UNIVERSIDADE CATÓLICA DE BRASÍLIA

REDES II - 1/2008

ÍNDICE

1. INTRODUÇÃO

O Wireshark, antigamente chamado *Ethereal*, é um programa que analisa o tráfego de rede, organizando-o através de protocolos. Registrado pela GNU *General Public License* (GPL), suporta as plataformas *Unix*, *Linux*, *Solaris*, *FreeBSB*, *NetBSD*, *OpenBSD*, *Mac OS X* e *Windows*.

Os capítulos seguintes do Manual de Funcionamento Wireshark, elaborado por Júlia de Castro e Leonardo Ribeiro, irão mostrar as principais funcionalidades do programa. Com uma breve apresentação da interface, juntamente com a descrição dos menus, ferramentas, painéis e barra de *status*, além de instruir como capturar, ver ou filtrar pacotes, o usuário estará pronto para administrar a rede de forma fácil e prática.

2. INICIANDO O WIRESHARK

Você pode iniciar o Wireshark através do *shell* ou do gerenciador de janela.

 Dica!

Quando iniciar o Wireshark, é possível especificar configurações adicionais usando a linha de comandos.

 Nota!

Nos próximos capítulos, algumas capturas de tela irão aparecer. Apesar das diferenças de interface entre versões e plataformas distintas, as funcionalidades permanecem as mesmas.

3. JANELA PRINCIPAL

A imagem a seguir, que exemplifica alguns pacotes sendo capturados ou carregados, servirá de base para uma breve descrição dos elementos contidos na janela principal do Wireshark.

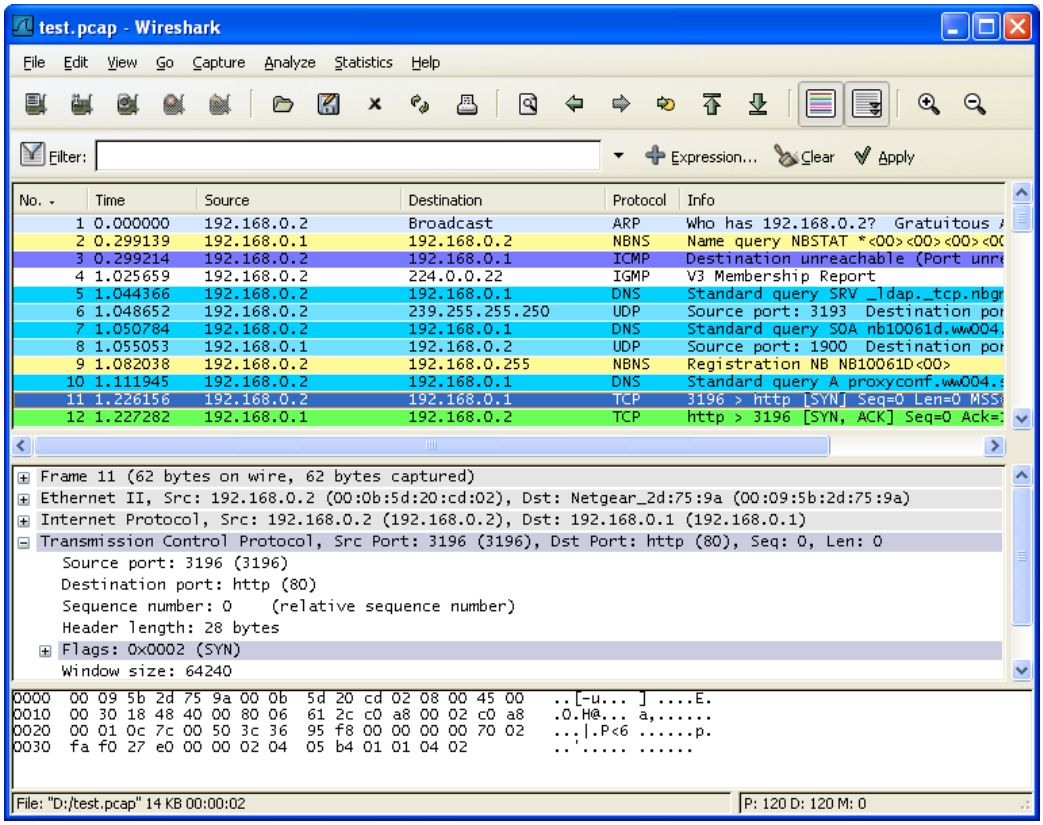

Figura 1. Janela principal.

1. O *menu* (ver seção 4) é usado para iniciar ações;
2. A *Barra de Ferramentas Principal* (ver seção 13) fornece um rápido acesso aos itens que são freqüentemente usados;
3. A *Ferramenta Filter* (ver seção 14) fornece um campo para manipular diretamente o que será exibido pelo filtro;
4. O *Painel de Lista dos Pacotes* (ver seção 15) exibe um resumo de cada pacote capturado. Clicando sobre um deles é possível controlar o que será mostrado nos painéis subseqüentes;
5. O *Painel de Detalhes dos Pacotes* (ver seção 16) exibe maiores detalhes dos pacotes selecionados no *Painel de Lista dos Pacotes*;
6. O *Painel de Bytes dos Pacotes* (ver seção 17) exibe os dados dos pacotes selecionados no *Painel de Lista dos Pacotes* e destaca o campo selecionado no *Painel de Detalhes dos Pacotes*;
7. A *Barra de Status* (ver seção 18) mostra algumas informações detalhadas acerca do estado atual do programa e dos dados capturados.

Dica!

O *layout* da janela principal pode ser personalizado modificando as configurações preferenciais (*Edit -> Preferences)*.

3.1. JANELA DE NAVEGAÇÃO PRINCIPAL

A lista de pacotes e detalhes de navegação podem ser feitos inteiramente pelo teclado. A tabela abaixo mostra os atalhos para uma manipulação mais rápida acerca do arquivo de captura.

Atalho	Descrição
Tab, Shift + Tab	Move entre os elementos da tela (da barra de ferramentas para a lista de pacotes e de detalhes).
↓	Move para o próximo pacote ou detalhe do item.
↑	Move para o pacote ou detalhe do item anterior.
Ctrl + ↓, F8	Move para o próximo pacote, mesmo se a lista de pacotes não estiver focalizada.
Ctrl + ↑, F7	Move para o pacote anterior, mesmo se a lista de pacotes não estiver focalizada.
←	Nos detalhes dos pacotes, fecha os sub-itens do item selecionado.
→	Nos detalhes dos pacotes, abre os sub-itens do item selecionado.
Shift + →	Nos detalhes dos pacotes, abre todos os sub-itens do item selecionado.
Ctrl + →	Nos detalhes dos pacotes, abre todos os sub-itens.
Ctrl + ←	Nos detalhes dos pacotes, fecha todos os sub-itens.
Backspace	Nos detalhes dos pacotes, quando está em um sub-item, retorna para o item que pertence.
Return, Enter	Nos detalhes dos pacotes, comprime ou expande um item selecionado.

Tabela 1. Teclas de atalho.

4. MENU

O menu do Wireshark, como pode ser visto na Figura 2, se encontra no topo da janela.

 Dica!

Os itens do menu ficarão cinza se o atributo correspondente não estiver disponível. Por exemplo, você não consegue salvar um arquivo se você não capturar ou carregar algum dado antes.

Figura 2. Menu do Wireshark.

