Wireshark

Roteiro

- Introdução
- Histórico
- Motivação
- Objetivos
- Funcionamento
- Funcionalidades
- Exemplos de uso

Introdução

- Wireshark, popularmente conhecido como tubarão dos fios, tem a função do monitorar os pacotes que trafegam na rede.
- Desenvolvido inicialmente pela Ethereal.
- É uma ferramenta Free.
- Utiliza PCAP para capturar pacotes.

Introdução

- Os dados podem ser capturados da Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, IP clássico sobre ATM e interface loopback
- Os arquivos capturados podem ser editados e convertidos via linha de comando.
- A saída pode ser salva ou impressa em texto plano ou PostScript.
- A exibição dos dados podem ser refinada usando um filtro

Histórico

- Os usuários de Linux costumavam observar suas redes com o popular e livre *Ethereal*.
- Ficou famoso, acabou aparecendo no filme *Firewall,* embora hoje ninguem mais fale nele.
- Em 2006 o autor original mudou de empresa e surgiu o Wireshark

Histórico

- O Wireshark está disponível para todos os sistemas operacionais com base no Unix, assim como para o Windows®.
- Normalmente usa uma interface gráfica, mas também há uma opção em modo texto, chamada *tethereal*

Motivação

- Este analisador de protocolos de rede é uma excelente ferramenta para inspecionar redes, desenvolver protocolos e, de quebra, pode ser usada para fins educacionais.
- Foi escrita por profissionais do ramo e é um exemplo do poder do software de código aberto.

Objetivos

- O objetivo deste tipo de software, também conhecido como sniffer, é detectar problemas de rede, conexões suspeitas, auxiliar no desenvolvimento de aplicativos e qualquer outra atividade relacionada a rede.
- Todo o tráfego de entrada e saída é analisado e mostrado.

