MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
CAMPUS SÃO JOSÉ – SANTA CATARINA

Administração de Redes
Redes e Sub-redes

Prof. Gustavo M. de Araújo/Juliana C. Inácio

gustavo.araujo@sj.cefetsc.edu.br

Ferramenta de Captura de Pacotes - Wireshark

- **Introdução**
- **Analisador de Pacotes**
- **Utilização de um Sniffer**
- **Histórico**
- **Características do Wireshark**
- **Utilidades**
- **Exemplos**

Introdução

- A ferramenta Wireshark possibilita a captura e a análise de pacotes.
- Esta ferramenta é utilizada por administradores de redes e usuários avançados que desejam monitorar o tráfego de uma rede, analisando e dissecando os pacotes de dados.

Analisador de Pacotes

- Um analisador de pacotes (packet sniffer) é uma aplicação que captura os pacotes que trafegam na rede, permitindo a sua análise.
- Diferentemente de outras aplicações que apenas analisam os pacotes em si destinados, um sniffer pode atuar em modo promíscuo, analisando todo o tráfego que passa no ponto da rede onde está ligado

Analisador de Pacotes

- A aplicação permite identificar problemas na rede, que de outra forma seriam de difícil detecção.
- De forma análoga pode-se pensar em um analisador de pacotes como um dispositivo de medição utilizado para analisar o que está acontecendo dentro de uma rede.

Utilização de um Sniffer

- Um sniffer pode também ser usado para fins menos próprios.
- Protocolos de comunicação que utilizam métodos pouco seguros para envio de informação importante, por exemplo, a validação de senha em um servidor de email POP3 que é enviada sem proteção.
- Um bom administrador de sistemas sabe onde ficam os limites.

Histórico

- Antigo Ethereal
- Ethereal teve sua primeira disponibilização em julho 1998
- Em maio de 2006 surgiu o WireShark

Características do Wireshark

- É um projeto do software livre, e é liberado sob a licença GNU General Public Licence (GPL).
- Pode-se usar livremente Wireshark no número de computadores que forem necessários, sem preocupar-se sobre chaves de licença ou possíveis taxas.
- É muito fácil para as pessoas adicionarem novos protocolos, quer como plugins, ou incorporados no código-fonte.

Características do Wireshark

- É escrita em C++, usando a biblioteca GTK, que também é portável em várias plataformas.
- Os dados geralmente são obtidos através da placa de rede, podendo ser lidos em tempo real das seguintes fontes: Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, Classical IP over ATM e interfaces loopback.

Características do Wireshark

- Os arquivos capturados podem ser editados e convertidos via linha de comando
- 750 protocolos podem ser dissecados
- A saída pode ser salva ou impressa em texto plano ou PostScript
- A exibição dos dados podem ser refinada usando um filtro

Utilidades

- Detecção de problemas na configuração da rede;
- Análise de segurança de redes;
- Desenvolvimento de novos protocolos ou aplicações;
- Interesse na aprendizagem sobre o funcionamento de uma rede.

Instalação

- Além das versões Linux, estão disponíveis também versões para Windows 2000, XP e Vista. Você pode baixá-las no www.wireshark.org

Exemplos

- O endereço MAC do destinatário é incluído no início de cada frame enviado através da rede.
- Os switches e hub-switches são mais discretos, encaminhando o tráfego apenas para o destinatário correto.

