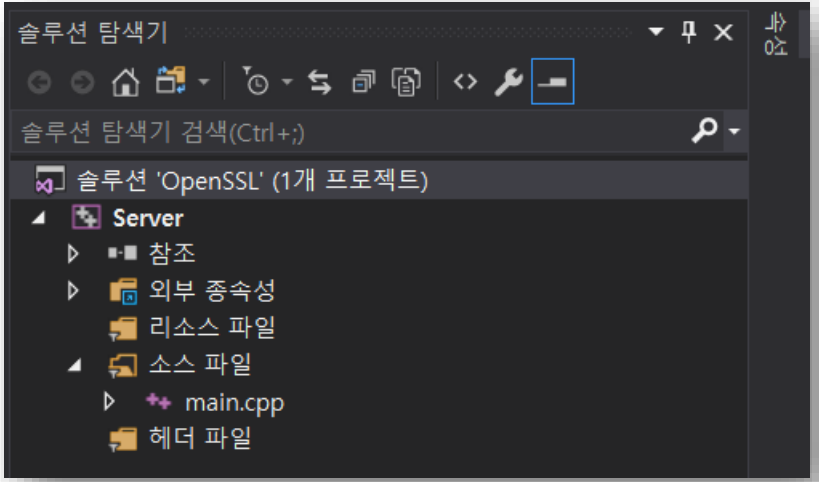
Fast campus

컴퓨터공학 All in One

C/C++ 문법, 자료구조 및 심화 프로젝트 (나동빈)
제 73강 - OpenSSL TCP 통신 예제

OpenSSL 설치하기

Server 프로젝트 구성하기



OpenSSL 설치하기

서버 프로그램 ①

```
#include <iostream>
#include <winsock.h>
#include <openssl/ssl.h>
#include <openssl/err.h>

using namespace std;

void init()
{
  WSADATA wsaData;
  WSAStartup(MAKEWORD(2, 2), &wsaData);
  SSL_load_error_strings();
  SSL_library_init();
  OpenSSL_add_all_algorithms();
}

void close()
{
  ERR_free_strings();
  EVP_cleanup();
  WSACleanup();
}
```

OpenSSL 설치하기

서버 프로그램 ②

```
int main()
{
  init();

  int sockfd = socket(AF_INET, SOCK_STREAM, 0);
  struct sockaddr_in serverAddress;
  int addressLength = sizeof(serverAddress);

  memset((char *)&serverAddress, 0, sizeof(serverAddress));
  serverAddress.sin_family = AF_INET;
  serverAddress.sin_addr.s_addr = htonl(INADDR_ANY);
  serverAddress.sin_port = htons(9876);

  bind(sockfd, (struct sockaddr *) &serverAddress, addressLength);

  listen(sockfd, 10);

  /* SSL 객체 초기화 */
  SSL_CTX *sslContext = SSL_CTX_new(SSLv23_server_method());
  SSL_CTX_set_options(sslContext, SSL_OP_SINGLE_DH_USE);

  /* 공개키와 개인키 초기화 */
  SSL_CTX_use_certificate_file(sslContext, "./cert.pem", SSL_FILETYPE_PEM);
  SSL_CTX_use_PrivateKey_file(sslContext, "./key.pem", SSL_FILETYPE_PEM);
```

