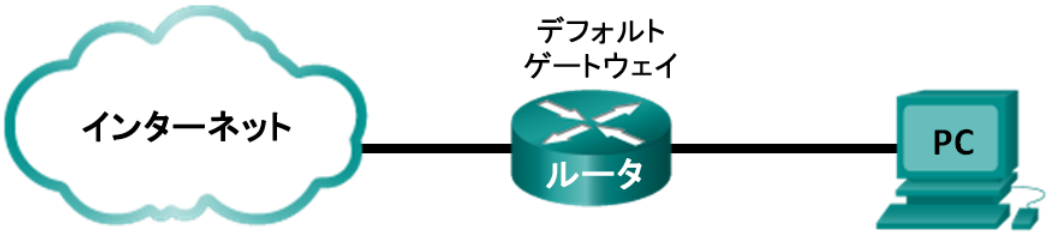
実習 - Wireshark を使用して TCP 3 ウェイ ハンドシェイクを監視する

トポロジ



目的

パート 1:パケットをキャプチャするために Wireshark を準備する

- パケットをキャプチャするために適切な NIC インターフェイスを選択します。

パート 2:パケットのキャプチャ、検索、および調査をする

- www.google.com への Web セッションをキャプチャします。
- Web セッションの適切なパケットを特定します。
- IP アドレス、TCP ポート番号、TCP 制御フラグなど、パケット内の情報を確認します。

背景/シナリオ

この実習では、HTTP(HyperText Transfer Protocol)を使用する PC ブラウザと www.google.com などの Web サーバの間で生成されるパケットを、Wireshark を使用して検出し、調べます。HTTP や FTP(File Transfer Protocol)などのアプリケーションがホストで最初に起動すると、TCP は 3 ウェイ ハンドシェイクを使用して 2 つのホスト間に信頼できる TCP セッションを確立します。たとえば、PC が Web ブラウザを使用してインターネットを閲覧すると、3 ウェイ ハンドシェイクが開始され、PC ホストと Web サーバの間にセッションが確立されます。PC は、さまざまな Web サイトとの間に複数のアクティブな TCP セッションを同時に持つことができます。

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:　パケットをキャプチャするための Wireshark の準備

パート 1 では、Wireshark プログラムを起動し、パケットを検出するために適切なインターフェイスを選択します。

手順 1:　PC インターフェイスのアドレスを取得します。

この実習では、PC の IP アドレスと、ネットワーク インターフェイス カード(NIC)の物理アドレス(MAC アドレスとも呼ばれます)を取得する必要があります。

