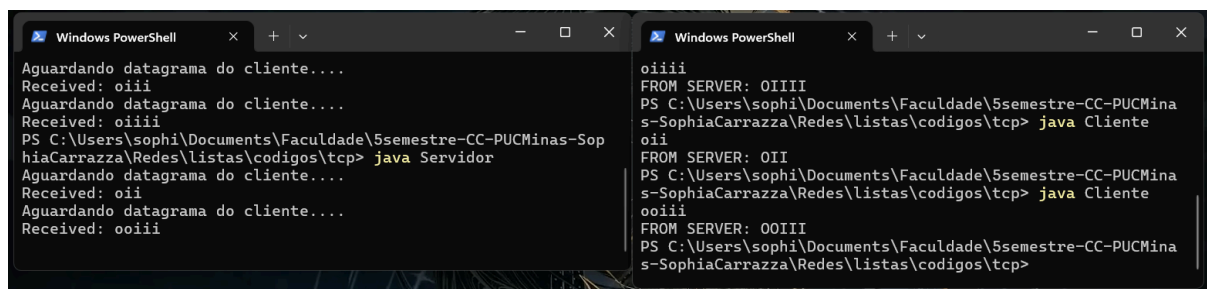
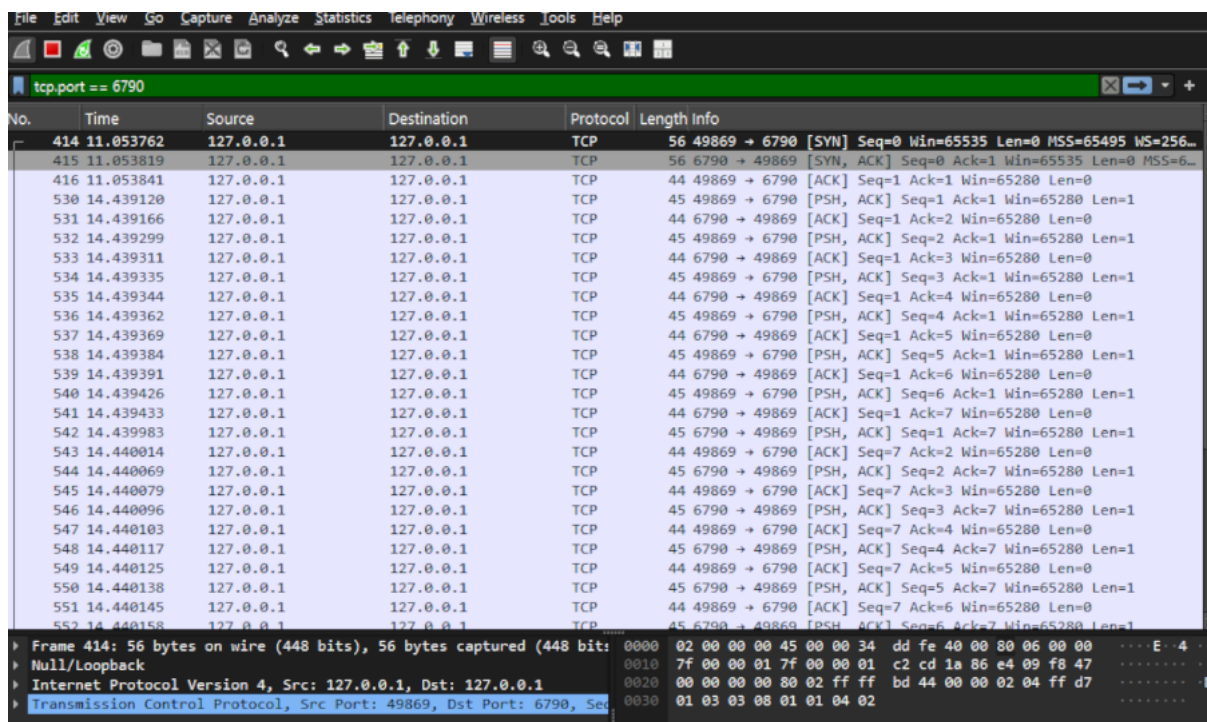


