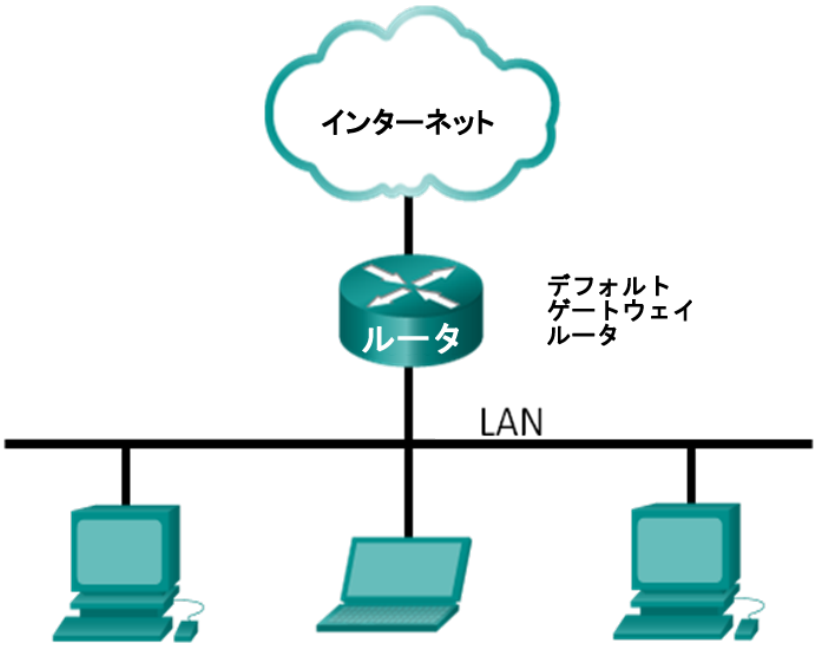
実習 - Wireshark を使用したネットワーク トラフィックの表示

トポロジ



目的

パート 1:(任意)Wireshark をダウンロードしてインストールする

パート 2:Wireshark でローカル ICMP データをキャプチャして分析する

- ローカル ホストへの ping トラフィックのデータ キャプチャを開始および停止します。
- 検出された PDU で IP および MAC アドレス情報を探します。

パート 3:Wireshark でリモート ICMP データをキャプチャして分析する

- リモート ホストへの ping トラフィックのデータ キャプチャを開始および停止します。
- 検出された PDU で IP および MAC アドレス情報を探します。
- リモート ホストの MAC アドレスがローカル ホストの MAC アドレスと異なる理由について説明します。

背景/シナリオ

Wireshark は、ネットワークのトラブルシューティング、分析、ソフトウェアとプロトコルの開発、および教育現場で使用されるソフトウェア プロトコル アナライザであり、「パケット スニファ」アプリケーションでもあります。Wireshark では、ネットワーク上を移動するデータ ストリームの各 PDU(Protocol Data Unit; プロトコル データ ユニット)を「キャプチャ」し、適切な RFC や他の仕様に従って PDU の内容をデコードして分析できます。

Wireshark は、ネットワークを使用するどのユーザにとっても便利なツールで、データ分析およびトラブルシューティングを扱う CCNA コースのほとんどの実習で使用できます。この実習では、Wireshark をダウンロードしてインストールするように指示します(すでにインストール済みの場合も)。この実習では、Wireshark を使用して、ICMP データ パケットの IP アドレスとイーサネット フレームの MAC アドレスをキャプチャします。

実習に必要なリソースや機器

- PC 1 台（インターネットを利用できる Windows 7、Vista、または XP 搭載 PC）
- LAN（Local-Area Network）上で ping 要求に応答できるその他の PC 1 台以上

パート 1:　（任意）Wireshark をダウンロードしてインストールする

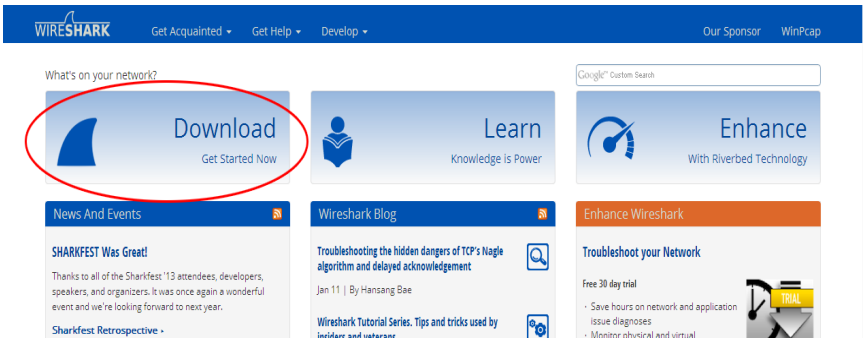
Wireshark は、ネットワーク エンジニアが使用する業界標準のパケット スニファ プログラムになっています。このオープン ソース ソフトウェアは、Windows、Mac、Linux など、さまざまな OS で使用できます。この実習のパート 1 では、Wireshark ソフトウェア プログラムをダウンロードして、PC にインストールします。

注：PC にすでに Wireshark がインストールされている場合は、パート 1 を省略し、パート 2 に直接移っても構いません。Wireshark が PC にインストールされていない場合は、インストラクタにアカデミーのダウンロード ポリシーを確認します。

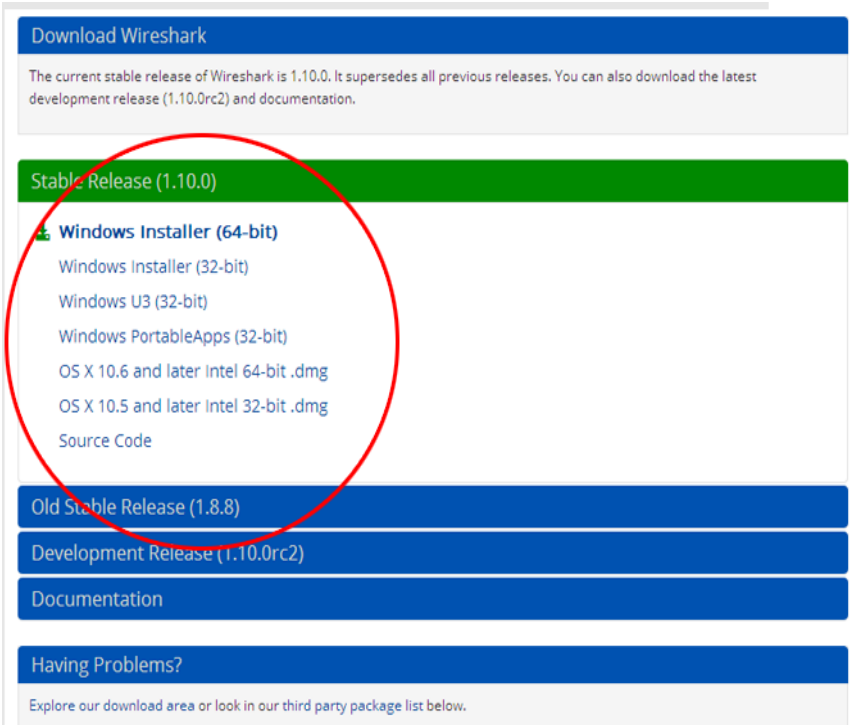
手順 1:　Wireshark をダウンロードする

a. Wireshark は www.wireshark.org からダウンロードできます。

b. [**Download Wireshark**] をクリックします。



c. PC のアーキテクチャと OS に基づいて、必要なソフトウェア バージョンを選択します。たとえば、64 ビット版 PC で Windows を実行している場合は、[**Windows Installer（64-bit）**] を選択します。

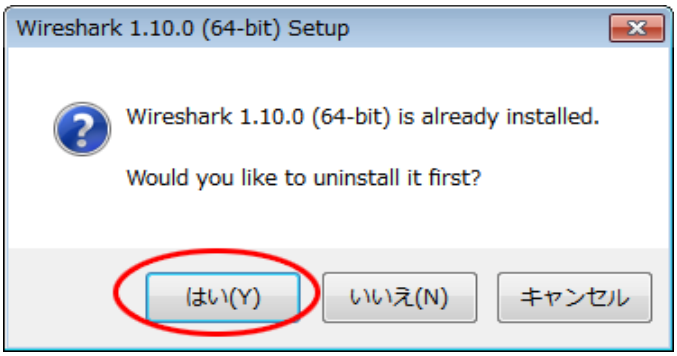


選択を終えると、ダウンロードが始まります。ファイルのダウンロード先は、使用するブラウザや OS によって異なります。Windows ユーザの場合、デフォルトの場所は **Downloads** フォルダです。

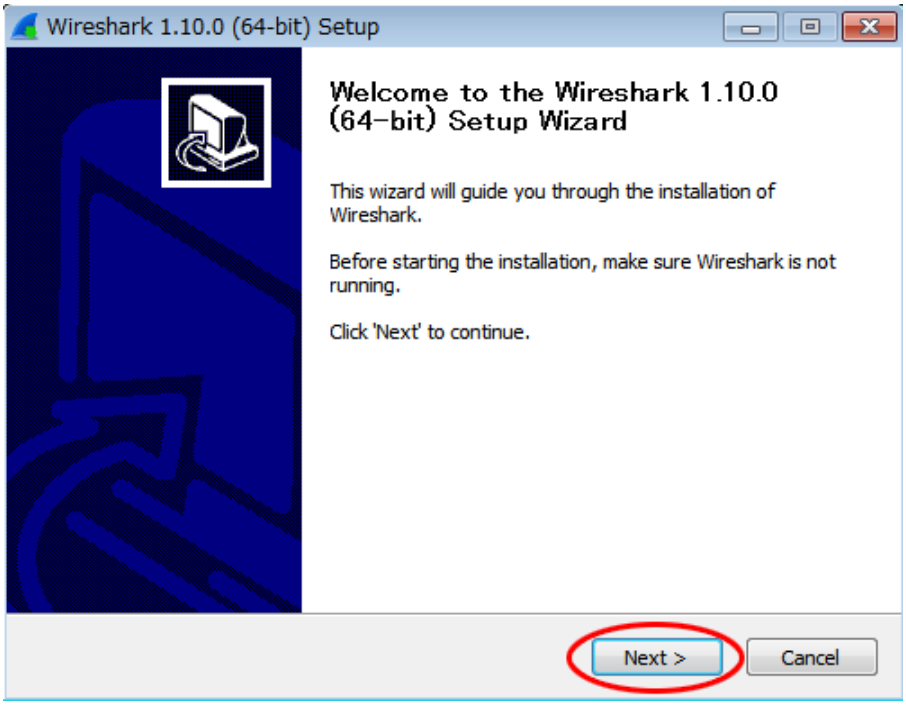
手順 2: Wireshark をインストールする

a. **Wireshark-win64-x.x.x.exe** というファイルがダウンロードされます（**x** はバージョン番号を表します）。ファイルをダブルクリックして、インストール プロセスを開始します。

