

Wireshark

Roteiro

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

Introdução

- Wireshark, popularmente conhecido como tubarão dos fios, tem a função de 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 ninguém 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.

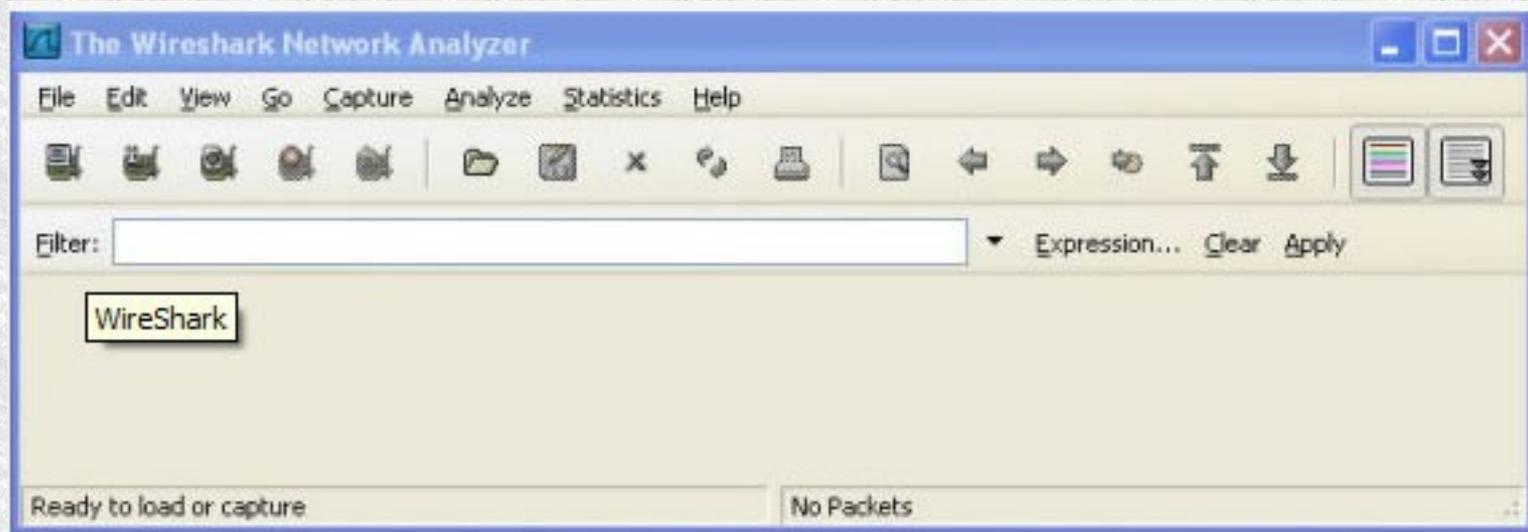
Funcionamento

- 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

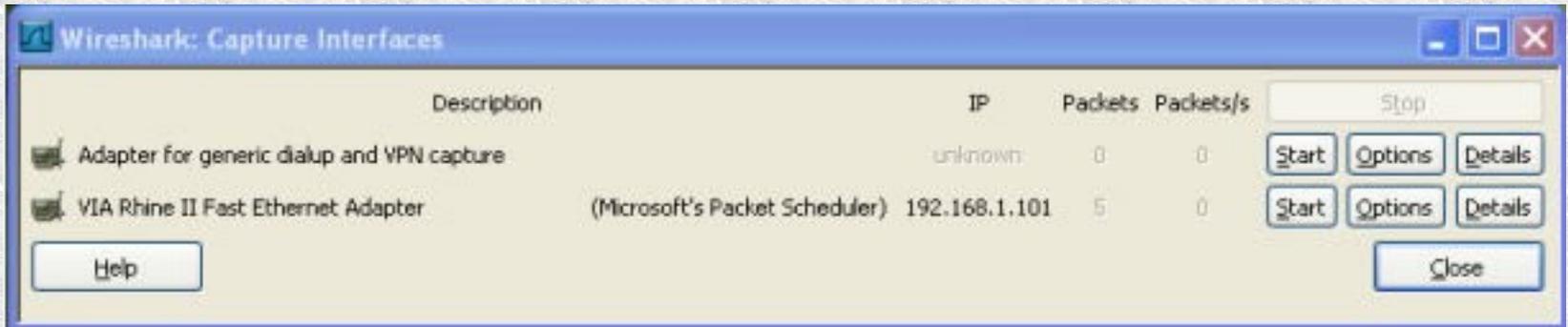
- A interface gráfica do usuário exibe os pacotes capturados em um quadro codificado por cores, que apresenta detalhes sobre a hora, a origem, o destino, o protocolo e uma descrição predeterminada do evento em horário próximo ao real.

Tela de execução do WireShark



Tela inicial do WireShark

Tela de execução do WireShark



Selecionando interface de rede

Tela de execução do Wireshark

The screenshot displays the Wireshark application window titled "(Untitled) - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations and network analysis. A filter field is present with the text "Expression... Clear Apply".

