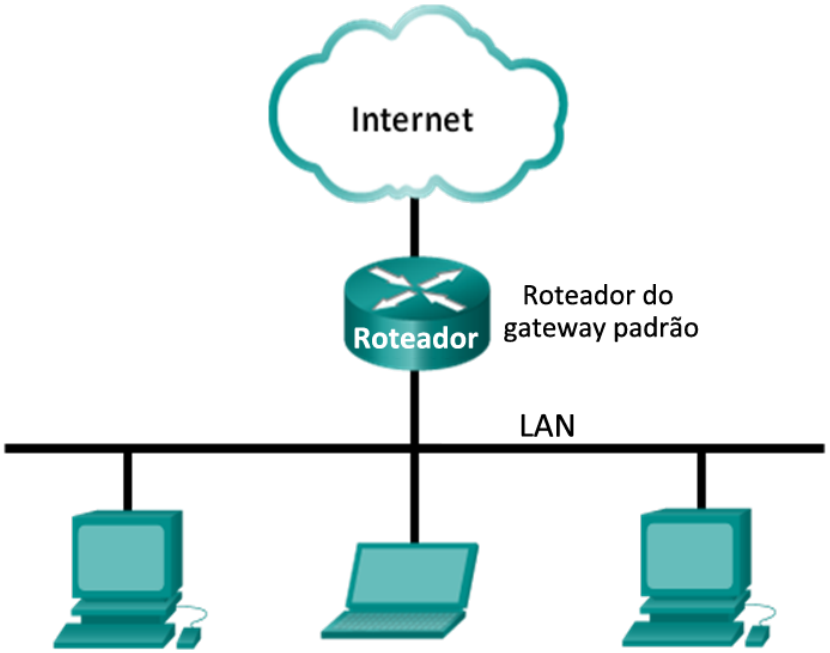
Laboratório - Uso do Wireshark para visualizar o tráfego de rede

Topologia



Objetivos

Parte 1: (Opcional) Baixar e instalar o Wireshark

Parte 2: Capturar e analisar dados locais ICMP no Wireshark

- Inicie e interrompa a captura de dados do tráfego de ping para os hosts locais.
- Localize informações sobre o endereço IP e MAC em PDUs capturadas.

Parte 3: Capturar e analisar dados remotos ICMP no Wireshark

- Inicie e interrompa a captura de dados do tráfego de ping para os hosts remotos.
- Localize informações sobre o endereço IP e MAC em PDUs capturadas.
- Explique por que os endereços MAC para hosts remotos são diferentes dos endereços MAC de hosts locais.

Histórico/cenário

O Wireshark é um software de análise de protocolo, ou aplicação de “packet sniffer”, usado para solução de problemas de rede, análise, desenvolvimento de software e protocolo, e educação. À medida que o fluxo de dados viaja em uma rede, o sniffer “captura” cada unidade de dados de protocolo (PDU) e pode decodificar e analisar seu conteúdo de acordo com o RFC apropriado ou com outras especificações.

O Wireshark é uma ferramenta útil para quem trabalha com redes e pode ser usado com a maioria dos laboratórios nos cursos CCNA para análise de dados e solução de problemas. Este laboratório apresenta instruções para baixar e instalar o Wireshark, embora talvez já esteja instalado. Neste laboratório, você usará o Wireshark para capturar endereços IP do pacote de dados ICMP e endereços MAC do quadro Ethernet.

Recursos necessários

- 1 PC (Windows 7, Vista ou XP com acesso à Internet)
- Serão usados outros PCs em uma rede local (LAN) para responder às solicitações de ping.

Parte 1: (Opcional) Baixar e instalar o Wireshark.

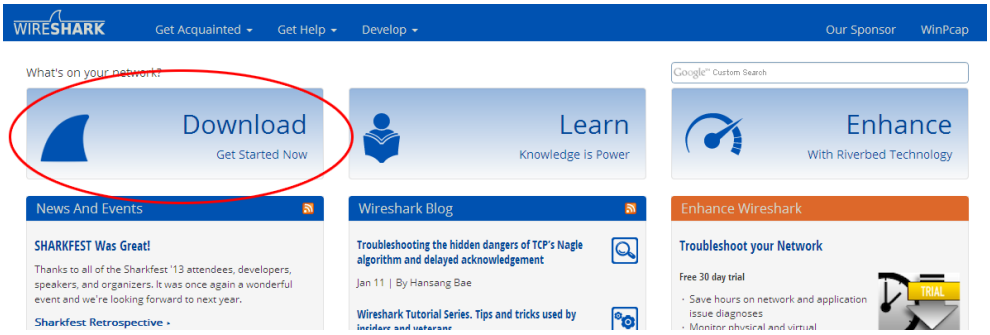
O Wireshark tornou-se o programa de sniffer de pacotes padrão do setor usado por engenheiros de rede. Este software aberto está disponível para vários sistemas operacionais diferentes, incluindo Windows, Mac e Linux. Na parte 1 deste laboratório, você baixará e instalará o programa de software Wireshark em seu PC.

Observação: se o Wireshark já estiver instalado no PC, você pode pular a parte 1 e ir direto para a parte 2. Se o Wireshark não estiver instalado no PC, verifique com seu instrutor a política de download de software de sua academia.

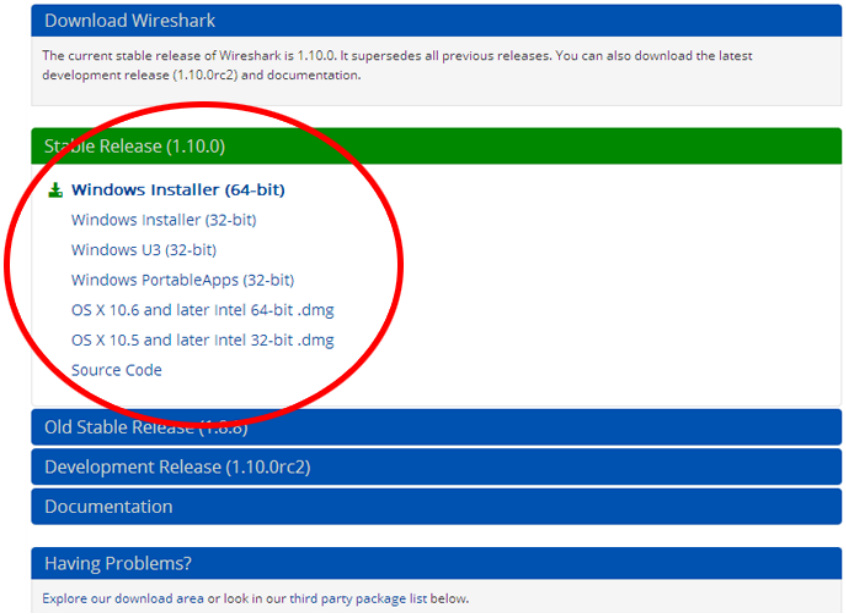
Etapa 1: Baixar o Wireshark.

a. O Wireshark pode ser baixado em www.wireshark.org.

b. Clique em **Baixar o Wireshark**.



c. Escolha a versão de software necessária com base na arquitetura e no sistema operacional do PC. Por exemplo, se você tiver um PC de 64 bits executando o Windows, selecione **Windows Installer (64-bit) (Instalador do Windows (64 bits))**.

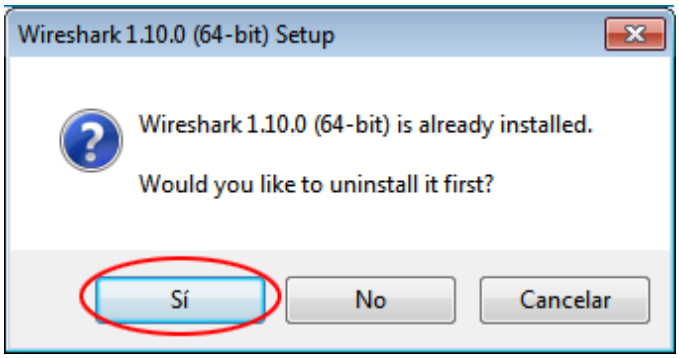


Depois de fazer uma seleção, o download será iniciado. O destino do download do arquivo depende do navegador e do sistema operacional usados. Para usuários do Windows, o local padrão é a pasta **Downloads**.

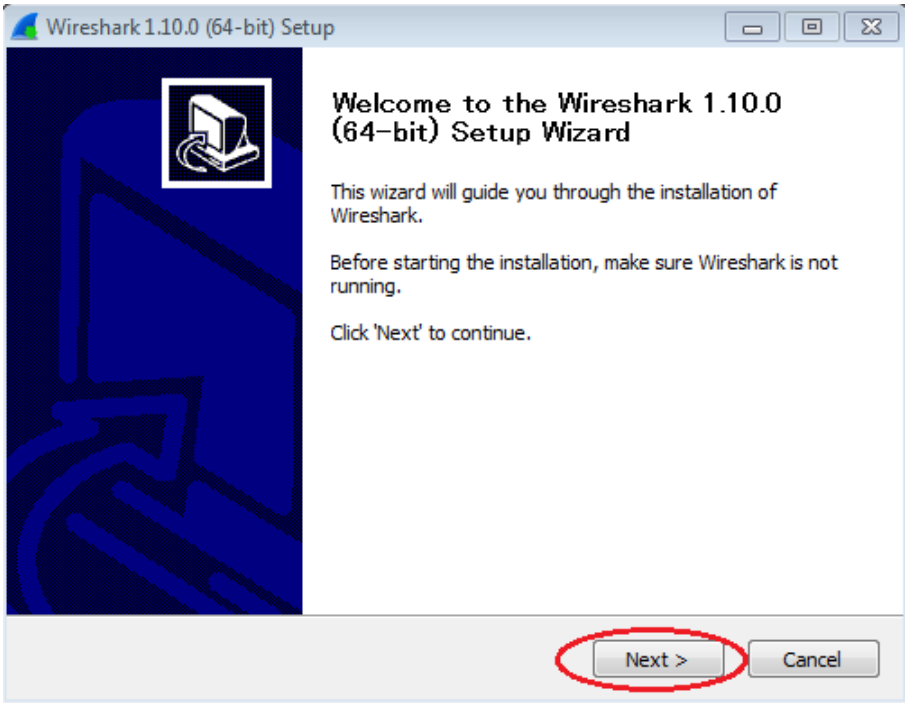
Etapa 2: Instalar o Wireshark.

a. O arquivo baixado é chamado **Wireshark-win64-x.x.x.exe**, em que **x** representa o número da versão. Clique duas vezes no arquivo para iniciar o processo de instalação.