a. コマンド プロンプト ウィンドウを開き、「**ipconfig /all**」と入力して、Enter キーを押します。

```
   Physical Address. . . . . . . . . : C8-0A-A9-FA-DE-0D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.130(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, December 01, 2012 1:43:35 PM
   Lease Expires . . . . . . . . . . : Sunday, December 02, 2012 1:43:35 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

b. 選択したイーサネット アダプタに関連付けられた IP アドレスと MAC アドレスは、キャプチャ パケットを調べるときに検索する送信元アドレスであるため、これを書き留めておきます。

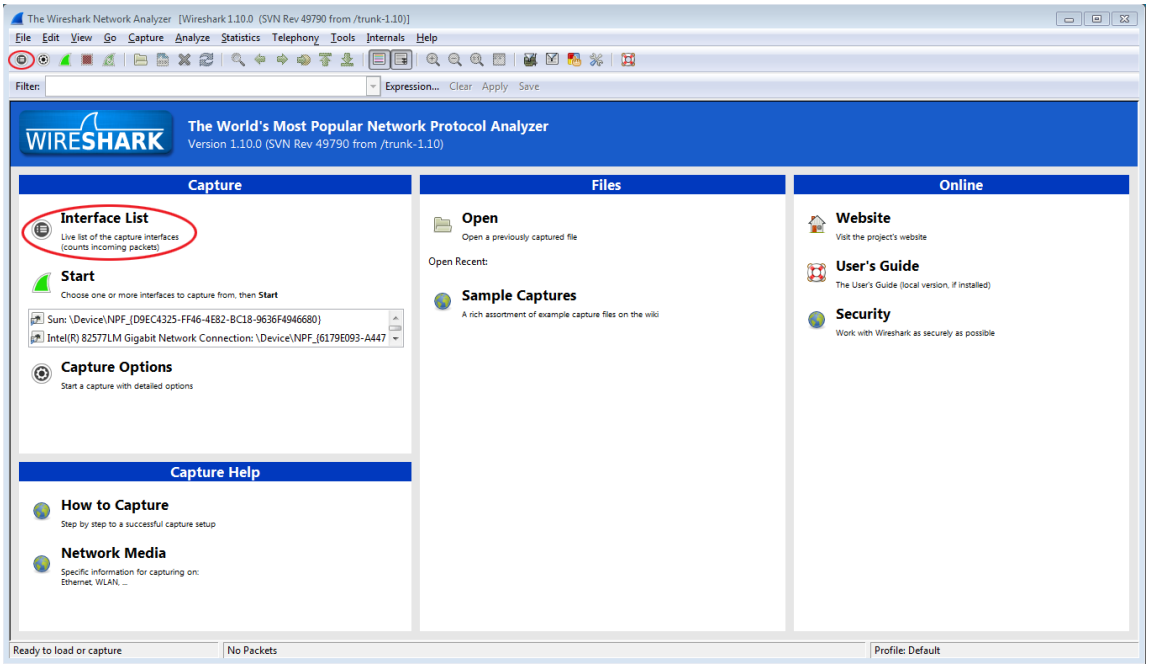
PC ホストの IP アドレス:

PC ホストの MAC アドレス:

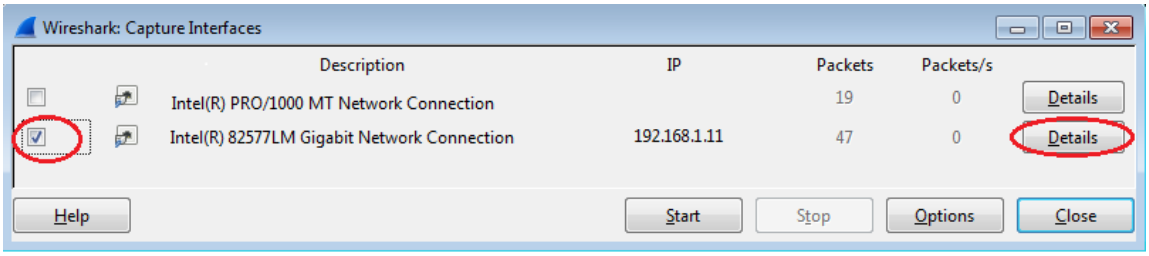
手順 2: Wireshark を開始し、適切なインターフェイスを選択します。

a. Windows の [**スタート**] ボタンをクリックし、ポップアップ メニューで [**Wireshark**] をダブルクリックします。

