Laboratório 2.6.2: Usando o Wireshark™ para Visualizar Unidades de Dados de Protocolo

Objetivos

- Ser capaz de explicar o propósito de um analisador de protocolo (Wireshark).
- Ser capaz de executar a captura de PDU básica usando o Wireshark.
- Ser capaz de executar a análise de PDU básica em tráfego de dados de rede.
- Experimentar recursos e opções do Wireshark, tais como captura de PDU e filtragem de exibição.

Contexto

O Wireshark é um software analisador de protocolo, ou aplicação de "packet sniffer", usado para resolução de problemas de rede, análise, desenvolvimento de software e protocolo, e educação. Antes de junho de 2006, o Wireshark era conhecido como Ethereal.

Um packet sniffer (também conhecido como analisador de rede ou de protocolo) é um software que pode interceptar e registrar tráfego de dados passando em uma rede de dados. À medida que o fluxo de dado 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 programado para reconhecer a estrutura de diferentes protocolos de rede. Isso permite que ele exiba o encapsulamento e campos individuais de uma PDU e interprete seu significado.

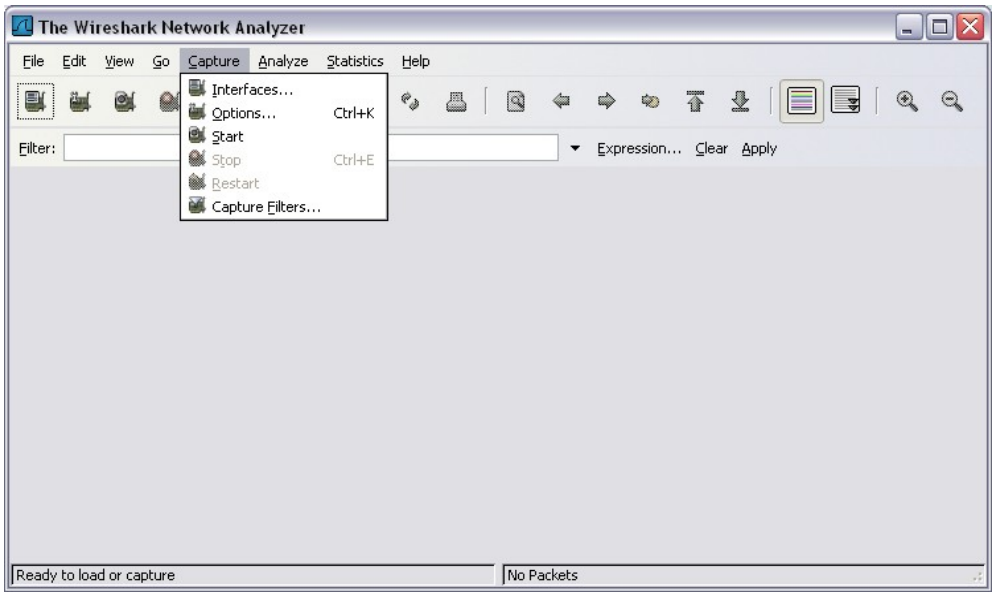
Ele é uma ferramenta útil para qualquer pessoa que trabalhe com redes e pode ser usado com a maioria dos laboratórios nos cursos CCNA para análise de dados e resolução de problemas.

Para informações ou fazer o download do programa, vá para http://www.Wireshark.org