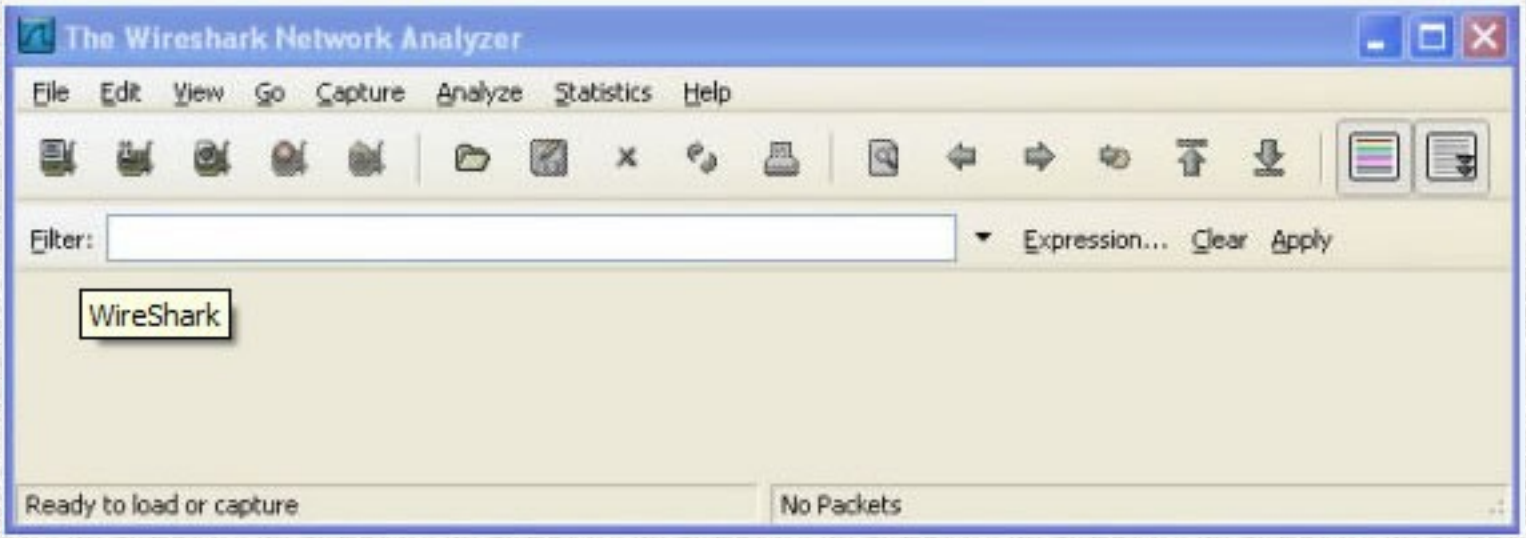
Funcionamento

- O Wireshark funciona capturando todo o tráfego de rede em uma ou mais interfaces de rede.
- Com o Wireshark, você pode capturar facilmente a passagem de tráfego na interface de rede e examinar os detalhes de cada pacote em uma interface gráfica e fácil de usar.

Funcionamento

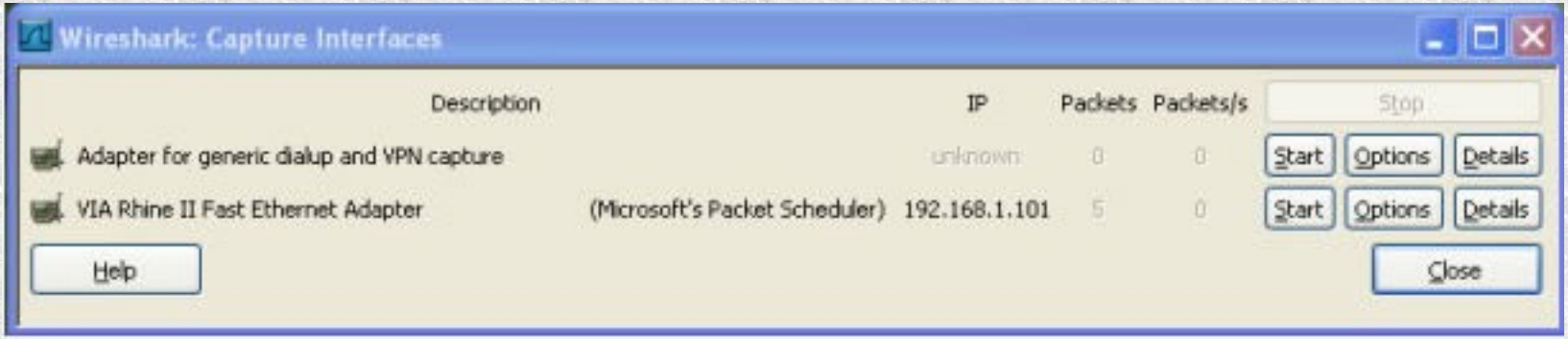
- A interface gráfica do usuário exibe os pacotes capturados em um quadro codificado por cores, que apresenta detalhes sobre a hora, a origem, o destino, o protocolo e uma descrição predeterminada do evento em horário próximo ao real.