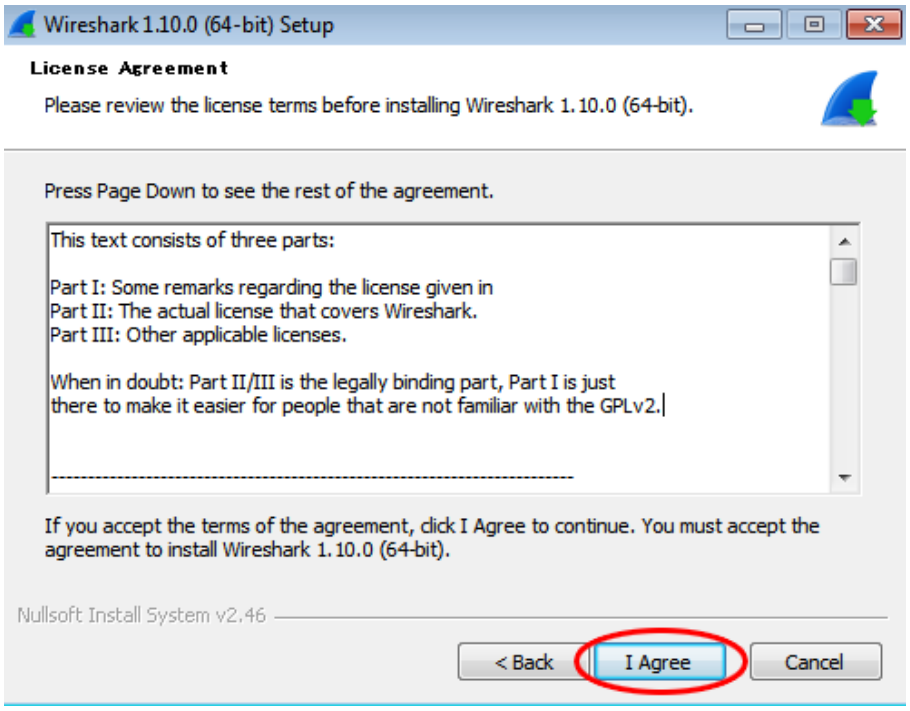
b. Responda a todas as mensagens de segurança que aparecerem na tela. Se já tiver uma cópia do Wireshark em seu PC, será solicitado que você desinstale a versão anterior antes de instalar a nova versão. Recomenda-se que você remova a versão antiga do Wireshark antes de instalar outra versão. Clique em **Sim** para desinstalar a versão anterior do Wireshark.



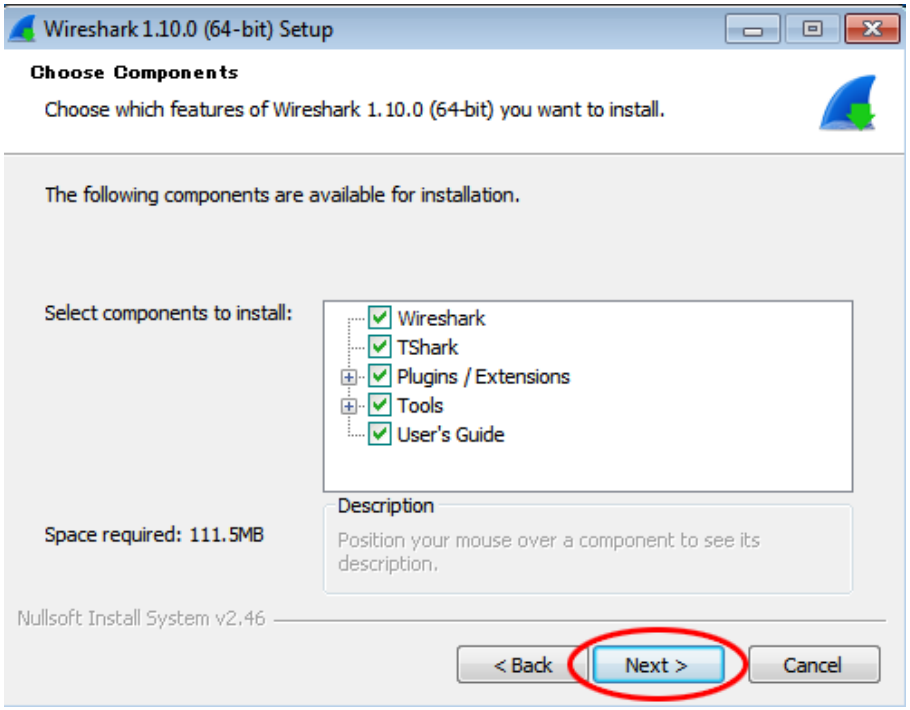
c. Se esta for a primeira instalação do Wireshark, ou após concluir o processo de desinstalação, você navegará para o assistente de configuração do Wireshark. Clique em **Next (Próximo)**.



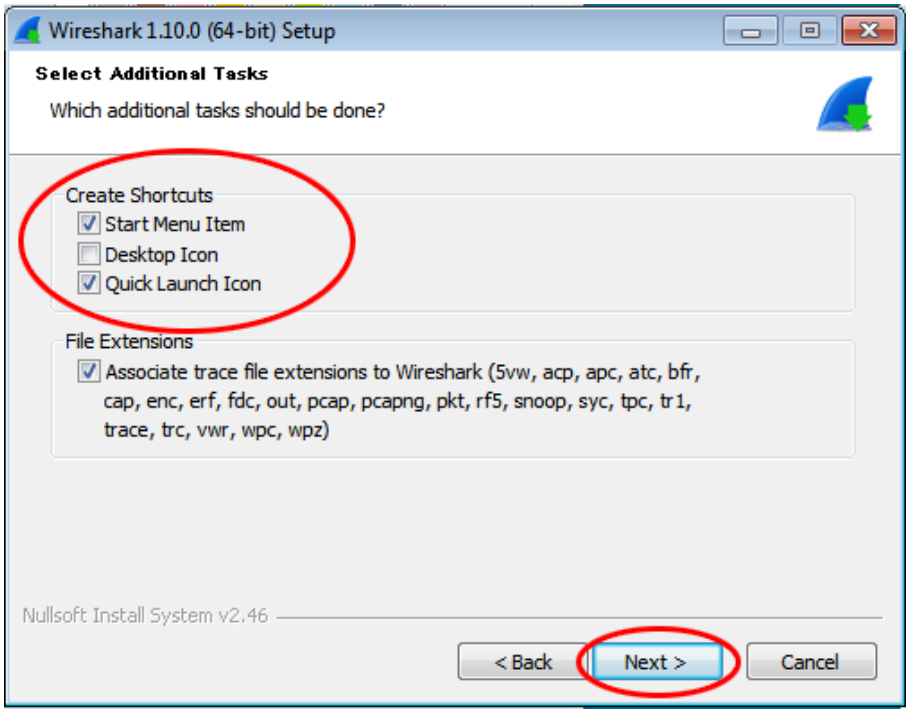
d. Continue avançando no processo de instalação. Clique em **I agree (Eu concordo)** quando a janela do contrato de licença for exibida.



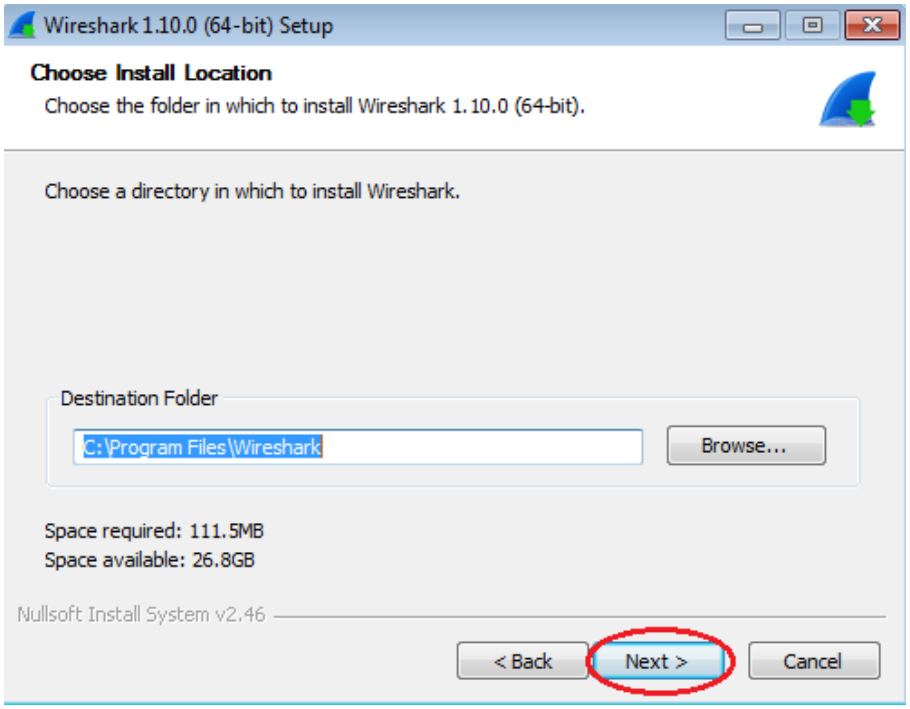
e. Mantenha as configurações padrão na janela Escolher componentes e clique em **Next (Próximo)**.



f. Escolha suas opções de atalho desejadas e clique em **Next (Próximo)**.

