

Forum:[Hack Forums](#)

Thread: [OpenSSL - Performing handshake on insecure bio](#)

Byte™ - August 6, 2017, 12:08 am

So I know how to create a bio and connect/perform a handshake right away using this plain method:
(Simplified with no error checking)

```
Quote: SSL_CTX ctx = SSL_CTX_new(TLSv1_2_client_method());
SSL ssl;
```

```
BIO *bio = BIO_new_ssl_connect("ctx");
BIO_get_ssl(bio, &ssl);
SSL_set_mode(ssl, SSL_MODE_AUTO_RETRY);
```

```
BIO_set_conn_hostname(bio, "smtp.gmail.com:465");
BIO_do_connect(bio);
```

But is there a way to create a connect with `BIO_new_connect()` and then perform a handshake later with the same bio that `BIO_new_connect()` made?

The reason I ask is because am creating a small email library for my self and the TLS SMTP server from gmail requires you to connect insecurely first, then send the STARTTLS command then perform the handshake. Problem is I don't know how to perform a handshake on non-insecure bio. I've been searching but it seems like the OpenSSL documentation is truly scattered and the information that is there is vague or not related to what I am looking for.

Goodies - August 7, 2017, 1:44 pm

Run an ltrace on the openssl utility connecting to your desired mail server. I chose live.com.

```
Code ltrace -o openssl openssl s_client -connect smtp.live.com:25 -starttls smtp
```

Kinda large ([Click to View](#))

Just a starting point since I have little openssl experience.

owonbo - August 8, 2017, 12:35 am

What are the programme detail.

I will like to practice it in class please.

im a student of computer programming year 1 in university of ireland