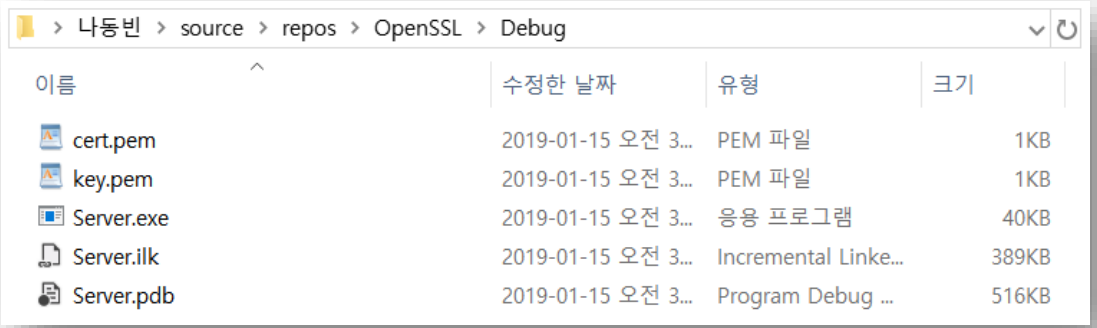
OpenSSL 설치하기

서버 프로그램 ③

```
  while (true)
  {
    int fd = accept(sockfd, (struct sockaddr *) &serverAddress, &addressLength);

    /* SSL 통신 처리 */
    SSL *ssl = SSL_new(sslContext);
    SSL_set_fd(ssl, fd);
    SSL_accept(ssl);

    /* SSL 입력 */
    char input[4096] = { 0 };
    SSL_read(ssl, (char *)input, 4096);

    /* SSL 출력 */
    char output[4096] = { 0 };
    int length = wsprintfA(output, "[Echo]: %s\n", input);
    SSL_write(ssl, output, length);

    SSL_free(ssl);
    closesocket(fd);
  }
  SSL_CTX_free(sslContext);

  close();
  return 0;
}
```