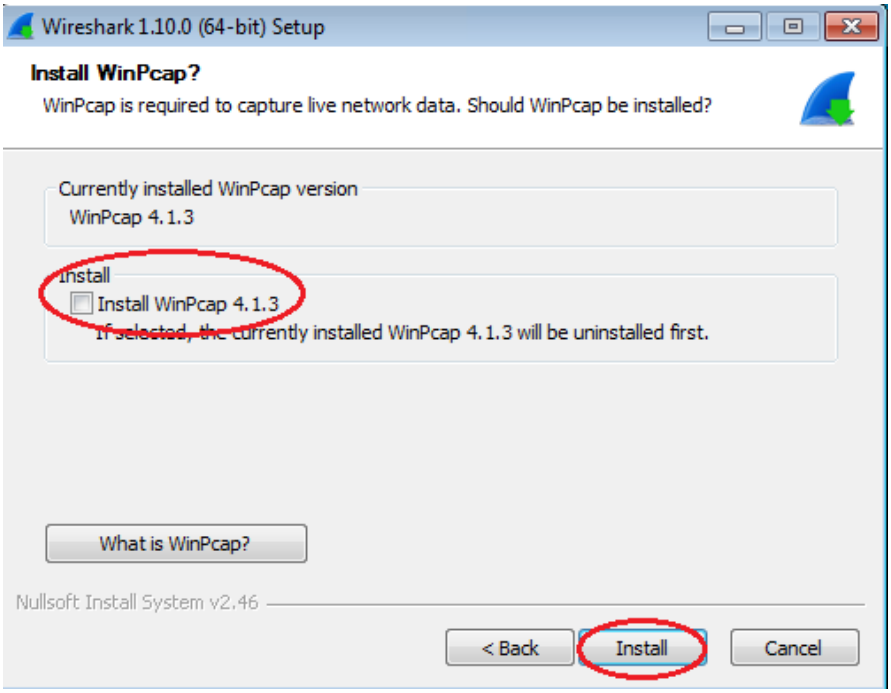


g. Você pode alterar o local de instalação do Wireshark, porém a menos que você tenha espaço em disco limitado, recomenda-se manter o local padrão.

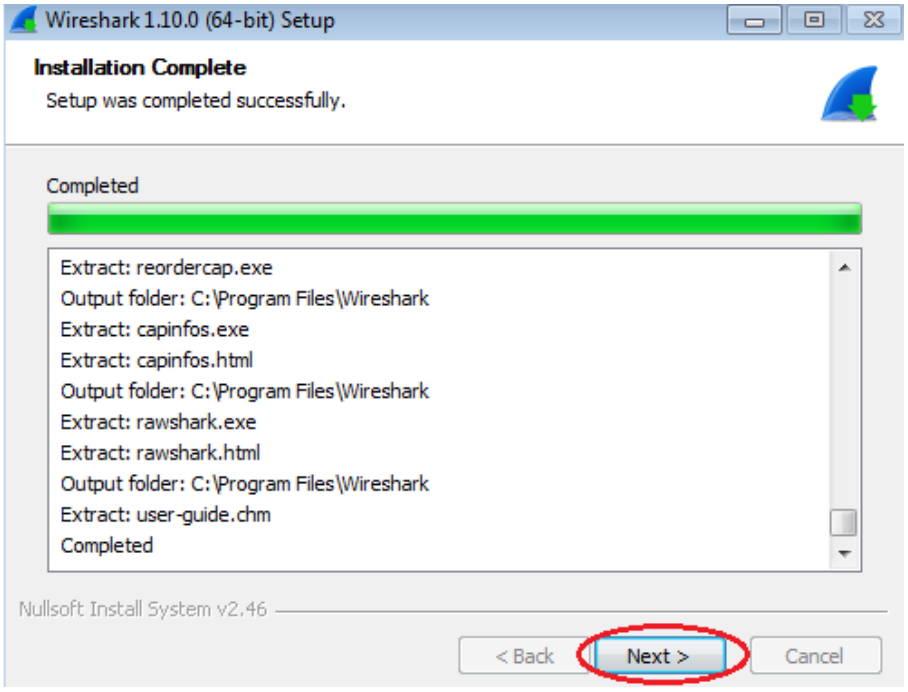


h. Para capturar dados da rede ativa, o WinPcap deve estar instalado no PC. Se o WinPcap já estiver instalado no PC, a caixa de seleção Instalar será desmarcada. Se a versão instalada do WinPcap for mais antiga que a versão que acompanha o Wireshark, recomenda-se que você permita que a versão mais recente seja instalada clicando na caixa de seleção **Install WinPcap x.x.x (Instalar o WinPcap x.x.x)** (número da versão).

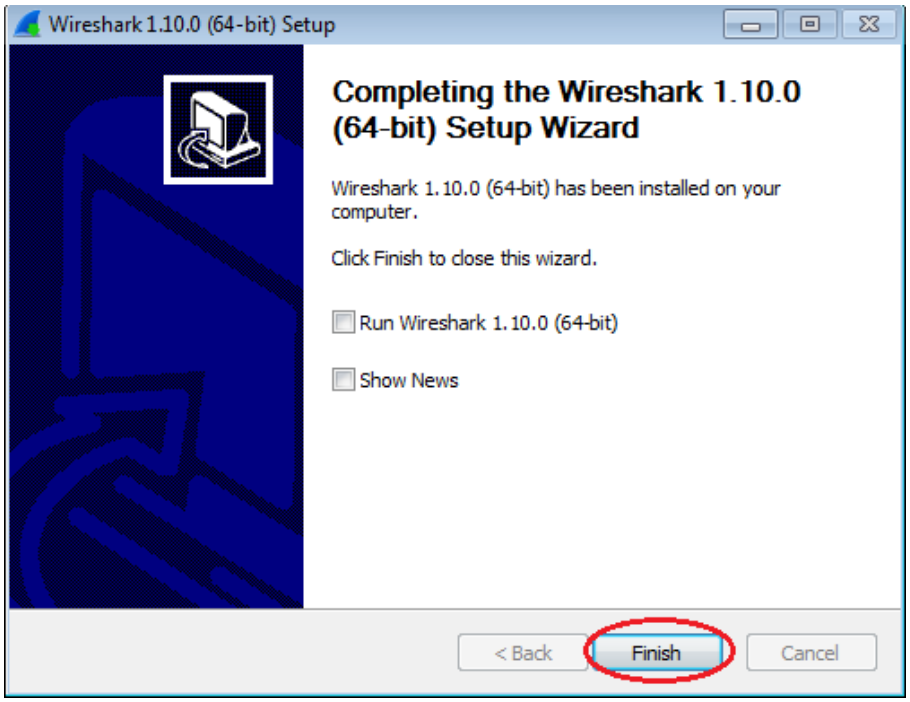
i. Conclua o assistente de configuração do WinPcap se estiver instalando o WinPcap.



j. O Wireshark começa a instalar seus arquivos e exibe uma janela separada com o status da instalação. Clique em **Next (Próximo)** quando a instalação estiver concluída.



k. Clique em **Finish (Concluir)** para encerrar o processo de instalação do Wireshark.



Parte 2: Capturar e analisar dados locais ICMP no Wireshark

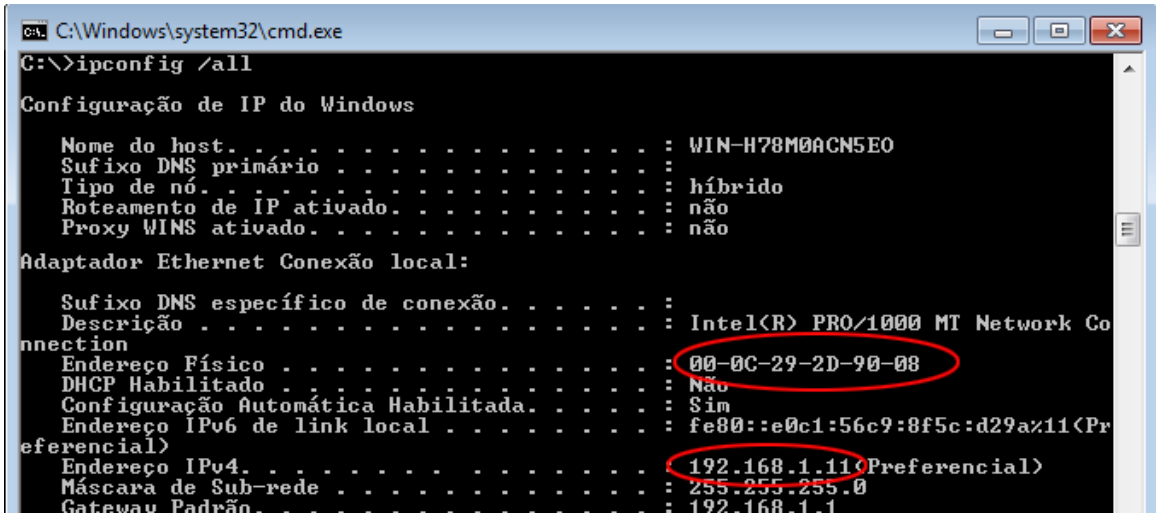
Na parte 2 deste laboratório, você efetuará ping em outro computador na LAN e capturará solicitações e respostas ICMP no Wireshark. Você também verá quadros capturados para obter informações específicas. Essa análise ajudará a esclarecer como os cabeçalhos dos pacotes são usados para transportar os dados até o destino.

Etapa 1: Recupere seus endereços de interface do PC.

Neste laboratório, você precisará recuperar o endereço IP do PC e o endereço físico da placa de rede (NIC), também chamado de endereço MAC.

a. Abra uma janela de comando, digite **ipconfig /all** e pressione Enter.

b. Observe o endereço IP da interface do PC e o endereço MAC (físico).