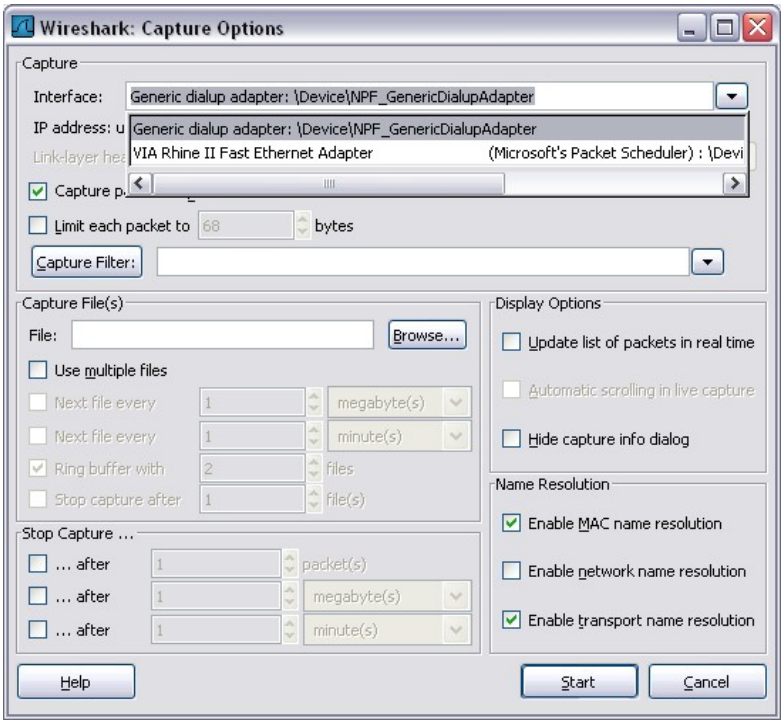
Cenário

Para capturar PDUs, o computador no qual o Wireshark está instalado deve ter uma conexão ativa na rede e o Wireshark deve estar sendo executado antes de qualquer dado ser capturado.

Quando o Wireshark é aberto, a tela abaixo é exibida.

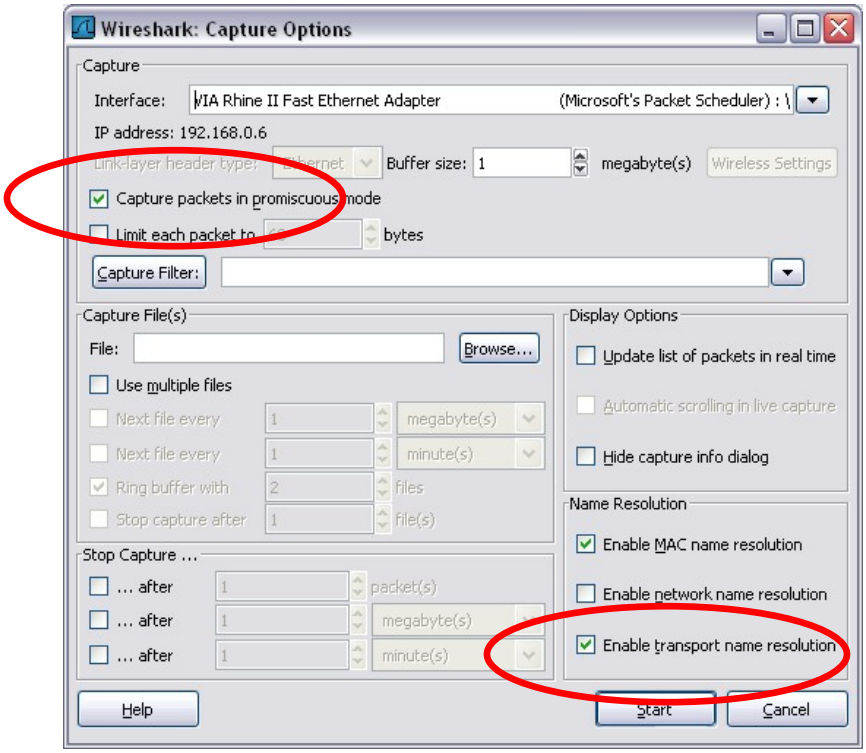


Para iniciar a captura de dados é, primeiramente, necessário ir ao menu **Capture** e selecionar a escolha **Options**.
O diálogo **Options** fornece uma série de configurações e filtros que determina qual e quanto tráfego de dados será capturado.



Primeiro, é necessário garantir que o Wireshark seja configurado para monitorar a interface correta. Da lista suspensa **Interface**, selecione o adaptador de rede em uso. Geralmente, para um computador, ele será o Adaptador Ethernet conectado.