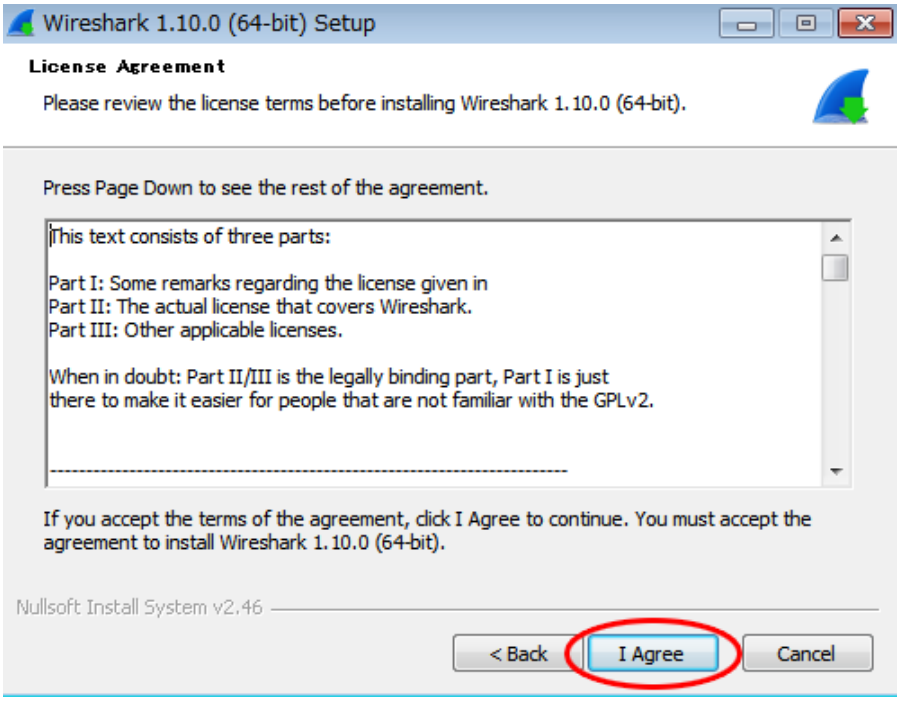
b. 画面にセキュリティ メッセージが表示された場合は応答します。PC に Wireshark のコピーがすでにある場合は、古いバージョンをアンインストールしてから、新しいバージョンをインストールするように指示されます。Wireshark の別のバージョンをインストールする前に、古いバージョンを削除することが推奨されます。[**Yes**] をクリックして、Wireshark の以前のバージョンをアンインストールします。



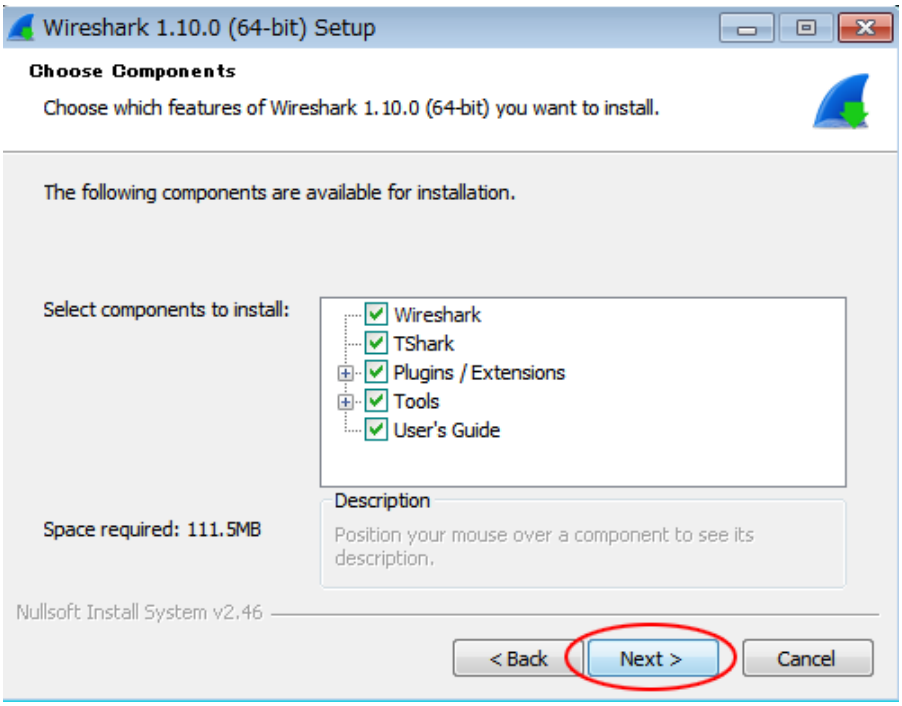
c. Wireshark を初めてインストールする場合、またはアンインストール プロセスが完了した場合は、Wireshark Setup ウィザードに移動します。[**Next**] をクリックします。



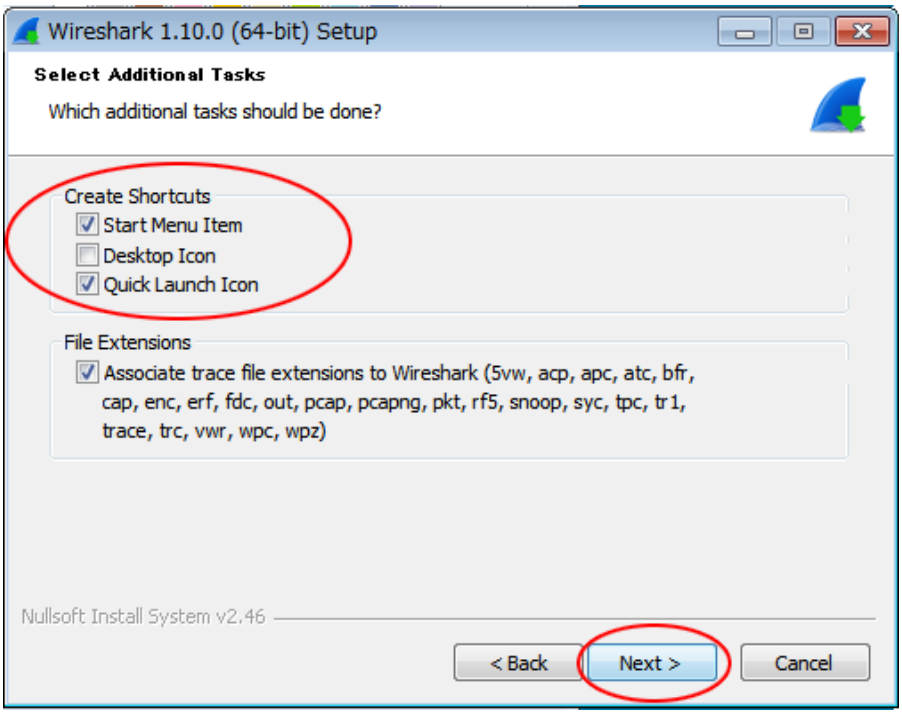
d. インストール プロセスを続行します。[License Agreement] ウィンドウが表示されたら、[**I Agree**] をクリックします。



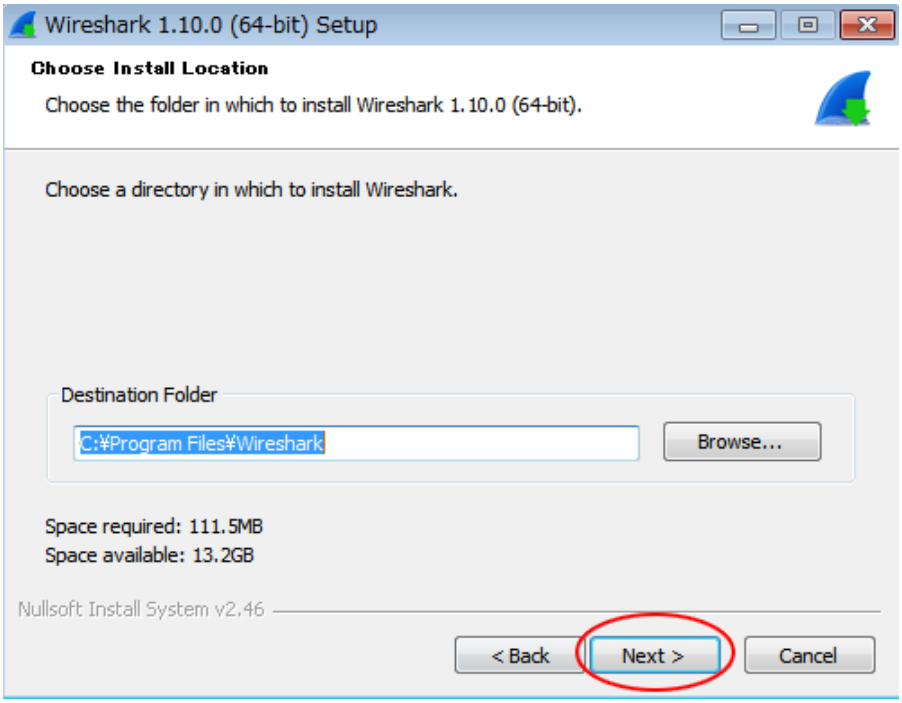
e. [Choose Components] ウィンドウのデフォルト設定をそのまま使用し、[**Next**] をクリックします。