b. Wireshark の起動後、[**Interface List**] をクリックします。



c. [**Wireshark: Capture Interfaces**] ウィンドウで、LAN に接続されているインターフェイスの横にあるチェック ボックスをオンにします。



注:複数のインターフェイスがリストされ、検査するインターフェイスが不確実な場合は、[**Details**] をクリックします。[**802.3(Ethernet)**] タブをクリックし、MAC アドレスが手順 1b で書き留めたものと一致することを確認します。確認後、[Interface Details] ウィンドウを閉じます。

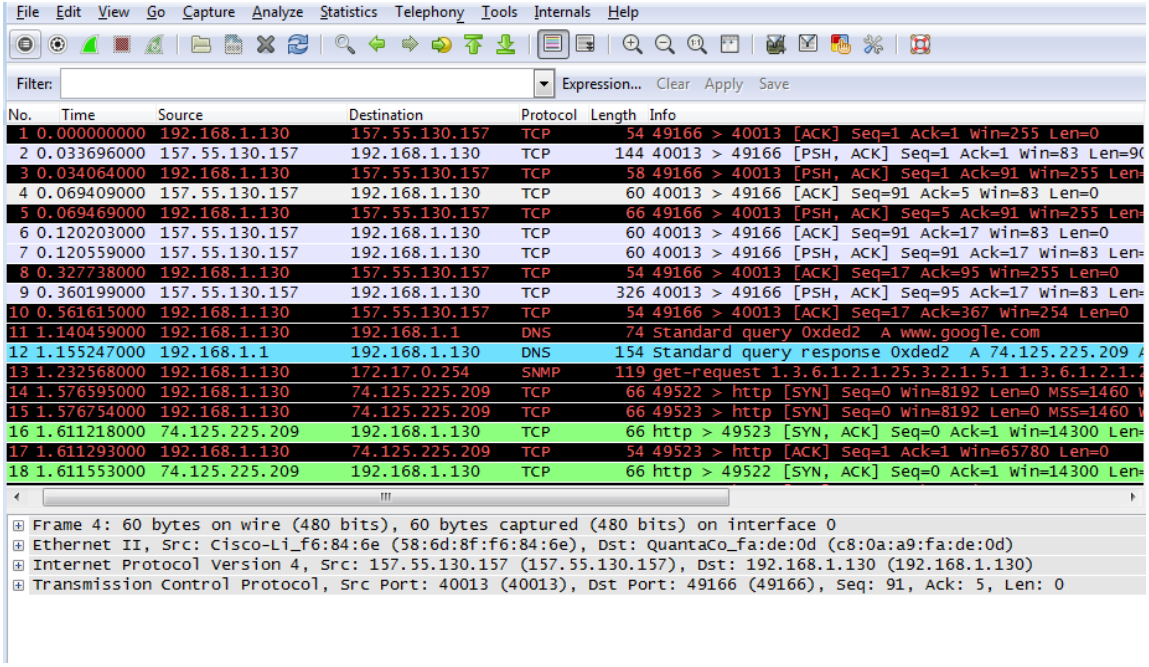
パート 2:　パケットのキャプチャ、検索、および調査

手順 1:　[Start] ボタンをクリックして、データのキャプチャを開始します。

a. www.google.com に移動します。Google のウィンドウを最小化して、Wireshark に戻ります。データのキャプチャを停止します。手順 b では次のようなトラフィックがキャプチャされます。

注:インストラクタから、別の Web サイトを提供される場合があります。その場合は、ここに Web サイト名またはアドレスを記入してください。

b. キャプチャ ウィンドウがアクティブになっています。[**Source**]、[**Destination**]、[**Protocol**] の各列を見つけます。



手順 2:　Web セッションの適切なパケットを特定します。

