Usando o Wireshark para diagnosticar problemas com o License Controller

Introdução

O Wireshark é uma ferramenta open source utilizada para diagnosticar o tráfego de redes. Através dele, é possível monitorar todo o conteúdo dos pacotes de rede que trafegam pelo sistema. Neste documento, será mostrado como utilizá-lo para diagnosticar problemas de conexão com o License Controller, serviço usado pelos produtos legado da linha Datasul para efetuar a comunicação com o TOTVS License Server.

Instalação

Importante: a instalação do Wireshark deverá ser feita no servidor onde roda o License Controller!

Windows

Para instalar o Wireshark no Windows, basta baixar e executar o instalador adequado de acordo com a plataforma do sistema (32 ou 64 bits) na página http://www.wireshark.org/download.html. O processo de instalação é bem simples, basta aceitar todas as opções padrão até a conclusão do instalador.

Nota: no Windows, o instalador do Wireshark também executa a instalação da ferramenta WinPcap, que possui um instalador separado que é executado automaticamente pelo instalador do Wireshark.

Linux

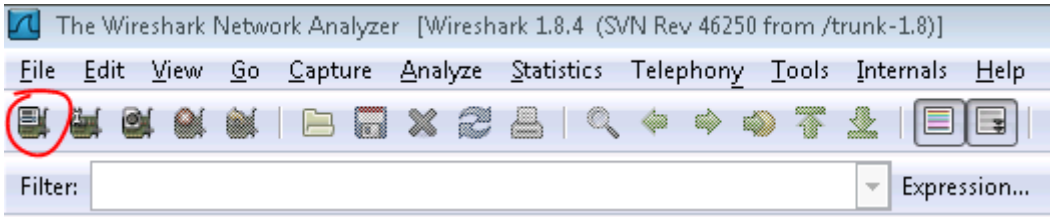
Em distribuições Linux, normalmente o Wireshark já se encontra disponível nos repositórios de pacotes do sistema. Para instalá-lo, basta executar no terminal o comando apropriado para realizar a instalação do pacote:

- Distribuições baseadas em Debian (p. ex. Ubuntu):
  - `sudo apt-get install wireshark`
- Distribuições baseadas no Fedora (p. ex. Red Hat, CentOS):
  - `su -c 'yum install wireshark-gnome'`

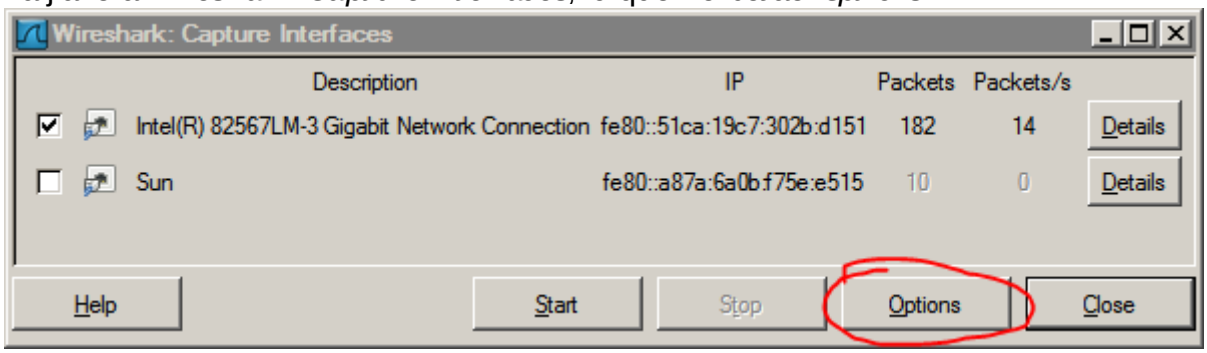
Executando uma captura

Para executar uma *captura* (monitoramento dos pacotes de rede) do tráfego referente ao License Controller, execute os seguintes passos:

1. Inicie o Wireshark
2. Clique no botão *List available capture interfaces...*, localizado na barra de ferramentas:

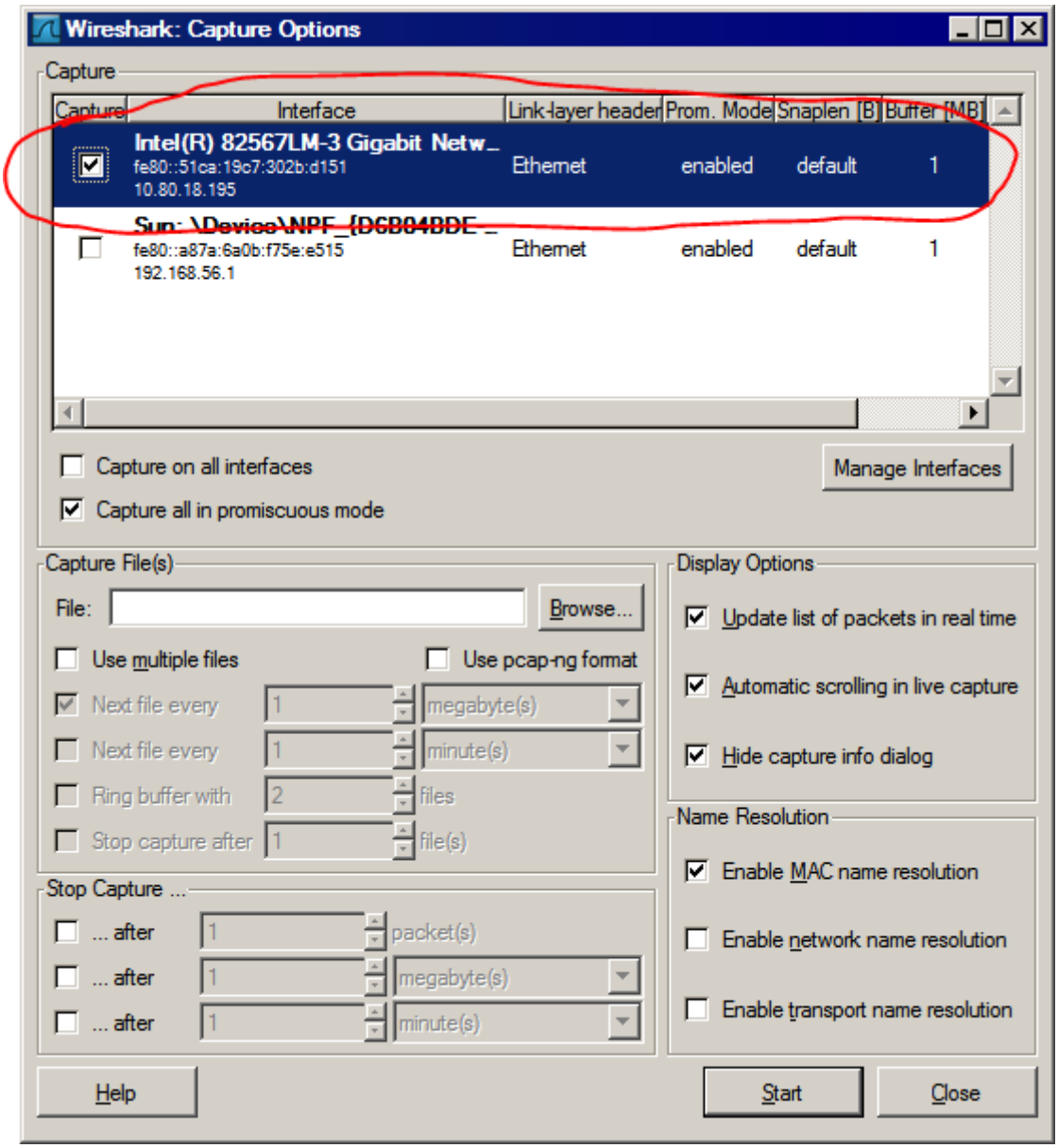


3. Na janela *Wireshark: Capture Interfaces*, clique no botão *Options*:

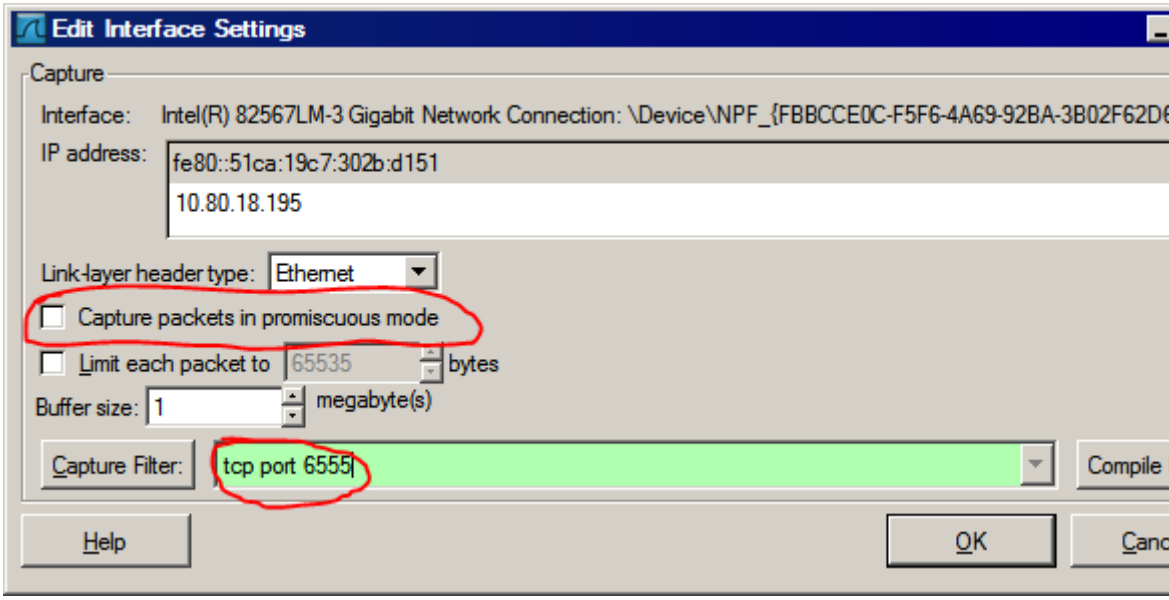


4. Na janela *Wireshark: Capture options*, clique duas vezes na interface de rede usada pelo LC. Se houver mais de uma interface de rede listada, confira através do endereço IP qual é a interface utilizada pelo License

Controller:



5. Na janela *Edit Interface Settings*:
    1. Desmarque a opção *Capture packets in promiscuous mode*
    2. Digite no campo *Capture Filter* o texto `tcp port <porta do lc>`.
       No exemplo abaixo, a porta do LC é 6555:

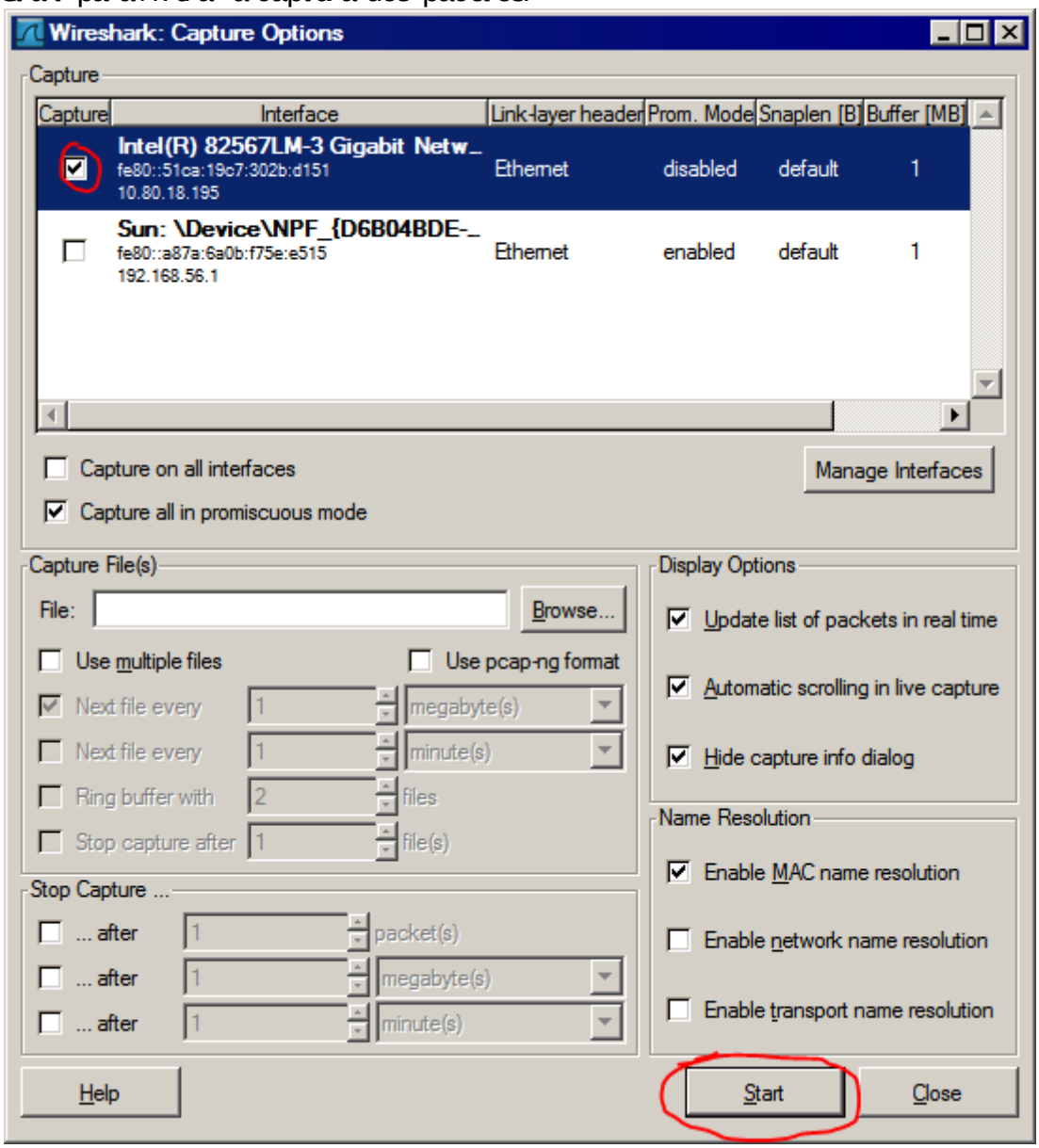


Se o fundo do campo ficar verde, significa que o filtro foi corretamente digitado e reconhecido pelo Wireshark.