f. 目的のショートカット オプションを選択し、[**Next**] をクリックします。

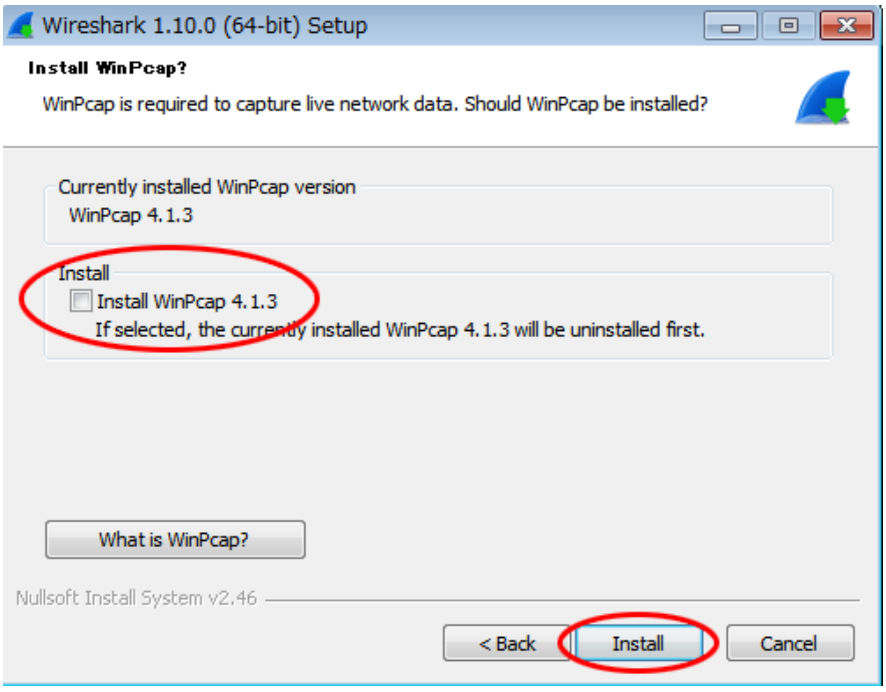


g. Wireshark をインストールする場所は変更できますが、ディスク スペースに制限がない限り、デフォルトの場所にインストールすることが推奨されます。

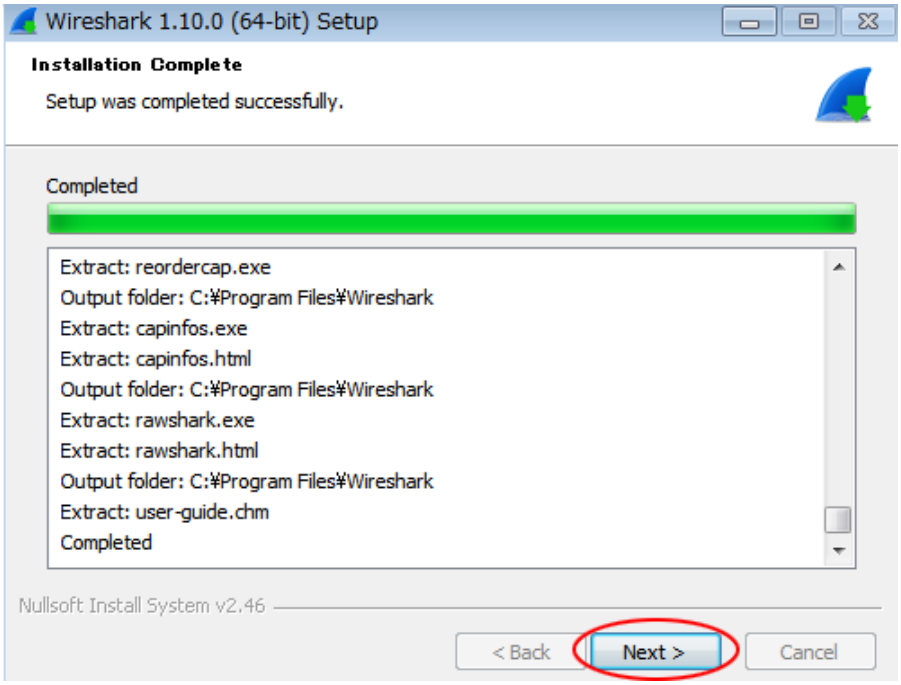


h. ライブ ネットワーク データをキャプチャするには、PC に WinPcap がインストールされている必要があります。WinPcap が PC にすでにインストールされている場合は、[Install] チェックボックスのチェックを外します。現在インストールされている WinPcap のバージョンが、Wireshark に付属するバージョンよりも古い場合は、[**Install WinPcap x.x.x**（バージョン番号）] チェックボックスをクリックして、より新しいバージョンをインストールすることが推奨されます。

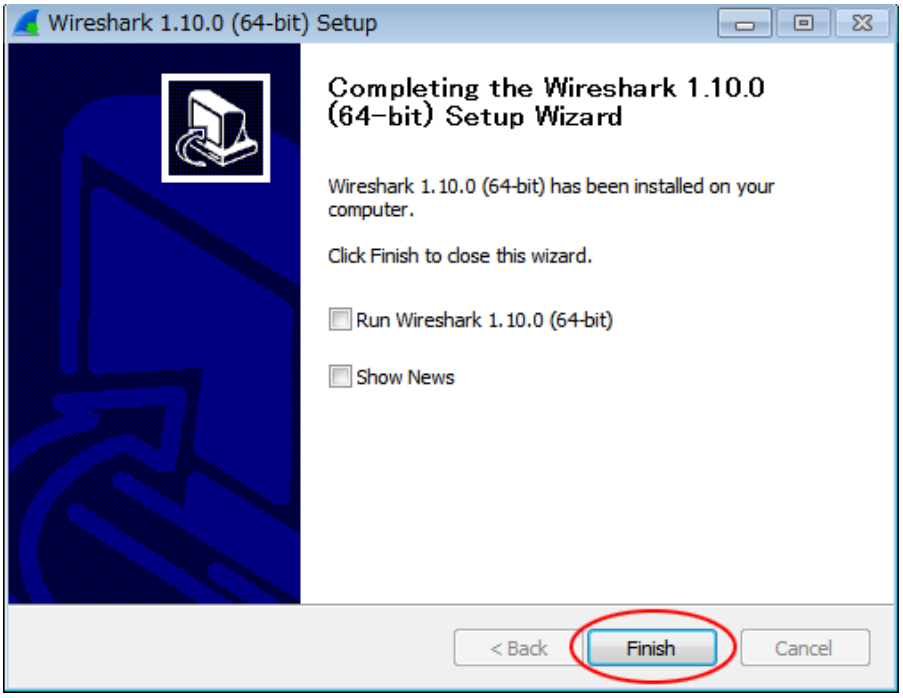
i. WinPcap がインストールされている場合は、WinPcap Setup ウィザードを終了します。



j. Wireshark ファイルのインストールが始まり、インストール状況を示す別のウィンドウが表示されます。インストールが完了したら、[**Next**] をクリックします。



k. [**Finish**] をクリックして、Wireshark インストール プロセスを完了します。



パート 2:　Wireshark でローカル ICMP データをキャプチャして分析する

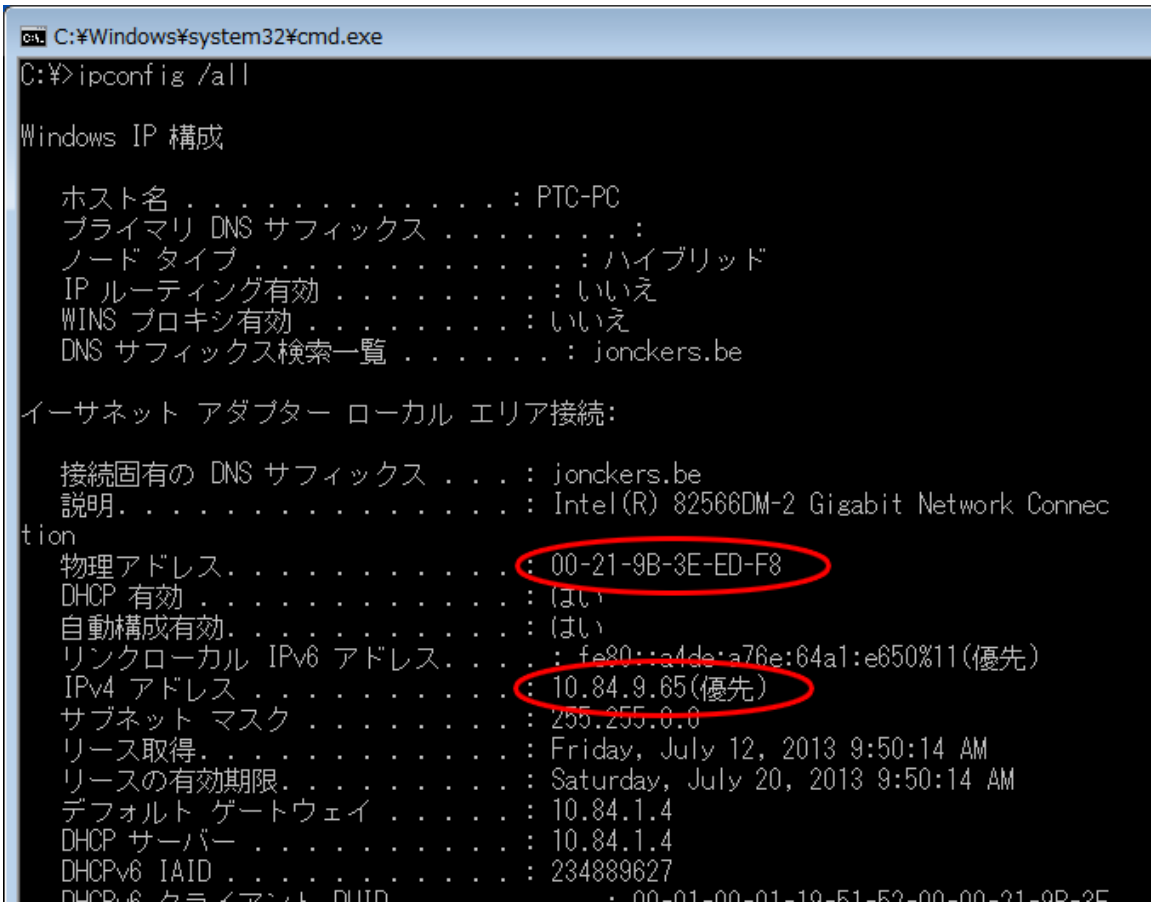
この実習のパート 2 では、LAN 上に存在する別の PC を ping し、ICMP 要求および応答を Wireshark でキャプチャします。また、キャプチャしたフレームの内部を見て特定の情報を調べます。この分析により、データを宛先に送るためにパケット ヘッダーがどのように使用されるかを明確に知ることができます。