Tela de execução do WireShark



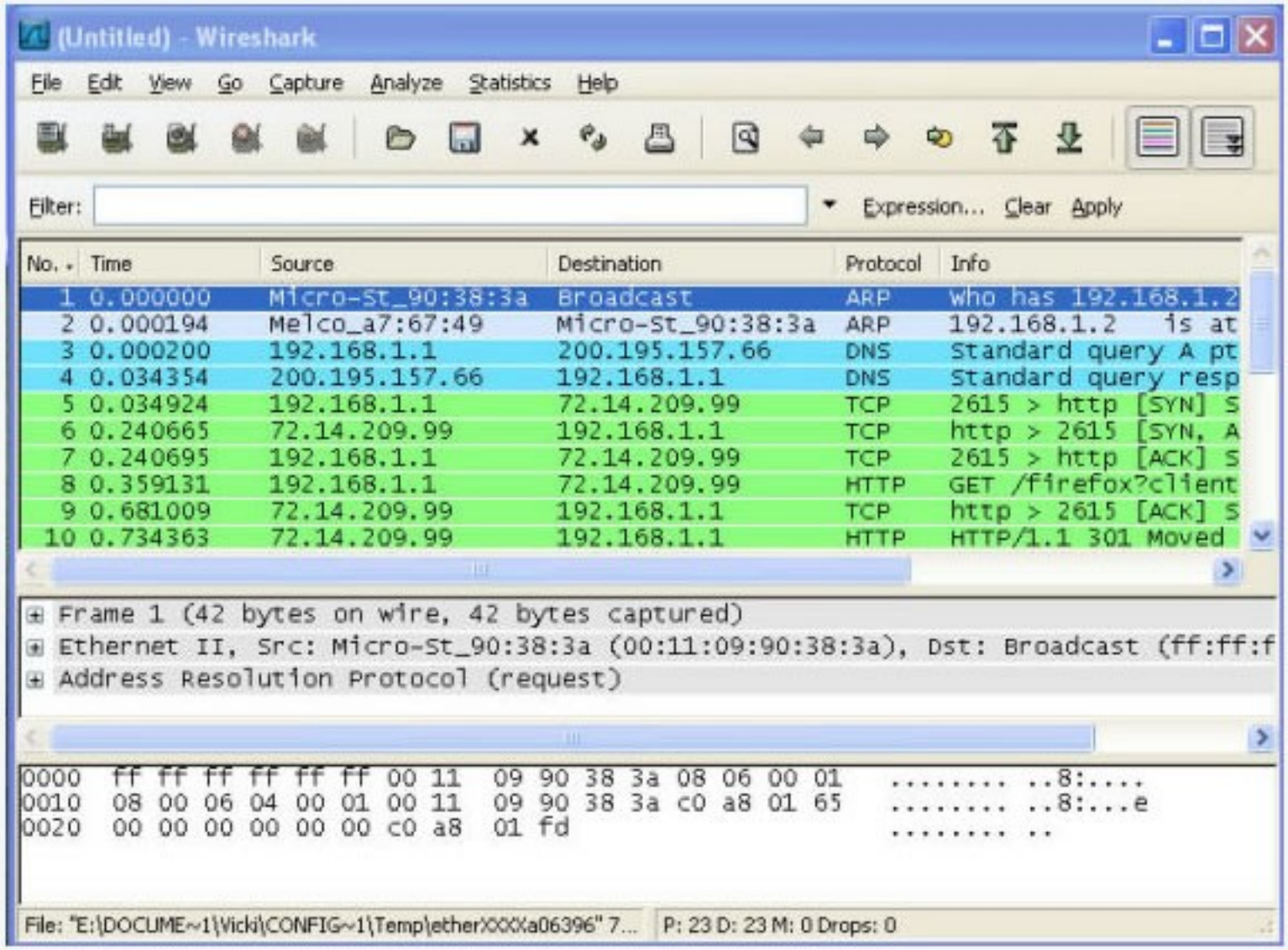
Tela inicial do WireShark

Tela de execução do WireShark



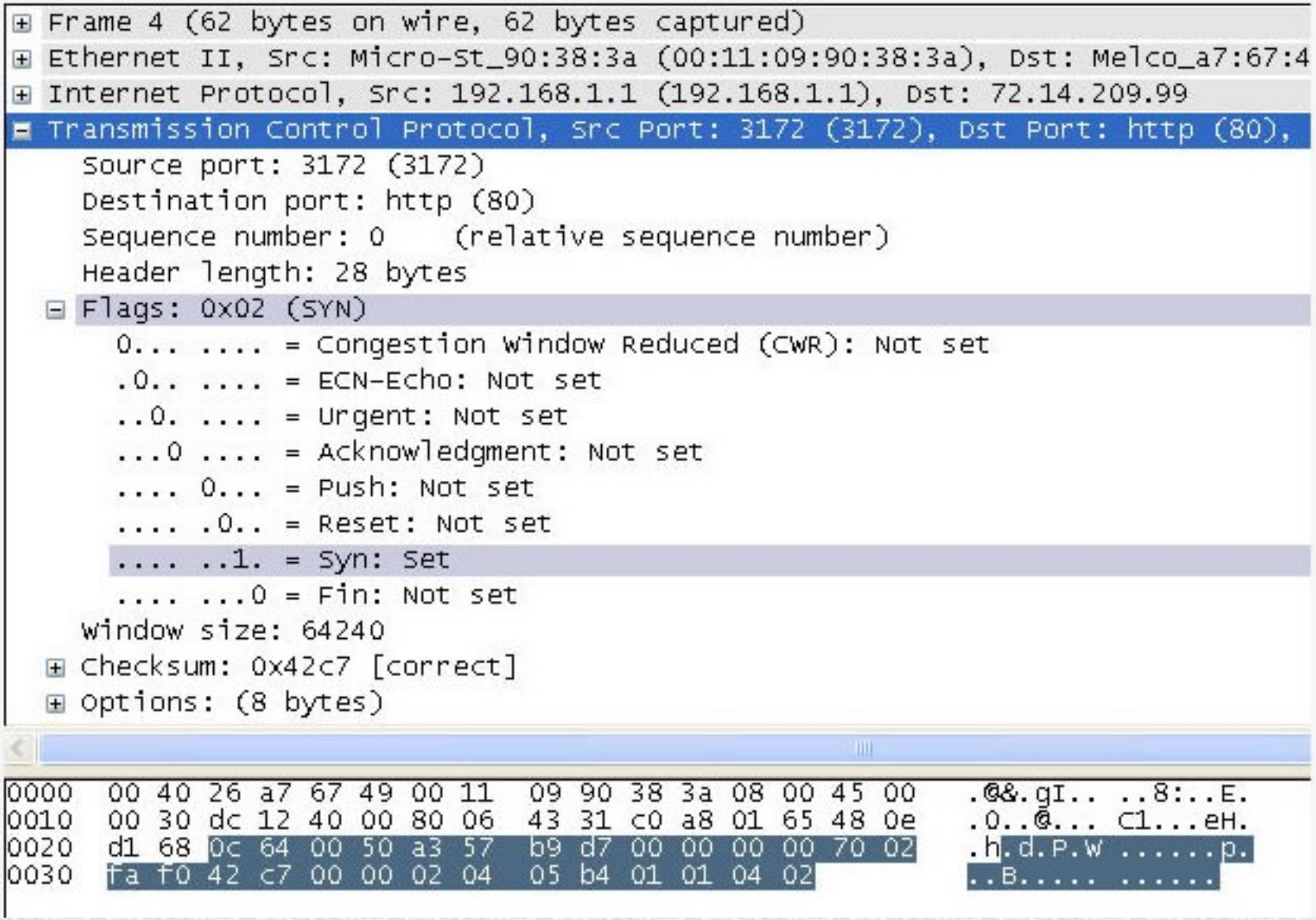
Selecionando interface de rede

Tela de execução do WireShark



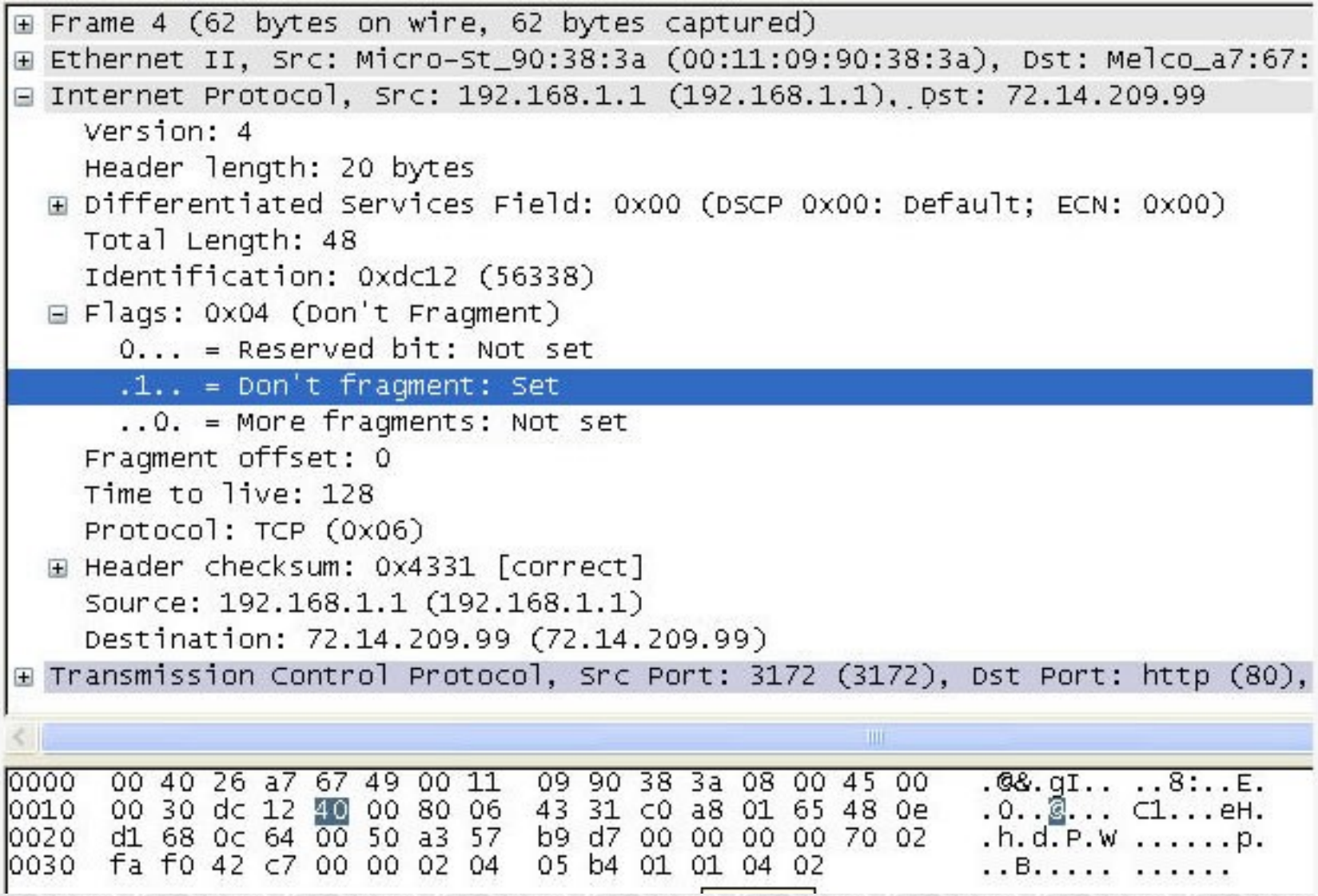