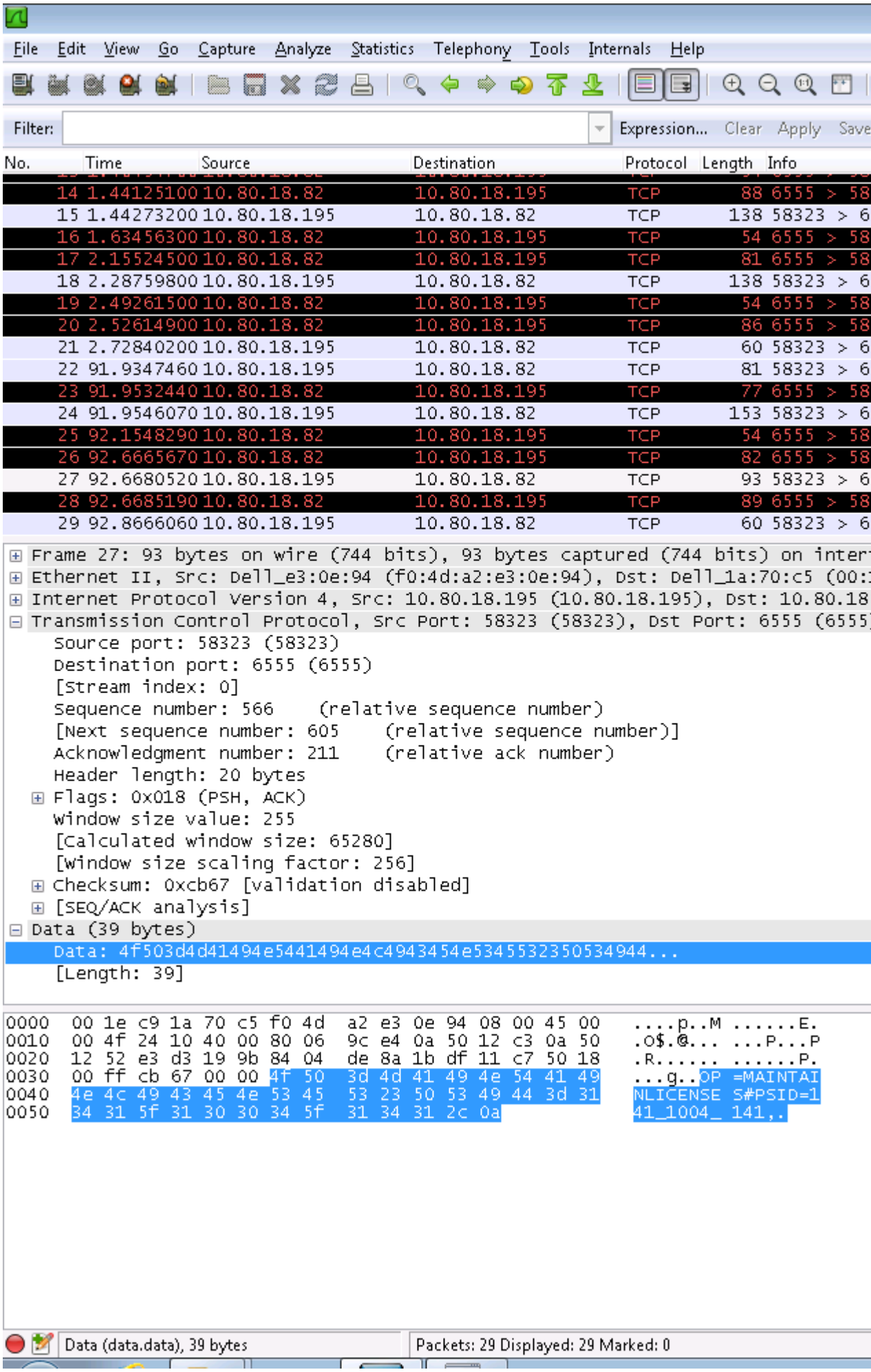
3. Clique no botão *OK* para confirmar

6. De volta à janela *Wireshark: Capture options*, certifique-se que a interface de rede que você acabou de configurar para a captura esteja com o checkbox na coluna *Capture* marcado. Clique então no botão

Start para iniciar a captura dos pacotes:



7. O Wireshark iniciará então a captura dos pacotes filtrada para considerar apenas os pacotes que trafegam na porta configurada:


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
14 1.44125100 10.80.18.82 10.80.18.195 TCP 88 6555 > 58
15 1.44273200 10.80.18.195 10.80.18.82 TCP 138 58323 > 6
16 1.63456300 10.80.18.82 10.80.18.195 TCP 54 6555 > 58
17 2.15524500 10.80.18.82 10.80.18.195 TCP 81 6555 > 58
18 2.28759800 10.80.18.195 10.80.18.82 TCP 138 58323 > 6
19 2.49261500 10.80.18.82 10.80.18.195 TCP 54 6555 > 58
20 2.52614900 10.80.18.82 10.80.18.195 TCP 86 6555 > 58
21 2.72840200 10.80.18.195 10.80.18.82 TCP 60 58323 > 6
22 91.9347460 10.80.18.195 10.80.18.82 TCP 81 58323 > 6
23 91.9532440 10.80.18.82 10.80.18.195 TCP 77 6555 > 58
24 91.9546070 10.80.18.195 10.80.18.82 TCP 153 58323 > 6
25 92.1548290 10.80.18.82 10.80.18.195 TCP 54 6555 > 58
26 92.6665670 10.80.18.82 10.80.18.195 TCP 82 6555 > 58
27 92.6680520 10.80.18.195 10.80.18.82 TCP 93 58323 > 6
28 92.6685190 10.80.18.82 10.80.18.195 TCP 89 6555 > 58
29 92.8666060 10.80.18.195 10.80.18.82 TCP 60 58323 > 6
Frame 27: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on inter
Ethernet II, Src: Dell_e3:0e:94 (f0:4d:a2:e3:0e:94), Dst: Dell_1a:70:c5 (00:
Internet Protocol Version 4, Src: 10.80.18.195 (10.80.18.195), Dst: 10.80.18
Transmission Control Protocol, Src Port: 58323 (58323), Dst Port: 6555 (6555)
Source port: 58323 (58323)
Destination port: 6555 (6555)
[Stream index: 0]
Sequence number: 566 (relative sequence number)
[Next sequence number: 605 (relative sequence number)]
Acknowledgment number: 211 (relative ack number)
Header length: 20 bytes
Flags: 0x018 (PSH, ACK)
Window size value: 255
[Calculated window size: 65280]
[window size scaling factor: 256]
Checksum: 0xcb67 [validation disabled]
[SEQ/ACK analysis]
Data (39 bytes)
Data: 4f503d4d41494e5441494e4c4943454e5345532350534944...
[Length: 39]
0000 00 1e c9 1a 70 c5 f0 4d a2 e3 0e 94 08 00 45 00 ....p..M ......E.
0010 00 4f 24 10 40 00 80 06 9c e4 0a 50 12 c3 0a 50 .O$.@... ...P...P
0020 12 52 e3 d3 19 9b 84 04 de 8a 1b df 11 c7 50 18 .R...... ......P.
0030 00 ff cb 67 00 00 4f 50 3d 4d 41 49 4e 54 41 49 ...g..OP =MAINTAI
0040 4e 4c 49 43 45 4e 53 45 53 23 50 53 49 44 3d 31 NLICENSE S#PSID=1
0050 34 31 5f 31 30 30 34 5f 31 34 31 2c 0a 41_1004_ 141,.
Data (data.data), 39 bytes
Packets: 29 Displayed: 29 Marked: 0

Como interpretar a captura

A janela de captura do Wireshark é dividida em três áreas:

1. A primeira área é uma lista de todos os pacotes capturados
2. A segunda área mostra o conteúdo de cada camada OSI do pacote
3. A terceira área mostra o conteúdo cru do pacote, tanto em bytes apresentados no formato hexadecimal quanto na sua representação em texto ASCII

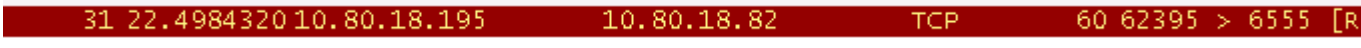
Na lista de pacotes capturados, temos as seguintes colunas:

- *No.*: número sequencial do pacote na captura
- *Time*: tempo decorrido desde o início da captura até a transmissão do pacote
- *Source*: endereço IP da origem do pacote
- *Destination*: endereço IP do destino do pacote
- *Protocol*: protocolo de transmissão. No caso do LC, será sempre TCP
- *Length*: tamanho em bytes do pacote
- *Info*: resumo das informações do pacote

Para identificar se o pacote se refere a um comando enviado do EMS ao LC ou se é um pacote de resposta do LC ao EMS, verifique os campos *Source* e *Destination* e *Info*. Caso o pacote tenha sido recebido pelo LC (um comando enviado pelo ERP, no caso), o campo *Source* conterá o endereço IP da máquina onde o ERP está rodando. Caso seja um pacote de retorno, o campo *Source* conterá o endereço IP do servidor onde roda o LC. No campo *Info*, constam as portas utilizadas na transmissão do pacote, no formato *porta origem > porta destino*. Nesse campo, os pacotes recebidos pelo LC ficam no formato *porta client > porta LC*, e os pacotes retornados pelo LC ao ERP ficam no formato *porta LC > porta client*.

Identificando perdas de conexão

As perdas repentinas de conexão são identificadas através da informação [RST] no campo *Info*. Isso indica que a conexão entre o LC e o ERP foi interrompida anormalmente, através de um reset no pacote TCP. O Wireshark destaca esses pacotes com um fundo vermelho escuro, conforme exemplo abaixo:

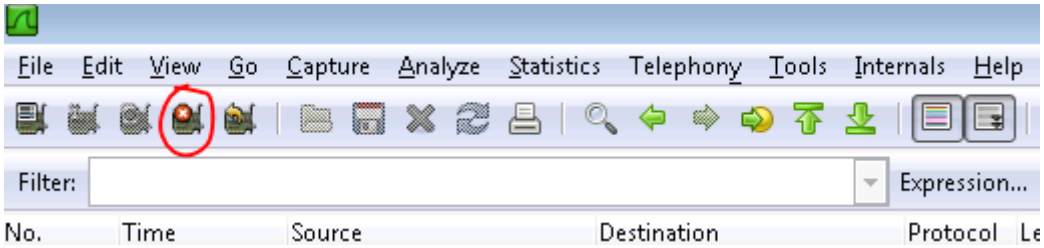


Neste exemplo, a conexão foi interrompida por iniciativa do client, conforme podemos identificar através do campo *Source* e da porta de origem no campo *Info*. Se a desconexão tivesse sido interrompida do lado do servidor do LC, os valores dos campos *Source* e *Destination* estariam invertidos entre si e no campo *Info* a porta do LC apareceria à esquerda do caractere ">".

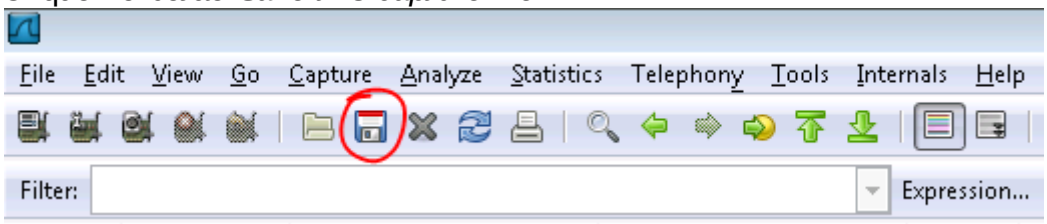
Exportando a captura para um arquivo

É possível exportar a captura realizada para um arquivo que poderá ser lido numa outra sessão do Wireshark. Para fazer isto:

1. Interrompa a captura clicando no botão *Stop the running live capture*:



2. Clique no botão *Save this capture file*:



3. Escolha um nome e um local para o arquivo de captura. O arquivo será gerado com a extensão `.pcapng`:

O arquivo gerado poderá ser aberto em qualquer instalação do Wireshark.