# 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

PC1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、<u>http://www.wireshark.org/download.html</u> 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。

💋 Capturing from Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_(6179E093-A447-4EC8-81DF-5E22D08A6F63} [Wireshark 1.10 🗔 📼 🔤
<u>File Edit View Go Capture A</u> nalyze <u>S</u> tatistics Telephon <u>y</u> <u>T</u> ools <u>I</u> nternals <u>H</u> elp
Filter: dns Expression Clear Apply Save
No. Time Source Destination Protocol Length Info
4 1.613556000 192.168.1.11 192.168.1.1 DNS 74 Standard query 0x3f76 A www.google.com
5 1.624376000 192.168.1.1 192.168.1.11 DNS 290 Standard query response 0x3f76 A 74.125.
47 2.180985000 192.168.1.11 192.168.1.1 DNS 75 Standard query Ox6bdc A plus.google.com
48 2.181866000 192.168.1.11 192.168.1.1 DNS 75 Standard query 0x318f A maps.google.com
49 2.182440000 192.168.1.11 192.168.1.1 DNS 75 Standard query 0x5d4f A play.google.com
۰
■ Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: HonHaiPr_be:15:63 (90:4c:e5:be:15:63), Dst: Netgear_99:c5:72 (30:46:9a:99:c5:72)
B Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.1 (192.168.1.1)
🗄 User Datagram Protocol, Src Port: 52110 (52110), Dst Port: domain (53)
🗄 Domain Name System (query)
0000 30 46 93 99 c5 72 90 4c e5 be 15 63 08 00 45 00 05 c L c 5
0010 00 3c 40 9f 00 00 80 11 76 b5 c0 a8 01 0b c0 a8
0020 01 01 cb 8e 00 35 00 28 e2 5f 3f 76 01 00 00 015.(?v
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6cw www.googl
💛 🌌  Microsoft: \Device\NPF_{853821E3-ACB7-40   Packets: 630 Displayed: 40   Profile: Default

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。

Ŧ	Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
±	Ethernet II, Src: HonHaiPr_be:15:63 (90:4c:e5:be:15:63), Dst: Netgear_99:c5:72 (30:46:9a:99:c5:72)
Œ	Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.1 (192.168.1.1)
Ε	User Datagram Protocol, Src Port: 52110 (52110), Dst Port: domain (53)
	Source port: 52110 (52110)
	Destination port: domain (53)
	Length: 40
	🗄 Checksum: 0xe25f [validation disabled]
Æ	Domain Name System (query)

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	長 UDP チェックサム			
データ				
<i>ī</i> -	-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。

```
    □ User Datagram Protocol, Src Port: 52110 (52110), Dst Port: domain (53)
Source port: 52110 (52110)
Destination port: domain (53)
Length: 40
    □ Checksum: 0xe25f [validation disabled]
[Good Checksum: False]
[Bad Checksum: False]
```

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。

= Domain Name System (query)	
[Response In: 5]	
Transaction ID: 0x3f76	
Questions: 1	=
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
🗆 Queries	
□ www.google.com: type A, class IN	
Name: www.google.com	
Type: A (Host address)	
Class: IN (0x0001)	-
< III III III III III III III III III I	•
0000 30 46 9a 99 c5 72 90 4c e5 be 15 63 08 00 45 00 0Fr.LCE.	
0010 00 3c 40 9f 00 00 80 11 76 b5 c0 a8 01 0b c0 a8 .<@ v	
0020 01 01 cb 8e 00 35 00 28 e2 5f 3f 76 01 00 00 015.(?v	
0030 00 00 00 00 00 03 77 77 77 06 67 67 67 67 66 67 www.googl	

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。

Filter:	dns			-	Expression Cle	lear Apply Sa	/e	
No.	Time	Source	Destination	Protocol	Length Info			*
	4 1.613556000	192.168.1.11	192.168.1.1	DNS	74 Star	ndard query	0x3f76	A www.google.com 📟
	5 1.624376000	192.168.1.1	192.168.1.11	DNS	290 Star	ndard query	respons	e 0x3f76 A 74.125
	47 2.180985000	192.168.1.11	192.168.1.1	DNS	75 Star	ndard query	0x6bdc	A plus.google.com
	48 2.181866000	192.168.1.11	192.168.1.1	DNS	75 Star	ndard query	0x318f	A maps.google.com
	49 2.182440000	192.168.1.11	192.168.1.1	DNS	75 Star	ndard query	0x5d4f	A play.google.com 👻
<								۱.
🕀 Fra	🗷 Frame 5: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface 0							
🕀 Etł	mernet II, Src:	Netgear_99:c5	:72 (30:46:9a:	99:c5:72	), Dst: HonH	HaiPr_be:15	:63 (90:	4c:e5:be:15:63)
🗄 Int	ernet Protocol	Version 4, Sr	c: 192.168.1.1	(192.16	8.1.1), Dst:	: 192.168.1	.11 (192	.168.1.11)
🗆 Use	er Datagram Pro	tocol, Src Por	t: domain (53)	, Dst Po	ort: 52110 (5	52110)		
5	ource port: do	main (53)						
	estination por	t: 52110 (5211	.0)					
L	ength: 256.							
	hecksum: 0xc4c	a [validation	disabled]					
	[Good Checksu	m: False]						
	[Bad Checksum	: False]						
+ Don	iain Name Syste	m (response)						

- 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。

<ul> <li>User Datagram Protocol, Src Port: domain (53), Dst Port: 52110 (52110)</li> <li>Source port: domain (53)</li> <li>Destination port: 52110 (52110)</li> <li>Length: 256</li> <li>Checksum: 0xc4ca [validation disabled]</li> <li>[Good Checksum: False]</li> <li>[Bad Checksum: False]</li> </ul>
🗖 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 /4.125.22/.81
Www.google.com: type A, class IN, addr 74.125.227.82
Www.google.com: type A, class IN, addr /4.125.227.83
Authoritative nameservers
B google.com: type NS, Class IN, NS NSI.google.com
B google.com: type NS, class IN, IS IS2.google.com
B google.com: type NS, class IN, is iss.google.com
□ google.com. type no, class in, is is4.google.com
Addretonal econe type A class TN addr 216 239 32 10
Bing ago a come type A, class IN, add 216,239,34.10
ns3.google.com: type A, class IN, addr 216,239,36.10
ms4.google.com: type A, class IN, addr 216.239.38.10

## 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。