手順 1:　PC のインターフェイス アドレスを取得する

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

a. コマンド ウィンドウを開いて、「**ipconfig /all**」と入力し、Enter キーを押します。

b. PC のインターフェイスの IP アドレスと MAC（物理）アドレスを書き留めます。

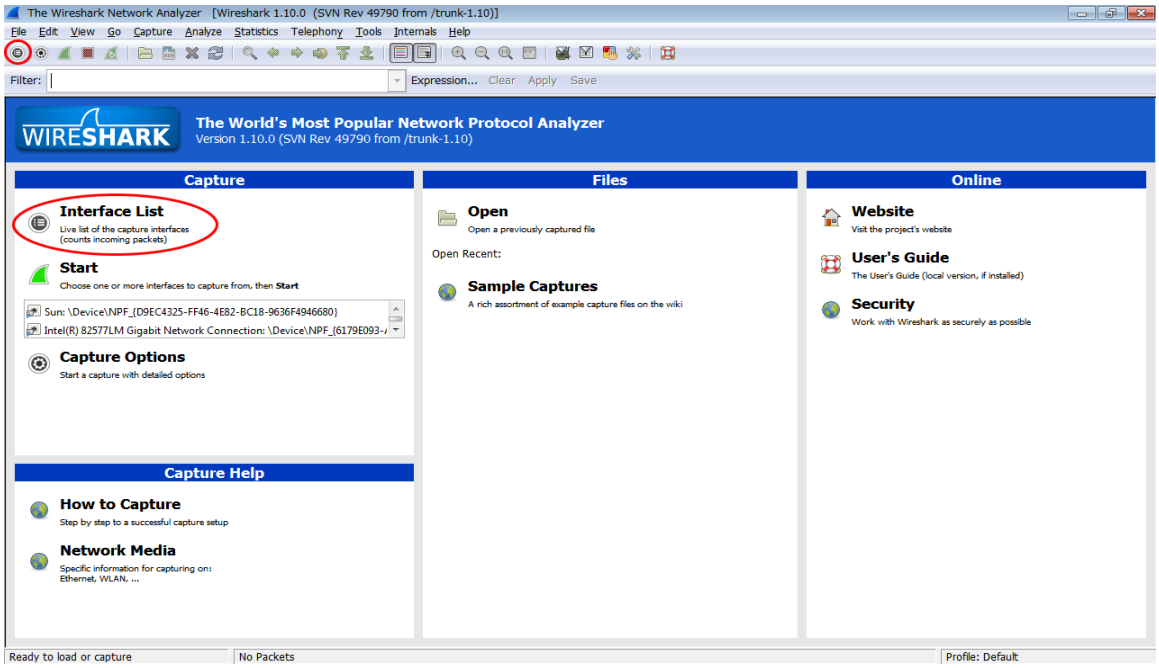


c. チーム メンバーの PC の IP アドレスを聞き、あなたの PC の IP アドレスをメンバーに教えます。このとき、あなたの PC の MAC アドレスはメンバーに教えないでください。

手順 2:　Wireshark を起動してデータのキャプチャを始める

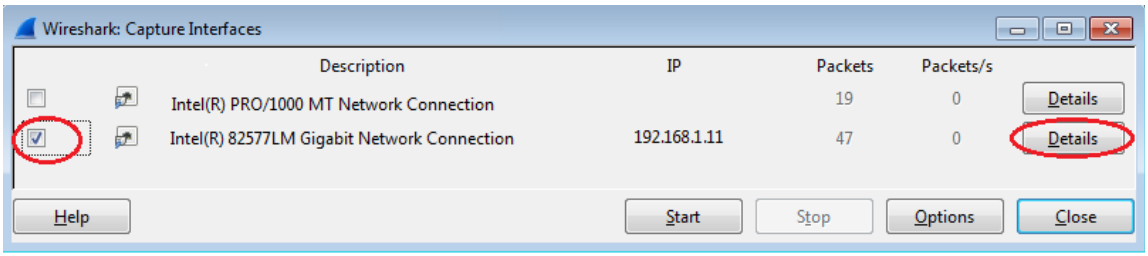
a. PC の Windows の [**スタート**] ボタンをクリックして、ポップアップ メニューのプログラムの一覧に Wireshark が表示されるのを確認します。[**Wireshark**] をダブルクリックします。

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

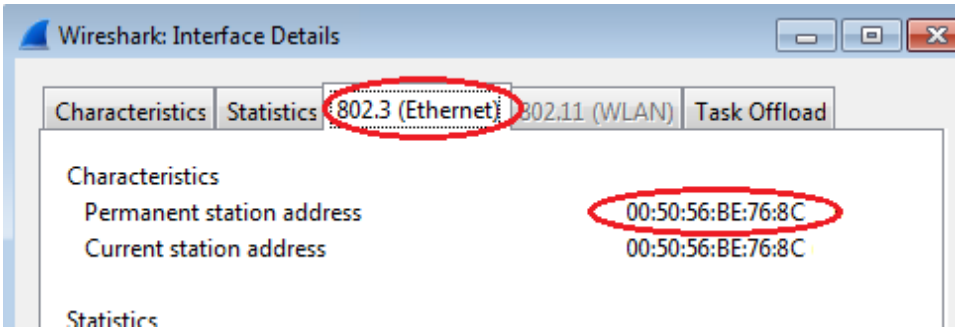


注：Interface List は、一連のアイコンの 1 番目にあるインターフェイス アイコンをクリックしても開くことができます。

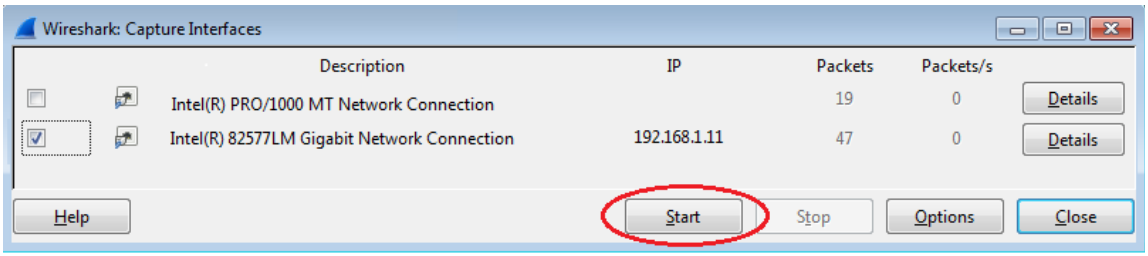
c. [Wireshark: Capture Interfaces] ウィンドウで、LAN に接続されているインターフェイスの横にあるチェックボックスをクリックします。



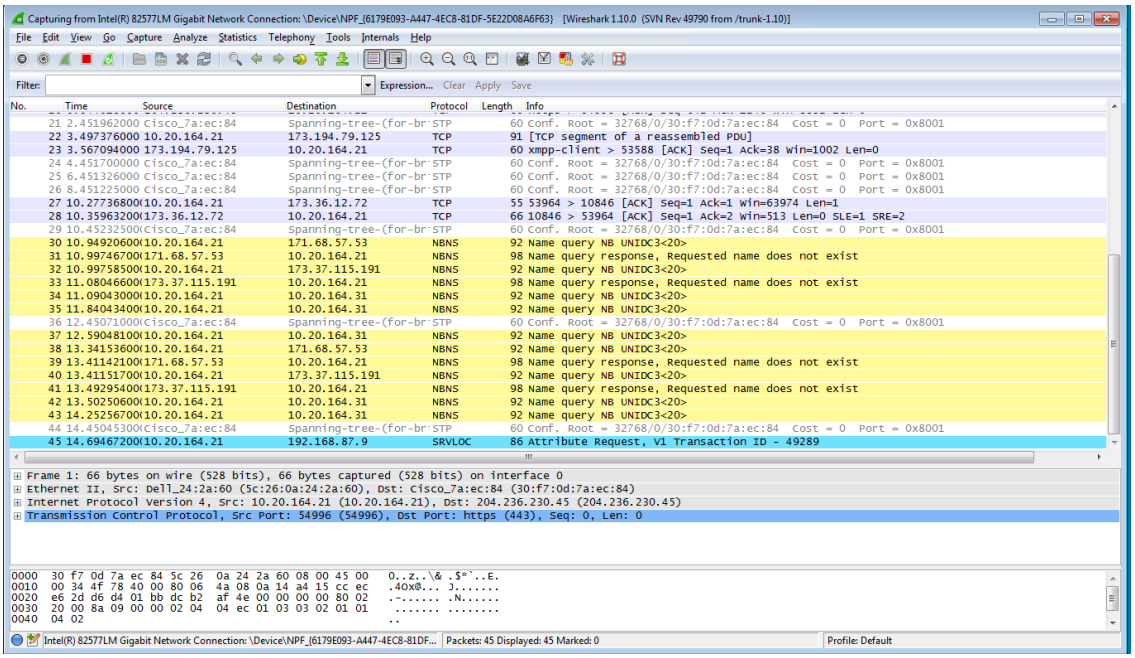
注：複数のインターフェイスが表示され、チェックするインターフェイスがわからない場合は、[**Details**] ボタンをクリックし、[**802.3（Ethernet）**] タブをクリックします。MAC アドレスが、手順 1b で書き留めた MAC アドレスと一致していることを確認します。正しいインターフェイスであることを確認したら、[Interface Details] ウィンドウを閉じます。