Analisando a figura anterior, pode-se descrever os seguintes elementos:

1. *File* (seção 5): contém itens para abrir (*open*), unir (*merge*), salvar (*save*), imprimir (*print*) ou exportar (*export*) arquivos de captura, seja por completo ou em partes, além da opção de sair do Wireshark (*quit*).
2. *Edit* (seção 6): contém itens para procurar (*find*) um pacote, referenciar o tempo (*set time reference*) ou marcar (*mark*) um ou mais pacotes, bem como alterar suas preferências (*preferences*). Recortar (*cut*), copiar (*copy*) e colar (*paste*) não serão mencionados agora.
3. *View* (seção 7): controla a exibição da captura de dados, incluindo coloração de pacotes (*coloring rules*), aumentar ou diminuir a fonte (*zoom in/ out*), mostrar um pacote em uma janela separada (*show packet in new window*), assim como expandir ou comprimir os itens selecionados no *Painel de Detalhes dos Pacotes* (*expand/ collapse all*).
4. *Go* (seção 8): contém itens que direcionam para um pacote específico.
5. *Capture* (seção 9): permite iniciar ou parar uma captura (*start/ stop/ restart*), além de editar os filtros (*capture filters*).
6. *Analyze* (seção 10): contém itens para controlar a exibição dos filtros (*display filters*), habilitar e desabilitar as operações dos protocolos (*enabled protocols*), configurar decodificações específicas do usuário (*user specified decodes*), entre outros.
7. *Statistics* (seção 11): possui itens para exibir várias janelas de estatística, incluindo um resumo (*summary*) dos pacotes que têm sido capturados, exibindo uma hierarquia de estatística dos protocolos (*protocol hierarchy*).
8. *Help* (seção 12): contém itens que irão auxiliar o usuário, como manuais (*manual pages*), conteúdos (*contents*) ou acesso online a páginas da web (*wireshark online*).

Cada um desses itens será descrito com maiores detalhes nas seções seguintes.

5. MENU *FILE*

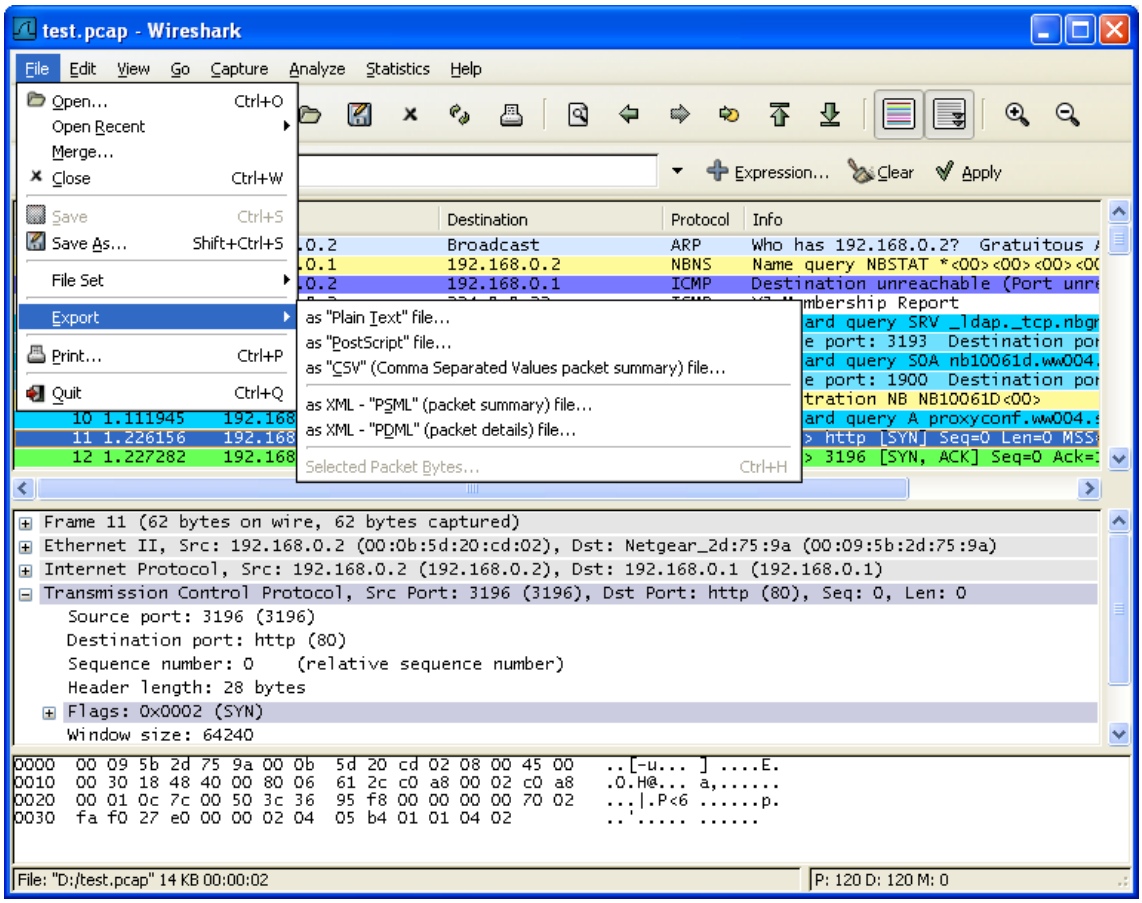

Figura 3. Menu *file*.

O menu *file* contém os campos mostrados na Figura 3. Uma breve descrição desses itens pode ser visto na Tabela 2:

Itens do menu	Teclas de atalho	Descrição
Open…	Ctrl + O	Este item traz uma caixa de diálogo que permite carregar um arquivo de captura para exibição.
Open Recent	-	Este item exibe um submenu que contém todos os arquivos de captura abertos recentemente.
Merge…	-	Este item traz uma caixa de diálogo que permite unir outros arquivos de captura dentro do que está atualmente carregado.
Close	Ctrl + W	Com este item é possível fechar um arquivo de captura.

Save	Ctrl + S	Este item permite salvar o arquivo de captura ou qualquer arquivo que desejar.  Nota! Se o arquivo atual já estiver salvo, este item ficará cinza.
Save As…	Shift + Ctrl + S	 Nota! Você não pode salvar um arquivo enquanto ele estiver em execução. É necessário pausá-lo primeiro.
File Set > List Files	-	Com este item é possível ver uma lista de arquivos em um grupo.
File Set > Next File	-	Se o atual arquivo carregado fizer parte de um grupo de arquivos, pula para o próximo arquivo deste mesmo grupo. Se não fizer parte ou for o primeiro da lista, este item ficará cinza.
File Set > Previous File	-	Se o atual arquivo carregado fizer parte de um grupo de arquivos, pula para o arquivo anterior deste mesmo grupo. Se não fizer parte ou for o primeiro da lista, este item ficará cinza.
Export > as "Plain Text" file…	-	Com este item é possível exportar pacotes do arquivo de captura para um formato texto (arquivo do tipo ASCII).
Export > as "PostScript" file…	-	Este item permite exportar pacotes do arquivo de captura para um arquivo *PostScript*.
Export > as "CSV" (Comma Separated Values packet summary) file…	-	Com este item é possível exportar resumos dos pacotes do arquivo de captura para um arquivo .csv (usado por programas de planilha eletrônica).
Export > as "PSML" file…	-	Este item permite exportar pacotes do arquivo de captura para XML PSML (*packet summary markup language*).
Export > as "PDML" file…	-	Este item permite exportar pacotes do arquivo de captura para um arquivo XML PDML (*packet details markup language*).

Export > Selected Packet Bytes…	Ctrl + H	Com este item é possível exportar os bytes selecionados no *Painel de Bytes dos Pacotes* para um arquivo binário.
Print…	Ctrl + P	Este item imprime todos ou alguns dos pacotes do arquivo de captura.
Quit	Ctrl + Q	Este item permite sair do programa. Quando acioná-lo, o Wireshark irá perguntar se deseja ou não salvar seu arquivo de captura (isto pode ser desabilitado conforme preferência).

Tabela 2. Itens do menu *file*.

