Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

Wireshark

O que é?

- Analisador de Protocolos
  - Captura pacotes da rede
    - Apresenta o máximo de detalhes sobre os protocolos utilizados na comunicação em rede
- Mostra “o que está acontecendo dentro de um cabo de rede”
- Serve para rastrear problemas

Histórico

- Ethereal
  - Criado por Gerald Combs em 1997
  - Aprender mais e rastrear problemas de rede
  - Software livre → Colaboradores
- Wireshark
  - Novo nome a partir de 2006
  - 2008: versão 1.0
  - 2015: versão 2.0

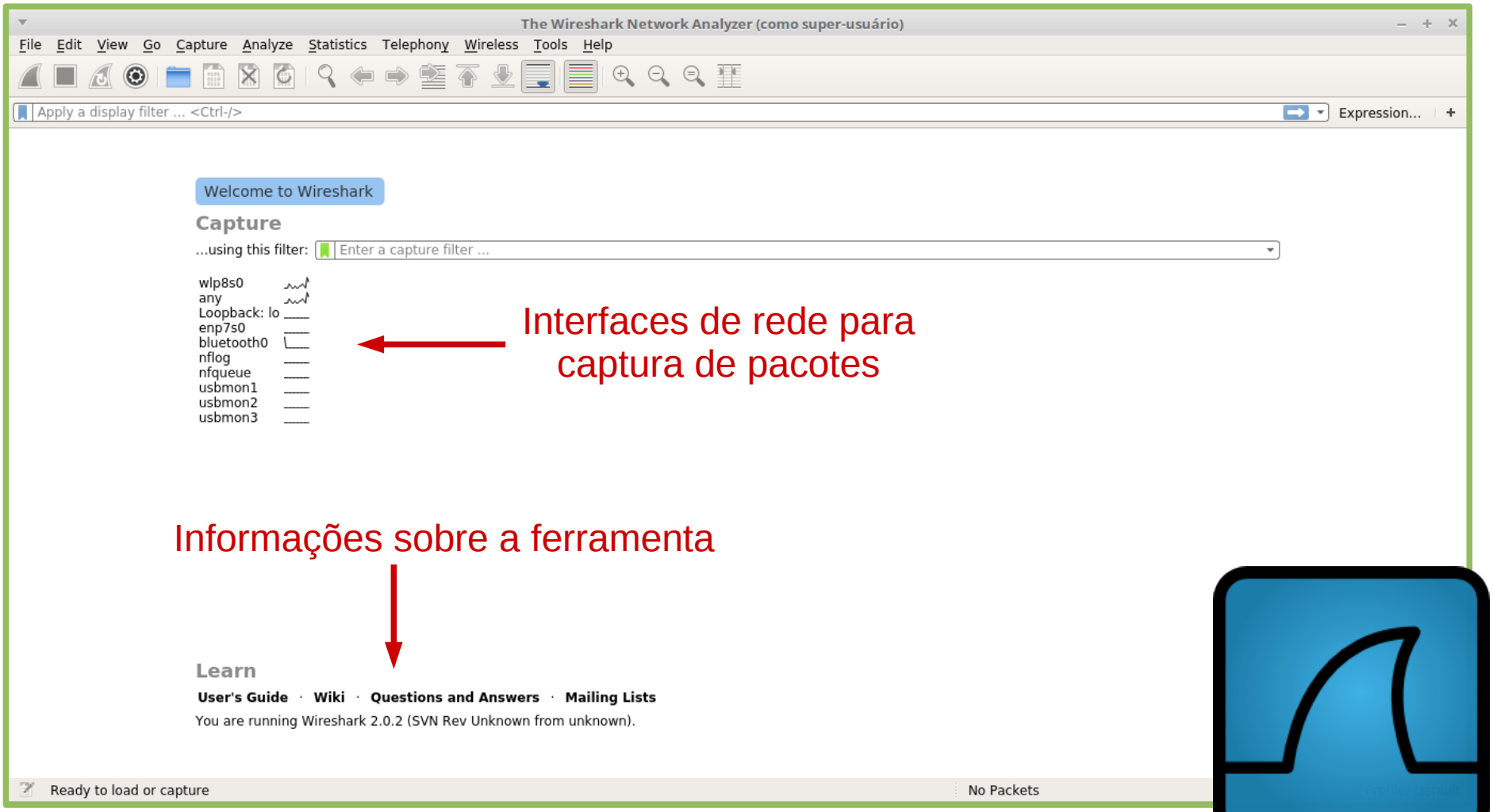
Aplicações

- Administradores usam para resolver problemas na rede
- Profissionais de segurança de redes usam para examinar problemas na segurança da rede
- Desenvolvedores usam para depurar implementações de protocolos
- Pessoas em geral utilizam para aprender mais sobre protocolos de rede

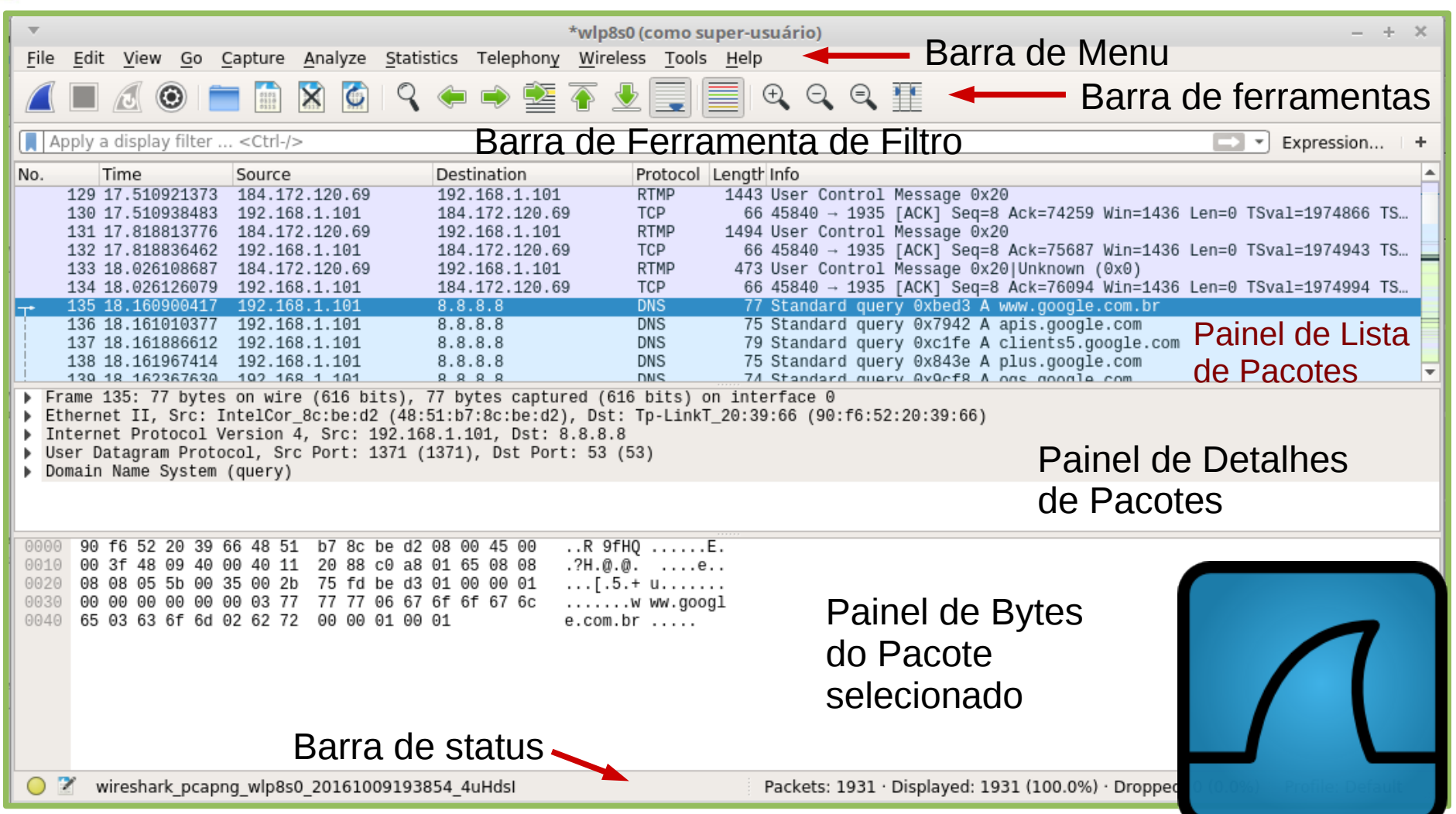
Onde obter?

