Universidade Estadual da Paraíba Departamento de Matemática, Estatística e Computação Disciplina: Redes de Computadores Professor: Edmar José do Nascimento

1º Exercício Prático: Usando o Wireshark (Ethereal)

Introdução

Uma das formas de estudar protocolos de redes de computadores é através de simulações ou vê-los funcionando na prática. Nesta atividade, vamos utilizar um software chamado de *Wireshark* (as versões anteriores eram chamadas de *Ethereal*) [1] para ver os protocolos na prática através da observação dos pacotes trocados entre os hospedeiros quando esses protocolos estão em funcionamento.

Para que possamos observar as mensagens trocadas na execução dos protocolos devemos capturar os pacotes que transportam essas mensagens, e para isso usamos um artifício chamado de farejador de pacotes (*packet sniffer*). Esse tipo de artifício normalmente é implementado em um software que roda em uma máquina e captura todos os pacotes enviados e recebidos por essa máquina, mesmo que não seja destinado a ela. Em seguida, pode-se observar o conteúdo dos pacotes capturados.

É importante observar que um farejador de pacotes tipicamente é passivo, ou seja, normalmente ele não insere qualquer pacote na rede. Além disso, os pacotes capturados não são endereçados ao farejador de pacotes, são uma cópia dos pacotes que são enviados ou recebidos na máquina em que esse software está sendo executado.

A Figura 1 apresenta a estrutura de um aspirador de pacotes, que consiste basicamente de uma biblioteca de captura de pacotes que é responsável por copiar todos os quadros da camada de enlace e de um analisador de pacotes que mostra o conteúdo de todos os campos da mensagem.



Figura 1 - Estrutura de um Farejador de Pacotes

Nós usaremos o aspirador de pacotes *Wireshark* [1]. Estritamente falando o Wireshark é um analisador de pacotes que usa uma biblioteca de captura de pacotes no seu computador.

Executando o Wireshark

Ao executar o *Wireshark* no Windows, a interface gráfica mostrada na Figura 2 é apresentada. Inicialmente nenhum dado é mostrado.



Figura 2 - Tela inicial do Wireshark

Testando o Wireshark

Siga os seguintes passos para testar o funcionamento desse software:

- 1. Inicie seu navegador web preferido e selecione uma página de sua preferência.
- 2. Inicie o *Wireshark*. Você verá uma tela como a que está mostrada na Figura 2, pois o software ainda não começou a capturar os pacotes.
- 3. Para começar a capturar os pacotes, selecione *Options* no menu *Capture*. Será mostrada uma tela como a que está representada na Figura 3, na qual pode-se escolher dentre outras opções qual a interface a ser monitorada. Isso é feito, pois a máquina que você está pode ter mais de uma interface (placa de rede), por exemplo, uma via rede cabeada e outra rede sem fio. Selecione uma das interfaces em seguida clique em *Start*. Isto fará que com que os pacotes que passam por essa interface sejam capturados.

📶 Wireshark: Capture Options 📃 🗖 🔀						
Capture						
Interface: Broadcom 440x 10/100 Integrated Controller (Microsoft's Packet Scheduler) : \Device						
IP address: 192.168.0.14						
Link-layer header ty	be: Ethernet	Buffer size: 1	megabyte(s) Wireless Settings			
Capture packets in promiscuous mode						
Limit each packet to 68 🗘 bytes						
Capture Filter:			•			
Capture File(s)			Display Options			
File: Browse Update list of packets in real time						
Use <u>m</u> ultiple files	Use multiple files					
Next file every	1	🗘 megabyte(s) 🗸	Automatic scrolling in live capture			
Next file every	1	🗘 minute(s) 🗸	✓ Hide capture info dialog			
Ring buffer with 2		🗘 files	Name Resolution			
Stop capture after 1		🗘 file(s)				
Stop Capture			Enable MAC name resolution			
🔲 after 🛛 1		packet(s)	Enable network name resolution			
🔲 after 🛛 1		🗘 megabyte(s) 🗸 🗸				
🗌 after 1		🗘 minute(s) 🗸	Enable transport name resolution			
Help			<u>S</u> tart <u>C</u> ancel			

Figura 3 - Tela de configuração de captura de pacotes

- 4. Ao clicar em *Stop*, a captura é interrompida. Para obter estatísticas sobre os pacotes capturados, clique em *Statistics -> Protocol Hierarchy*.
- 5. Interrompida a captura de pacotes, uma lista dos pacotes capturados é apresentada na tela do Wireshark, assim como está representado na Figura 4.