6. MENU *EDIT*

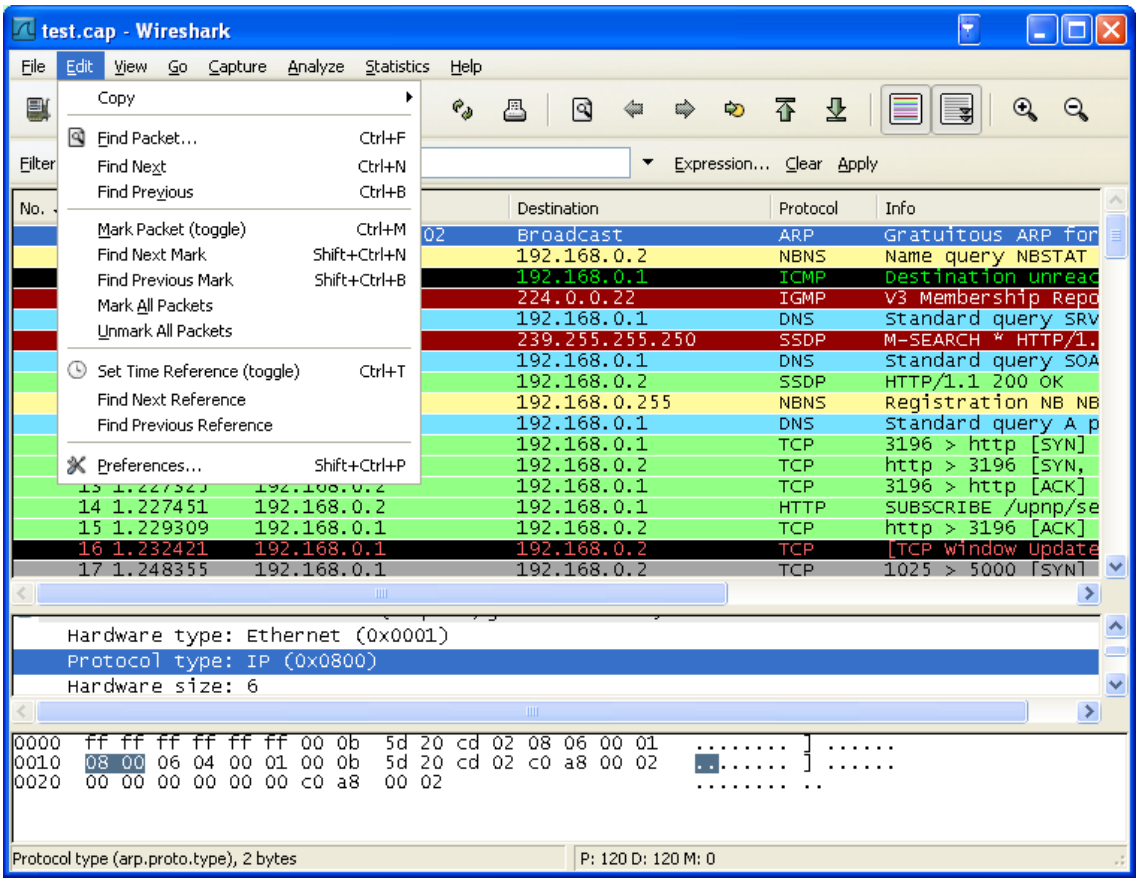

Figura 4. Menu *edit*.

O menu *edit* contém os campos mostrados na Figura 4. Uma breve descrição desses itens pode ser visto na Tabela 3:

Itens do menu	Teclas de atalho	Descrição
Copy > As Filter	Shift + Ctrl + C	Este item utiliza o elemento selecionado no *Painel de Detalhes dos Pacotes* para criar um filtro de exibição. Esse filtro será copiado para o *clipboard*.
Find Packet...	Ctrl + F	Este item traz uma caixa de diálogo que permite localizar um pacote de acordo com alguns critérios.
Find Next	Ctrl + N	Este item tenta localizar o próximo pacote com as mesmas configurações de "*Find Packet...*"
Find Previous	Ctrl + B	Este item tenta localizar o pacote anterior com as mesmas configurações de "*Find Packet...*"
Mark Packet (toggle)	Ctrl + M	Este item sinaliza o atual pacote selecionado.
Find Next Mark	Shift + Ctrl + N	Procura o próximo pacote sinalizado.
Find Previous Mark	Shift + Ctrl + B	Procura o pacote sinalizado anterior.
Mark All Packets	-	Com este item é possível sinalizar todos os pacotes.

Unmark All Packets	-	Com este item é possível desmarcar todos os pacotes sinalizados.
Set Time Reference (toggle)	Ctrl + T	Este item referencia o tempo dentro do atual pacote selecionado.
Find Next Reference	-	Este item tenta localizar o próximo pacote com tempo referenciado.
Find Previous Reference	-	Este item tenta localizar o pacote anterior com tempo referenciado.
Preferences…	Shift + Ctrl + P	Este item traz uma caixa de diálogo que permite ajustar as preferências conforme alguns parâmetros.

Tabela 3. Itens do menu *edit*.

7. MENU *VIEW*

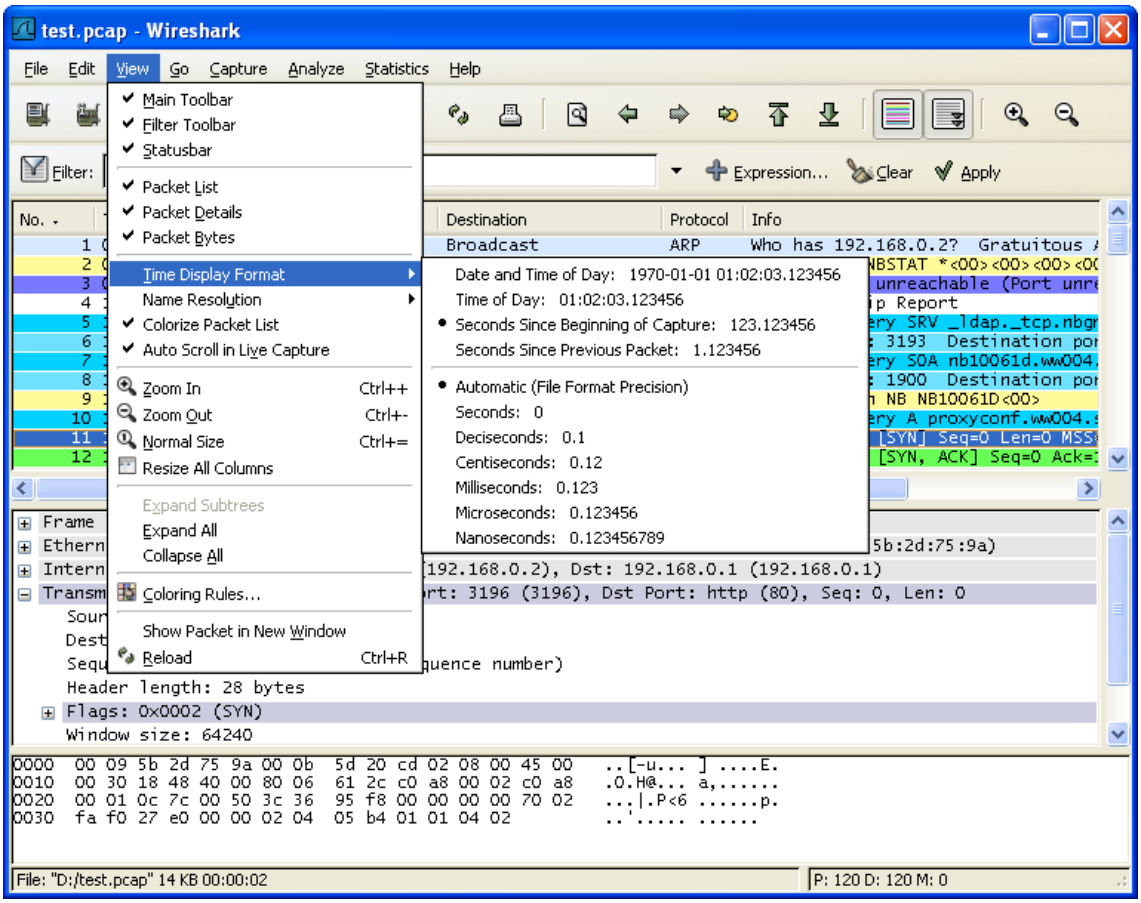

Figura 5. Menu *view*.