- Página oficial
  - https://www.wireshark.org/download.html
- Versões para
  - Windows
  - Linux
- Guia do Usuário
  - https://www.wireshark.org/docs/wsug_html_chunked/index.html

Interface


The Wireshark Network Analyzer (como super-usuário)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
wlp8s0
any
Loopback: lo
enp7s0
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
usbmon3
Interfaces de rede para captura de pacotes
Informações sobre a ferramenta
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.0.2 (SVN Rev Unknown from unknown).
Ready to load or capture
No Packets

Interface


Barra de título
*wlp8s0 (como super-usuário)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Barra de Menu
Barra de ferramentas
Apply a display filter ... <Ctrl-/>
Barra de Ferramenta de Filtro
Expression...
No. Time Source Destination Protocol Length Info
129 17.510921373 184.172.120.69 192.168.1.101 RTMP 1443 User Control Message 0x20
130 17.510938483 192.168.1.101 184.172.120.69 TCP 66 45840 → 1935 [ACK] Seq=8 Ack=74259 Win=1436 Len=0 TSval=1974866 TS…
131 17.818813776 184.172.120.69 192.168.1.101 RTMP 1494 User Control Message 0x20
132 17.818836462 192.168.1.101 184.172.120.69 TCP 66 45840 → 1935 [ACK] Seq=8 Ack=75687 Win=1436 Len=0 TSval=1974943 TS…
133 18.026108687 184.172.120.69 192.168.1.101 RTMP 473 User Control Message 0x20|Unknown (0x0)
134 18.026126079 192.168.1.101 184.172.120.69 TCP 66 45840 → 1935 [ACK] Seq=8 Ack=76094 Win=1436 Len=0 TSval=1974994 TS…
135 18.160900417 192.168.1.101 8.8.8.8 DNS 77 Standard query 0xbed3 A www.google.com.br
136 18.161010377 192.168.1.101 8.8.8.8 DNS 75 Standard query 0x7942 A apis.google.com
137 18.161886612 192.168.1.101 8.8.8.8 DNS 79 Standard query 0xc1fe A clients5.google.com
138 18.161967414 192.168.1.101 8.8.8.8 DNS 75 Standard query 0x843e A plus.google.com
Painel de Lista de Pacotes
Frame 135: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
Ethernet II, Src: IntelCor_8c:be:d2 (48:51:b7:8c:be:d2), Dst: Tp-LinkT_20:39:66 (90:f6:52:20:39:66)
Internet Protocol Version 4, Src: 192.168.1.101, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 1371 (1371), Dst Port: 53 (53)
Domain Name System (query)
Painel de Detalhes de Pacotes
0000 90 f6 52 20 39 66 48 51 b7 8c be d2 08 00 45 00 ..R 9fHQ ......E.
0010 00 3f 48 09 40 00 40 11 20 88 c0 a8 01 65 08 08 .?H.@.@. ....e..
0020 08 08 05 5b 00 35 00 2b 75 fd be d3 01 00 00 01 ...[.5.+ u.......
0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c ....w ww.googl
0040 65 03 63 6f 6d 02 62 72 00 00 01 00 01 e.com.br .....
Painel de Bytes do Pacote selecionado
Barra de status
wireshark_pcapng_wlp8s0_20161009193854_4uHdsl
Packets: 1931 · Displayed: 1931 (100.0%) · Dropped

Referências

- Wireshark User's Guide. Disponível em: <https://www.wireshark.org/docs/wsug_html_chunked/index.html>