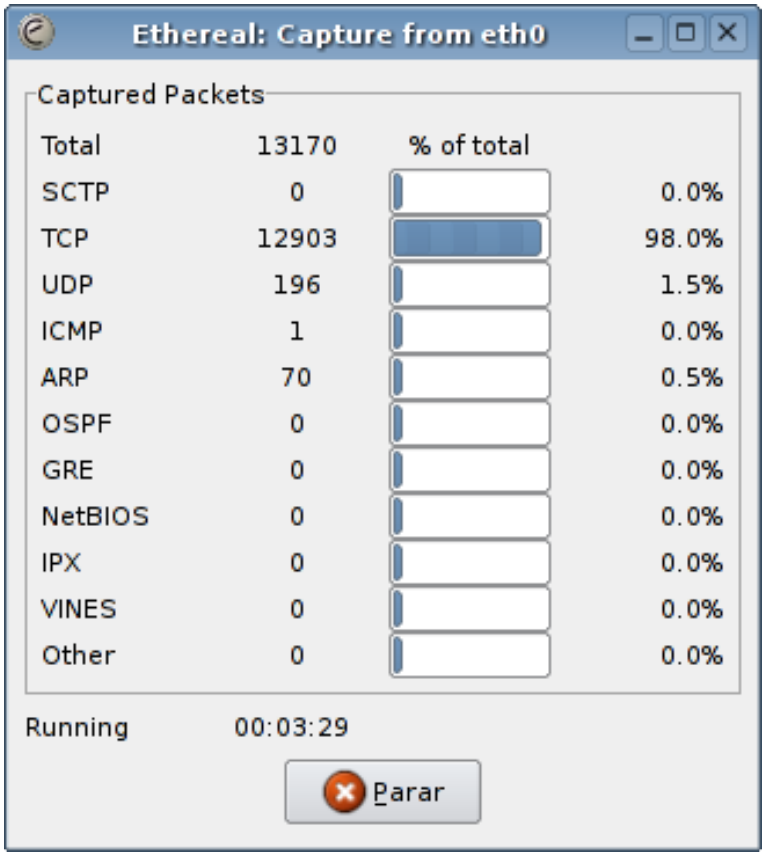
Exemplos

- A opção "Update list of packets in real time". Ativando esta opção, os pacotes vão aparecendo na tela conforme são capturados, em tempo real.
- Caso contrário, você precisa capturar um certo número de pacotes para só depois visualizar todo o bolo.

Exemplos

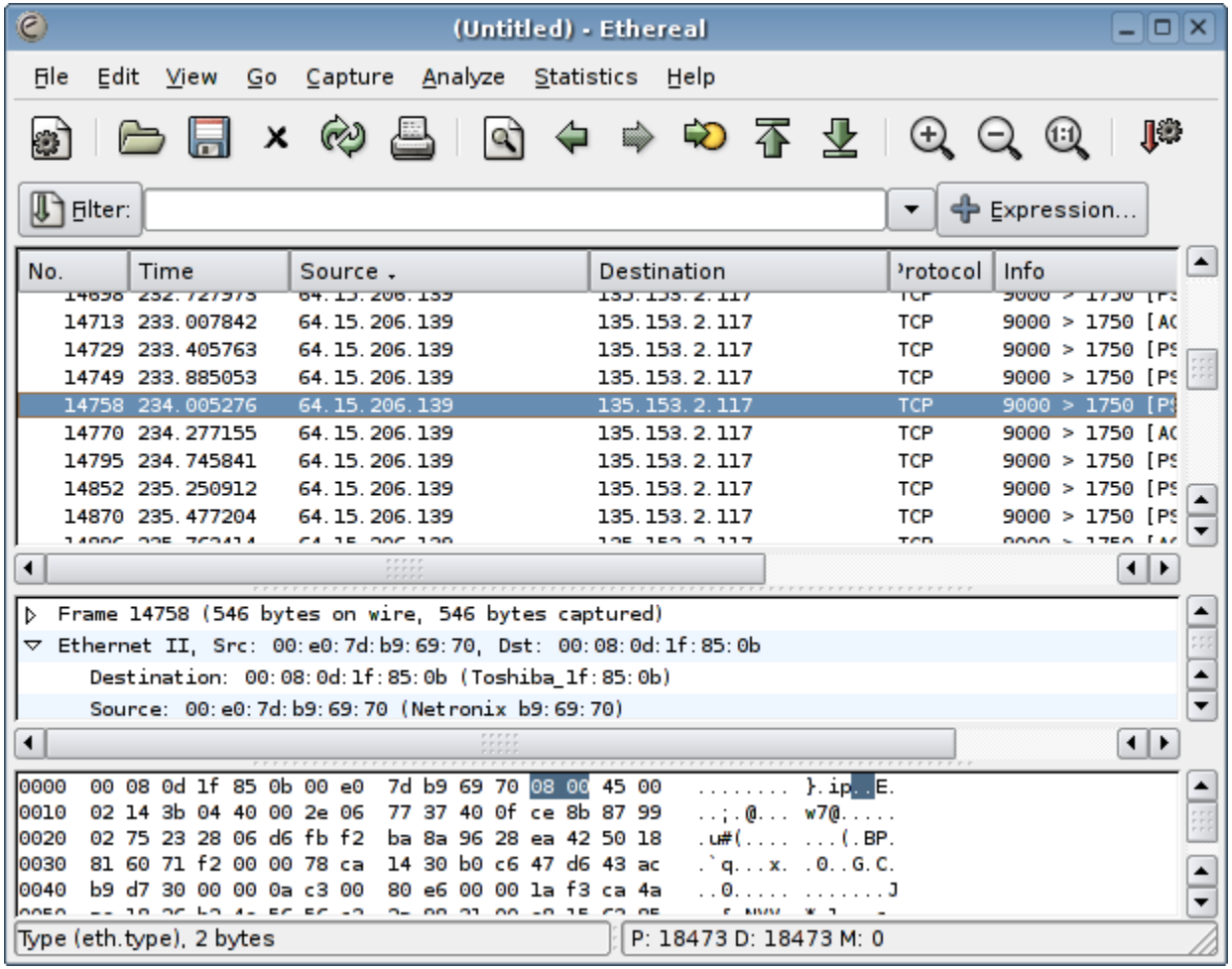
- Também possui algumas opções para interromper a captura depois de um certo tempo, ou depois de capturar uma certa quantidade de dados.