The main window is divided into three panes:

- Packet List:** A table showing 10 captured packets. The columns are No., Time, Source, Destination, Protocol, and Info.
- Packet Details:** A pane showing the structure of the selected packet (Frame 1), including Ethernet II and Address Resolution Protocol (request).
- Packet Bytes:** A pane showing the raw hexadecimal and ASCII data of the selected packet.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Micro-St_90:38:3a	Broadcast	ARP	who has 192.168.1.2
2	0.000194	Me]co_a7:67:49	Micro-St_90:38:3a	ARP	192.168.1.2 is at
3	0.000200	192.168.1.1	200.195.157.66	DNS	Standard query A pt
4	0.034354	200.195.157.66	192.168.1.1	DNS	Standard query resp
5	0.034924	192.168.1.1	72.14.209.99	TCP	2615 > http [SYN] S
6	0.240665	72.14.209.99	192.168.1.1	TCP	http > 2615 [SYN, A
7	0.240695	192.168.1.1	72.14.209.99	TCP	2615 > http [ACK] S
8	0.359131	192.168.1.1	72.14.209.99	HTTP	GET /firefox?client
9	0.681009	72.14.209.99	192.168.1.1	TCP	http > 2615 [ACK] S
10	0.734363	72.14.209.99	192.168.1.1	HTTP	HTTP/1.1 301 Moved

File: "E:\DOCUME~1\Wicki\CONFIG~1\Temp\ether\XXX\06396" 7... P: 23 D: 23 M: 0 Drops: 0

Lista de leituras de pacote\$3

Tela de execução do WireShark

```
⊕ Frame 4 (62 bytes on wire, 62 bytes captured)
⊕ Ethernet II, Src: Micro-st_90:38:3a (00:11:09:90:38:3a), Dst: Me1co_a7:67:4
⊕ Internet Protocol, src: 192.168.1.1 (192.168.1.1), Dst: 72.14.209.99
⊖ Transmission Control Protocol, Src Port: 3172 (3172), Dst Port: http (80),
  Source port: 3172 (3172)
  Destination port: http (80)
  Sequence number: 0 (relative sequence number)
  Header length: 28 bytes
⊖ Flags: 0x02 (SYN)
  0... .... = Congestion window Reduced (CWR): Not set
  .0.. .... = ECN-Echo: Not set
  ..0. .... = Urgent: Not set
  ...0 .... = Acknowledgment: Not set
  .... 0... = Push: Not set
  .... .0.. = Reset: Not set
  .... ..1. = Syn: set
  .... ...0 = Fin: Not set
  window size: 64240
⊕ Checksum: 0x42c7 [correct]
⊕ Options: (8 bytes)
```

```
0000  00 40 26 a7 67 49 00 11 09 90 38 3a 08 00 45 00  .@&.gI.. ..8:...E.
0010  00 30 dc 12 40 00 80 06 43 31 c0 a8 01 65 48 0e  .0..@... C1...eH.
0020  d1 68 0c 64 00 50 a3 57 b9 d7 00 00 00 00 70 02  .h.d.P.W .....p.
0030  fa f0 42 c7 00 00 02 04 05 b4 01 01 04 02     ..B.....
```

Conteúdo de um pacote TCP

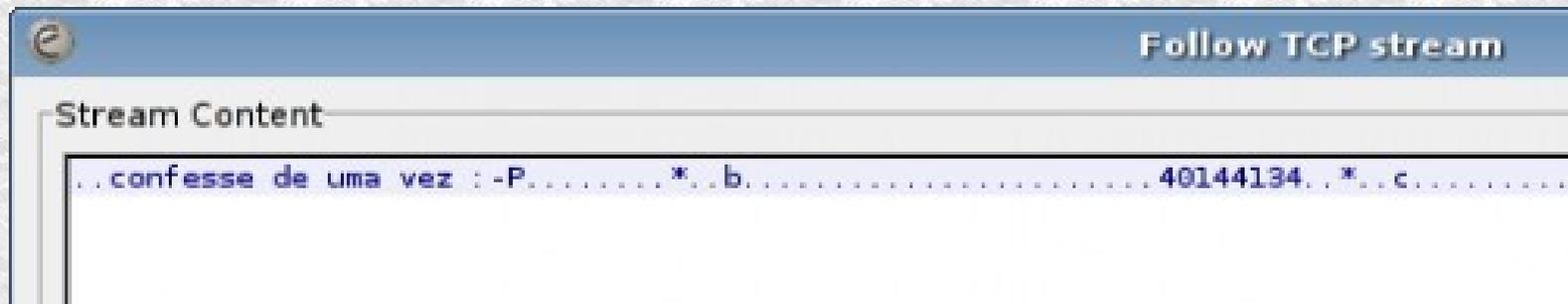
Tela de execução do WireShark

```
⊕ Frame 4 (62 bytes on wire, 62 bytes captured)
⊕ Ethernet II, Src: Micro-st_90:38:3a (00:11:09:90:38:3a), Dst: Melco_a7:67:
⊖ Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 72.14.209.99
  Version: 4
  Header length: 20 bytes
  ⊕ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 48
  Identification: 0xdc12 (56338)
  ⊖ Flags: 0x04 (Don't Fragment)
    0... = Reserved bit: Not set
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (0x06)
  ⊕ Header checksum: 0x4331 [correct]
  Source: 192.168.1.1 (192.168.1.1)
  Destination: 72.14.209.99 (72.14.209.99)
⊕ Transmission Control Protocol, Src Port: 3172 (3172), Dst Port: http (80),
<
0000  00 40 26 a7 67 49 00 11 09 90 38 3a 08 00 45 00  .@&.qI.. ..8:...E.
0010  00 30 dc 12 40 00 80 06 43 31 c0 a8 01 65 48 0e  .0..@... c1...eH.
0020  d1 68 0c 64 00 50 a3 57 b9 d7 00 00 00 00 70 02  .h.d.P.w .....p.
0030  fa f0 42 c7 00 00 02 04 05 b4 01 01 04 02      ..B..... .....
```

Conteúdo de um pacote IP₁₅

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/