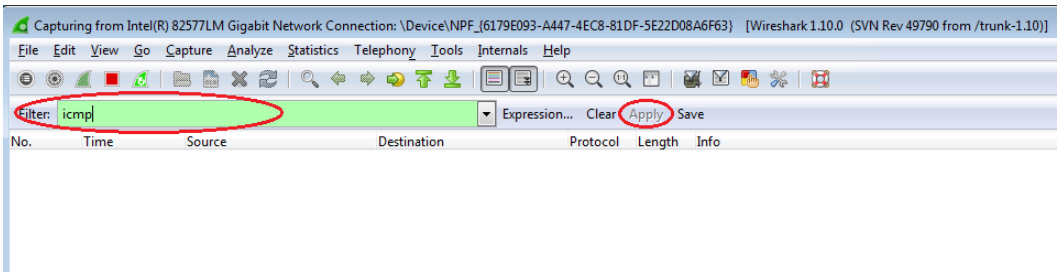
d. 正しいインターフェイスをチェックしたら、[**Start**] をクリックしてデータ キャプチャを始めます。



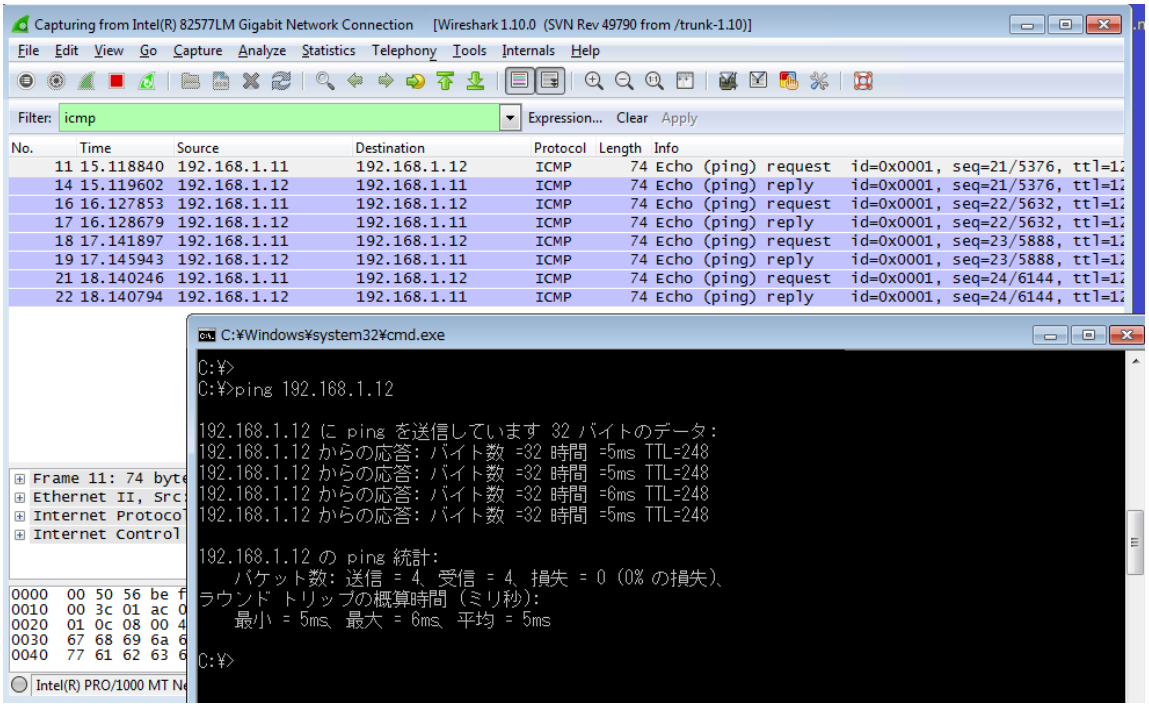
情報が Wireshark の一番上のセクションから下方へスクロールを始めます。データ行の色は、プロトコルの違いによって異なります。



e. この情報は、PC と LAN の間で実行されている通信の種類によっては高速でスクロールすることがあります。フィルタを適用すると、Wireshark がキャプチャしているデータを表示および操作するのが容易になります。この実習では、ICMP（ping）PDU のみを表示します。Wireshark の上部にある [Filter] ボックスに「**icmp**」と入力して Enter キーを押すか、[**Apply**] ボタンをクリックして ICMP（ping）PDU のみを表示します。

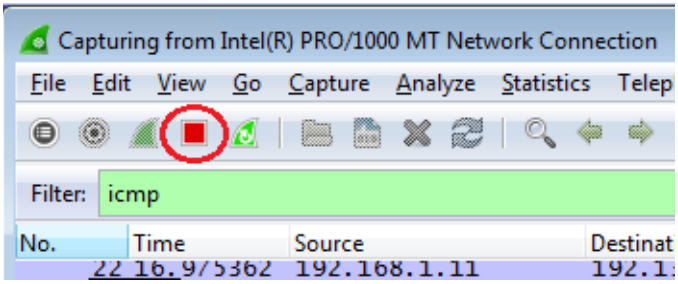


f. このフィルタを適用すると、上部のウィンドウにデータが何も表示されなくなりますが、インターフェイスのトラフィックのキャプチャは継続しています。前の手順で開いたコマンド プロンプト ウィンドウを表示し、チーム メンバーから聞いた IP アドレスを ping します。Wireshark の上部のウィンドウにデータが再度表示されるのを確認します。



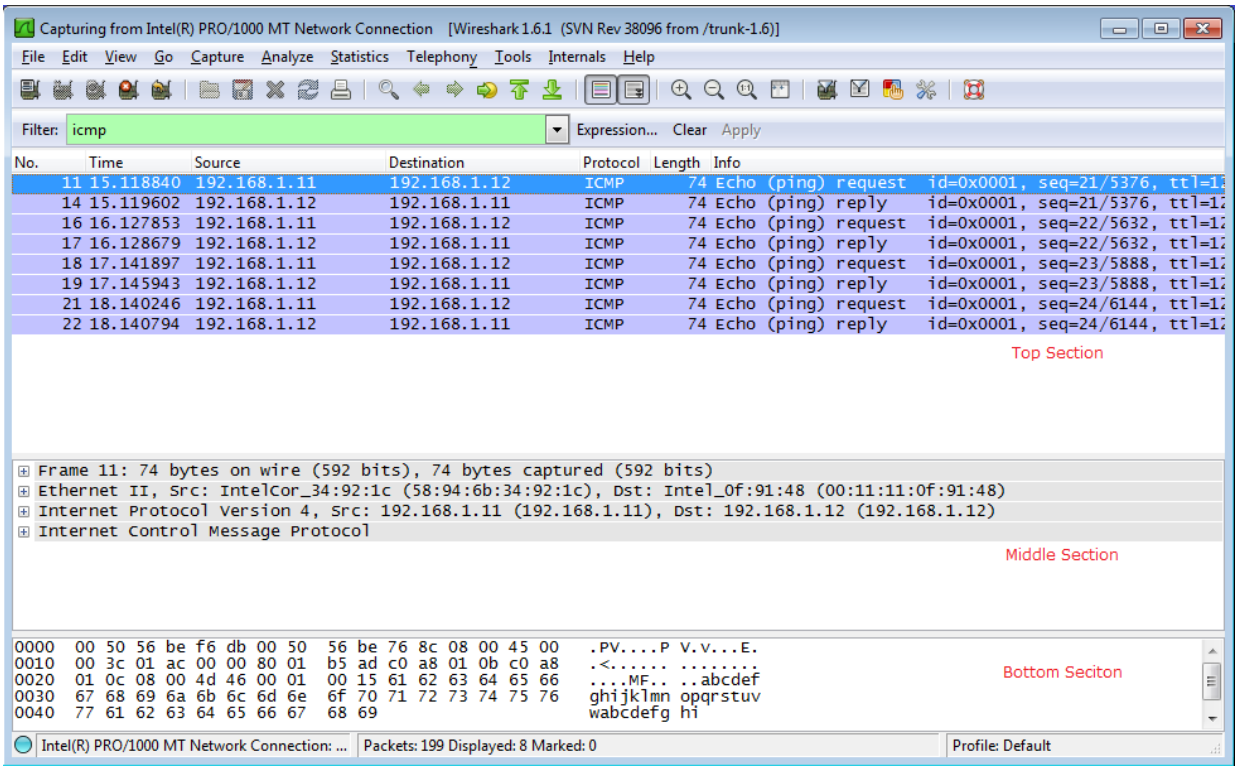
注:チーム メンバーの PC が ping に応答しない場合は、PC のファイアウォールが ping 要求をブロックしている可能性があります。Windows 7 を使用したファイアウォールで ICMP トラフィックの通過を許可する方法については、Appendix A: Allowing ICMP Traffic Through a Firewall を参照してください。