コンピュータが起動したばかりで、インターネット アクセスのアクティビティがない場合、アドレス解決プロトコル(ARP)、ドメイン ネーム システム(DNS)、TCP の 3 ウェイ ハンドシェイクを含むプロセス全体がキャプチャされた出力に表示される場合があります。パート 2 の手順 1 のキャプチャ画面には、コンピュータが www.google.com にアクセスするために必要なすべてのパケットが示されています。この場合、PC にはすでにデフォルト ゲートウェイの ARP エントリがあったため、www.google.com を解決するための DNS クエリーで開始しました。

a. フレーム 11 で示されている PC から DNS サーバへの DNS クエリーでは、ドメイン名 www.google.com から Web サーバの IP アドレスへの解決が試みられています。PC が最初のパケットを Web サーバに送信するには、IP アドレスが必要です。

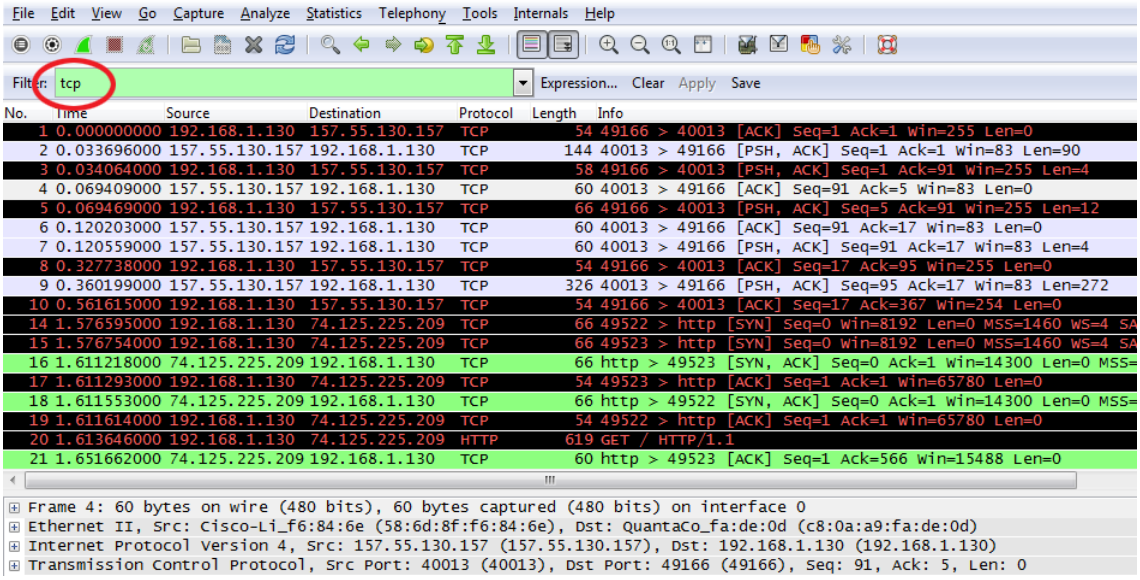
コンピュータがクエリーを発行した DNS サーバの IP アドレスは何ですか。

b. フレーム 12 は、www.google.com の IP アドレスを含む DNS サーバからの応答です。

c. 3 ウェイ ハンドシェイクを開始する適切なパケットを検索します。この例では、フレーム 15 で TCP 3 ウェイ ハンドシェイクが開始しています。

Google Web サーバの IP アドレスは何ですか。

d. TCP 接続に関係のない多数のパケットがある場合は、Wireshark フィルタ機能を使用できます。Wireshark のフィルタ入力領域に「**tcp**」と入力し、Enter キーを押します。