Então, outras Opções podem ser configuradas. Entre as disponíveis em **Capture Options,** as duas destacadas abaixo são válidas para verificação.



Configurando o Wireshark para capturar pacotes em modo promíscuo

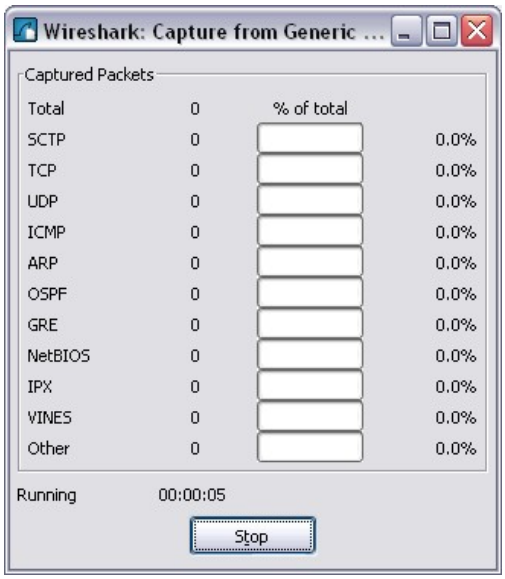
Se este recurso NÃO estiver marcado, somente PDUs destinadas para este computador serão capturadas.
Se este recurso estiver marcado, todas as PDUs destinadas para este computador E todas aquelas detectadas pelo computador NIC no mesmo segmento de rede (ou seja, aquelas que "passam" pela NIC, mas não estão destinadas ao computador) são capturadas.
Nota: A captura destas outras PDUs depende do dispositivo intermediário que conecta os computadores nesta rede. À medida que usar dispositivos intermediários diferentes (hubs, switches, roteadores) ao longo dos cursos, você verificará os diferentes resultados do Wireshark.

Configurando o Wireshark para resolução de nome de rede

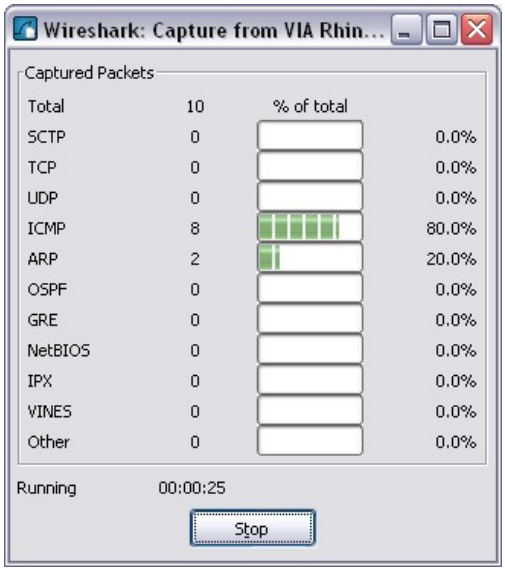
Esta opção permite que você controle se o Wireshark traduz endereços de rede encontrados em PDUs em nomes ou não. Embora seja um recurso útil, o processo de resolução de nome pode adicionar PDUs extras a seus dados capturados, talvez distorcendo a análise.

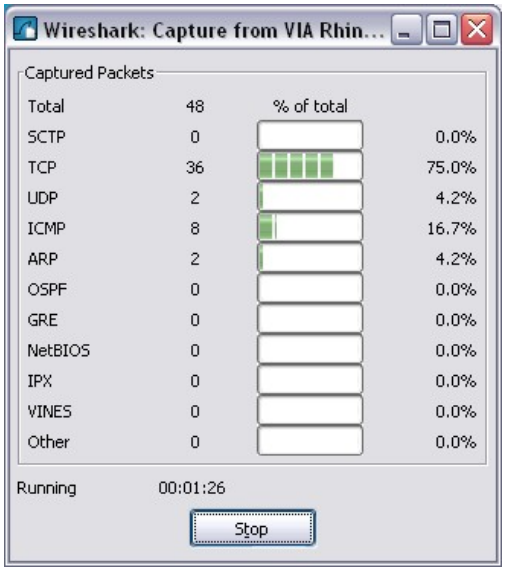
Existe ainda uma variedade de outras configurações de filtragem de captura e processo disponíveis.