O menu *view* contém os campos mostrados na Figura 5. Uma breve descrição desses itens pode ser visto na Tabela 4:

Itens do menu	Teclas de atalho	Descrição
Main Toolbar	-	Este item oculta ou exibe a barra de ferramentas principal (ver seção 13).
Filter Toolbar	-	Este item oculta ou exibe a ferramenta *filter* (ver seção 14).
Statusbar	-	Este item oculta ou exibe a barra de *status* (ver seção 18).
Packet List	-	Este item oculta ou exibe o *Painel de Lista dos Pacotes* (ver seção 15).
Packet Details	-	Este item oculta ou exibe o *Painel de Detalhes dos Pacotes* (ver seção 16).
Packet Bytes	-	Este item oculta ou exibe o *Painel de Bytes dos*

		Pacotes (ver seção 17).
Time Display Format > Date and Time of Day: 1970-01-01 01:02:03.123456	-	Selecionando isto o Wireshark irá exibir a marcação de tempo na data e no horário especificados de acordo com a formatação do dia.  Nota! O campo "*Time of Day*", "*Date and Time of Day*", "*Seconds Since Beginning of Capture*", "*Seconds Since Previous Captured Packet*" and "*Seconds Since Previous Displayed Packet*" são mutuamente exclusivos.
Time Display Format > Time of Day: 01:02:03.123456	-	Selecionando isto o Wireshark irá exibir a marcação de tempo no horário especificado de acordo com a formatação do dia.
Time Display Format > Seconds Since Beginning of Capture: 123.123456	-	Selecionando isto o Wireshark irá exibir a marcação de tempo em segundos desde o início da captura.
Time Display Format > Seconds Since Previous Captured Packet: 1.123456	-	Selecionando isto o Wireshark irá exibir a marcação de tempo em segundos desde os pacotes capturados anteriormente.
Time Display Format > Seconds Since Previous Displayed Packet: 1.123456	-	Selecionando isto o Wireshark irá exibir a marcação de tempo em segundos desde a exibição dos pacotes capturados anteriormente.
Time Display Format > Automatic (File Format Precision)	-	Selecionando isto o Wireshark irá exibir a marcação de tempo com uma precisão determinada pela formatação do arquivo de captura utilizado.  Nota! Os campos "*Automatic*", "*Seconds*" and "*... seconds*" são mutuamente exclusivos.
Time Display Format > Seconds: 0	-	Selecionando isto o Wireshark irá exibir a marcação de tempo com uma precisão de um segundo.
Time Display	-	Selecionando isto o Wireshark irá exibir a

Format > ... seconds: 0...		marcação de tempo com uma precisão de um segundo, 10^{-1} segundos, 10^{-2} segundos, 10^{-3} segundos, 10^{-6} segundos ou 10^{-9} segundos.
Name Resolution > Resolve Name	-	Este item permite resolver o nome que determina somente o pacote atual.
Name Resolution > Enable for MAC Layer	-	Este item permite controlar se o Wireshark traduz ou não o endereço MAC em nomes.
Name Resolution > Enable for Network Layer	-	Este item permite controlar se o Wireshark traduz ou não o endereço da rede em nomes.
Name Resolution > Enable for Transport Layer	-	Este item permite controlar se o Wireshark traduz ou não o endereço de transporte em nomes.
Colorize Packet List	-	Este item permite controlar se o Wireshark deverá ou não colorir a lista de pacotes.  Nota! Habilitando a coloração, ficará mais lento exibir a captura / carregamento dos arquivos de captura.
Auto Scroll in Live Capture	-	Este item permite que o Wireshark mostre os últimos pacotes capturados. Se estiver desabilitado, o Wireshark adiciona novos pacotes ao final da lista, mas é necessário descer a barra de rolagem para visualizá-los.
Zoom In	Ctrl++	Aumenta o *zoom* dos dados dos pacotes (aumenta o tamanho da fonte).
Zoom Out	Ctrl+-	Diminui o *zoom* dos dados dos pacotes (diminui o tamanho da fonte).
Normal Size	Ctrl+=	Configura o nível do *zoom* para 100% (o tamanho da fonte volta para o normal).
Resize All Columns	-	Modifica a largura de todas as colunas para ajustar ao conteúdo.
Expand Subtrees	-	Este item expande o item selecionado dentro da *Lista de Detalhes dos Pacotes*.
Expand All	-	Expande todos os itens e sub-itens da *Lista de Detalhes dos Pacotes*.

Collapse All	-	Comprime todos os itens e sub-itens da *Lista de Detalhes dos Pacotes*.
Coloring Converation	-	Este item traz um submenu que permite colorir pacotes no *Painel de Lista dos Pacotes* baseado no endereço daquele que está atualmente selecionado. Com isto, fica fácil distinguir pacotes que pertencem a diferentes contextos.
Coloring Converation > Color 1-10	-	Este item habilita um dos dez filtros de cor baseado no contexto em que se insere o pacote atualmente selecionado.
Coloring Converation > Reset coloring	-	Este item apaga todas as cores temporárias.
Coloring Converation > New Coloring Rule…	-	Este item abre uma janela de diálogo na qual uma nova coloração pode ser feita baseada no contexto em que se insere o pacote atualmente selecionado.
Coloring Rules…	-	Este item traz uma caixa de diálogo que permite colorir pacotes dentro do *Painel de Lista dos Pacotes*, conforme expressão inserida no filtro.
Show Packet in New Window	-	Este item abre um pacote selecionado em uma janela separada, mostrando somente seu painel de bytes e de detalhes.
Reload	Ctrl-R	Este item permite carregar novamente o atual arquivo de captura.

Tabela 4. Itens do menu *view*.

8. MENU *GO*

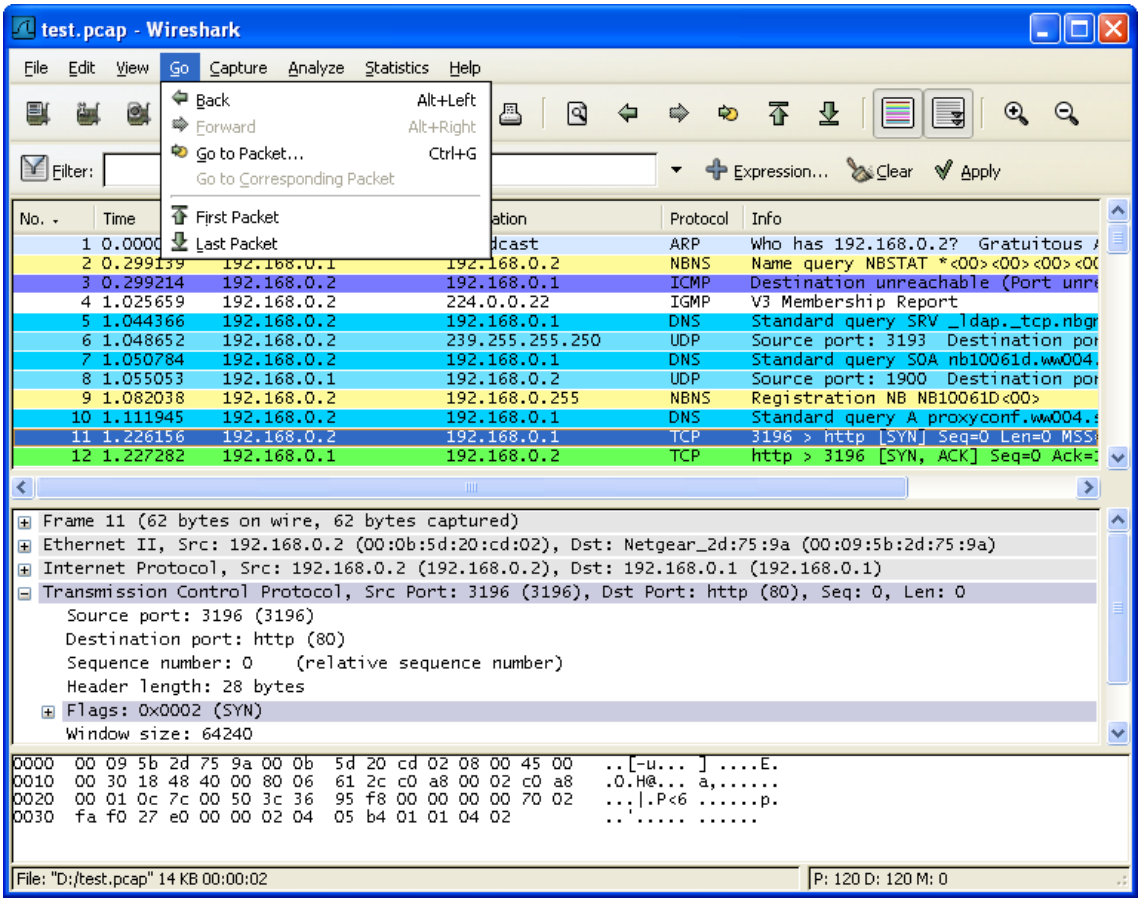

Figura 6. Menu *go*.