g. [**Stop Capture**] アイコンをクリックして、データのキャプチャを停止します。

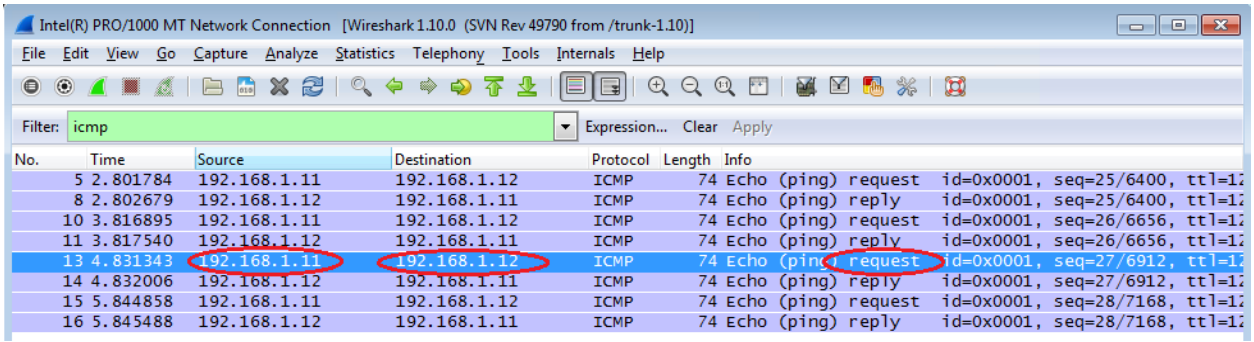


手順 3:　キャプチャしたデータを調べる

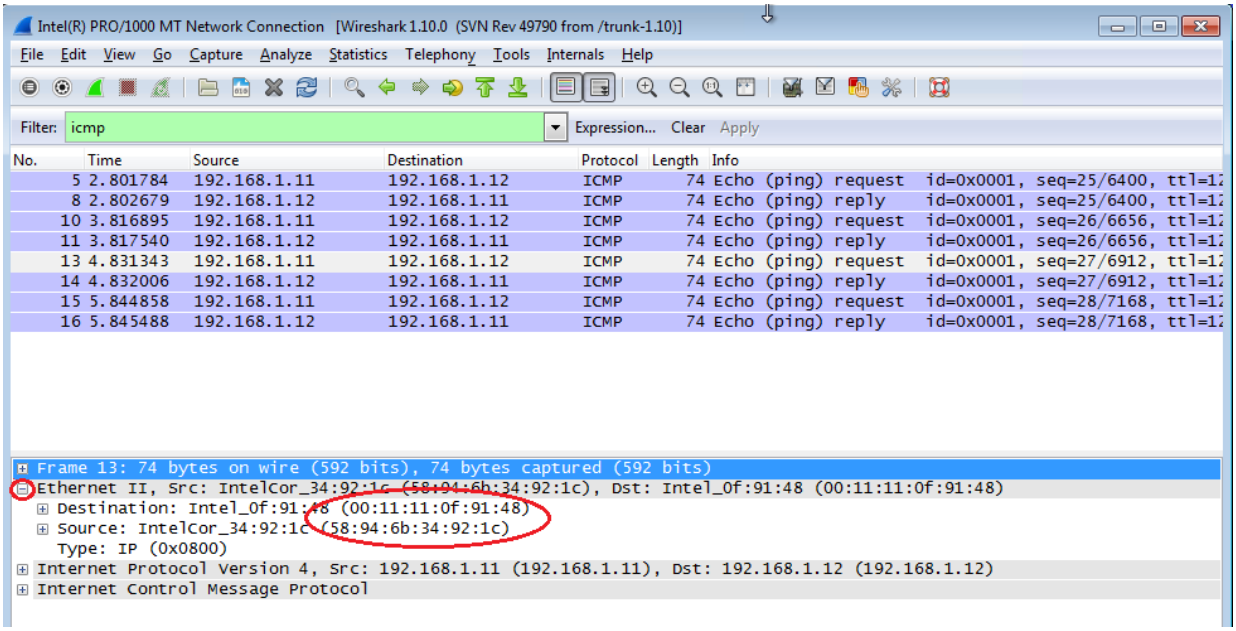
手順 3 では、チーム メンバーの PC の ping 要求によって生成されたデータを調べます。Wireshark データは 3 つのセクションに表示されます。1）上部セクションには、キャプチャされた PDU フレームのリストと IP パケット情報の要約が表示されます。2）中央セクションには、画面上部で選択されたフレームの PDU 情報が表示されます。キャプチャされた PDU フレームは、プロトコル層別に分けて表示されます。3）下部セクションには、各層の未加工のデータが表示されます。未加工のデータは、16 進形式と 10 進形式の両方で表示されます。



a. Wireshark の上部セクションで、最初の ICMP 要求の PDU フレームをクリックします。[Source] 列に PC の IP アドレスが表示され、[Destination] 列には、ping 先のチームメイトの PC の IP アドレスが表示されます。



b. この PDU フレームを上部セクションで選択した状態で、中央セクションに移動します。Ethernet II の行の左側にあるプラス記号をクリックして、宛先と送信元の MAC アドレスを表示します。



送信元 MAC アドレスが、あなたの PC のインターフェイスと一致していますか。

Wireshark の宛先 MAC アドレスが、あなたのチーム メンバーの PC の MAC アドレスと一致していますか。

ping した PC の MAC アドレスは、あなたの PC からどのような方法で取得されていますか。

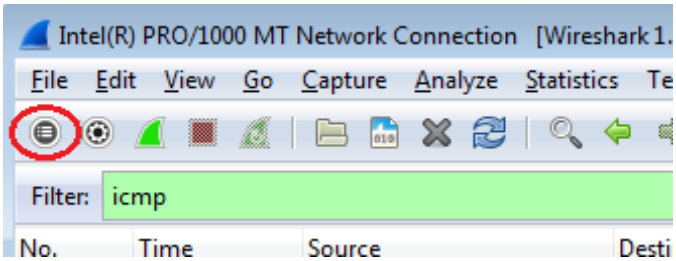
注:ICMP 要求をキャプチャした前の例では、ICMP データは、まず IPv4 パケット PDU(IPv4 ヘッダー)にカプセル化され、その後、LAN 上で転送できるようにイーサネット II フレーム PDU(イーサネット II ヘッダー)にカプセル化されます。

パート 3:　Wireshark でリモート ICMP データをキャプチャして分析する

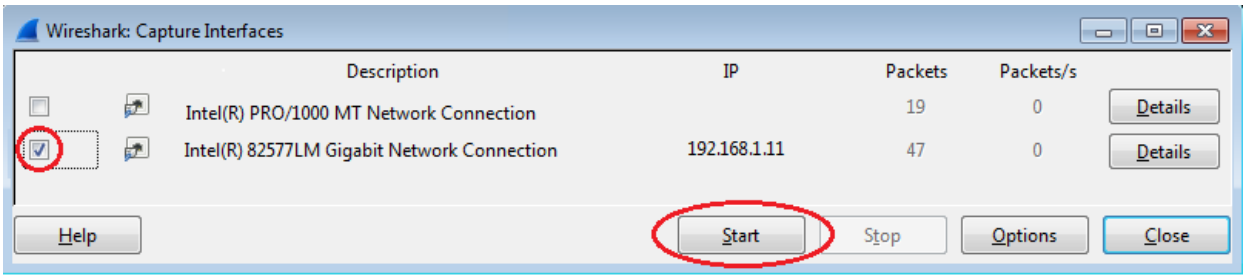
パート 3 では、リモート ホスト（LAN 上に存在しないホスト）を ping し、それらの ping から生成されたデータを調べます。その後、このデータと手順 2 で調べたデータとの違いを調べます。

手順 1:　インターフェイスのデータのキャプチャを始める

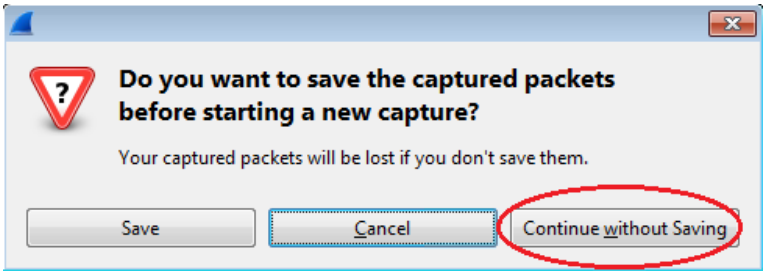
a. [**Interface List**] アイコンをクリックして、PC のインターフェイスの一覧を再度表示します。



b. LAN インターフェイスの横にあるチェックボックスがチェックされていることを確認したら、[**Start**] をクリックします。

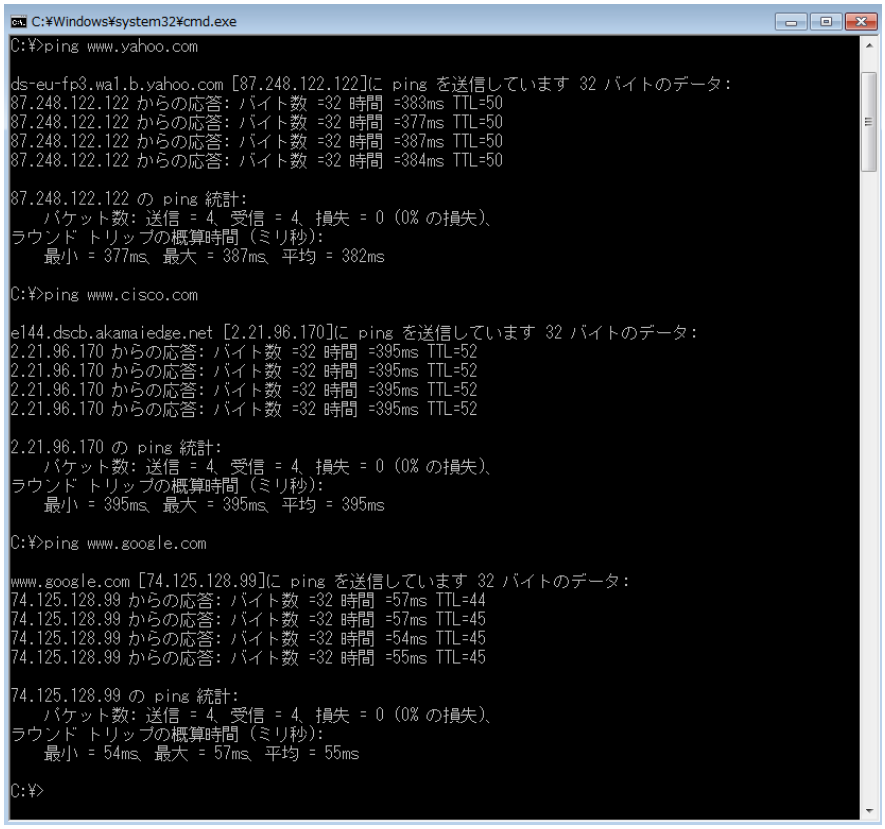


c. 新しいキャプチャを始める前に、以前のキャプチャ データを保存するように指示するウィンドウが表示されます。このデータを保存する必要はありません。[**Continue without Saving**] をクリックします。