Clicar no botão **Iniciar** para iniciar o processo de captura de dados e uma caixa de mensagem exibe o progresso deste processo.



À medida que os dados de PDUs são capturados, os tipos e o número são indicados na caixa de mensagem.

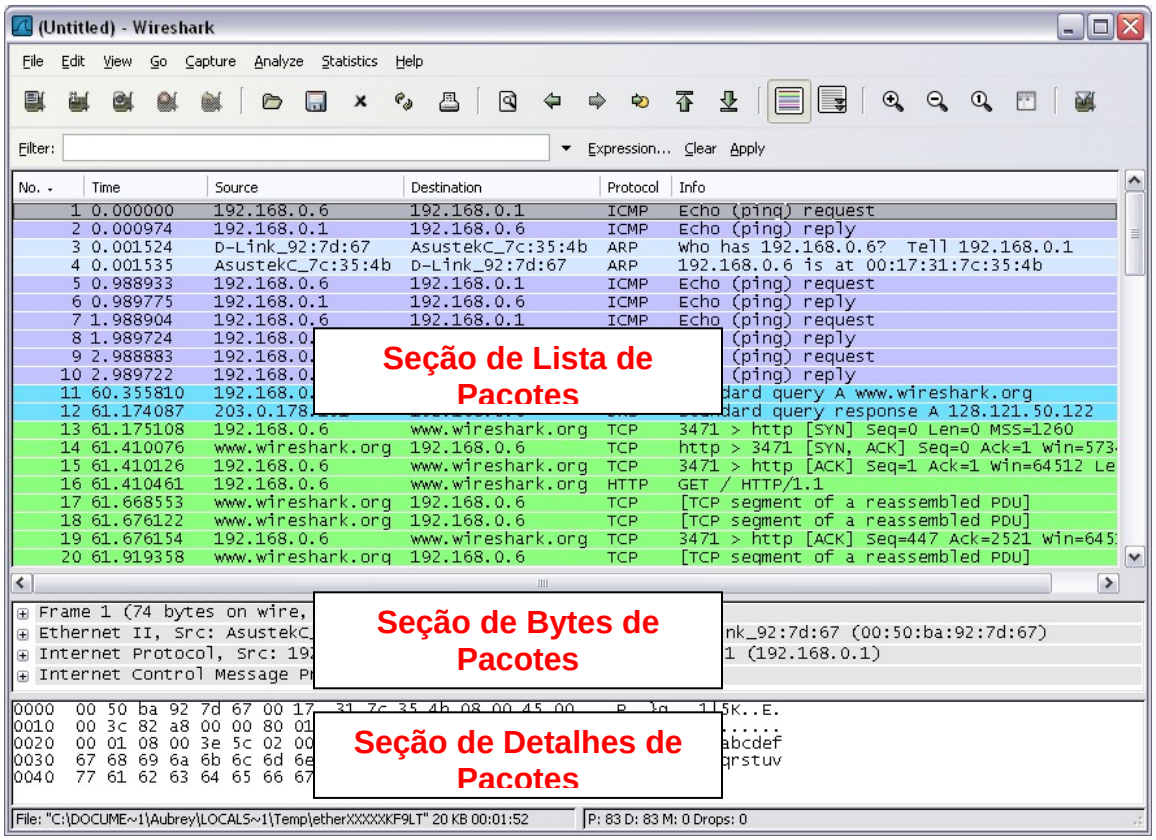




Os exemplos acima mostram a captura de um processo ping e o acesso a uma página web.

Quando o botão **Stop** é clicado, o processo de captura é finalizado e a tela principal é exibida.

Esta principal janela de exibição do Wireshark possui três seções.



A Seção de Lista de PDU (ou de Pacotes) no topo do diagrama exibe um resumo de cada pacote capturado. Ao clicar em pacotes nesta seção, você controla o que é exibido nas outras duas seções.

