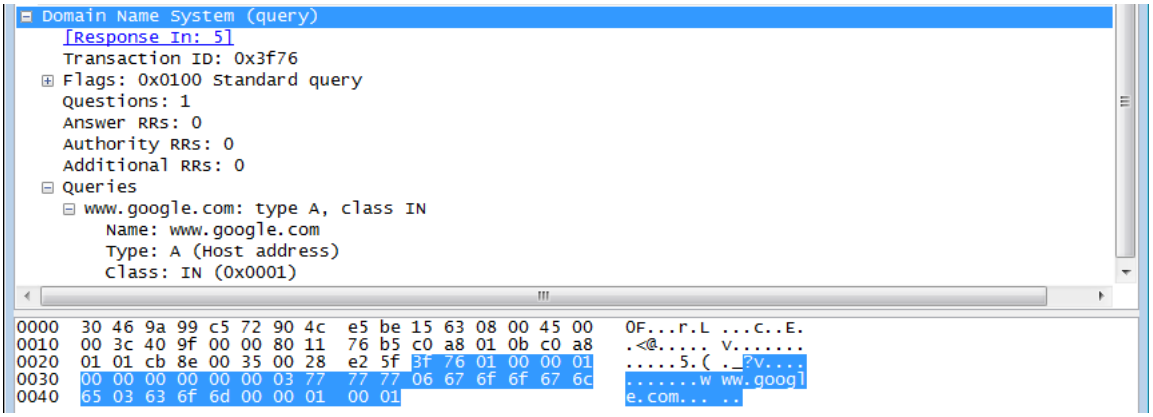
UDP セグメント

0	16	31
UDP 送信元ポート	UDP 宛先ポート	
UDP メッセージ長	UDP チェックサム	
データ		
データ ...		

パケット詳細ペインで [User Datagram Protocol] を展開します。それには、プラス(+)記号をクリックします。フィールドが 4 つしかないことを確認してください。この例の送信元ポート番号は 52110 です。送信元ポートは、予約されていないポート番号を使用してローカル PC によってランダムに生成されています。宛先ポートは 53 です。ポート 53 は、DNS 用として予約されている既知の(well-known)ポートです。DNS サーバは、クライアントからの DNS クエリーをポート 53 でリッスンします。



この例では、この UDP セグメントの長さは 40 バイトです。40 バイトのうち、8 バイトがヘッダーとして使用されます。他の 32 バイトは DNS クエリー データに使用されます。次の図では、Wireshark のメイン ウィンドウのパケット バイト ペイン（下部のセクション）内で 32 バイトの DNS クエリー データが強調されています。



チェックサムは、インターネットを通過した後のパケットの完全性を判定するために使用されます。

UDP ヘッダーのオーバーヘッドが少ないのは、UDP には TCP における 3 ウェイ ハンドシェイクに関係するフィールドがないからです。データ転送の信頼性に関する問題が発生した場合、アプリケーション層で処理する必要があります。

Wireshark の結果を次の表に記録してください。

フレーム サイズ	
送信元 MAC アドレス	
宛先 MAC アドレス	
送信元 IP アドレス	
宛先 IP アドレス	
送信元ポート	
宛先ポート	

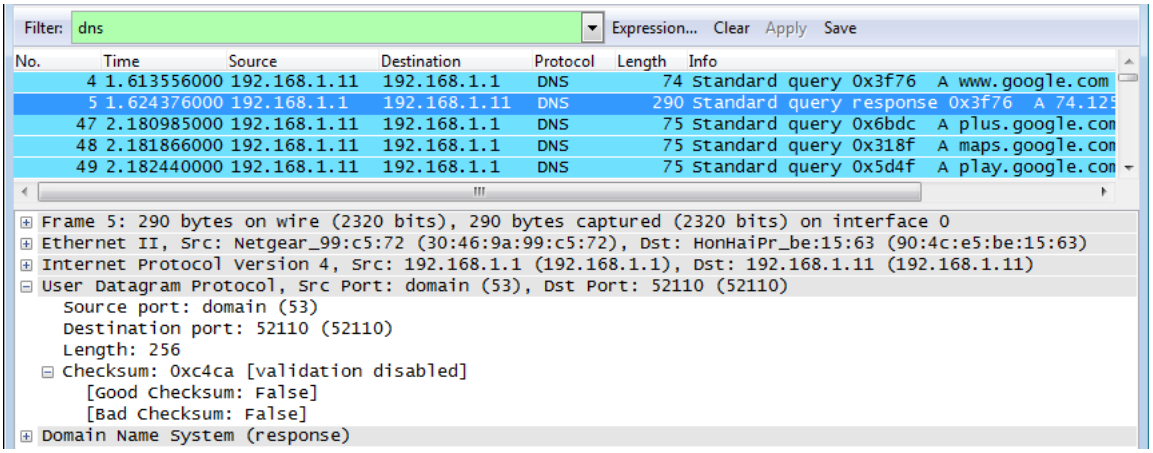
送信元 IP アドレスは、パート 1 で記録したローカル PC の IP アドレスと同じですか。