Lista de leituras de pacotes

Tela de execução do WireShark



Conteúdo de um pacote TCP

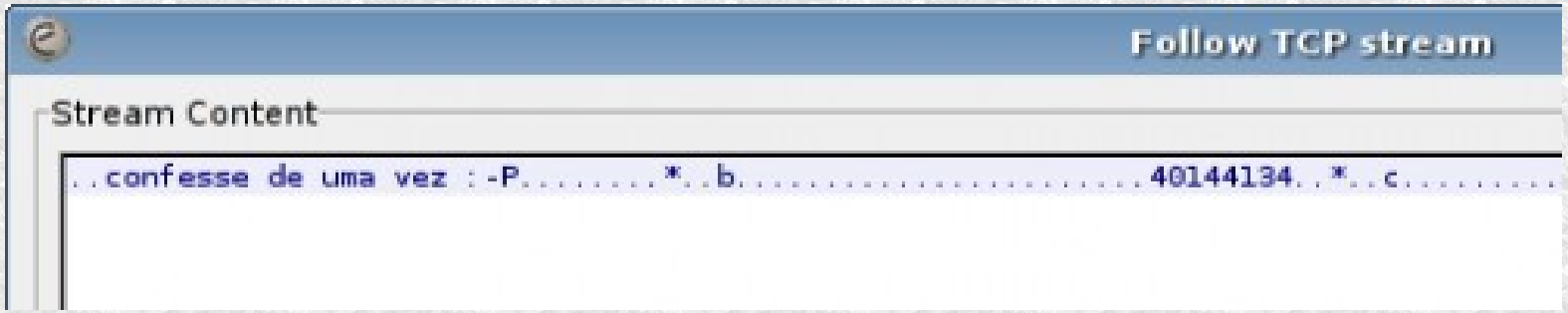
Tela de execução do WireShark



Conteúdo de um pacote IP

A maior parte do que você vai ver serão dados binários, incluindo imagens de páginas web e arquivos diversos.

Mesmo o html das páginas chega muitas vezes de forma compactada (para economizar banda), novamente em um formato ilegível. 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:



Referências

http://pt.scribd.com/doc/51021249/Usos-praticos-do-Wi

http://www.wireshark.org/docs/wsug_html_chunked/