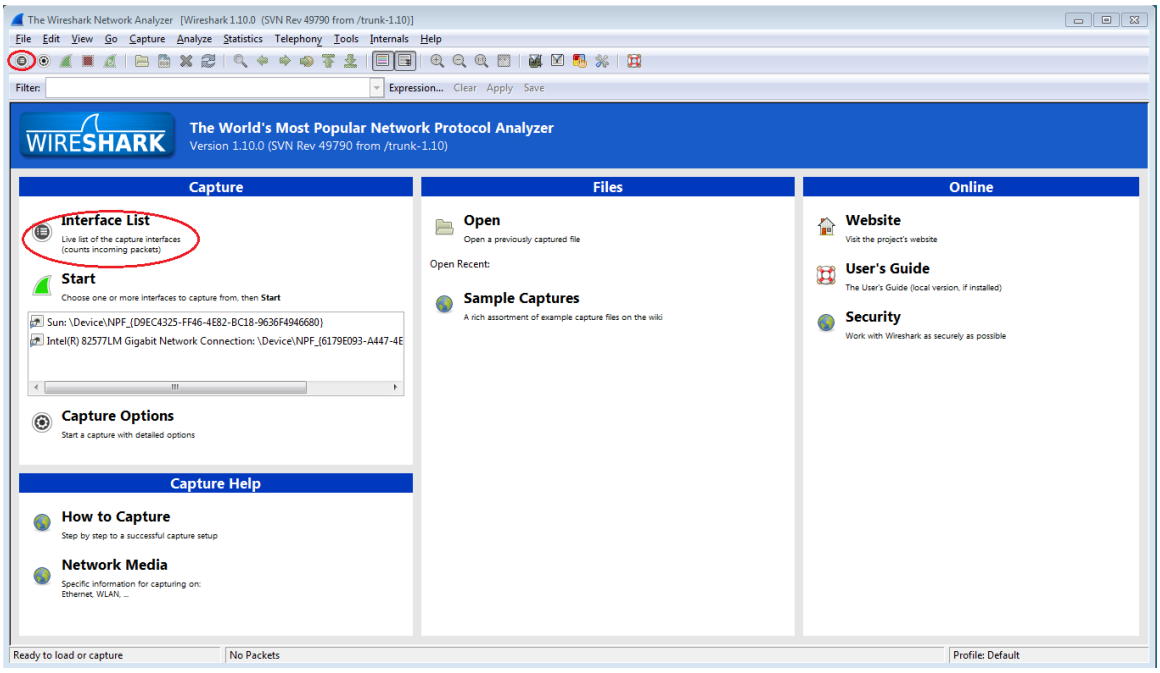


c. Solicite a um membro da equipe o endereço IP do PC dele e forneça-lhe o endereço IP do seu PC. Não forneça o seu endereço MAC a ele agora.

Etapa 2: Inicie o Wireshark e comece a capturar os dados.

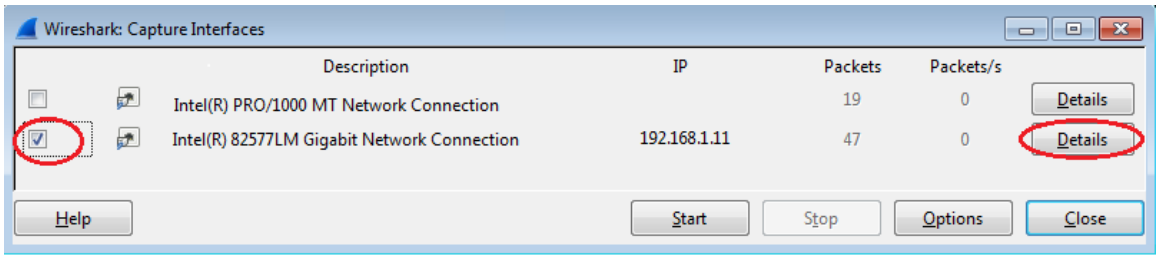
a. Em seu computador, clique no botão **Iniciar** do Windows para ver o Wireshark listado como um dos programas no menu pop-up. Clique duas vezes no **Wireshark**.

b. Após iniciar o Wireshark, clique na **Interface List (Lista de interface)**.

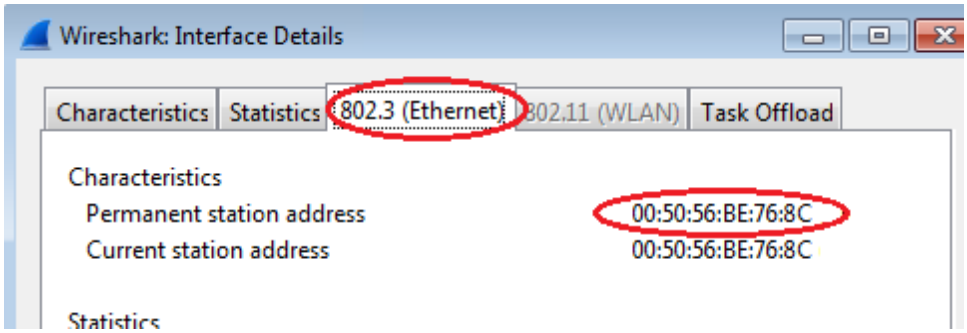


Observação: clicar no primeiro ícone de interface na linha de ícones também abre a lista de interface.

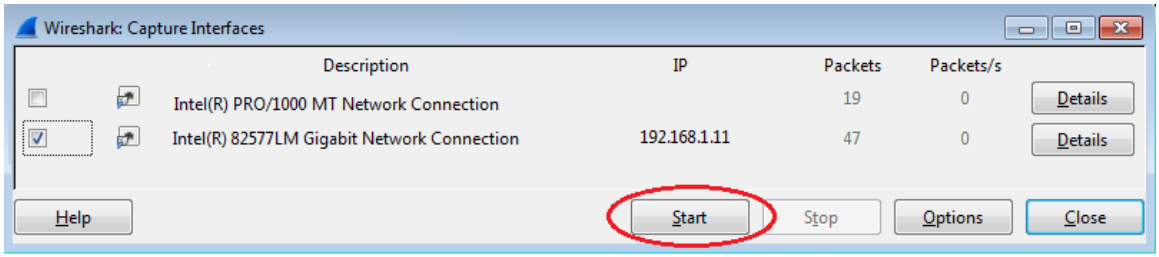
c. No Wireshark: na janela Capture Interfaces (interfaces de captura), clique na caixa de seleção ao lado da interface conectada à LAN.



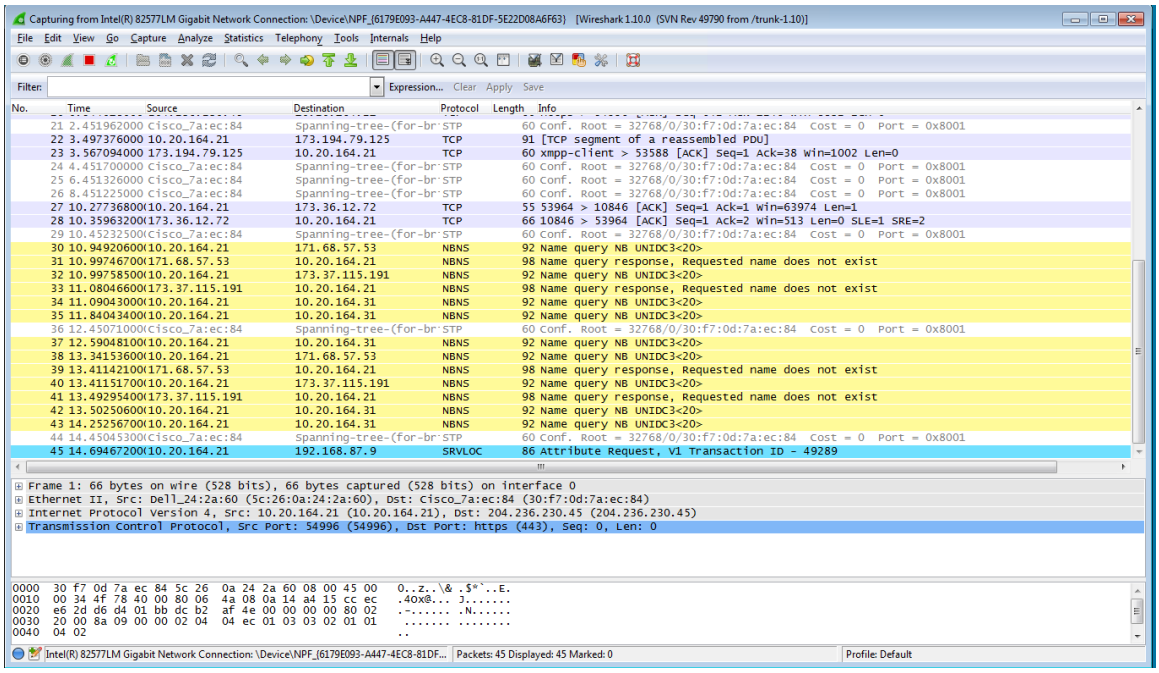
Observação: se várias interfaces estiverem listadas e você não tiver certeza sobre qual interface verificar, clique no botão **Details (Detalhes)** e na guia **802.3 (Ethernet)**. Verifique se o endereço MAC corresponde ao que você observou na etapa 1b. Feche a janela de Interface Details (detalhes da interface) após verificar a interface correta.



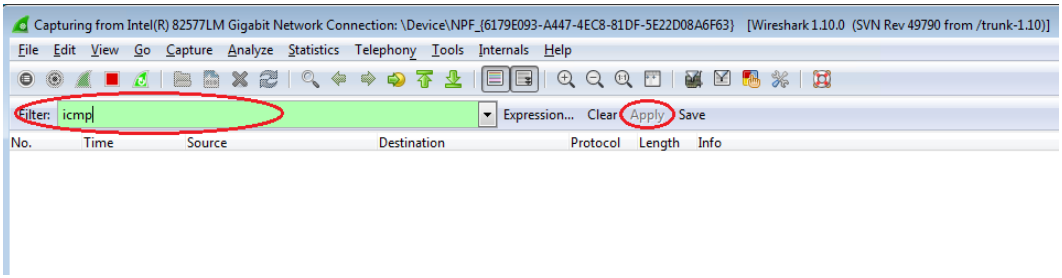
d. Depois de verificar a interface correta, clique em **Start (Iniciar)** para iniciar a captura de dados.