Lista 07 - Identificar os Serviços do TCP com o Wireshark

Sophia Carrazza - CC PUC Minas



```
Windows PowerShell
Aguardando datagrama do cliente....
Received: oiii
Aguardando datagrama do cliente....
Received: oiiii
PS C:\Users\sophi\Documents\Faculdade\5semestre-CC-PUCMinas-SophiaCarrazza\Redes\listas\codigos\tcp> java Cliente
FROM SERVER: OIIII
PS C:\Users\sophi\Documents\Faculdade\5semestre-CC-PUCMinas-SophiaCarrazza\Redes\listas\codigos\tcp> java Cliente
FROM SERVER: OII
PS C:\Users\sophi\Documents\Faculdade\5semestre-CC-PUCMinas-SophiaCarrazza\Redes\listas\codigos\tcp> java Cliente
FROM SERVER: OIIII
PS C:\Users\sophi\Documents\Faculdade\5semestre-CC-PUCMinas-SophiaCarrazza\Redes\listas\codigos\tcp>
```



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-----------|-------------|----------|--------|---|
| 414 | 11.053762 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 49869 → 6790 [SYN, Seq=0 Win=65535 Len=0 MSS=65495 WS=256...] |
| 415 | 11.053819 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 6790 → 49869 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=6... |
| 416 | 11.053841 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 530 | 14.439120 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=1 |
| 531 | 14.439166 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=1 Ack=2 Win=65280 Len=0 |
| 532 | 14.439299 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=2 Ack=1 Win=65280 Len=1 |
| 533 | 14.439311 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=1 Ack=3 Win=65280 Len=0 |
| 534 | 14.439335 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=3 Ack=1 Win=65280 Len=1 |
| 535 | 14.439344 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=1 Ack=4 Win=65280 Len=0 |
| 536 | 14.439362 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=4 Ack=1 Win=65280 Len=1 |
| 537 | 14.439369 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=1 Ack=5 Win=65280 Len=0 |
| 538 | 14.439384 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=5 Ack=1 Win=65280 Len=1 |
| 539 | 14.439391 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=1 Ack=6 Win=65280 Len=0 |
| 540 | 14.439426 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=6 Ack=1 Win=65280 Len=1 |
| 541 | 14.439433 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=1 Ack=7 Win=65280 Len=0 |
| 542 | 14.439983 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=1 Ack=7 Win=65280 Len=1 |
| 543 | 14.440014 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [ACK] Seq=7 Ack=2 Win=65280 Len=0 |
| 544 | 14.440069 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 6790 → 49869 [PSH, ACK] Seq=2 Ack=7 Win=65280 Len=1 |
| 545 | 14.440079 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [ACK] Seq=7 Ack=3 Win=65280 Len=0 |
| 546 | 14.440096 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 6790 → 49869 [PSH, ACK] Seq=3 Ack=7 Win=65280 Len=1 |
| 547 | 14.440103 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [ACK] Seq=7 Ack=4 Win=65280 Len=0 |
| 548 | 14.440117 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 6790 → 49869 [PSH, ACK] Seq=4 Ack=7 Win=65280 Len=1 |
| 549 | 14.440125 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [ACK] Seq=7 Ack=5 Win=65280 Len=0 |
| 550 | 14.440138 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 6790 → 49869 [PSH, ACK] Seq=5 Ack=7 Win=65280 Len=1 |
| 551 | 14.440145 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [ACK] Seq=7 Ack=6 Win=65280 Len=0 |
| 552 | 14.440158 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 6790 → 49869 [PSH, ACK] Seq=6 Ack=7 Win=65280 Len=1 |

Frame 414: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 49869, Dst Port: 6790, Seq: 0, Win: 0, Len: 0

a) Transferência Confiável

O TCP está garantindo que cada pacote enviado seja confirmado por um ACK (Acknowledgement)