<pre>Ele Edt Yew Go Capture Analyze Statistics Help Eler: Fler: Fler: Fler</pre>	🔟 (Untitled) - Wireshark						
Image: Solution: Solution	Eile Edit View Go Capture Analyze Statistics Help						
Efter: Expression Glear Apply No Time Source Destination Protocol Info 1 2008-09-30 22:41:34.924320 189.55.37.110 192.168.0.14 TCP 44784 > 2 2008-09-30 22:41:34.924320 189.55.37.110 192.168.0.14 TCP 44784 > 2 2008-09-30 22:41:34.996966 189.71.192.153 TCP netview-i 4 2008-09-30 22:41:35.098939 189.71.192.168.0.14 189.75.37.10 TCP netview-i 5 2008-09-30 22:41:35.039839 189.55.10.47 102.168.0.14 BitTorre Handshak 7 2008-09-30 22:41:35.039839 189.51.0.47 100 Dose-09-30 22:41:35.039839 189.55.10.47 100 Dose-09-30 22:41:35.13748 192.168.0.14 TCP 25199 > 1 10 2008-09-30 22:41:35.13748 192.168.0.14 TCP 25199 > 1 10 2008-09-30 22:41:35.13748 192.168.0.14 TCP 250919 > 1 10 2008-09-30 22:41:35.13748 192.168.0.14 TCP 20919 > 1 12 2008-09-30	$\blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare X \textcircled = [< + + $		🍇 🗹 🕵 % 🕽				
No Time Source Destination Protocol Info 1 2008-09-30 22:41:34.924320 189.55.37.110 192.168.0.14 TCP 44784 > 1 2 2008-09-30 22:41:34.996996 189.71.192.153 TCP netview-i 3 2008-09-30 22:41:34.996996 189.71.192.153 TCP netview-i 4 2008-09-30 22:41:35.029837 192.168.0.14 189.75.37.110 TCP h323gate: 6 2008-09-30 22:41:35.039886 192.168.0.14 189.55.10.47 TCP h323gate: 6 2008-09-30 22:41:35.039886 192.168.0.14 189.55.10.47 TCP rkbacks 8 2008-09-30 22:41:35.039886 192.168.0.14 189.55.10.47 UDP Source pt 9 2008-09-30 22:41:35.131748 192.168.0.14 TCP 25199 > 1 10 2008-09-30 22:41:35.131748 192.1168.0.14 TCP 25199 > 1 12 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 2019 > 1 12 2008-09-30	Elter: Expression Clear Apply						
1 2008-09-30 22:41:34.924320 189.55.37.110 192.168.0.14 TCP 44784 > 1 2 2008-09-30 22:41:34.929696 189.71.192.153 192.168.0.14 TCP 25199 > 1 4 2008-09-30 22:41:34.996996 189.71.192.153 192.168.0.14 TCP 25199 > 1 4 2008-09-30 22:41:35.029857 192.168.0.14 189.71.192.153 TCP netview-: 5 2008-09-30 22:41:35.029857 192.168.0.14 189.55.70.47 TCP hetview-: 6 2008-09-30 22:41:35.039868 192.168.0.14 189.55.10.47 TCP rk32gate: 6 2008-09-30 22:41:35.039868 192.168.0.14 189.55.10.47 UDP Source pt 9 2008-09-30 22:41:35.082023 189.71.192.153 192.168.0.14 TCP 11380 > (10 2008-09-30 22:41:35.133748 199.111.171.199 192.168.0.14 TCP 11380 > (11 2008-09-30 22:41:35.133748 199.111.71.199 192.168.0.14 TCP 2019 > (12 2008-09-30 22:41:35.163378 189.106.147.112 192.168.0.14 TCP 2019 > (12 2008-09-30 22:41:35.163378 189.106.147.112 192.168.0.14 TCP 2019 > (12 2008-09-30 22:41:35.163378 189.106.147.112 192.168.0.14 TCP 2019 > (12 2008-09-30 22:41:35.163378 189.106.147.112 192.1	No Time Source	Destination	Protocol Info	-			