O menu *go* contém os campos mostrados na Figura 6. Uma breve descrição desses itens pode ser visto na Tabela 5:

Itens do menu	Teclas de atalho	Descrição
Back	Alt + ←	Pula para o pacote visitado recentemente no histórico de pacotes, bem como no histórico de páginas em um navegador.
Forward	Alt + →	Pula para o próximo pacote visitado no histórico de pacotes, bem como no histórico de páginas em um navegador.
Go to Packet...	Ctrl – G	Traz uma caixa de diálogo que permite especificar o número do pacote e depois ir até ele.
Go to Corresponding Packet	-	Vai para o pacote correspondente da área de protocolo atualmente selecionado. Se o campo selecionado não for correspondente ao pacote, este item ficará cinza.

Previous Packet	Ctrl + ↑	Passa para o pacote anterior da lista.
Next Packet	Ctrl + ↓	Passa para o próximo pacote da lista.
First Packet	-	Pula para o primeiro pacote do arquivo de captura.
Last Packet	-	Pula para o último pacote do arquivo de captura.

Tabela 5. Itens do menu *go*.

9. MENU *CAPTURE*

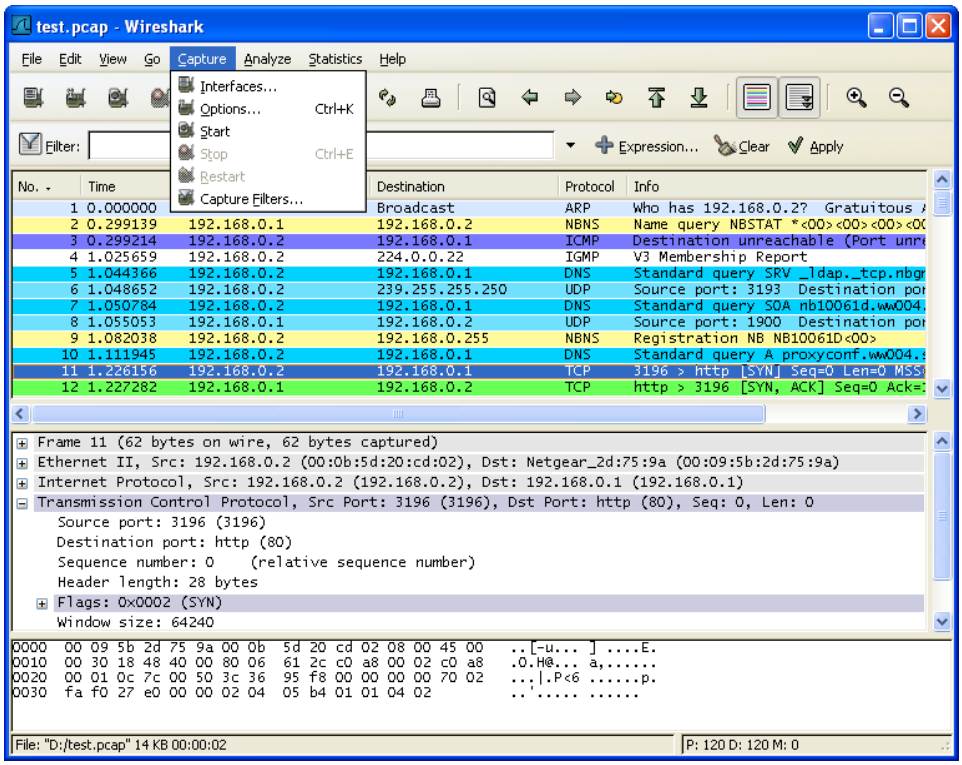

Figura 7. Menu *Capture*

O menu *capture* contém os campos mostrados na Figura 7. Uma breve descrição desses itens pode ser visto na Tabela 6:

Itens do menu	Teclas de atalho	Descrição
Interfaces ...	-	Este item traz uma caixa de diálogo que mostra o que está acontecendo com as interfaces de rede das quais o Wireshark tem conhecimento.
Options...	Ctrl + K	Este item traz uma caixa de diálogo que mostra as opções de captura.
Start	-	Inicia imediatamente a captura de pacotes com a mesma configuração anterior.
Stop	Ctrl + E	Pára a execução da atual captura.
Restart	-	Pára a execução da atual captura e inicia novamente com a mesma configuração.
Capture Filters...	-	Este item traz uma caixa de diálogo que permite criar e editar os filtros de captura. Você pode nomeá-los e salvá-los para uso futuro.

Tabela 6. Itens do menu *capture*.