宛先 IP アドレスは、パート 1 で記録したデフォルト ゲートウェイのものと同じですか。

手順 3:　DNS 応答を使用して UDP を調べます。

このステップでは、DNS 応答パケットを調べ、DNS 応答パケットでも UDP が使用されていることを確認します。

a. この例では、フレーム 5 が該当する DNS 応答パケットです。ワイヤ上でのバイト数が 290 バイトであることに注目してください。これは DNS クエリー パケットに比べると大きなパケットです。



b. DNS 応答のイーサネット II フレームでは、送信元 MAC アドレスのデバイスは何で、宛先 MAC アドレスのデバイスは何ですか。

c. IP パケット内の送信元 IP アドレスと宛先 IP アドレスに注目してください。宛先 IP アドレスは何と表示されていますか。送信元 IP アドレスは何と表示されていますか。

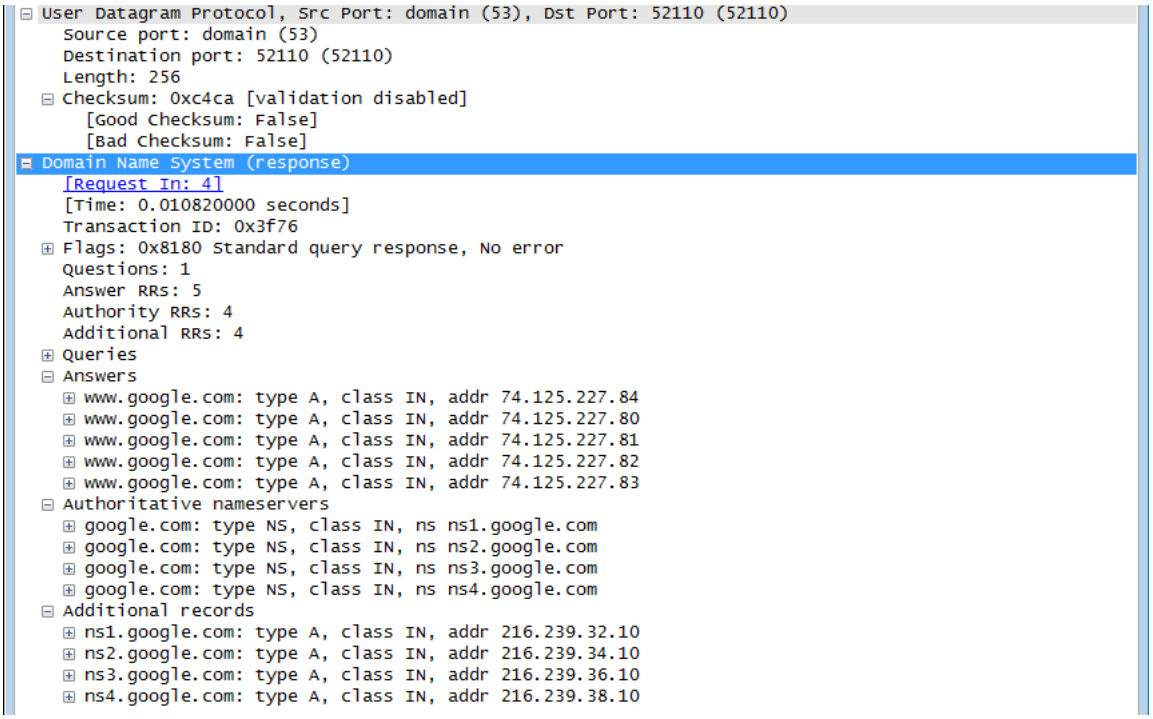
宛先 IP アドレス:　　送信元 IP アドレス:

ローカル ホストとデフォルト ゲートウェイの送信元と宛先の役割はどうなっていましたか。

d. UDP セグメントでは、ポート番号の役割も逆転しています。宛先ポート番号は 52110 です。ポート番号 52110 は、DNS クエリーが DNS サーバに送信されたときにローカル PC によって生成されたものと同じポートです。ローカル PC は、このポートで DNS 応答をリッスンします。

送信元ポート番号は 53 です。DNS サーバは、ポート 53 で DNS クエリーをリッスンし、送信元ポート番号 53 を使用して、DNS クエリーの送信元に DNS 応答を返します。

DNS 応答を展開して、[**Answers**] セクションで www.google.com に対して解決された IP アドレスを見てください。



復習

DNS のトランスポート プロトコルとして、TCP の代わりに UDP を使用する利点は何ですか。