- No print, todo pacote é confirmado por um ACK.

| tcp.port == 6790 | | | | | | |
|------------------|-----------|-----------|-------------|----------|--------|--|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 414 | 11.053762 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 49869 → 6790 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256... |
| 415 | 11.053819 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 6790 → 49869 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=6... |
| 416 | 11.053841 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 530 | 14.439120 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=1 |
| 531 | 14.439166 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=1 Ack=2 Win=65280 Len=0 |
| 532 | 14.439299 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=2 Ack=1 Win=65280 Len=1 |
| 533 | 14.439311 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=1 Ack=3 Win=65280 Len=0 |
| 534 | 14.439335 | 127.0.0.1 | 127.0.0.1 | TCP | 45 | 49869 → 6790 [PSH, ACK] Seq=3 Ack=1 Win=65280 Len=1 |
| 535 | 14.439344 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=1 Ack=4 Win=65280 Len=0 |

b) Início de Conexão

Three-way handshake visto no wireshark:

- A conexão é iniciada com uma solicitação do cliente com SYN=1 (deseja sincronizar) e ACK=0 (ainda não teve nenhuma confirmação);
- O servidor responde com SYN=1 e ACK=1 (sincronização + confirmação);
- O cliente envia ACK de volta (confirmação final).

| | | | | | | |
|-----|-----------|-----------|-----------|-----|----|--|
| 414 | 11.053762 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 49869 → 6790 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256... |
| 415 | 11.053819 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 6790 → 49869 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=6... |
| 416 | 11.053841 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |

c) Término de Conexão

Encerramento unidirecional da conexão:

- O cliente envia um pedido de encerramento com FIN=1 e ACK=1, indicando que ele está encerrando a transmissão de dados do lado dele;
- O servidor responde com uma confirmação ACK;
- A flag RST (reset) indica que a conexão foi forçada a ser encerrada.

| | | | | | | |
|------|------------|-----------|-----------|-----|----|---|
| 554 | 14.441937 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [FIN, ACK] Seq=7 Ack=7 Win=65280 Len=0 |
| 555 | 14.441959 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 6790 → 49869 [ACK] Seq=7 Ack=8 Win=65280 Len=0 |
| 4696 | 134.447273 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 49869 → 6790 [RST, ACK] Seq=8 Ack=7 Win=0 Len=0 |

d) Controle de Fluxo

- O campo do window size no cabeçalho do TCP mostra ao emissor a capacidade de recepção do receptor, e o emissor ajusta a taxa de envio de acordo com o tamanho dessa janela;

- Quando o buffer do receptor já está quase cheio, a janela é reduzida (Win=255) para evitar sobrecarga.

| | | | | | |
|-----|-----------|-----------|-----------|-----|---|
| 412 | 10.059312 | 127.0.0.1 | 127.0.0.1 | TCP | 44 49868 → 5354 [ACK] Seq=54 Ack=5 Win=65280 Len=0 |
| 414 | 11.053762 | 127.0.0.1 | 127.0.0.1 | TCP | 56 49869 → 6790 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256... |
| 415 | 11.053819 | 127.0.0.1 | 127.0.0.1 | TCP | 56 6790 → 49869 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=6... |
| 416 | 11.053841 | 127.0.0.1 | 127.0.0.1 | TCP | 44 49869 → 6790 [ACK] Seq=1 Ack=1 Win=65280 Len=0 |
| 417 | 11.174164 | 127.0.0.1 | 127.0.0.1 | TCP | 45 49768 → 49767 [PSH, ACK] Seq=62 Ack=1 Win=255 Len=1 |
| 418 | 11.174231 | 127.0.0.1 | 127.0.0.1 | TCP | 44 49767 → 49768 [ACK] Seq=1 Ack=63 Win=835 Len=0 |
| 419 | 11.174962 | 127.0.0.1 | 127.0.0.1 | TCP | 45 49764 → 49765 [PSH, ACK] Seq=62 Ack=1 Win=255 Len=1 |