10. MENU *ANALYZE*

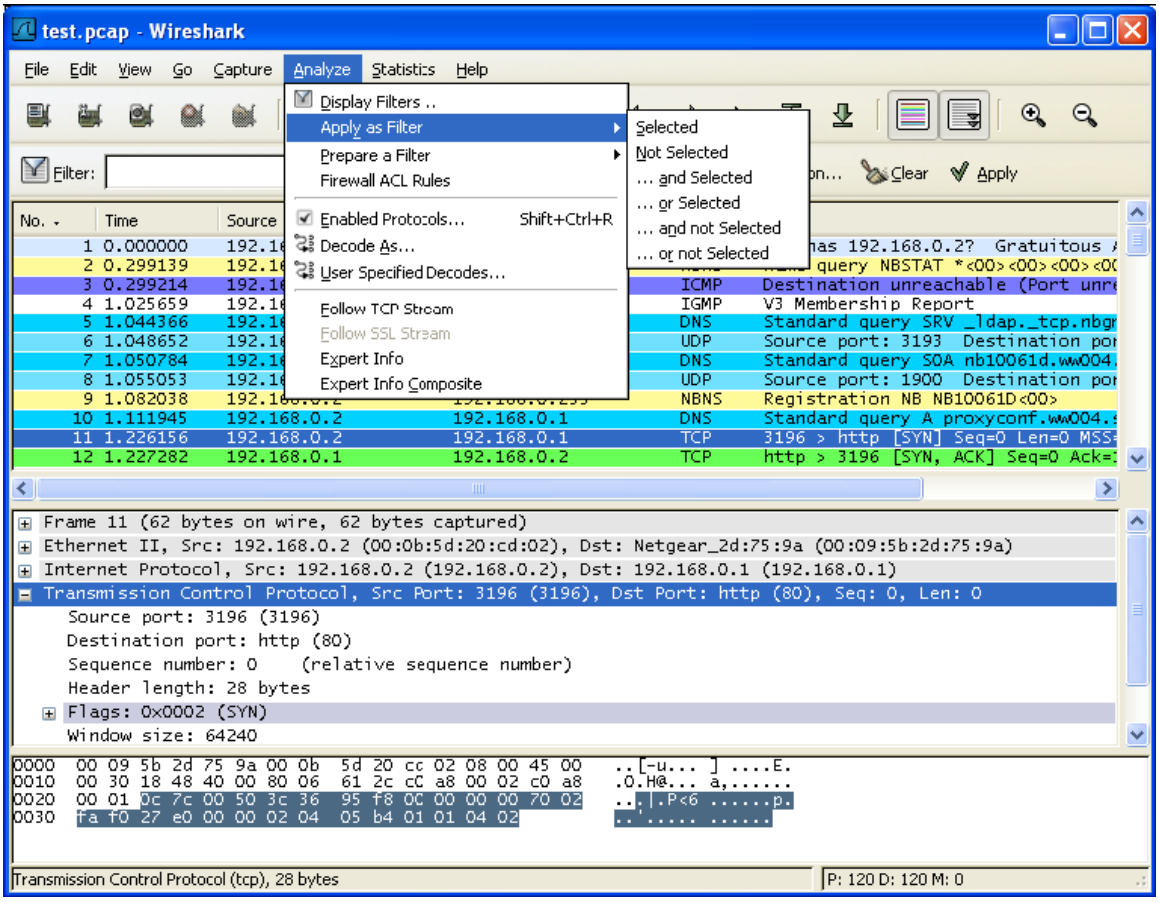

Figura 8. Menu *Analyze*

O menu *analyze* contém os campos mostrados na Figura 8. Uma breve descrição desses itens pode ser visto na Tabela 7:

Item	Atalhos	Descrição
Display Filters...	-	Este item do menu abre uma caixa de diálogo que permite criar e editar filtros. Os filtros podem ser nomeados e salvos para uso futuro.
Aplly as filters > ...	-	Este item do menu mudará o filtro atual e aplicará o filtro escolhido imediatamente. Dependendo da escolha, o atual é substituído ou adicionado ao campo do filtro selecionado no *Painel de Detalhes dos Pacotes*.
Prepare a filter > ...	-	Este item mudará o filtro atual, mas não aplicará o filtro escolhido. Dependendo da escolha, o atual é substituído ou adicionado ao campo do filtro selecionado no *Painel de Detalhes dos Pacotes*.

Firewall Acl Rules	-	Este item permite criar regras de linha de comando ACL para vários *firewalls* diferentes. Regras para endereço MAC, endereço IPV4, portas TCP e UDP, além de IPV4 + combinações de portas são suportados.
Enabled Protocols...	Shift + Ctrl + R	Esse item permite habilitar/desabilitar protocolos.
Decode As...	-	Esse item permite forçar o Wireshark a decodificar o pacote com um protocolo em particular.
User Specified Decodes...	-	Esse item permite forçar o Wireshark a decodificar o pacote com um protocolo em particular.
Follow TCP Stream	-	Esse item traz uma janela separada e exibe segmentos TCP que são capturados na mesma conexão TCP que o pacote selecionado.
Follow UDP Stream	-	Funciona igual ao *Follow TCP Stream*, mas para UDP.
Follow SSL Stream	-	Funciona igual ao *Follow TCP Stream*, mas para SSL.
Expert Info	-	Abre um diálogo que exibe algumas informações especiais acerca da captura de pacotes em um *log* de exibição. A contagem de informações dependerá do protocolo e varia de muito detalhado a não existente. Funciona quando a captura está em processo.
Expert Info Composite	-	Semelhante ao *Expert Info*, mas separa os itens por grupo para uma análise mais rápida.

Tabela 7. Itens do menu *analyze*.

11. MENU *STATISTICS*

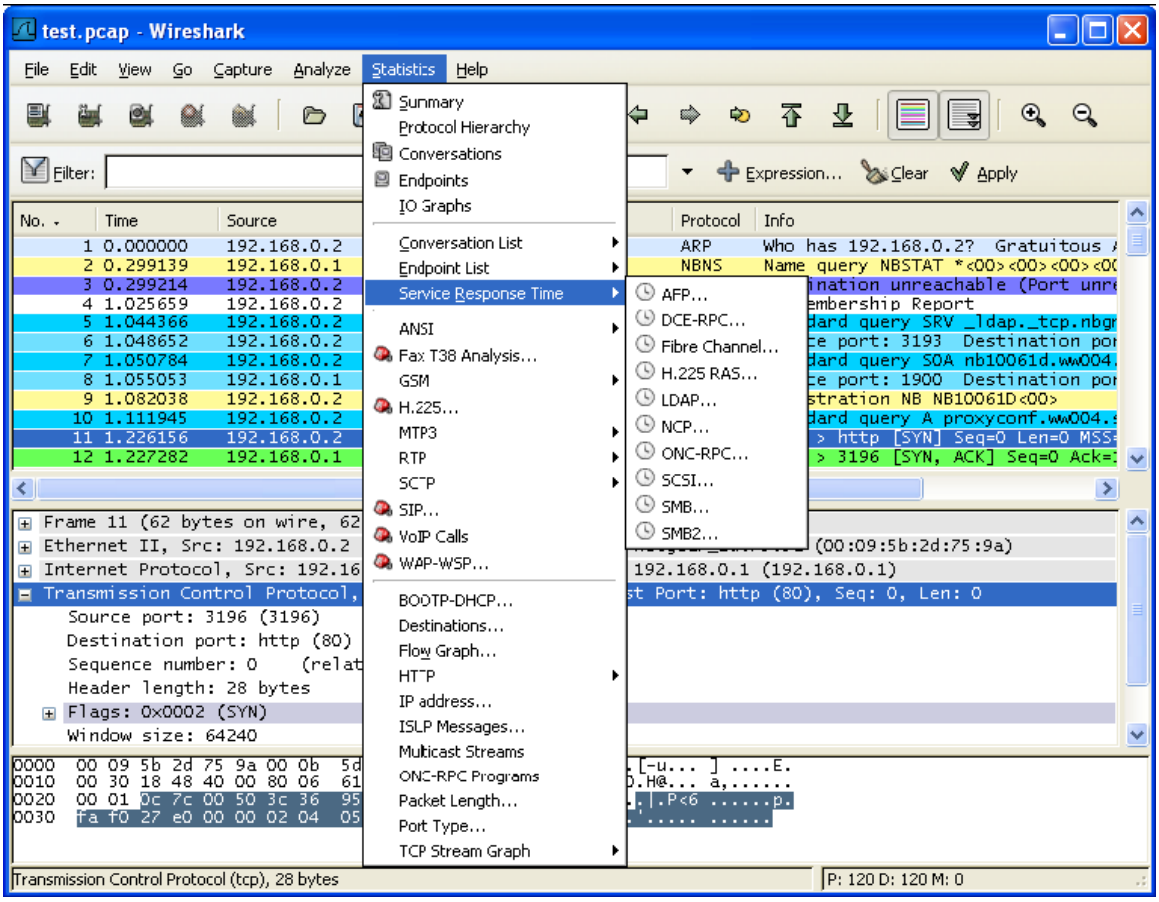

Figura 9. Menu *Statistics*

O menu *statistics* contém os campos mostrados na Figura 9. Uma breve descrição desses itens pode ser visto na Tabela 8:

Itens do menu	Teclas de atalho	Descrição
Summary	-	Apresenta informações sobre a captura de dados.
Protocol Hierarchy	-	Mostra uma árvore hierárquica de estatísticas do protocolo.
Conversations	-	Mostra uma lista de conversação (tráfico entre dois *endpoints*).
Endpoints	-	Mostra uma lista de *endpoints* (tráfico de/para um endereço).
IO Graphs	-	Mostra gráficos específicos (ex.: o número de pacotes em tráfico no momento).
Conversation List	-	Mostra uma lista de conversação, tornando a anterior obsoleta.
Endpoint List	-	Mostra uma lista de *endpoints*, tornando a anterior obsoleta.

Service Response Time	-	Mostra o tempo entre uma solicitação e a sua resposta correspondente.
http	-	Estatísitica de solicitação/resposta HTTP.

Tabela 8. Itens do menu *statistics*.

Existem protocolos específicos como o *ANSI*, *GSM*, *H.225*, *ISUP Message* e outros que tem suas estatísticas apresentadas nesse menu.