2 2008-09-30 22:41:34.99272 192.168.0.14 189.71.192.153 TCP netview-i 3 2008-09-30 22:41:34.99696 189.71.192.153 129.168.0.14 TCP 25199 > i 4 2008-09-30 22:41:35.02857 192.168.0.14 189.57.37.110 TCP h323gate: 5 2008-09-30 22:41:35.03838 192.168.0.14 189.55.37.110 TCP h323gate: 6 2008-09-30 22:41:35.03886 192.168.0.14 189.55.10.47 TCP rkb-oscs 8 2008-09-30 22:41:35.038086 192.168.0.14 189.55.10.47 TCP rkb-oscs 8 2008-09-30 22:41:35.03808 192.168.0.14 189.55.10.47 TCP rkb-oscs 10 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 25199 > i 10 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 25199 > i 11 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 20919 > i 12 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > i 13 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > i Frame 1 (140 bytes on wire, 140 bytes captured) ⊕ Ethernet II, Src: Netronix_cf:dd:c8 (00:e0:7d:cf:dd:c8), Dst: Dell_98:6a:7d (00:14:22:98:6a:7d) # Transmission Control Protocol, Src Port: 44784 (44784), Dst Port: h323gatestat (1719), Seq: 1, A # Data (86 bytes) 	1 2008-09-30 22:41:34.924320 189.55.37.110	192.168.0.14	TCP 44784 >				
3 2008-09-30 22:41:34.996996 189.71.192.153 192.168.0.14 TCP 25199 > t 4 2008-09-30 22:41:35.029857 192.168.0.14 189.71.192.153 TCP netview-; 5 2008-09-30 22:41:35.029857 192.168.0.14 189.55.37.110 TCP h323gate: 6 2008-09-30 22:41:35.039839 189.55.10.47 192.168.0.14 BitTorre Handshak; 8 2008-09-30 22:41:35.039836 192.168.0.14 189.55.10.47 UDP Source pt 9 2008-09-30 22:41:35.13748 192.1168.0.14 189.55.10.47 UDP Source pt 9 2008-09-30 22:41:35.13748 192.1168.0.14 189.55.10.47 UDP Source pt 9 2008-09-30 22:41:35.13748 192.168.0.14 199.111.171.199 192.168.0.14 TCP 25199 > t 10 2008-09-30 22:41:35.13748 199.111.171.199 192.168.0.14 TCP 20919 > t 12 2008-09-30 22:41:35.13748 199.111.171.199 192.168.0.14 TCP 20919 > t 13 2008-09-30 22:41:35.163788 190.16.147.112 192.168.0.14 TCP 20919 > t 13 2008-09-30 22:41:35.163788 190.6.147.112 192.168.0.14 TCP 20919 > t 2 CP 20919 > t 2 TCP 20919 > t 13 2008-09-30 22:41:35.163788 190.16.147.112 192.168.0.14 TCP 20919 > t 2 TCP 20919 > t 2 TCP 20919 > t 2 TTernet 11, Src: Netronix_cf:dd:c8 (00:e0:7d:cf:dd:c8), Dst: Dell_98:6a:7d (00:14:22:98:6a:7d) # Ethernet II, Src: Netronix_cf:dd:c8 (00:e0:7d:cf:dd:c8), Dst: Dell_98:6a:7d (00:14:22:98:6a:7d) # Transmission Control Protocol, Src Port: 44784 (44784), Dst Port: h323gatestat (1719), Seq: 1, A # Data (86 bytes) C C C C C C C C C C	2 2008-09-30 22:41:34.929272 192.168.0.14	189.71.192.153	TCP netview	(-i			
<pre>4 2008-09-30 22:41:34.997058 192.168.0.14 189.71.192.153 TCP netview-i 5 2008-09-30 22:41:35.029837 192.168.0.14 189.55.37.110 TCP h323gate: 6 2008-09-30 22:41:35.039836 192.168.0.14 189.55.10.47 TCP rkb-oscs 8 2008-09-30 22:41:35.039886 192.168.0.14 189.55.10.47 UDP Source pt 9 2008-09-30 22:41:35.082023 189.71.192.153 192.168.0.14 TCP 25199 > t 10 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 11380 > t 11 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 11380 > t 12 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 20919 > t 10 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 20919 > t 12 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 20919 > t 12 2008-09-30 22:41:35.131748 199.106.147.112 192.168.0.14 TCP 20919 > t 2 008-09-30 22:41:35.131748 199.106.147.112 192.168.0.14 TCP 20919 > t 12 2008-09-30 22:41:35.131748 199.106.147.112 192.168.0.14 TCP 20919 > t 2 008-09-30 22:41:35.131748 199.106.147.112 192.168.0.14 TCP 20919 > t 12 2008-09-30 22:41:35.131748 199.106.147.112 192.168.0.14 TCP 20919 > t 2 008-09-30 22:41:35.131748 199.106.147.112 192.168.0.14 TCP 20919 > t 12 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > t 13 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > t</pre>	3 2008-09-30 22:41:34.996996 189.71.192.153	192.168.0.14	TCP 25199 >	• 1			