A Seção de Detalhes de PDU (ou de Pacotes) no meio do diagrama exibe o pacote selecionado na Seção de Lista de Pacotes em mais detalhes.

A Seção de Bytes de PDU (ou de Pacotes) na parte inferior do diagrama exibe os dados reais (em forma hexadecimal representando o binário real) de pacote selecionado na Seção de Lista de Pacotes e destaca o campo selecionado na Seção de Detalhes de Pacotes.

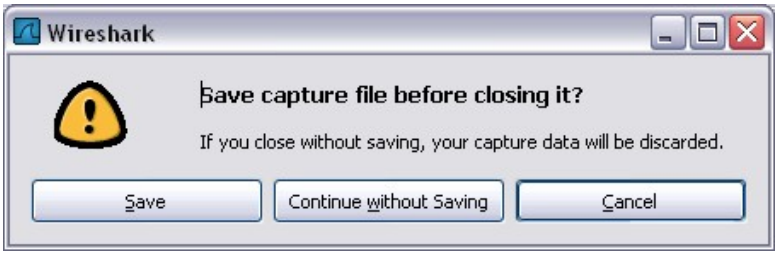
Cada linha na Lista de Pacotes corresponde a uma PDU ou pacote dos dados capturados. Se você selecionar uma linha nesta seção, mais detalhes serão exibidos nas seções de "Detalhes de Pacotes" e "Bytes de Pacotes". O exemplo acima mostra as PDUs capturadas quando o ping foi usado e http://www.Wireshark.org foi acessado. O Pacote número 1 é selecionado nesta seção.

A seção de Detalhes de Pacotes mostra o pacote atual (selecionado na seção de "Lista de Pacotes") de forma mais detalhada. Esta seção mostra os protocolos e os campos de protocolos do pacote selecionado. Os protocolos e campos do pacote são exibidos usando uma árvore, que pode ser expandida e sofrer um colapso.

A seção de Bytes de Pacotes mostra os dados do pacote atual (selecionado na seção de "Lista de Pacotes") que é conhecido como estilo "hexdump". Neste laboratório, esta seção não será examinada em detalhes. No entanto, quando uma análise mais aprofundada for necessária, essas informações exibidas serão úteis para examinar os valores binários e o conteúdo das PDUs.

As informações capturadas para as PDUs de dados podem ser salvas em um arquivo. Este arquivo pode ser aberto no Wireshark para futura análise sem necessidade de re-capturar o mesmo tráfego de dados novamente. As informações exibidas quando um arquivo de captura é aberto são as mesmas da captura original.

Ao fechar uma tela de captura de dados ou sair do Wireshark você é avisado a salvar as PDUs capturadas.



Clicar em **Continue without Saving** fecha o arquivo ou sai do Wireshark sem salvar os dados capturados exibidos.

Tarefa 1: Captura de PDU Ping

Passo 1: Após se assegurar que a topologia do laboratório padrão e a configuração estão corretas, abra o Wireshark em um computador em um pod do laboratório.

Configure as Opções de Captura conforme descrito acima na visão geral e inicie o processo de captura.

Da linha de comando do computador, faça ping no endereço IP de outra rede conectada e ligada em um dispositivo final na topologia de laboratório. Neste caso, faça o ping do Eagle Server usando o comando ping 192.168.254.254.

Após receber as respostas com sucesso do ping na janela de linha de comando, pare a captura de pacotes.

Passo 2: Examine a seção de Lista de Pacotes.

A seção de Lista de Pacotes no Wireshark deve agora parecer com isso:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Olhe os pacotes listados acima; estamos interessados em números de pacote 6, 7, 8, 9, 11, 12, 14 e 15.

Localize os pacotes equivalentes na lista de pacotes em seu computador.
Se você executou o Passo 1A acima, compare as mensagens exibidas na janela de linha de comando quando o ping foi emitido com os seis pacotes capturados pelo Wireshark.