12. MENU *HELP*

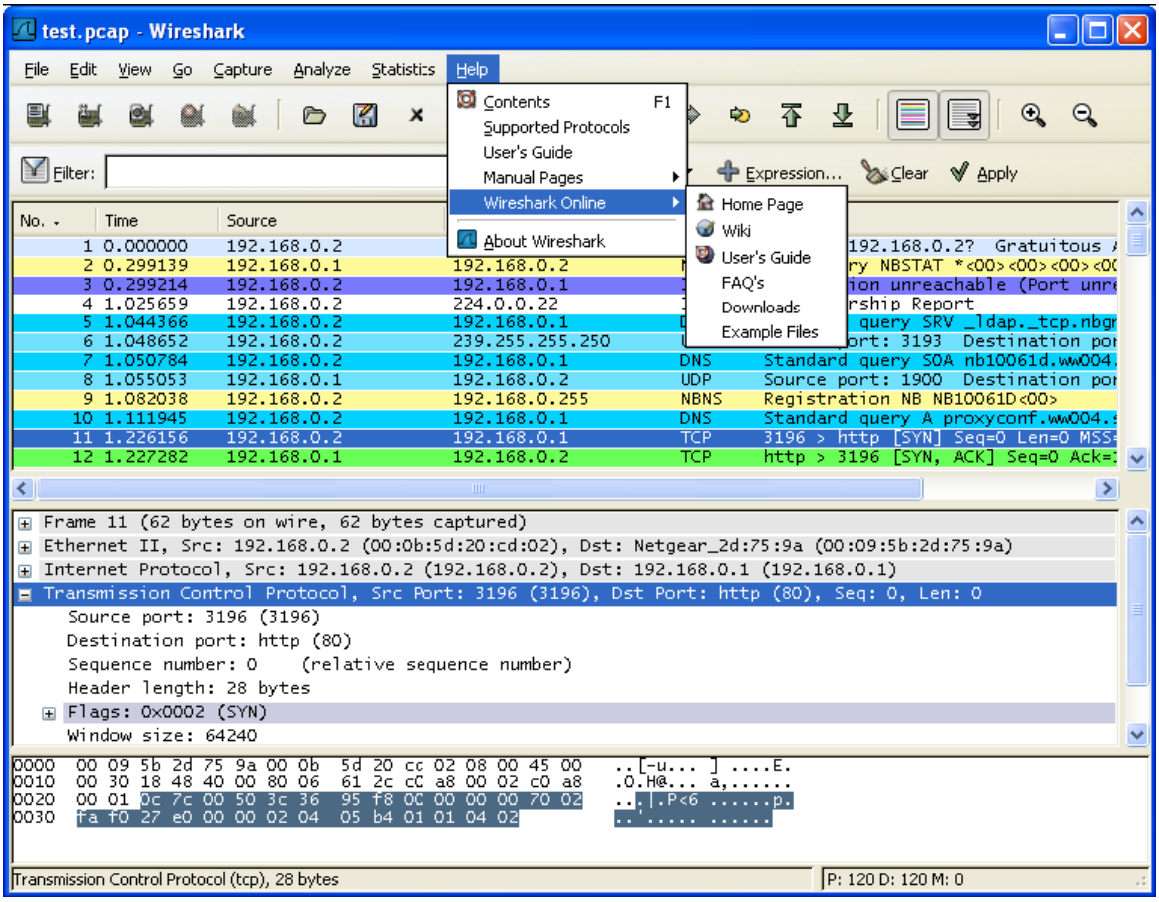

Figura 10. Menu *Help*

O menu *help* contém os campos mostrados na Figura 10. Uma breve descrição desses itens pode ser visto na Tabela 9:

Itens do menu	Teclas de atalho	Descrição
Contents	F1	Este item traz um sistema de ajuda básico.
Supported Protocols	-	Este item traz uma janela de diálogo apresentando os protocolos suportados e os campos dos protocolos.
Manual Pages > ...	-	Este item inicia o navegador *web*, apresentando a página escolhida: *http://www.wireshark.org*.
About Wireshark	-	Este item abre uma janela com algumas informações sobre o Wireshark, tais como *plugins*, pastas utilizadas, entre outros.

Tabela 9. Itens do menu *help*.

13. BARRA DE FERRAMENTAS PRINCIPAL

Figura 11. Barra de ferramentas principal.

A barra de ferramentas permite um acesso rápido aos itens do menu que são usados com mais freqüência, como pode ser visto na Figura 11. Uma breve descrição desses itens pode ser visto na Tabela 10:

Ícone	Item	Item correspondente no menu	Descrição
	Interfaces...	*Capture > Interfaces...*	Esse item traz uma lista de interfaces de captura.
	Options...	*Capture > Options...*	Esse item traz opções de captura.
	Start	*Capture > Start*	Esse item inicia a captura de pacotes com as últimas opções de formatação.
	Stop	*Capture > Stop*	Esse item pára o processo de captura atual.
	Restart	*Capture > Restart*	Esse item pára o processo de captura atual e o inicia novamente.
	Open...	*File > Open...*	Este item traz uma caixa de diálogo que permite carregar um arquivo de captura para exibição.
	Save As...	*File > Save As...*	Esse item permite salvar o arquivo de captura no diretório que desejar.
	Close	*File > Close*	Esse item fecha a captura atual.
	Reload	*View > Reload*	Esse item permite recarregar o arquivo de captura atual.
	Print...	*File > Print...*	Este item imprime todos ou alguns dos pacotes do arquivo capturado.
	Find Packet...	*Edit > Find Packet...*	Este item traz uma caixa de diálogo que permite localizar um pacote de acordo com alguns critérios.
	Go Back	*Go > Go Back*	Esse item retorna no histórico de pacotes.
	Go Forward	*Go > Go Forward*	Esse item avança no histórico de pacotes.
	Go to Packet...	*Go > Go to Packet...*	Esse item traz uma caixa de diálogo que permite a inserção do número de um pacote para em seguida ir até ele.
	Go To First Packet	*Go > Go To First Packet*	Esse item pula para o primeiro pacote no arquivo de captura.
	Go To Last Packet	*Go > Go To Last Packet*	Esse item pula para o último pacote no arquivo de captura.
	Colorize	*View > Colorize*	Colore ou não a lista de pacotes.

	*Auto Scroll in Live Capture*	*View > Auto Scroll in Live Capture*	Aciona ou não a barra de rolagem automática enquanto ocorre a captura.
	*Zoom In*	*View > Zoom In*	Aumenta o *zoom* do pacote de dados (aumenta o tamanho da fonte).
	*Zoom Out*	*View > Zoom Out*	Diminui o *zoom* do pacote de dados (diminui o tamanho da fonte).
	*Normal Size*	*View > Normal Size*	Volta o nível de *zoom* para 100%.
	*Resize Columns*	*View > Resize Columns*	Redimensiona as colunas, de forma que o conteúdo se ajuste a elas.
	*Capture Filters...*	*Capture > Capture Filters...*	Este item traz uma caixa de diálogo que permite criar e editar os filtros de captura. Você pode nomeá-los e salvá-los para uso futuro.
	*Display Filters...*	*Analyze > Display Filters...*	Este item do menu abre uma caixa de diálogo que permite criar e editar filtros. Os filtros podem ser nomeados e salvos para serem usados no futuro.
	*Coloring Rules...*	*View > Coloring Rules...*	Este item traz uma caixa de diálogo que permite colorir pacotes no *Painel de Lista dos Pacotes*.
	*Preferences...*	*Edit > Preferences*	Este item traz uma caixa de diálogo que permite ajustar as preferências conforme alguns parâmetros.
	*Help*	*Help > Contents*	Este item traz uma caixa de diálogo de ajuda básica.

Tabela 10. Itens da barra de ferramentas principal.

14. FERRAMENTA *FILTER*

Figura 12. Ferramenta *filter*.