Exemplos



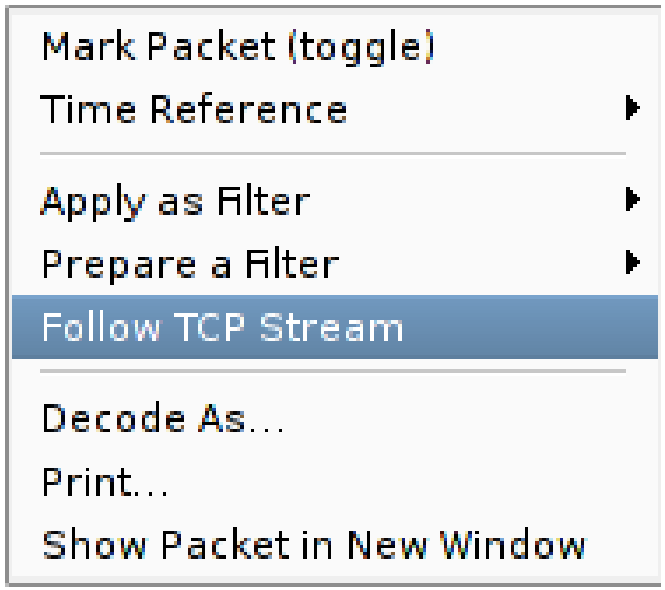
Tela de captura de pacotes, onde você poderá acompanhar o número de pacotes capturados.

Exemplos


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
No. Time Source Destination Protocol Info
14713 233.007842 64.15.206.139 135.153.2.117 TCP 9000 > 1750 [AC
14729 233.405763 64.15.206.139 135.153.2.117 TCP 9000 > 1750 [PS
14749 233.885053 64.15.206.139 135.153.2.117 TCP 9000 > 1750 [PS
14758 234.005276 64.15.206.139 135.153.2.117 TCP 9000 > 1750 [PS
14770 234.277155 64.15.206.139 135.153.2.117 TCP 9000 > 1750 [AC
14795 234.745841 64.15.206.139 135.153.2.117 TCP 9000 > 1750 [PS
14852 235.250912 64.15.206.139 135.153.2.117 TCP 9000 > 1750 [PS
14870 235.477204 64.15.206.139 135.153.2.117 TCP 9000 > 1750 [PS
Frame 14758 (546 bytes on wire, 546 bytes captured)
Ethernet II, Src: 00:e0:7d:b9:69:70, Dst: 00:08:0d:1f:85:0b
Destination: 00:08:0d:1f:85:0b (Toshiba_1f:85:0b)
Source: 00:e0:7d:b9:69:70 (Netronix b9:69:70)
0000 00 08 0d 1f 85 0b 00 e0 7d b9 69 70 08 00 45 00 .... }.ip..E.
0010 02 14 3b 04 40 00 2e 06 77 37 40 0f ce 8b 87 99 ..;.@... w7@.....
0020 02 75 23 28 06 d6 fb f2 ba 8a 96 28 ea 42 50 18 .u#(.... ...(.BP.
0030 81 60 71 f2 00 00 78 ca 14 30 b0 c6 47 d6 43 ac .`q...x. .0..G.C.
0040 b9 d7 30 00 00 0a c3 00 80 e6 00 00 1a f3 ca 4a ..0..... ....J
Type (eth.type), 2 bytes
P: 18473 D: 18473 M: 0

Exemplos

Clicando sobre um dos pacotes e, em seguida, no "Follow TCP Stream", o WireShark mostrará uma janela com toda a conversão, exibida em modo texto.



Exemplos

- A maior parte do que você vai ver serão dados binários, incluindo imagens de páginas web e arquivos diversos.
- Mas, garimpando, você vai encontrar muitas coisas interessantes, como, por exemplo, mensagens (MSN e ICQ) e e-mails, que, por padrão, são transmitidos em texto puro. Usando a opção "Follow TCP Stream", é possível rastrear toda a conversa:

Conclusão

- O Wireshark é um software fabuloso, que pode auxiliar imensamente a resolução de problemas de rede com relativamente pouco esforço.
- Além disso, ele também é uma excelente ferramenta para aprender como funcionam os diversos protocolos de rede.