<pre>5 2008-09-30 22:41:35.029857 192.168.0.14 189.55.37.110 TCP h323gate: 6 2008-09-30 22:41:35.039886 192.168.0.14 189.55.10.47 TCP rkb-oscs 8 2008-09-30 22:41:35.039886 192.168.0.14 189.55.10.47 UDP Source pt 9 2008-09-30 22:41:35.03203 189.71.192.153 192.168.0.14 TCP 11380 > (10 2008-09-30 22:41:35.131781 192.168.0.14 199.111.171.199 TCP d20g1ser 11 2008-09-30 22:41:35.131781 192.168.0.14 199.111.171.199 TCP d20g1ser 12 2008-09-30 22:41:35.163138 189.106.147.112 192.168.0.14 TCP 20919 > (13 2008-09-30 22:41:35.163138 189.106.147.112 192.168.0.14 TCP 20919 > (14 Transmission Control Protocol, src port: 44784 (44784), Dst port: h323gatestat (1719), Seq: 1, A Data (86 bytes)</pre>	4 2008-09-30 22:41:34.997058 192.168.0.14	189.71.192.153	TCP netview	(— i			
6 2008-09-30 22:41:35.039839 189.55.10.47 192.168.0.14 BitTorre Handshakt 7 2008-09-30 22:41:35.039886 192.168.0.14 189.55.10.47 TCP rkb-oscs 8 2008-09-30 22:41:35.082023 189.71.192.153 192.168.0.14 TCP 25199 > t 10 2008-09-30 22:41:35.131781 199.111.171.199 192.168.0.14 TCP 11380 > t 11 2008-09-30 22:41:35.131781 199.168.0.14 199.111.171.199 TCP dzoglserv 12 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > t 13 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > t 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > t 20000 00 14 22 98 6a 7d 00 e0 7d cf dd c8 08 00 45 00",j},E. 0000 00 14 22 98 6a 7d 00 e0 7d cf dd c8 08 00 45 00",j},Sec. 0010 00 7e 81 72 40 00 73 06 e2 ab bd 37 25 6e c0 a89 .poP. 0020 00 ea ef 0 66 b7 fd 39 f1 70 80 18 ef 4f 50 189 .poP. 0030 fb 20 66 10 000 00 00 00 52 14 01 64 35 36 619 .poP. 0030 fb 20 66 10 000 00 00 00 52 14 01 64 35 36 619 .poP. 0030 fb 20 66 10 000 00 00 00 52 14 01 64 35 36 619 .poP. 0030 fb 20 66 10 000 00 00 00 52 14 01 64 35 36 619 .poP. 0030 fb 20 66 10 000 00 00 00 52 14 01 64 35 36 619 .poP. 0030 fb 20 66 10 000 00 00 00 52 14 01 64 35 26 66 30 dded0:7: added.f0 1050 22 62 25 25 25 25 25 25 20 20 22 29 20 21 26 20 20 20 20 20 20 20 20 20 20 20 20 20	5 2008-09-30 22:41:35.029857 192.168.0.14	189.55.37.110	TCP h323gat	e:			
7 2008-09-30 22:41:35.039886 192.168.0.14 189.55.10.47 TCP rkb-oscs 8 2008-09-30 22:41:35.040085 192.168.0.14 189.55.10.47 UDP Source pt 9 2008-09-30 22:41:35.082023 189.71.192.153 192.168.0.14 TCP 25199 > t 10 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 11380 > (11 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > (13 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > (13 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > (13 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > (14 Transmission Control Protocol, src: 189.55.37.110 (189.55.37.110), Dst: 192.168.0.14 (192.168.0.14) Transmission Control Protocol, src Port: 44784 (44784), Dst Port: h323gatestat (1719), Seq: 1, A Data (86 bytes) 0000 00 014 22 98 6a 7d 00 e0 7d cf dd c8 08 00 45 00", i)E.	6 2008-09-30 22:41:35.039839 189.55.10.47	192.168.0.14	BitTorre Handsha	ik≀			