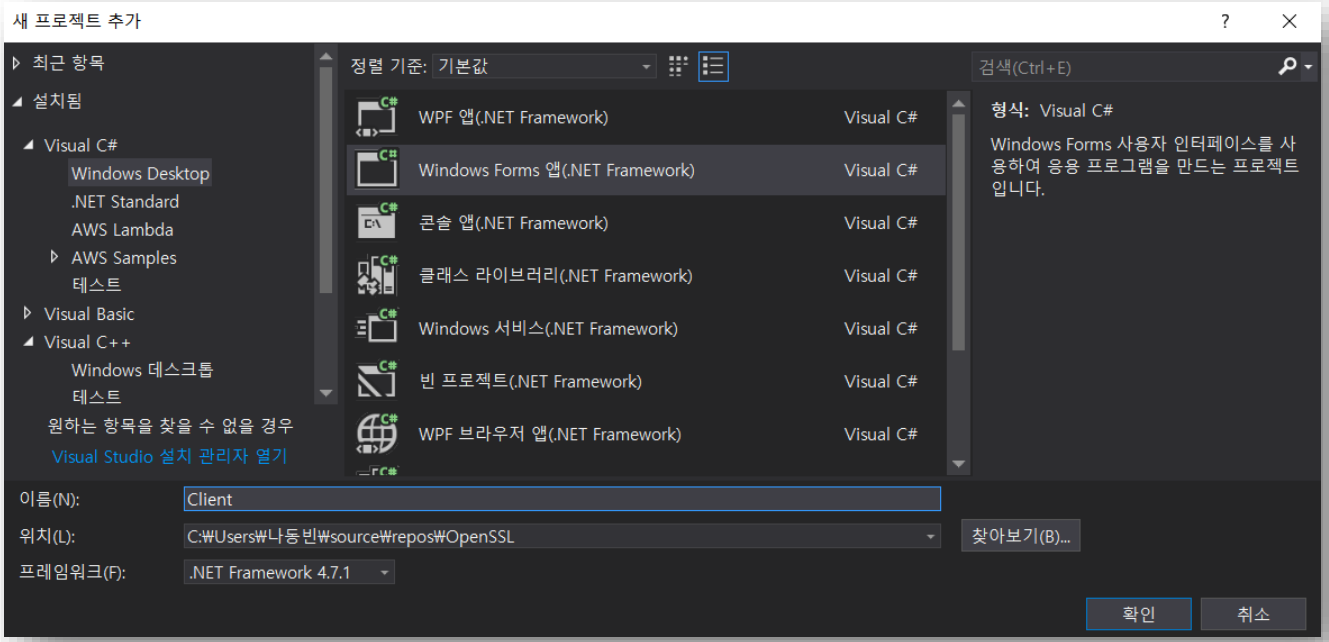
OpenSSL 설치하기

서버 인증서 준비하기



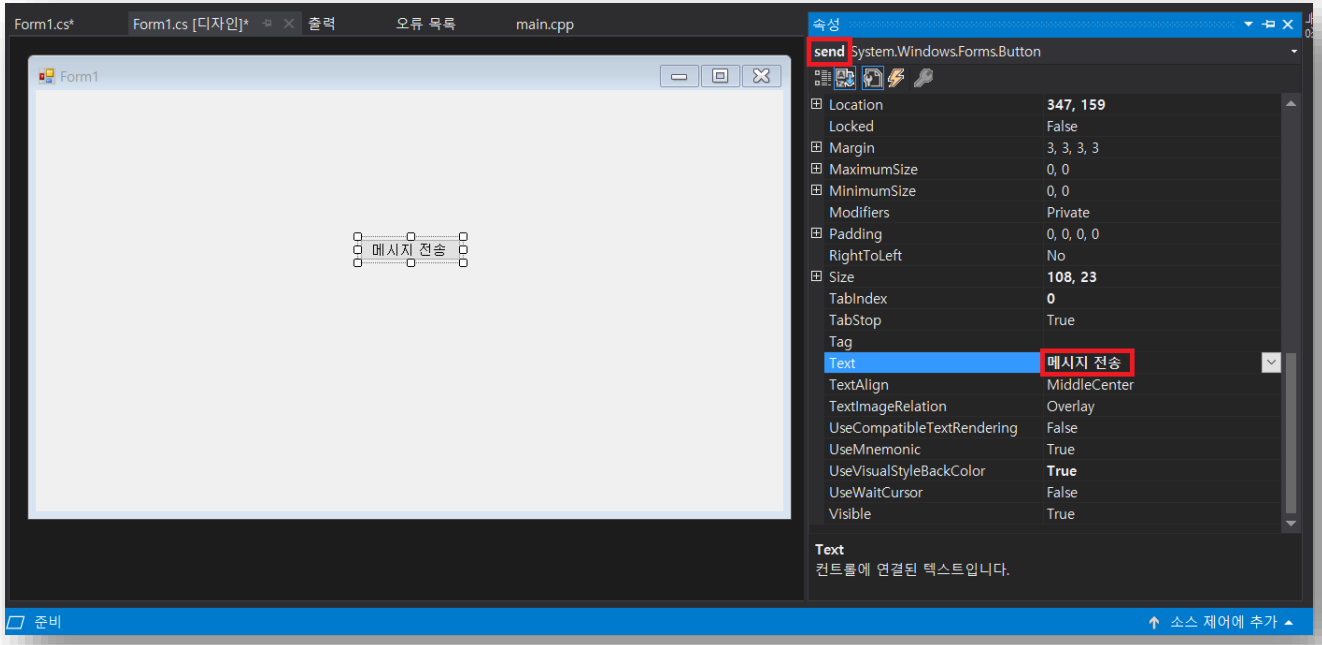
OpenSSL 설치하기

클라이언트 프로젝트 추가하기



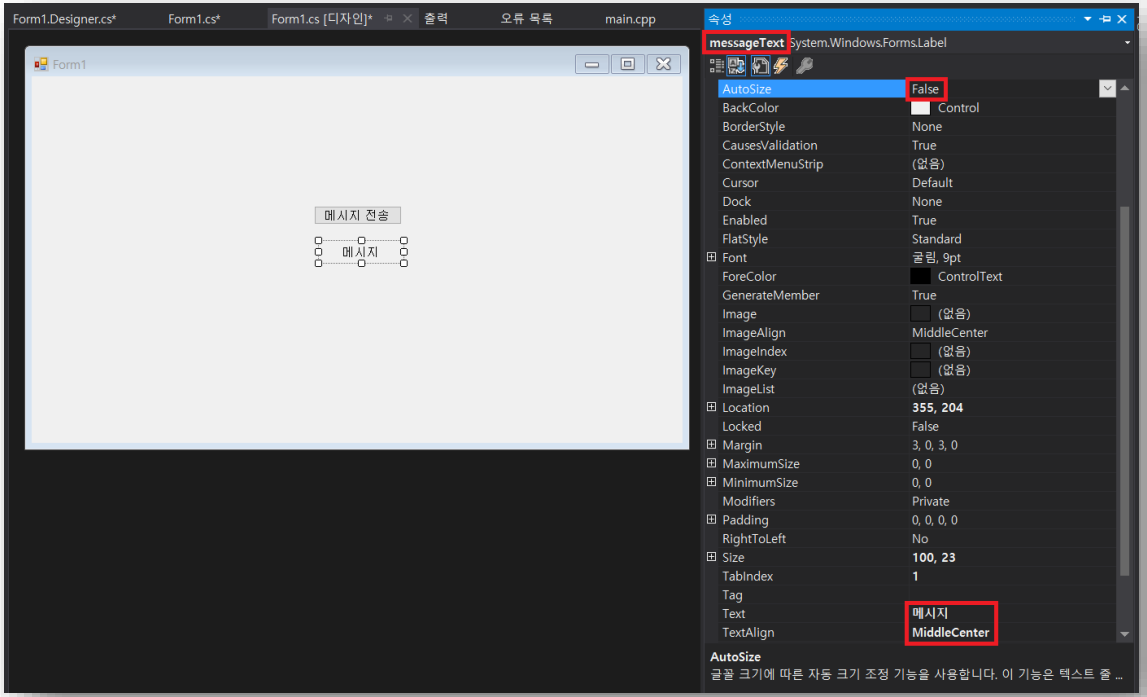
OpenSSL 설치하기

클라이언트 프로젝트 구성하기



OpenSSL 설치하기

클라이언트 프로젝트 구성하기



OpenSSL 설치하기

클라이언트 프로그램 ①

```
using System;
using System.Text;
using System.Windows.Forms;
using System.Net.Sockets;
using System.Net.Security;
using System.Security.Cryptography.X509Certificates;

namespace Client
{
  public partial class Form1 : Form
  {
    public string serverIP = "127.0.0.1";
    public int port = 9876;
    public string serverDomain = "localhost";

    public Form1()
    {
      InitializeComponent();
    }
```

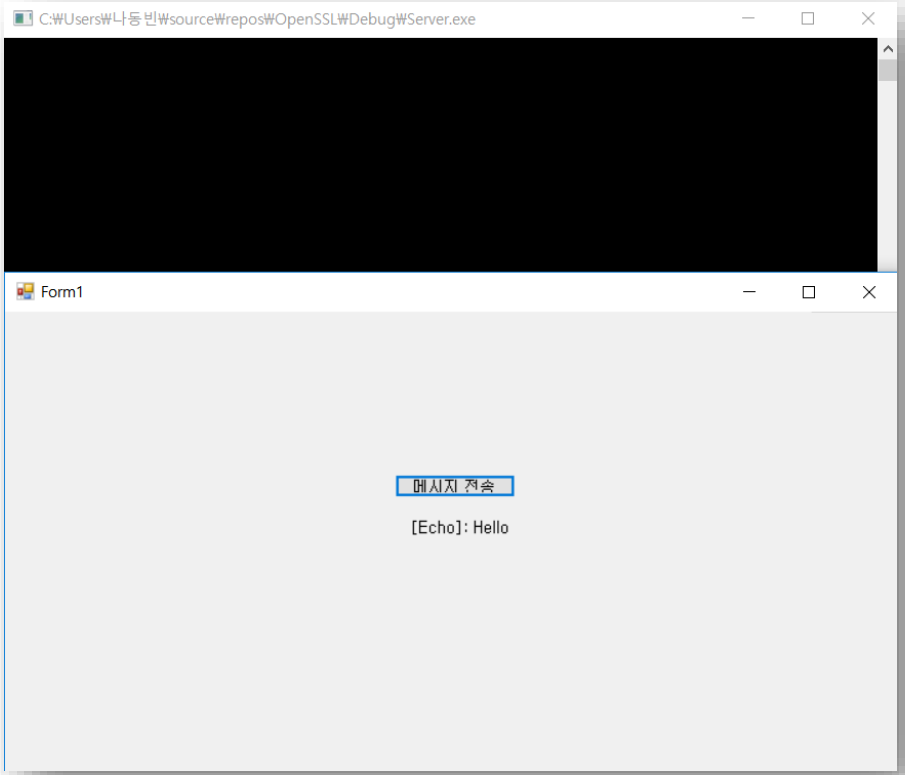
OpenSSL 설치하기

클라이언트 프로그램 ②

```
    private void send_Click(object sender, EventArgs e)
    {
      TcpClient client = new TcpClient(serverIP, port);
      SslStream sslStream = new SslStream(client.GetStream(), false, validateCertificate, null);
      sslStream.AuthenticateAsClient(serverDomain);

      byte[] buf = Encoding.ASCII.GetBytes("Hello SSL!");
      sslStream.Write(buf, 0, buf.Length);
      sslStream.Flush();

      buf = new byte[4096];
      int length = sslStream.Read(buf, 0, 4096);
      messageText.Text = Encoding.ASCII.GetString(buf, 0, length);
    }

    private bool validateCertificate(object sender, X509Certificate certificate, X509Chain chain, SslPolicyErrors sslPolicyErrors)
    {
      return true;
    }
  }
}
```

OpenSSL 설치하기

실행 결과



OpenSSL 설치하기

실행 결과