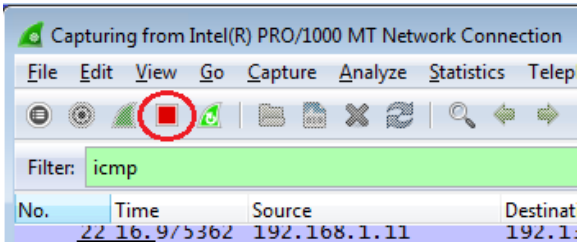
d. キャプチャをアクティブにした状態で、次の 3 つの Web サイトの URL を ping します。

1) www.yahoo.com
2) www.cisco.com
3) www.google.com



注: 記載されている URL を ping すると、これらの URL を DNS（Domain Name Service）サーバが IP アドレスに変換します。受信した各 URL の IP アドレスを書き留めます。

e. [**Stop Capture**] アイコンをクリックして、データのキャプチャを停止できます。



手順 2: リモート ホストからのデータを調査および分析する

a. Wireshark でキャプチャしたデータを確認し、ping した 3 ヵ所の IP アドレスと MAC アドレスを調べます。下の空欄に、3 ヵ所すべての宛先 IP アドレスと宛先 MAC アドレスを記入します。

1 番目の場所: IP: MAC:

2 番目の場所: IP: MAC:

3 番目の場所: IP: MAC:

b. この情報では特にどのような点が重要ですか。

c. この情報は、パート 2 で受信したローカル ping 情報とどのような点で異なりますか。

復習

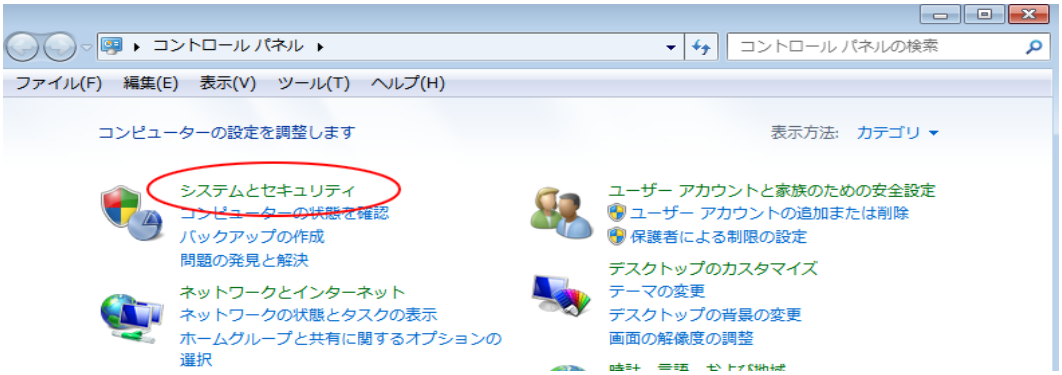
Wireshark では、ローカル ホストの実際の MAC アドレスが表示されますが、リモート ホストの実際の MAC アドレスは表示されません。それはなぜですか。

付録 A:ファイアウォールで ICMP トラフィックの通過を許可する

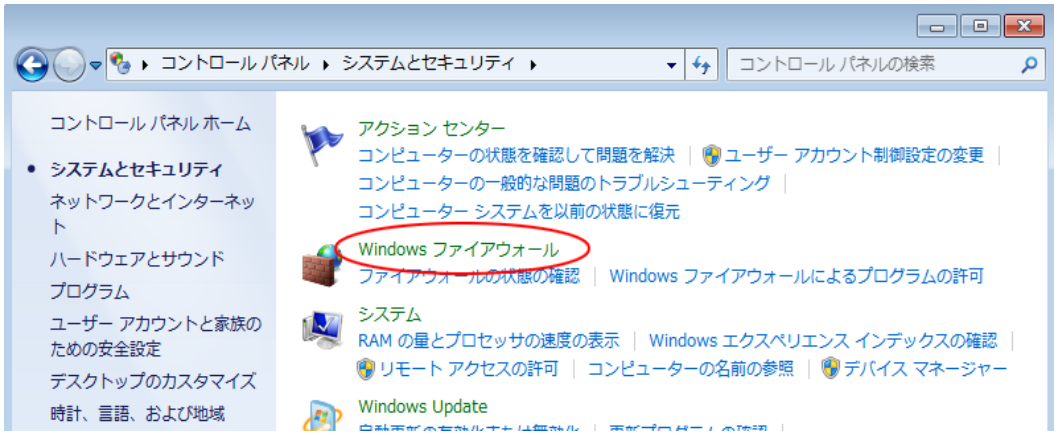
チームのメンバーがあなたの PC を ping できない場合、ファイアウォールが ping 要求をブロックしている可能性があります。この付録では、ping 要求を許可するファイアウォール規則を作成する方法について説明します。また、実習が終了したら、新しい ICMP 規則を無効にする方法についても説明します。