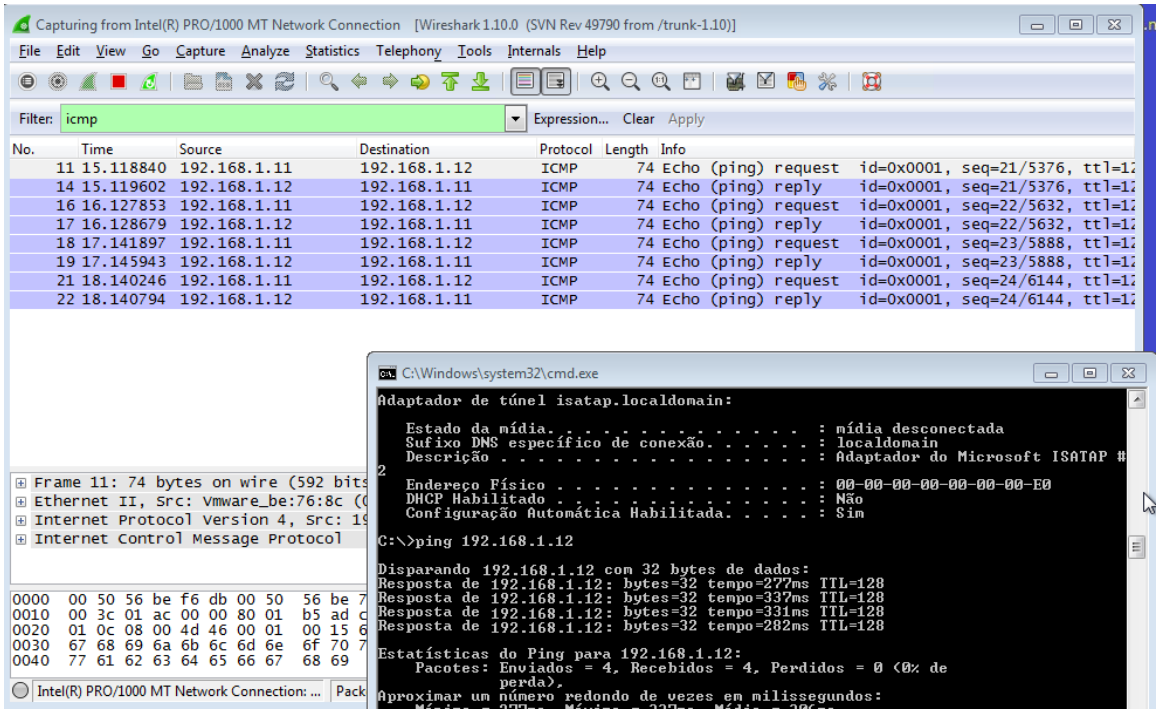
As informações começarão a rolar abaixo da seção superior no Wireshark. As linhas de dados serão exibidas em cores diferentes com base no protocolo.



e. Essas informações podem passar rapidamente dependendo da comunicação que estiver ocorrendo entre o PC e a LAN. Podemos aplicar um filtro para facilitar a visualização e o trabalho com os dados que estão sendo capturados pelo Wireshark. Neste laboratório, estamos apenas interessados em exibir as PDUs do ICMP (ping). Digite **icmp** na caixa Filtro na parte superior do Wireshark e pressione Enter ou clique no botão **Apply (Aplicar)** para exibir somente as PDUs do ICMP (ping).

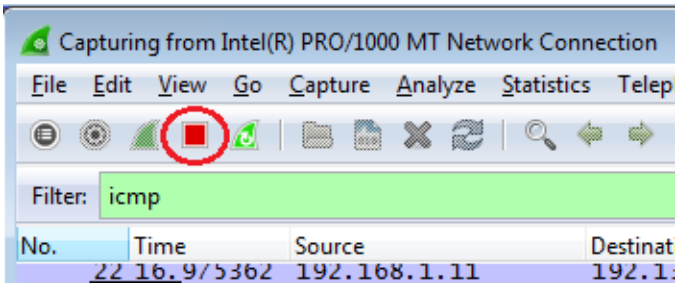


f. Este filtro faz com que todos os dados na janela superior desapareçam, mas você ainda estará capturando o tráfego na interface. Exiba a janela do prompt de comando que você abriu anteriormente e efetue ping no endereço IP que você recebeu de sua equipe. Observe que começa a ver novamente os dados na janela superior do Wireshark.



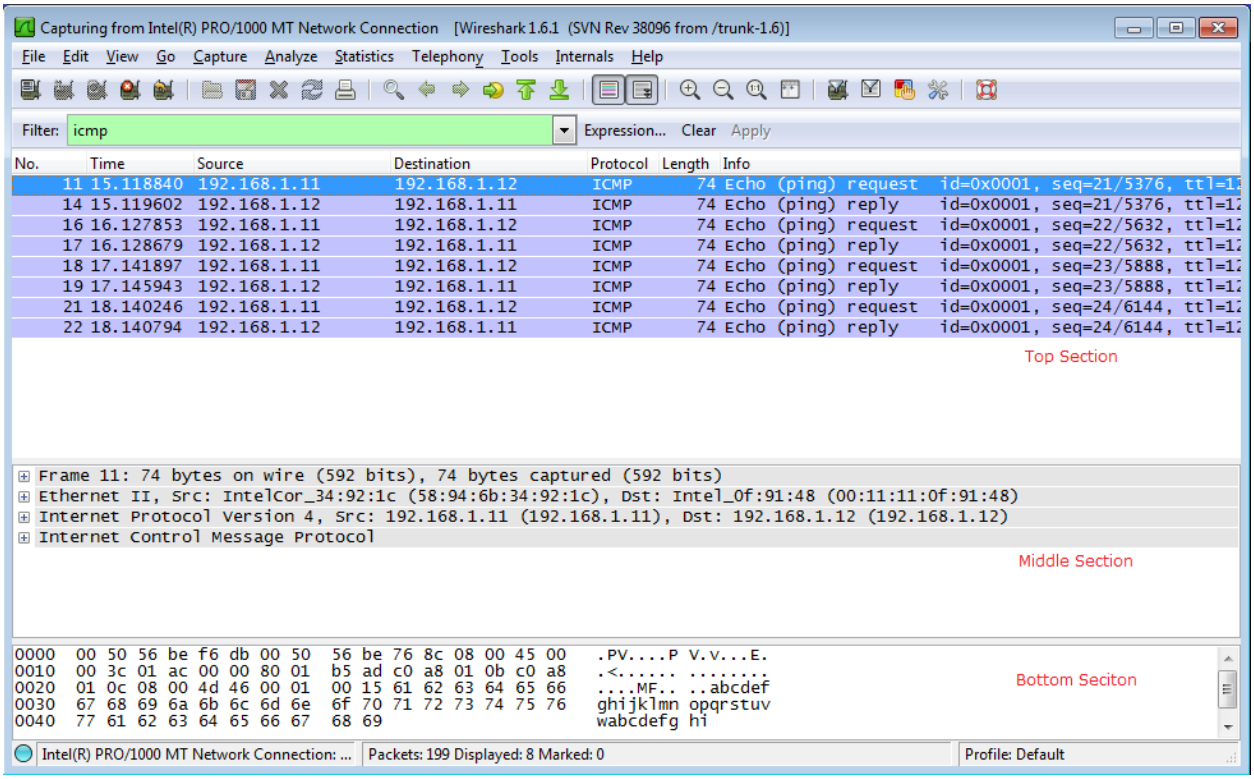
Observação: se o PC de sua equipe não responde aos pings, isso pode acontecer porque o firewall do PC está bloqueando as solicitações. ConsulteAppendix A: Allowing ICMP Traffic Through a Firewall para obter informações sobre como permitir o tráfego ICMP pelo firewall usando o Windows 7.

g. Pare a captura de dados clicando no ícone **Stop Capture (Parar a captura)**.

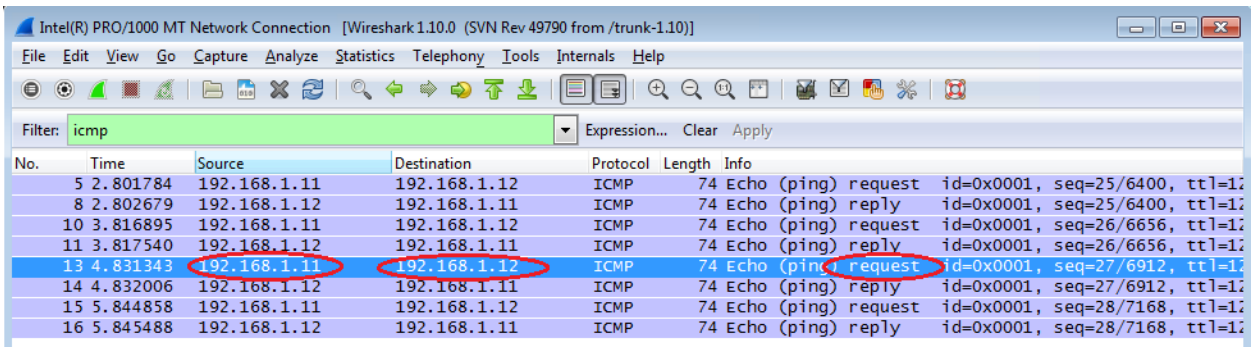


Etapa 3: Examine os dados capturados.