Da Lista de Pacotes do Wireshark, responda o seguinte:

Qual protocolo é usado pelo ping? _____

Qual o nome completo do protocolo? _____

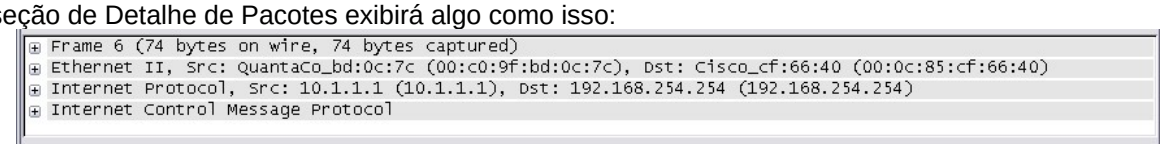
Quais são os nomes das duas mensagens ping? _____

_____
Os endereços IP de origem e destino listados são o que você esperava? Sim / Não

Por quê? _____

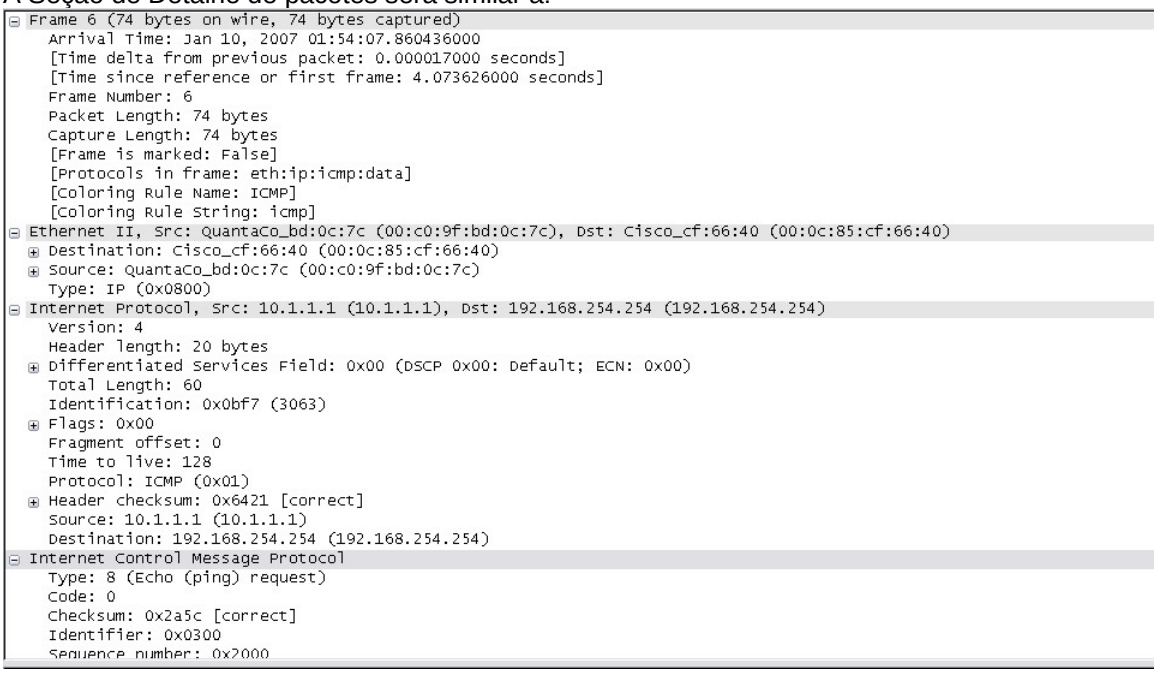
Passo 3: Selecione (destaque) o primeiro pacote de solicitação echo na lista com o mouse.

A seção de Detalhe de Pacotes exibirá algo como isso:



Clique em cada um dos quatro "+" para expandir a informação.

A Seção de Detalhe de pacotes será similar a:



Como você pode ver, os detalhes para cada seção e protocolo podem ser mais expandidos. Passe algum tempo verificando essas informações. Neste estágio do curso, você pode não compreender totalmente as informações exibidas, mas faça anotações das informações que você reconhece.