8 2008-09-30 22:41:35.040085 192.168.0.14 189.55.10.47 UDP Source pt 9 2008-09-30 22:41:35.082023 189.71.192.153 192.168.0.14 TCP 25199 > t 10 2008-09-30 22:41:35.131781 192.168.0.14 192.1168.0.14 TCP 11380 > t 11 2008-09-30 22:41:35.131781 192.168.0.14 199.111.171.199 TCP dzog1ser. 12 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > t 13 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > t 13 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > t 14 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > t 13 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > t 15 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > t 14 3008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > t 15 Ethernet II, Src: Netronix_Cf:dd:c8 (00:e0:7d:cf:dd:c8), Dst: Dell_98:6a:7d (00:14:22:98:6a:7d) Image: State s	7 2008-09-30 22:41:35.039886 192.168.0.14	189.55.10.47	TCP rkb-osc	S			
9 2008-09-30 22:41:35.082023 189.71.192.153 192.168.0.14 TCP 25199 > t 10 2008-09-30 22:41:35.131781 192.168.0.14 TCP 11380 > (11 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > (12 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > (13 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > (Frame 1 (140 bytes on wire, 140 bytes captured)	8 2008-09-30 22:41:35.040085 192.168.0.14	189.55.10.47	UDP Source	pr			
10 2008-09-30 22:41:35.131748 199.111.171.199 192.168.0.14 TCP 11380 > (11 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > (13 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > (13 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > (13 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > (Frame 1 (140 bytes on wire, 140 bytes captured) Ethernet II, Src: Netronix_cf:dd:c8 (00:e0:7d:cf:dd:c8), Dst: Dell_98:6a:7d (00:14:22:98:6a:7d) Internet Protocol, Src: 189.55.37.110 (189.55.37.110), Dst: 192.168.0.14 (192.168.0.14) Transmission Control Protocol, Src Port: 44784 (44784), Dst Port: h323gatestat (1719), Seq: 1, A Data (86 bytes) 0000 00 14 22 98 6a 7d 00 e0 7d cf dd c8 08 00 45 00",j} }E. 0010 00 7e 81 72 40 00 73 06 e2 ab bd 37 25 6e c0 a89.poP. 0020 00 00 ae f0 06 b7 fd 39 f1 70 80 18 ef 4f 50 189.poP. 0030 fb 20 66 10 00 00 00 00 52 14 01 64 35 3a 619.poP. 0030 64 64 65 64 30 3a 37 3a 61 64 64 65 64 22 66 30 dded0:7: added.f0 0040 64 64 65 64 30 3a 37 3a 61 64 64 65 64 22 62 22 22 22 22 22 22 22 22 22 22 22	9 2008-09-30 22:41:35.082023 189.71.192.153	192.168.0.14	TCP 25199 >	1 -			
11 2008-09-30 22:41:35.151781 192.168.0.14 199.111.171.199 TCP d2ogiserv 12 2008-09-30 22:41:35.163058 189.106.147.112 192.168.0.14 TCP 20919 > 13 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > I 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > I 3 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > I 3 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > I 3 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > I 1 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > I 1 2008-09-30 22:41:35.163139 189.106.147.112 192.168.0.14 TCP 20919 > I 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	10 2008-09-30 22:41:35.131/48 199.111.1/1.199	192.168.0.14	TCP 11380 >	• (
12 2008-09-30 22:41:35.163038 189.106.147.112 192.168.0.14 TCP 20919 > (■ ■ ■ ●	11 2008-09-30 22:41:35.131/81 192.168.0.14	199.111.1/1.199	TCP dzogise	en v			
14 2008-09-30 22:41:35.164139 189.106.147.112 192.168.0.14 TCP 20919 5 (***********************************	12 2008-09-30 22:41:35.163058 189.106.147.112	192.168.0.14	TCP 20919 >	-			