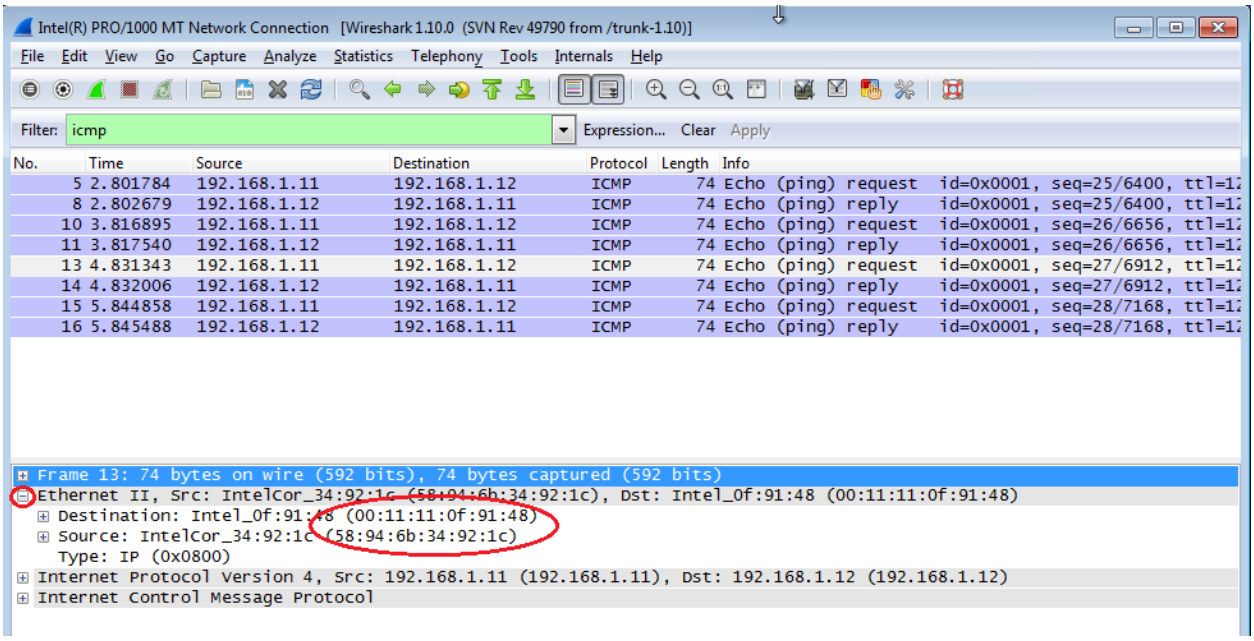
Na etapa 3, examine os dados gerados pelas solicitações ping do PC de sua equipe. Os dados do Wireshark são exibidos em três seções: 1) A seção superior exibe a lista de quadros de PDU capturada com um resumo das informações do pacote IP listadas, 2) a seção média mostra as informações de PDU para o quadro selecionado na parte superior da tela e separa um quadro PDU capturado pelas camadas de protocolo, e 3) a seção inferior exibe os dados brutos de cada camada. Os dados são exibidos em formato hexadecimal e decimal.



a. Clique nos primeiros quadros de PDU de solicitação ICMP na seção da parte superior do Wireshark. Observe que a coluna Origem tem o endereço IP do PC, e a Destino contém o endereço IP do PC do colega em que você efetuou ping.



b. Com esse quadro de PDU ainda selecionado na seção superior, vá até a seção média. Clique no sinal mais à esquerda da linha Ethernet II para ver os endereços MAC origem e destino.



O endereço MAC origem corresponde à interface do PC?

O endereço MAC destino no Wireshark corresponde ao endereço MAC de sua equipe?

Como o endereço MAC do PC que recebeu ping é obtido pelo seu PC?

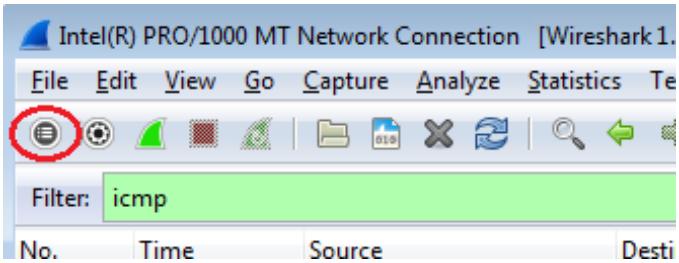
Observação: no exemplo anterior de uma solicitação ICMP capturada, os dados do ICMP são encapsulados dentro da PDU do pacote IPv4 (cabeçalho IPv4) que é, então, encapsulada em uma PDU do quadro Ethernet II (cabeçalho Ethernet II) para transmissão na LAN.

Parte 3: Capturar e analisar dados ICMP remotos no Wireshark

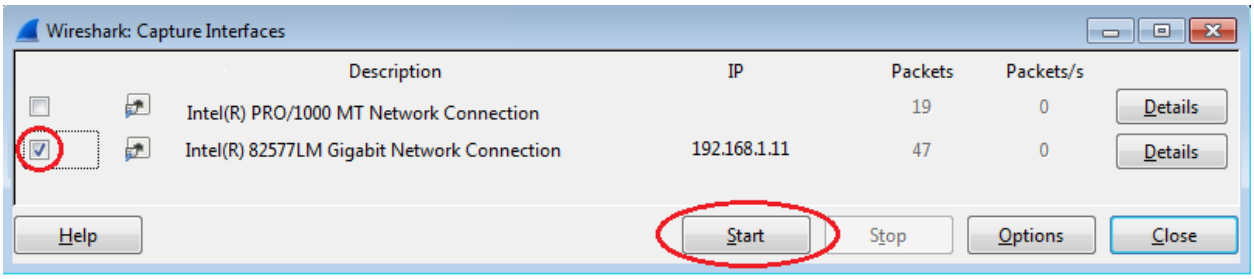
Na parte 3, você efetuará ping nos hosts remotos (não nos hosts da LAN) e examinará os dados gerados desses pings. Você determinará o que há de diferente nesses dados a partir dos dados pesquisados na parte 2.

Etapa 1: Inicie a captura de dados na interface.

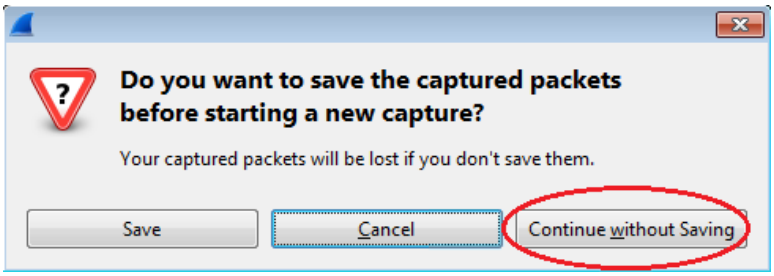
a. Clique no ícone **Interface List (Lista de interface)** para exibir novamente as interfaces do PC na lista.



b. Verifique se a caixa de seleção ao lado da interface da LAN está marcada e clique em **Start (Iniciar)**.



c. Uma janela solicitará que salve os dados capturados anteriormente antes de iniciar outra captura. Não é necessário salvar esses dados. Clique em **Continue without Saving (Continuar sem salvar)**.

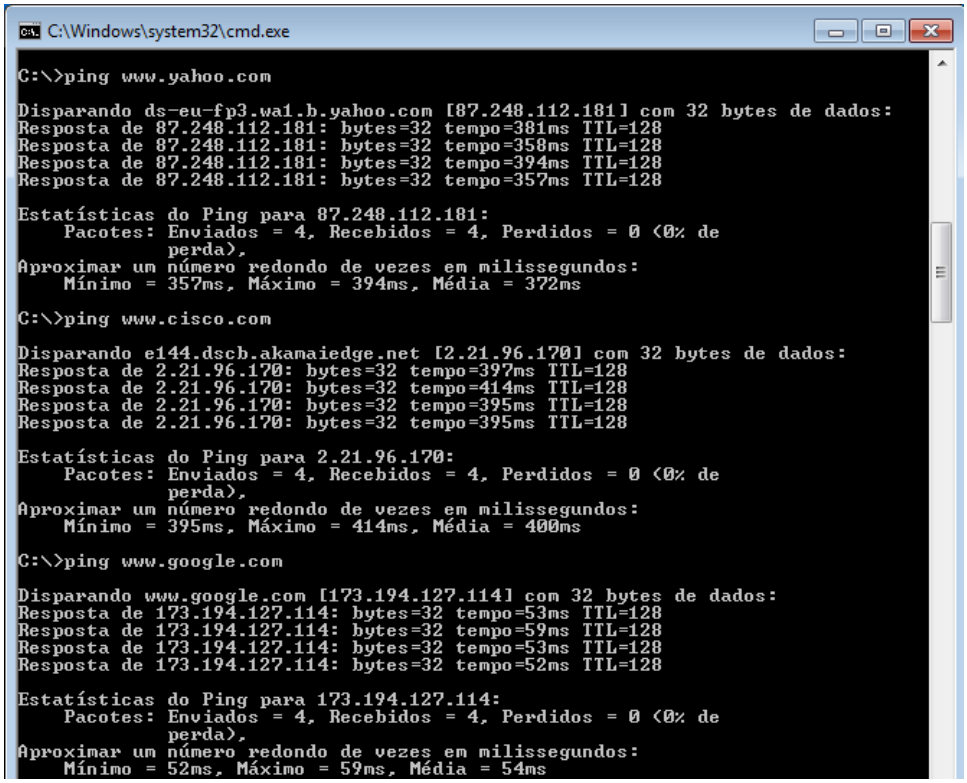


d. Com a captura ativa, efetue ping nos três URLs de sites a seguir:

1) www.yahoo.com

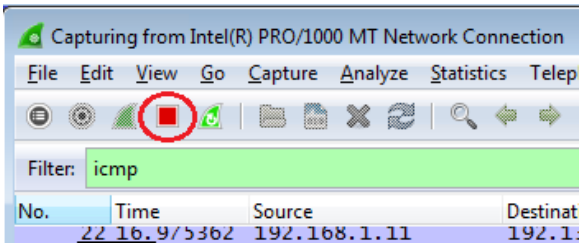
2) www.cisco.com

3) www.google.com



Observação: quando você efetuar ping nos URLs listados, observe que o Servidor de Nome de Domínio (DNS) converte o URL para um endereço IP. Observe o endereço IP recebido para cada URL.

e. É possível parar a captura de dados clicando no ícone **Stop Capture (Parar a captura)**.



