# Trabalho Final Seg Info

Diego V. S. de Matos – 120098723

November 27, 2025

## 1 Comparação de Implementações

Foi implementado em Python dois programas cliente e servidor para cada caso: com TLS e sem TLS. As rotinas para cada caso são parecidas e suas diferenças principais são:

1) Inicialização dos programas: No caso com TLS o servidor deve carregar os certificado criar seu socket normalmente

Listing 1: Inicializacao Servidor

```
# Rotina abaixo apenas para o caso com TLS
context = ssl.SSLContext(ssl.PROTOCOL_TLS_SERVER)
context.load_cert_chain(certfile="cert.pem", keyfile="key.pem")

# Rotina abaixo em comum para ambos os casos
server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server.bind((HOST, PORT))
server.listen(1)
```

2) Envólucro na conexão: Na conexão com TLS é feita a encriptação/decriptação automática no conteúdo da mensagem tanto no cliente como no servidor. Passo não necessário no caso sem TLS.

Listing 2: Conexão servidor

```
conn, addr = server.accept()
# Conexao segura TLS
secure_conn = context.wrap_socket(conn, server_side=True)
```

Listing 3: Conexão cliente

```
# Apenas para o caso TLS
context = ssl.create_default_context()
context.check_hostname = False
context.verify_mode = ssl.CERT_NONE  # aceitar certificado autoassinado

# O caso sem TLS chama apenas a funcao abaixo
raw_sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

```
# Envolucro na conexao socket do cliente
secure_sock = context.wrap_socket(raw_sock, server_hostname=HOST)
```

## 2 Captura dos Pacotes

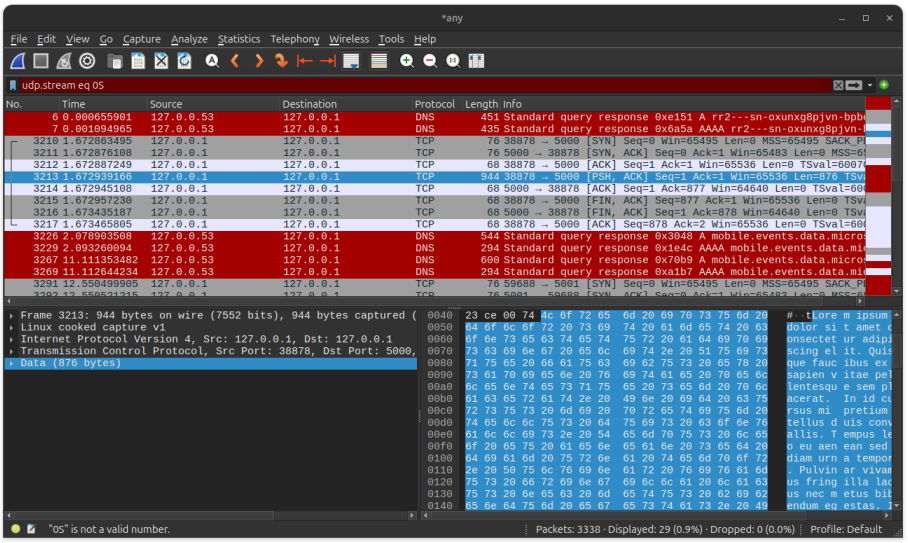


Figure 1: Pacotes enviados sem tls

Na figura 1 é possível compararmos o fluxo de pacotes para cada implementação. No caso sem TLS observamos uma sequência de pacotes padrão do protocolo TCP (SYN, ACK) entre o cliente (porta 38898) e o servidor (porta 5000) além de conseguirmos ler o conteúdo da mensagem como destacado na imagem.

Já para o caso com TLS observamos na figura 2 os pacotes o TLS e não conseguimos ler o conteúdo da mensagem.

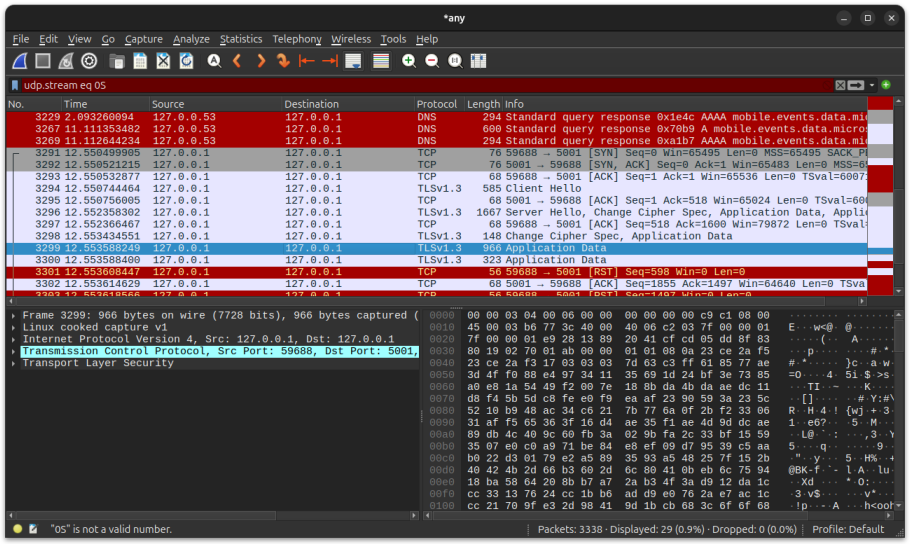


Figure 2: Pacotes enviados com tls