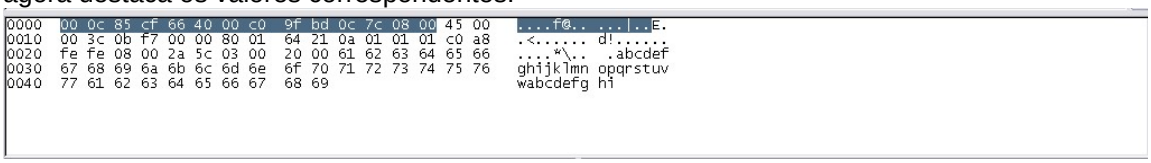
Localize os dois tipos diferentes de 'Origem" e "Destino". Por que existem dois tipos?

Quais protocolos estão no quadro Ethernet?

_____

Quando você seleciona uma linha na seção de Detalhe de Pacotes, toda ou parte da informação na seção de Bytes de Pacotes também fica destacada.

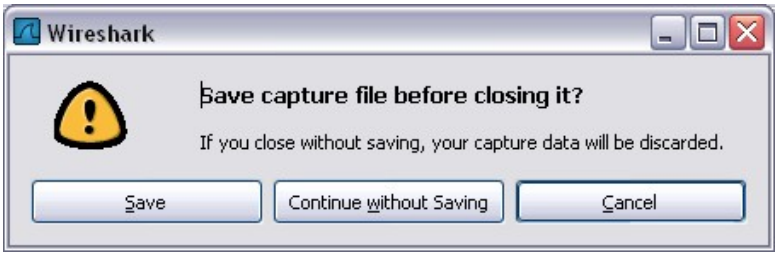
Por exemplo, se a segunda linha (+ Ethernet II) for destacada na seção de Detalhes, a seção de Bytes agora destaca os valores correspondentes.



Isso mostra os valores binários específicos que representam aquela informação na PDU. Neste estágio do curso, não é necessário entender essa informação em detalhes.

Passo 4: Vá ao menu Arquivo e selecione Fechar.

Clique em Continuar sem Salvar quando esta caixa de mensagem aparecer.



Tarefa 2: Captura de PDU FTP

Passo 1: Inicie a captura do pacote.

Considerando que o Wireshark ainda está sendo executado dos passos anteriores, inicie a captura de pacote clicando na opção Iniciar no menu Capturar do Wireshark.

Na linha de comando no seu computador onde o Wireshark está sendo executado, insira ftp 192.168.254.254.

Quando a conexão é estabelecida, insira anônimo como o usuário sem uma senha.
ID de usuário: **anônimo**
Senha: <ENTER>
Você pode, alternativamente, usar login com o ID de usuário **cisco** e com senha **cisco**.

Quando já tiver feito o login com êxito, insira **get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe** e pressione a tecla <ENTER>. Isso iniciará o download do arquivo do servidor ftp. O resultado parecerá similar a:

```
C:\Documents and Settings\ccna1>ftp eagle-server.example.com
Conectado a eagle-server.example.com.
220 Bem vindo ao serviço de FTP eagle-server.
Usuário (eagle-server.example.com:(nenhum)): anônimo
331 Por favor, especifique a senha.
Senha:<ENTER>
230 Login com sucesso.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
200 comando de PORTA com sucesso. Considere usando PASV.
150 Abrindo conexão de dados em modo BINÁRIO para
pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
226 Arquivo enviado OK.
ftp: 6967072 bytes recebidos em 0.59Segundos 11729.08Kbytes/sec.
```

Quando o download do arquivo estiver completo, insira **exit**

```
ftp> exit
221 Adeus.
C:\Documents and Settings\ccna1>
```

Quando tiver feito o download com sucesso do arquivo, pare a captura de PDU no Wireshark.

Passo 2: Aumente o tamanho da seção de Lista de Pacotes do Wireshark e passe pelas PDUs listadas.

Localize e anote as PDUs associadas ao download de arquivos.
Estas serão as PDUs do protocolo TCP da Camada 4 e do protocolo FTP da Camada 7.