Etapa 2: Examinar e analisar os dados dos hosts remotos.

a. Analise os dados capturados no Wireshark, examine os endereços IP e MAC dos três locais em que você efetuou ping. Liste os endereços IP e MAC destino para todos os três locais no espaço fornecido.

1° Local: IP: _____ _____ _____ _____ MAC:

2° Local: IP: MAC:

3° Local: IP: MAC:

b. Qual é a importância dessas informações?

c. Como essas informações diferem das informações do ping local que você recebeu na parte 2?

Reflexão

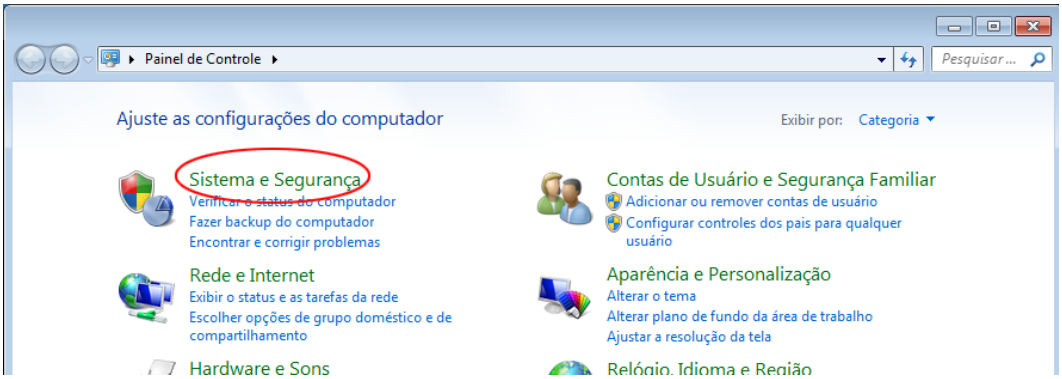
Por que o Wireshark mostra o endereço MAC real dos hosts locais, mas não o endereço MAC real para os hosts remotos?

Anexo A: Permitir o tráfego ICMP pelo firewall

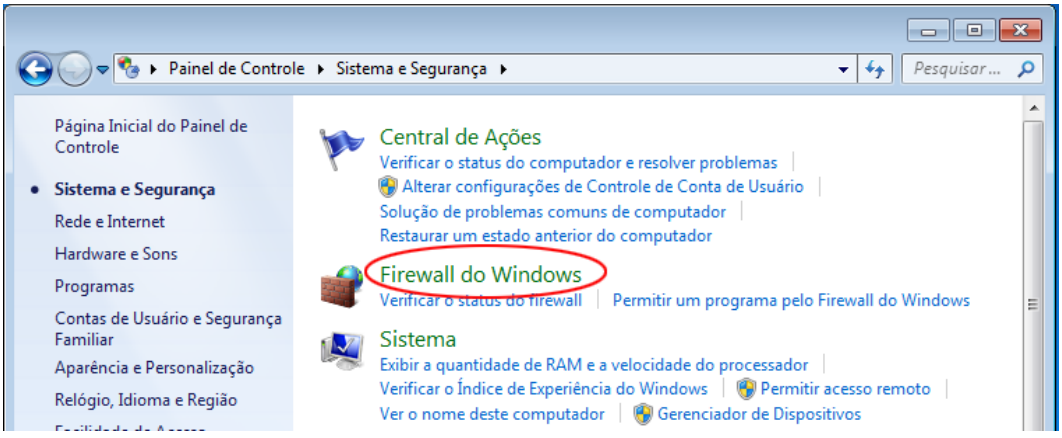
Se os membros de sua equipe não conseguirem efetuar ping em seu PC, o firewall pode estar bloqueando essas solicitações. Este anexo descreve como criar uma regra no firewall para permitir solicitações de ping. Também descreve como desativar a nova regra ICMP depois que você tiver concluído o laboratório.

Etapa 1: Crie uma regra de entrada nova permitindo o tráfego ICMP pelo firewall.

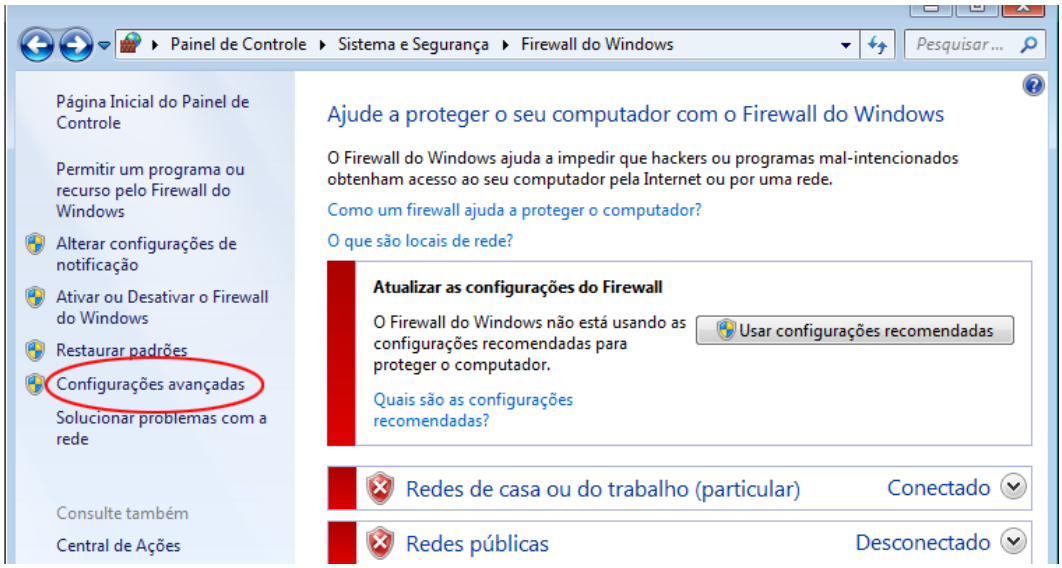
a. No Painel de controle, clique na opção **Sistema e Segurança**.



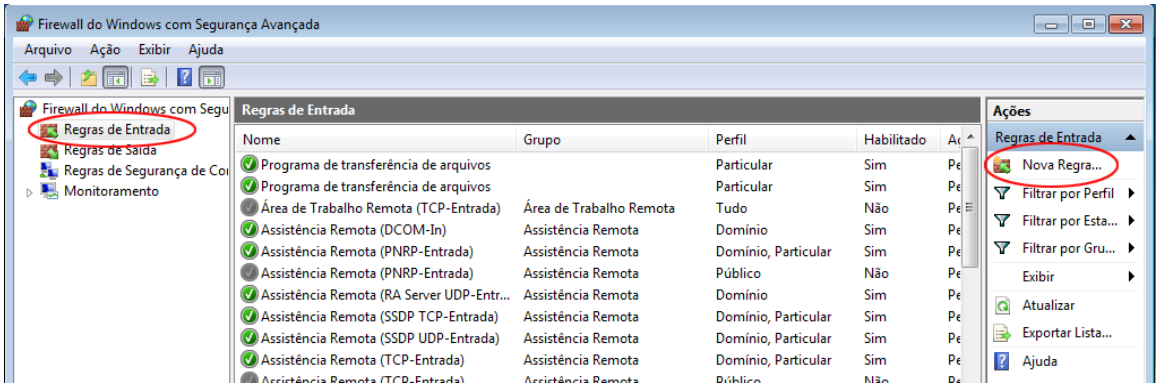
b. Na janela Sistema e Segurança, clique em **Firewall do Windows**.



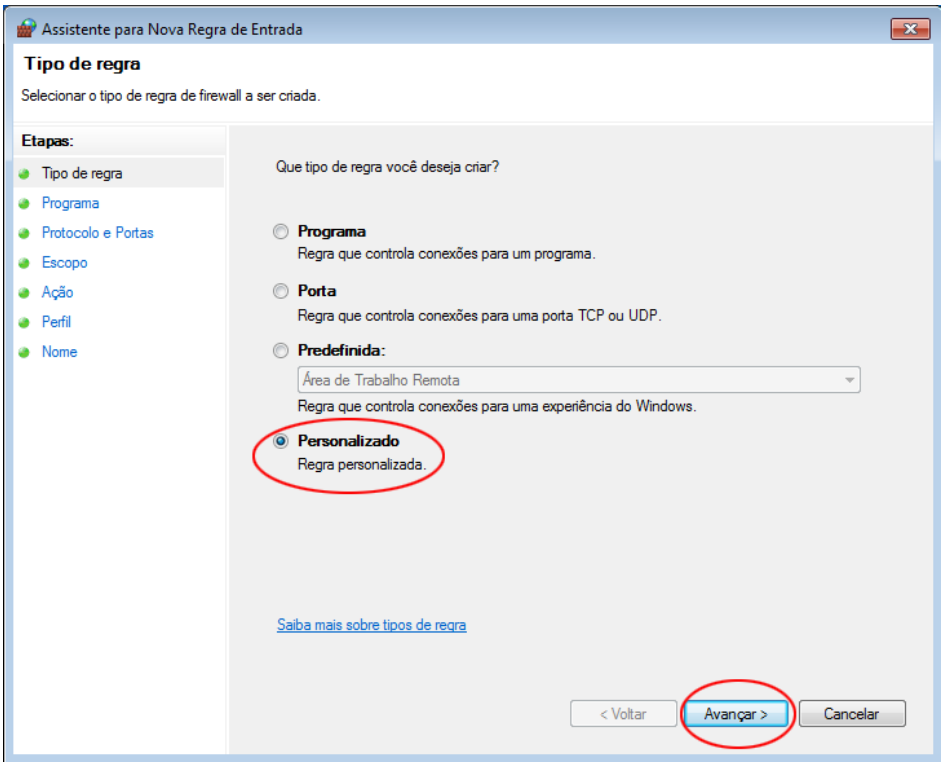
c. No painel esquerdo da janela de firewall do Windows, clique em **Configurações avançadas**.