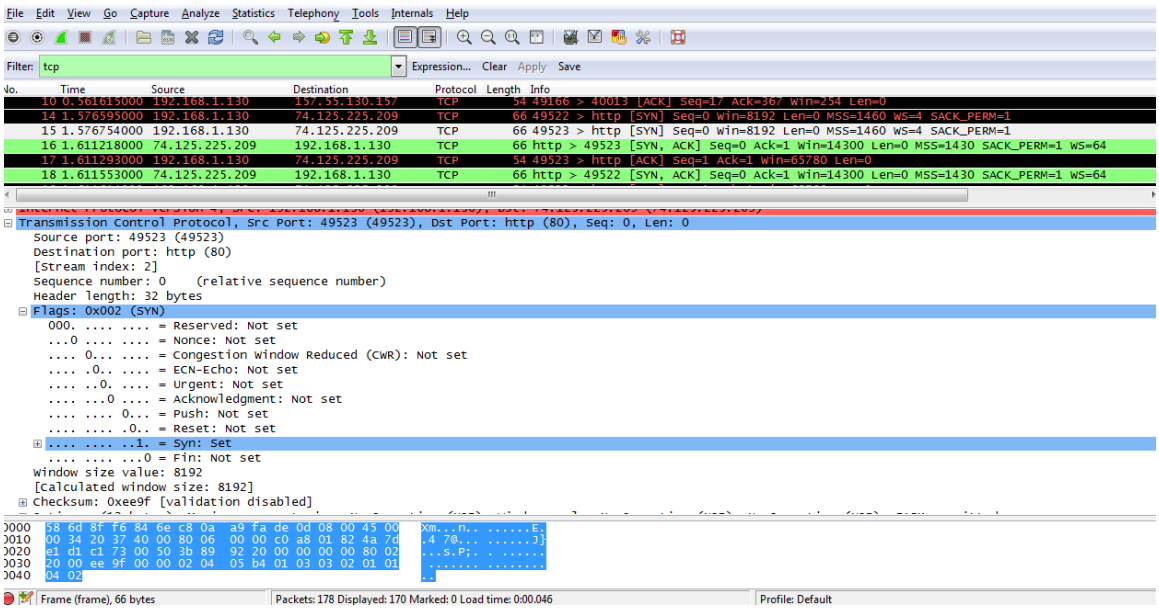
手順 3: IP アドレス、TCP ポート番号、TCP 制御フラグなど、パケット内の情報を確認します。

a. この例では、フレーム 15 で PC と Google Web サーバの間の 3 ウェイ ハンドシェイクが開始しています。パケット リスト ペイン（メイン ウィンドウの上部）で、フレームを選択します。これにより行が強調表示されて、そのパケットの復号化された情報が 2 つの下部ペインに表示されます。パケットの詳細ペイン（メイン ウィンドウの中央部分）で TCP の情報を調べます。

b. パケット詳細ペインの [Transmission Control Protocol] の左側にある [+] アイコンをクリックし、TCP 情報の表示を展開します。

c. [Flags] の左側にある [+] アイコンをクリックします。送信元ポートと宛先ポートおよび設定されているフラグを確認します。

注：必要な情報を表示するには、Wireshark の上部と中央のウィンドウ サイズを調整しなければならない場合があります。



TCP 送信元ポートの番号は何ですか。

送信元ポートはどのように分類されますか。

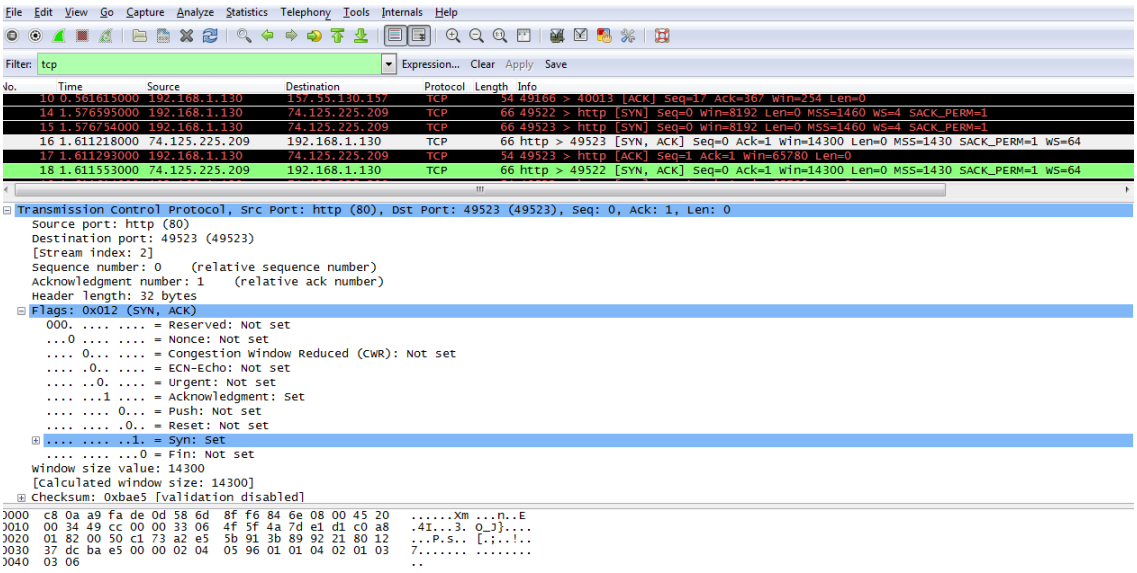
TCP 宛先ポートの番号は何ですか。

宛先ポートはどのように分類されますか。

どのフラグ（1 つまたは複数）が設定されていますか。

相対シーケンス番号は何に設定されていますか。