A barra de filtros permite que sejam criados e editados filtros de forma rápida, conforme pode ser observado na Figura 12. Uma breve descrição desses itens pode ser visto na Tabela 11:

Itens do menu	Teclas de atalho	Descrição
	Filter:	Traz a janela de construção do filtro.
	*Filter input*	Área para acessar ou editar um filtro. A verificação de sintaxe é feita enquanto o usuário está digitando. O fundo fica vermelho se for digitada uma palavra inválida ou incompleta, e fica verde quando a palavra é válida.
	*Expression...*	Abre uma caixa de diálogo que permite editar o filtro em exibição de um campo com uma lista de protocolos.
	*Clear*	Reinicia o filtro em exibição atual e limpa a área de edição.
	*Apply*	Aplica o valor atual da área de edição no novo filtro.

Tabela 11. Itens da ferramenta *filter*.

15. PAINEL DE LISTA DOS PACOTES

O *Painel de Lista dos Pacotes* exibe todos os pacotes no arquivo de captura atual, conforme mostra a Figura 13.

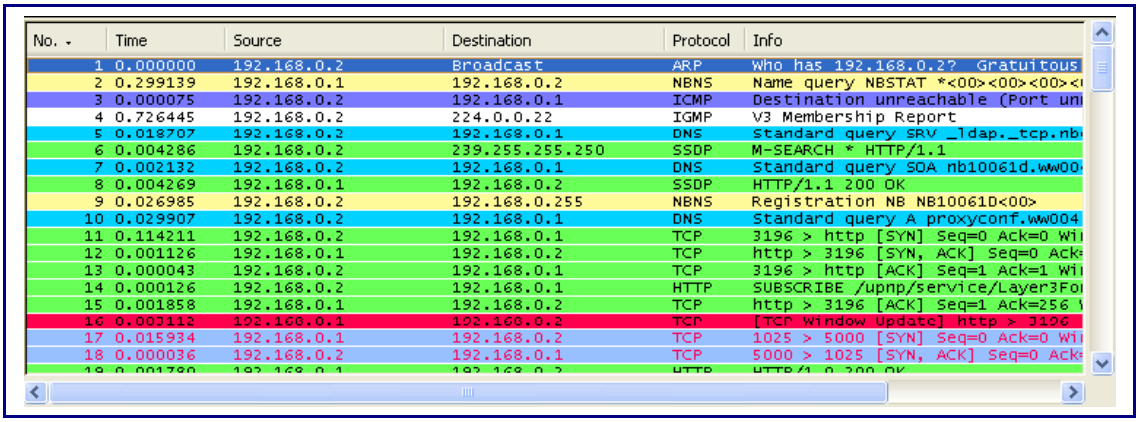

Figura 13. Painel de Lista dos Pacotes.

Cada linha na lista de pacote corresponde a um pacote no arquivo de captura. Se uma linha for selecionada no painel, maiores detalhes serão exibidos no *Painel de Detalhes dos Pacotes* ou no *Painel de Bytes dos Pacotes*. Enquanto opera um pacote, o Wireshark vai colocando informações do operador de protocolos dentro das colunas. Protocolos de níveis mais elevados podem sobrescrever os de níveis mais baixos.

A seguir, as colunas básicas:

- *No.*: o número do pacote no arquivo de captura (não sofre alterações, mesmo usando um filtro).
- *Time*: o tempo do pacote. O formato de apresentação desse tempo pode ser mudado.
- *Source*: o endereço de origem do pacote.
- *Destination*: o endereço de destino do pacote.
- *Protocol*: abreviação do nome do protocolo.
- *Info*: informações adicionais sobre o pacote.

16. PAINEL DE DETALHES DOS PACOTES

O *Painel de Detalhes dos Pacotes* apresenta o pacote atual (selecionado no *Painel de Lista dos Pacotes*) em maiores detalhes, como pode ser observado na Figura 14.

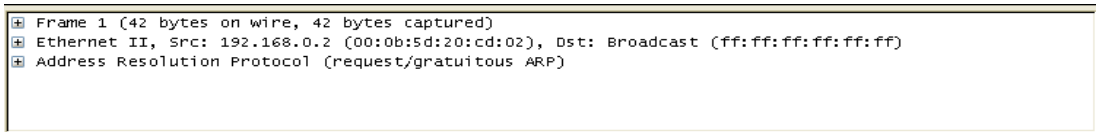

Figura 14. Painel de Detalhes dos Pacotes.

Este painel apresenta os protocolos e os campos dos protocolos do pacote selecionado (serão exibidos através dos itens, que podem ser expandidos ou comprimidos). Alguns campos são especialmente exibidos:

- *Generated fields*: o próprio Wireshark irá gerar campos de protocolo adicional, que serão delimitados por parênteses.
- *Links*: se o Wireshark detectar a relação com outro pacote no arquivo de captura, ele irá gerar um *link* para aquele pacote.

17. PAINEL DE BYTES DOS PACOTES

O *Painel de Bytes dos Pacotes* apresenta os dados do pacote atual (selecionado no *Painel de Lista dos Pacotes*) no formato hexadecimal, como mostra a Figura 15.

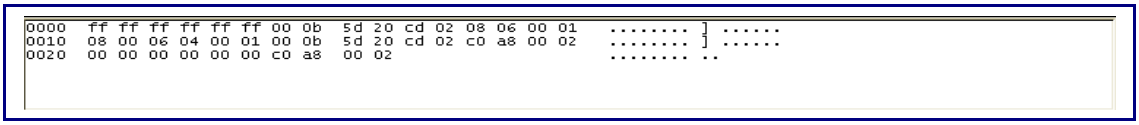

Figura 15. Painel de Bytes dos Pacotes.

Como é usual para um hexadecimal, o lado esquerdo apresenta o equivalente no pacote de dados, o centro mostra uma representação hexadecimal, enquanto o lado direito exibe os caracteres ASCII correspondentes.

Dependendo do pacote de dados, algumas vezes será necessário mais de uma página. Por exemplo, quando o Wireshark tem que reunir alguns pacotes em um pequeno espaço de dados. Isso pode ser observado na Figura 16.

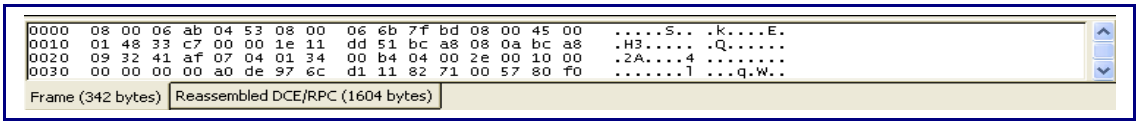

Figura 16. Painel de Bytes dos Pacotes com mais de uma página.

18. BARRA DE *STATUS*

A barra de *status* mostra mensagens informativas. Em geral, o lado esquerdo apresentará informações relacionadas ao contexto, enquanto o lado direito apresentará o número de pacotes atuais. Essa barra é mostrada pela Figura 17.

Figura 17. Barra de *status* sem captura de pacotes.

A barra de *status* ficará desta forma quando não estiver ocorrendo a captura de pacotes. Do contrário, o lado esquerdo apresentará informações acerca da captura de arquivos, seu nome, tamanho e o tempo decorrido enquanto estiver sendo capturado. O lado direito, por sua vez, mostra o número de pacotes que foram capturados. Isto pode ser observado na Figura 18.

Figura 18. Barra de *status* com captura de pacotes.

Os seguintes valores são mostrados no lado direito:

- *P*: o número do pacote capturado.
- *D*: o número de pacotes sendo exibidos atualmente.
- *M*: o número de pacotes marcados.

Se for selecionada uma área de protocolo com o *Painel de Detalhes dos Pacotes*, a barra ficará conforme mostra a Figura 19.

Figura 19. Barra de *status* com um campo de pacote selecionado.

REFERÊNCIAS BIBLIOGRÁFICAS

Wireshark. Disponível em http://www.wireshark.org/docs/wsug_html_chunked/ChapterUsing.html. Acessado em 17 de março de 2008.