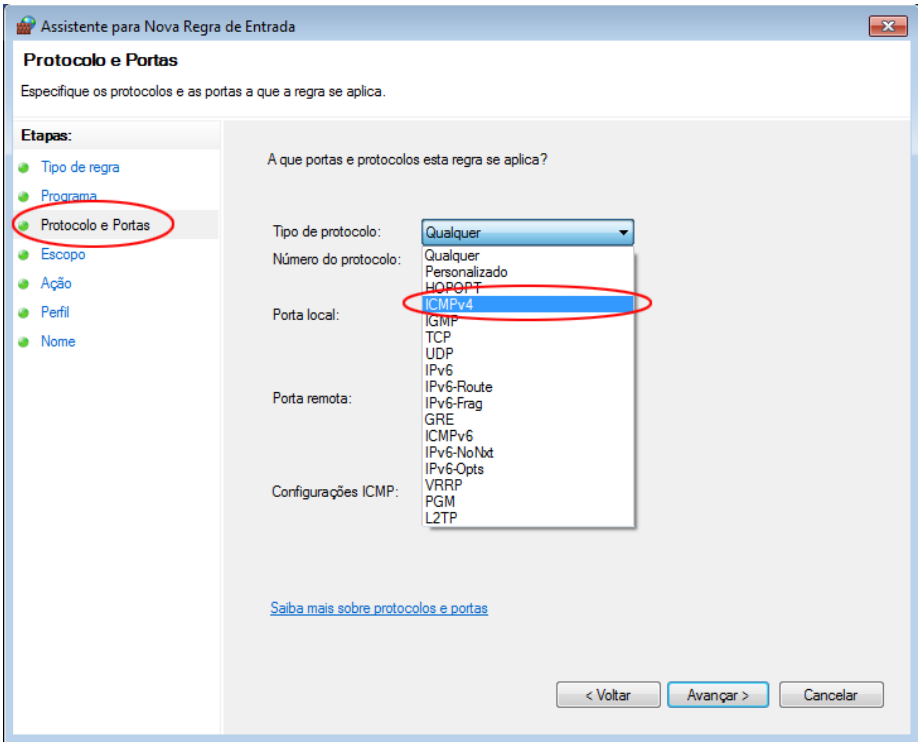
d. Na janela Segurança avançada, selecione a opção **Regras de Entrada** na barra lateral esquerda e clique em **Nova regra…** na barra lateral direita.



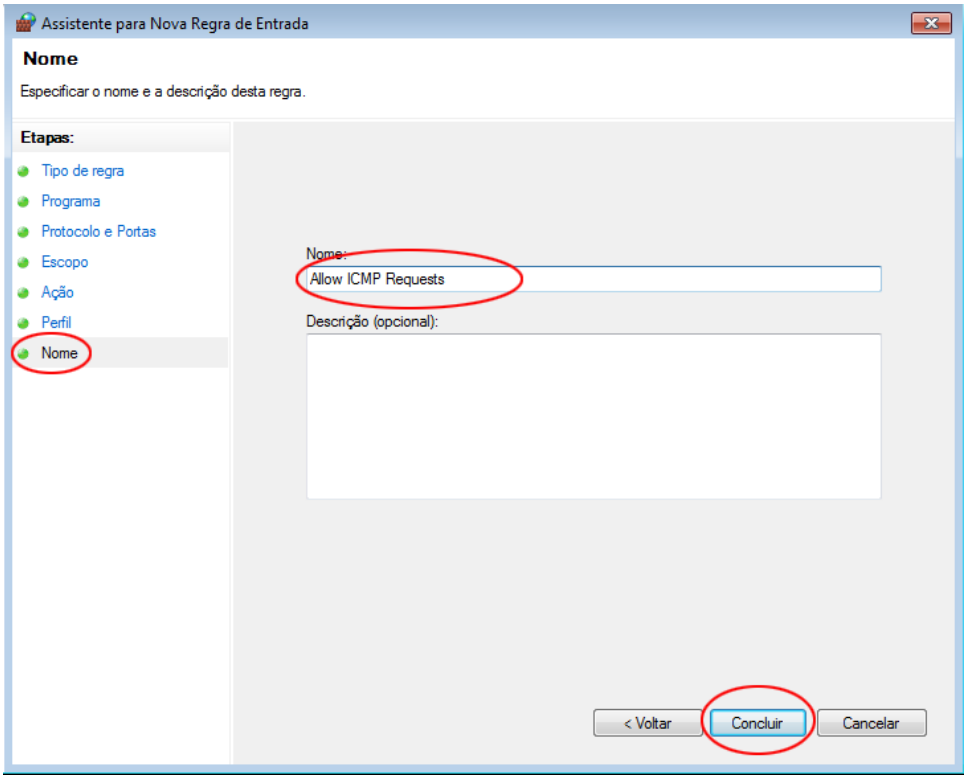
e. Isso inicia o assistente Nova regra de entrada. Na tela Tipo de regra, clique no botão de opção **Personalizar** e em **Avançar**.



f. No painel esquerdo, clique na opção **Protocolo e Portas** e, usando o menu suspenso Tipo de protocolo, selecione **ICMPv4** e clique em **Avançar**.



g. No painel esquerdo, clique na opção **Nome** e, no campo Nome, digite **Permitir solicitações do ICMP**. Clique em **Concluir**.

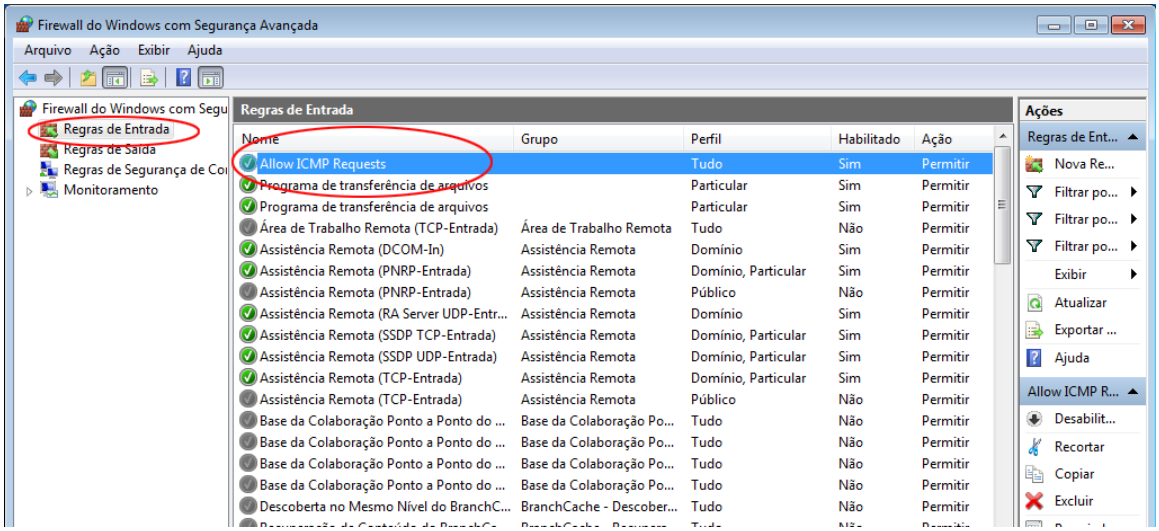


Essa nova regra deve permitir que os membros da equipe recebam respostas de ping no PC.

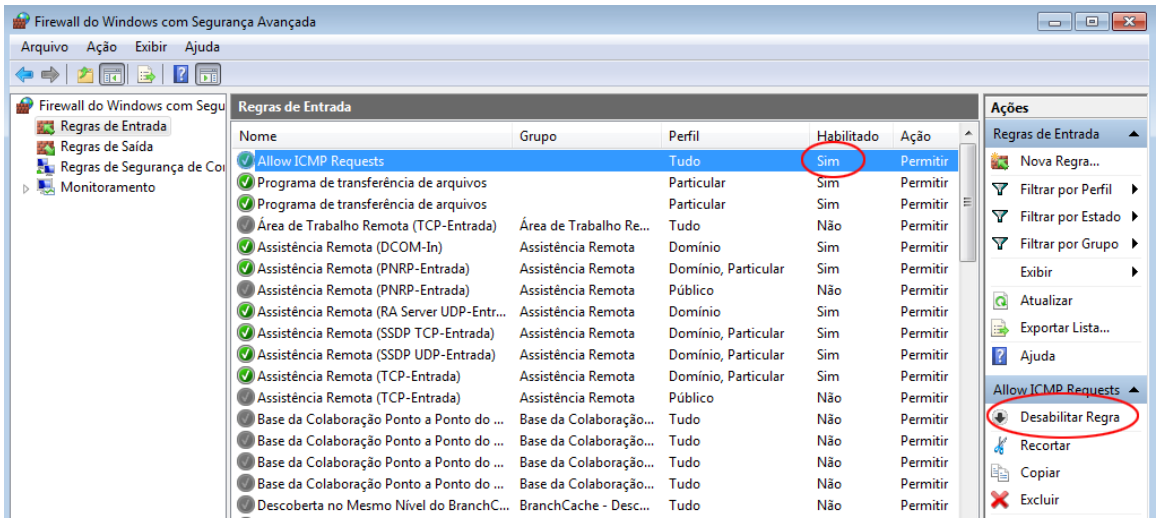
Etapa 2: Desativar ou excluir a nova regra do ICMP.

Após o laboratório ser concluído, você talvez queira desativar ou até mesmo excluir a nova regra criada na etapa 1. Usar a opção **Desativar Regra** permite que posteriormente a regra seja ativada de novo. Excluir a regra permanentemente a exclui da lista de Regras de entrada.

a. Na janela Segurança avançada, no painel esquerdo, clique em **Regras de Entrada** e localize a regra que você criou na etapa 1.



b. Para desativar a regra, clique na opção **Desativar Regra**. Ao escolher essa opção, você a verá mudar para **Ativar Regra**. Você pode alternar entre Desativar Regra e Ativar Regra; o status da regra também é exibido na coluna Ativado na lista de Regras de entrada.



c. Para excluir permanentemente a regra do ICMP, clique em **Excluir**. Se você selecionar essa opção, você pode recriar a regra novamente para permitir respostas ICMP.