d. 3 ウェイ ハンドシェイクの次のフレームを選択するには、Wireshark メニューで [**Go**] を選択し、[**Next Packet In Conversation**] を選択します。この例ではフレーム 16 です。これは、セッションを開始するための初期要求に対する Google Web サーバの応答です。

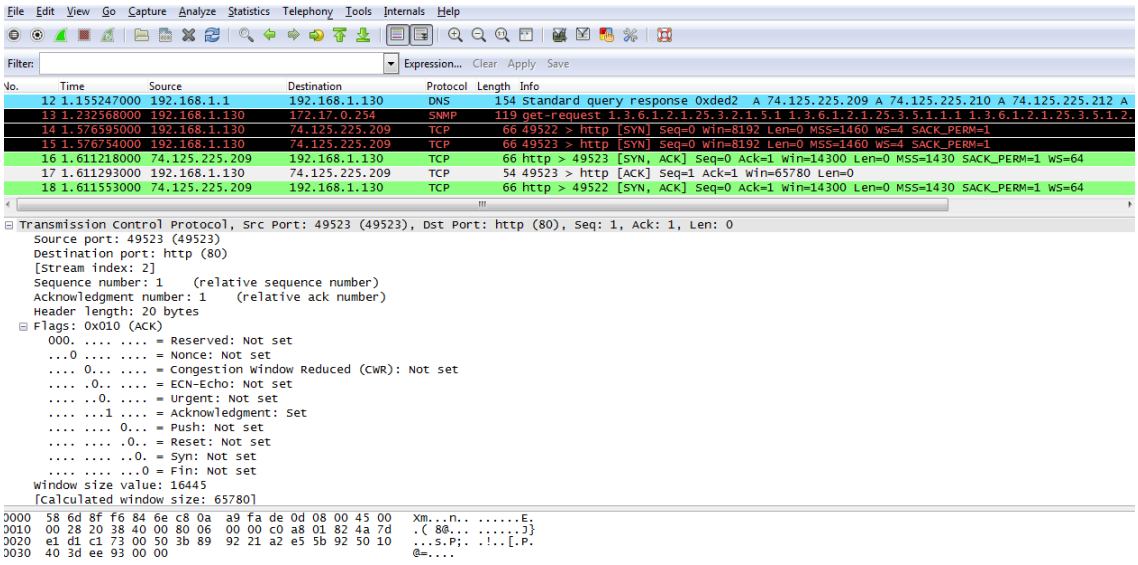


送信元ポートと宛先ポートの値は何ですか。

どのフラグが設定されていますか。

相対シーケンス番号および確認応答番号は何に設定されていますか。

e. 最後に、例の 3 ウェイ ハンドシェイクの 3 番目のパケットを検査します。上部ウィンドウでフレーム 17 をクリックすると、この例では次の情報が表示されます。



ハンドシェイクの 3 番目と最後のパケットを調べます。

どのフラグ（1 つまたは複数）が設定されていますか。

相対シーケンス番号および確認応答番号は、開始位置として 1 に設定されています。この時点で TCP 接続が確立され、送信元コンピュータと Web サーバ間のコミュニケーションを開始できます。

f. Wireshark プログラムを終了します。

復習

1. Wireshark では、何百ものフィルタを使用できます。大規模ネットワークには、さまざまなタイプのトラフィックが存在し、数多くのフィルタが利用される場合があります。このリストの中で、ネットワーク管理者に最も役立つ 3 つのフィルタはどれでしょうか。

2. 実稼働ネットワークでは Wireshark を他にどのように使用できますか。