Identifique os três grupos de PDUs associadas à transferência de arquivos.

Se você executou o passo acima, compare os pacotes com as mensagens e os prompts na janela da linha de comando do FTP.

O primeiro grupo é associado à fase de “conexão” e com o login ao servidor.
Liste exemplos de mensagens trocadas nesta fase.

_____

Localize e liste exemplos de mensagens trocadas na segunda fase que é a solicitação real de download e a transferência de dados.

_____

_____

O terceiro grupo de PDUs se relaciona a fazer o logout e "quebrar a conexão".

Liste exemplos de mensagens trocadas durante este processo.

_____

_____

Localize trocas de TCP recorrentes ao longo do processo de FTP. Qual recurso TCP isso indica?

_____ ____

Passo 3: Examine Detalhes de Pacotes.

Selecione (destaque) um pacote na lista associada à primeira fase do processo de FTP.
Visualize os detalhes do pacote na seção de Detalhes.

Quais são os protocolos encapsulados no quadro?

_____

Destaque os pacotes contendo o nome de usuário e a senha.
Examine a parte destacada na seção de Byte de Pacotes.

O que isso diz sobre a segurança deste processo de login de FTP?

_____

Destaque um pacote associado à segunda fase.
De qualquer seção, localize o pacote contendo o nome do arquivo.

O nome do arquivo é: _____

Destaque um pacote contendo o conteúdo real do arquivo - note o texto básico visível na seção de Byte.

Destaque e examine, nas seções de Detalhes e Bytes, alguns pacotes trocados na terceira fase de download do arquivo.
Quais recursos distinguem o conteúdo desses pacotes?
_____

Ao terminar, feche o arquivo do Wireshark e continue sem salvar

Tarefa 3: Captura de PDU HTTP

Passo 1: Inicie a captura do pacote.

Considerando que o Wireshark ainda está sendo executado dos passos anteriores, inicie a captura de pacote clicando na opção Iniciar no menu Capturar do Wireshark.

Nota: Opções de Captura não precisam estar configuradas, se estiverem continuando dos passos anteriores deste laboratório.

Abra um navegador no computador que está executando o Wireshark.

Insira a URL do Eagle Server de example.com ou insira o endereço de IP -192.168.254.254. Quando a página web tiver concluído seu download, pare a captura de pacote do Wireshark.

Passo 2: Aumente o tamanho da seção de Lista de Pacotes do Wireshark e passe pelas PDUs listadas.

Localize e identifique os pacotes TCP e HTTP associados ao download da página web.

Note a similaridade entre esta troca de mensagens e a troca FTP.

Passo 3: Na seção de Lista de Pacotes, destaque um pacote HTTP que possua a anotação "(text/html)" na coluna Info.

Na seção de Detalhe de Pacotes, clique em "+" próximo a "Dados de texto baseados em linha: html" Quando essa informação é expandida, o que é exibido?

_____

Examine a parte destacada do Painel de Bytes.
Isso mostra os dados HTML trazidos pelo pacote.

Ao finalizar, feche o arquivo do Wireshark e continue sem salvar.

Tarefa 4: Reflexão

Considere as informações de encapsulamento pertencentes aos dados de rede capturados que o Wireshark pode fornecer. Relacione isso aos modelos de camada OSI e TCP/IP. É importante que você possa reconhecer e fazer o link de ambos os protocolos representados e da camada de protocolo e dos tipos de encapsulamento dos modelos com as informações fornecidas pelo Wireshark.

Tarefa 5: Desafio

Discuta como você poderia usar um analisador de protocolo, como o Wireshark para:

(1) Resolver a falha de uma página web para fazer o download com sucesso de um navegador em um computador.

e

(2) Identificar tráfego de dados em uma rede que é solicitada por usuários.

_____

_____

_____

_____

_____

_____

Tarefa 6: Limpeza

A menos que instruído de outra forma pelo seu instrutor, saia do Wireshark e desligue de maneira adequada o computador.