Frame 1 (140 bytes on wire, 140 bytes captured) Ethernet II, Src: Netronix_cf:dd:c8 (00:e0:7d:cf:dd:c8), Dst: Dell_98:6a:7d (00:14:22:98:6a:7d) Internet Protocol, Src: 189.55.37.110 (189.55.37.110), Dst: 192.168.0.14 (192.168.0.14) Transmission Control Protocol, Src Port: 44784 (44784), Dst Port: h323gatestat (1719), Seq: 1, A Data (86 bytes) 0000 00 14 22 98 6a 7d 00 e0 7d cf dd c8 08 00 45 00",j}jE. 0010 00 7e 81 72 40 00 73 06 e2 ab bd 37 25 6e c0 a8r@.s7%n 0020 00 0e ae f0 06 b7 fd 39 f1 70 80 18 ef 4f 50 189 ppoP. 0030 fb 20 66 10 00 000 00 00 52 14 01 64 35 3a 619 ppoP. 0030 fb 20 66 10 00 00 00 00 52 24 01 64 25 52 61 64 24 64	1 13 2008-09-30 22:41:35.163139 189.106.147.112	192.168.0.14	TCP 20414 >				
Frame 1 (140 bytes on wire, 140 bytes captured) Ethernet II, Src: Netronix_cf:dd:c8 (00:e0:7d:cf:dd:c8), Dst: Dell_98:6a:7d (00:14:22:98:6a:7d) Internet Protocol, Src: 189.55.37.110 (189.55.37.110), Dst: 192.168.0.14 (192.168.0.14) Transmission Control Protocol, Src Port: 44784 (44784), Dst Port: h323gatestat (1719), Seq: 1, A Data (86 bytes) 0000 00 14 22 98 6a 7d 00 e0 7d cf dd c8 08 00 45 00".j}}E. 0010 00 7e 81 72 40 00 73 06 e2 ab bd 37 25 6e c0 a8	<u>s</u>			>			
Image: Construction of the construction of	 B Frame 1 (140 bytes on wrre, 140 bytes captured) B Ethernet II, Src: Netronix_cf:dd:c8 (00:e0:7d:cf:dd:c8), Dst: Dell_98:6a:7d (00:14:22:98:6a:7d) B Internet Protocol, Src: 189.55.37.110 (189.55.37.110), Dst: 192.168.0.14 (192.168.0.14) B Transmission Control Protocol, Src Port: 44784 (44784), Dst Port: h323gatestat (1719), Seq: 1, A B Data (86 bytes) 						
0030 fb 20 66 10 00 00 00 00 00 52 14 01 64 35 3a 61 . f kd5:a 0040 64 64 65 64 30 3a 37 3a 61 64 64 65 64 2e 66 30 dded0:7: added f0 0050 2a 2a 1 64 64 65 64 2e 20 2a 2a 2a 2a 1 64 64 65 ed 2e 20 61 64 ed 20 2a 2d 2a	0000 00 14 22 98 6a 7d 00 e0 7d cf dd c8 08 00 45 0010 00 7e 81 72 40 00 73 06 e2 ab bd 37 25 6e c0 0020 00 0e ae f0 06 b7 fd 39 f1 70 80 18 ef 4f 50	00".j} }E. a8 .~.r@.s7%n 189.p09.		>			
0040 64 64 65 64 30 3a 37 3a 61 64 64 65 64 26 66 30 dded0:7: added. T0 0050 25 26 25 61 64 65 64 26 20 27 28 25 61 64 64 c65 64 c85 rdd File: "C:\DOCUME~1\EDMARJ~1\CONFIG~11Fc Packets: 362 Displayed: 362 Marked: 0 Dropped: 0 Profile: Default	0030 fb 20 66 10 00 00 00 00 00 52 14 01 64 35 3a	61 . fRd5:a					
File: "C\DOCUME~1\EDMARJ~1\CONFIG~1\Te Packets: 362 Displayed: 362 Marked: 0 Dropped: 0 Profile: Default	UU4U 64 64 65 64 30 3a 37 3a 61 64 64 65 64 2e 66 0050 25 26 25 61 64 64 65 64 26 20 25 28 25 61 64	SU ddedu:/: added.f0		~			
	File: "C:\DOCUME~1\EDMARJ~1\CONFIG~1\Te Packets: 362 Displayed: 362 Ma	rked: 0 Dropped: 0 Profile: Defau	ult	14			

Figura 4 - Pacotes capturados

- 6. Vamos filtrar os pacotes capturados. Para isso, no campo *Filter* digite *http* e selecione *Apply*. Agora temos somente os pacotes trocados em mensagens *http*;
- Selecione a primeira mensagem na lista de mensagens, na janela logo abaixo da lista de pacotes são mostrados os dados relativos ao cabeçalho do pacote selecionado. Cada um dos dados apresentados tem detalhes que podem ser observados clicando em + ao lado do seu nome.
- 8. Na última janela do Wireshark tem-se o conteúdo do pacote em hexadecimal.
- 9. Para terminar, saia do Wireshark.