手順 1: ファイアウォールで ICMP トラフィックの通過を許可する新しい受信の規則を作成する

a. コントロール パネルから、[**システムとセキュリティ**] オプションをクリックします。

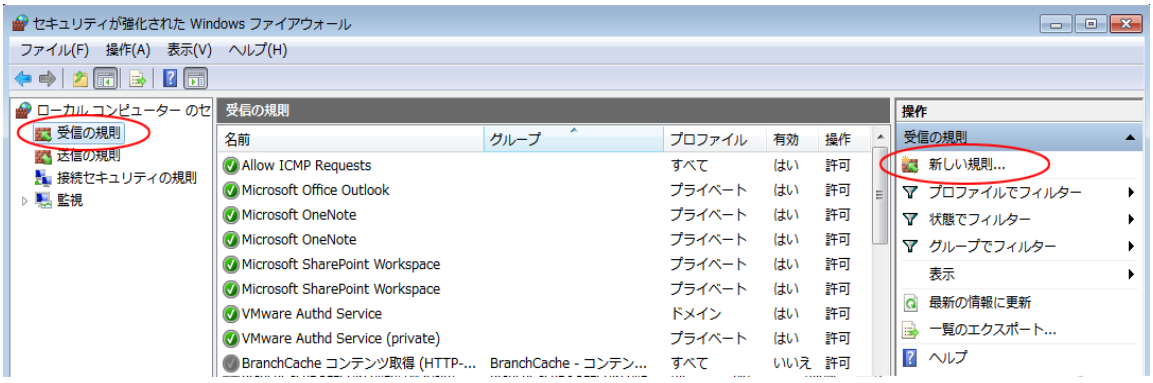


b. [システムとセキュリティ] ウィンドウで、[**Windows ファイアウォール**] をクリックします。

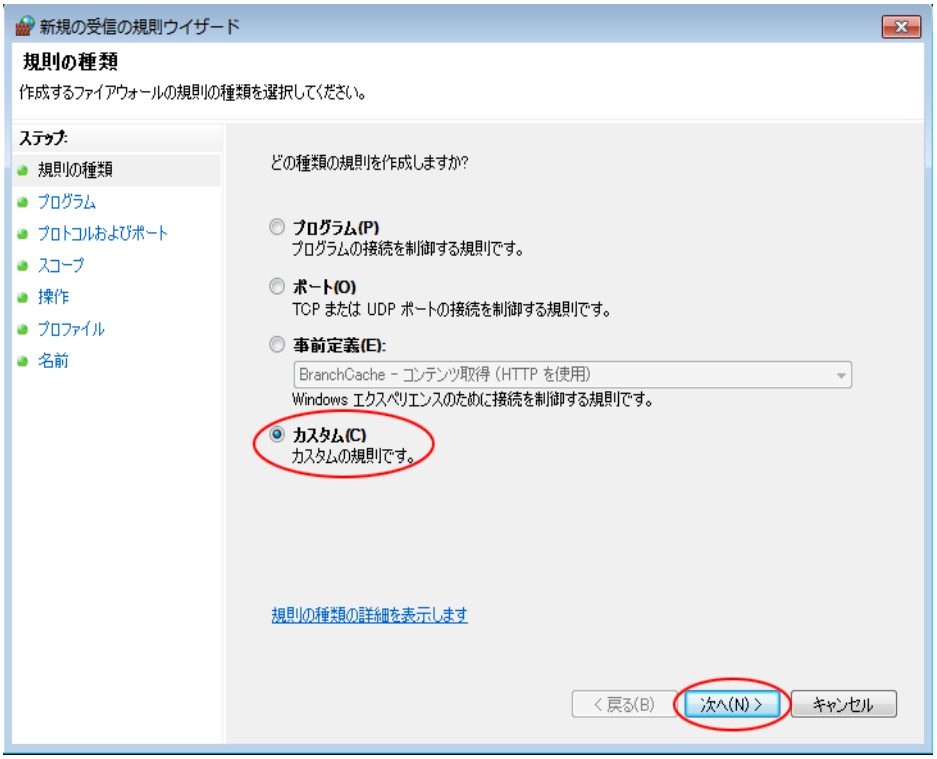


c. [Windows ファイアウォール] ウィンドウの左ペインで、[**詳細設定**] をクリックします。

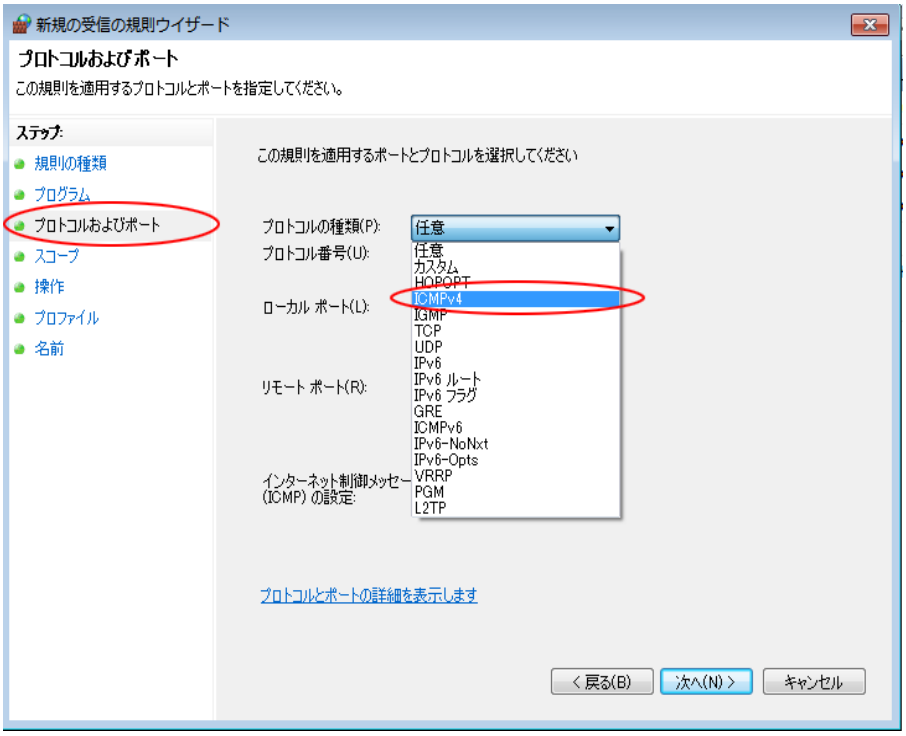
d. [セキュリティが強化された Windows ファイアウォール] ウィンドウで、左サイドバーの [**受信の規則**] オプションを選択し、右サイドバーの [**新しい規則**] をクリックします。



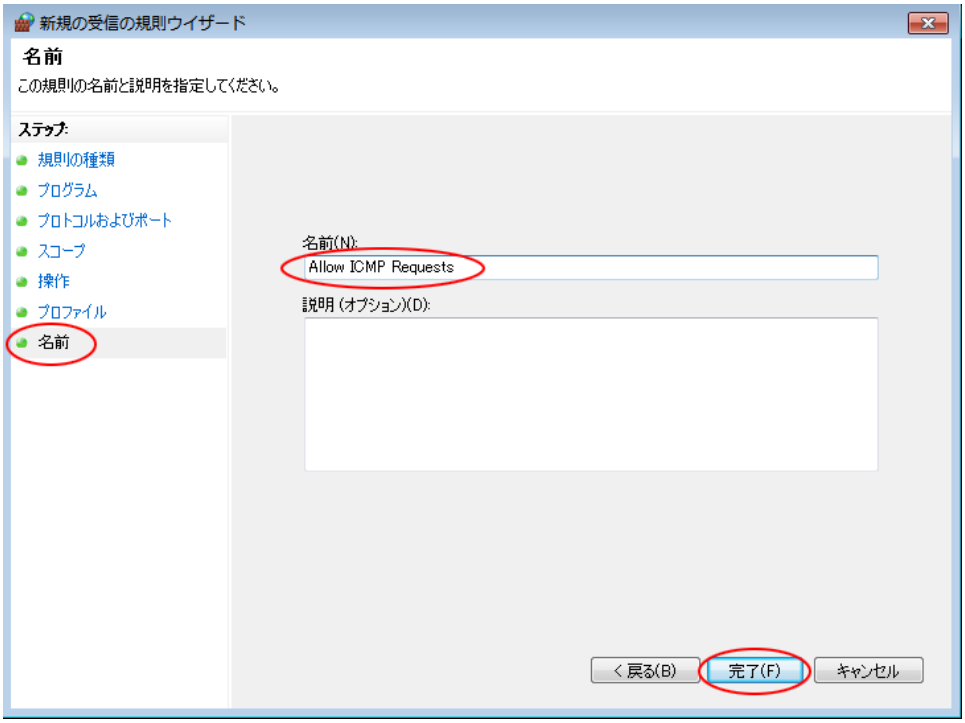
e. 新規の受信の規則ウィザードが起動します。[規則の種類] 画面で、[**カスタム**] オプション ボタンをクリックし、[**次へ**] をクリックします。



f. 左ペインで、[**プロトコルおよびポート**] オプションをクリックし、[プロトコルの種類] ドロップダウン メニューの [**ICMPv4**] を選択し、[**次へ**] をクリックします。



g. 左ペインで、[**名前**] オプションをクリックし、[名前] フィールドに「**Allow ICMP Requests**」と入力します。[**Finish**] をクリックします。

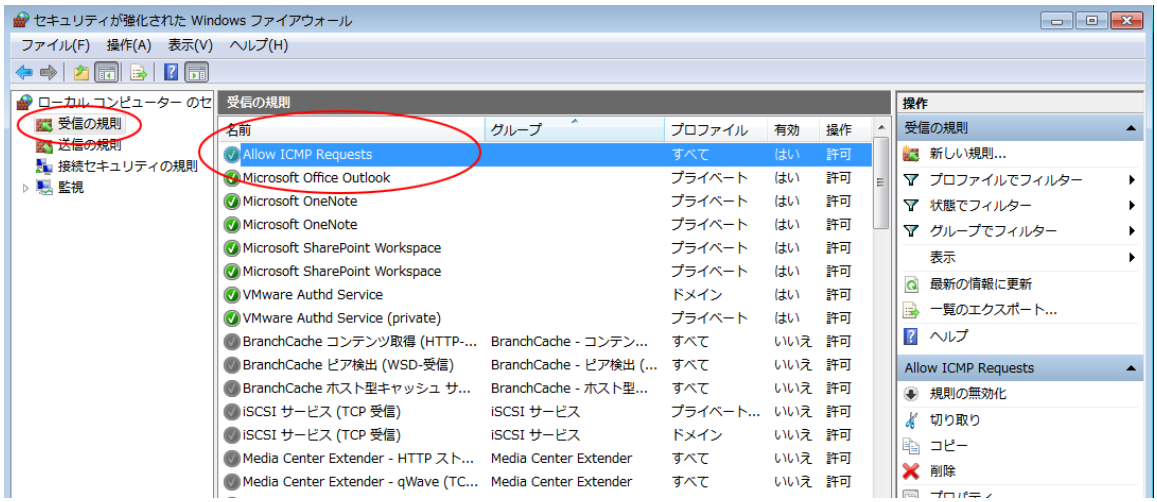


この新しい規則を使用すると、チーム メンバーは、あなたの PC から ping 応答を受信できます。

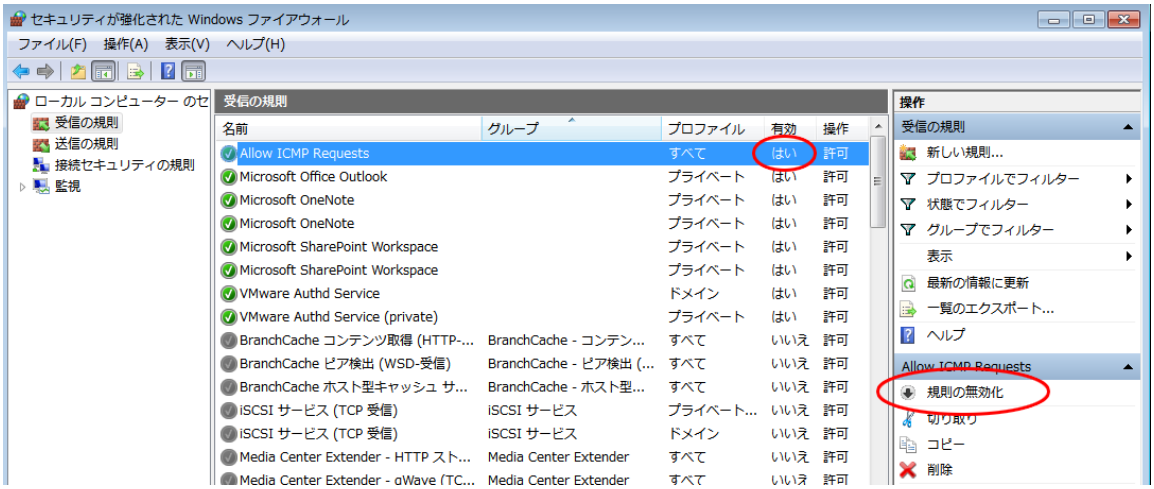
手順 2: 新しい ICMP 規則を無効化または削除する

実習が終了したら、手順 1 で作成した新しい規則を無効化または削除できます。[**規則の無効化**] オプションを使用すると、後日、規則を再度有効にできます。規則を完全に削除すると、[受信の規則] の一覧から規則が削除されます。

a. [セキュリティが強化された Windows ファイアウォール] ウィンドウの左ペインで、[**受信の規則**] をクリックし、手順 1 で作成した規則を見つけます。



b. 規則を無効にするには、[**規則の無効化**] オプションをクリックします。このオプションを選択すると、オプション名が [**規則の有効化**] に変わります。このオプションは [規則の無効化] と [規則の有効化] の間で切り替えることができます。規則の状態は [受信の規則] の一覧の [有効] 列に表示されます。



c. ICMP 規則を完全に削除するには、[**削除**] をクリックします。このオプションを選択した場合は、ICMP 応答を許可する規則を再度作成する必要があります。