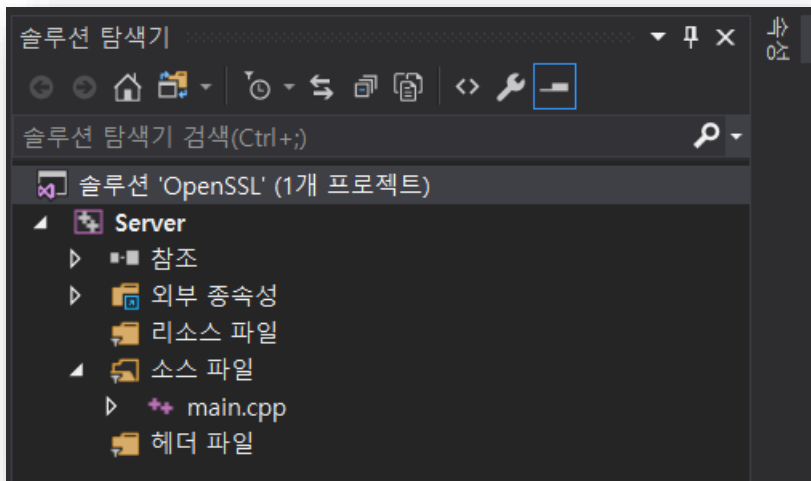


컴퓨터공학 All in One

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);

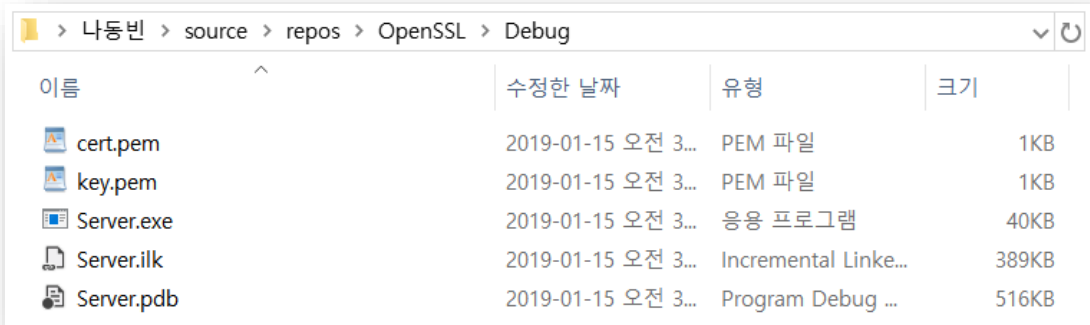
    /* SSL 출력 */
    char output[4096] = { 0 };
    int length = wprintfA(output, "[Echo]: %s\n", input);
    SSL_write(ssl, output, length);






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

close();
return 0;
}
```

OpenSSL 설치하기

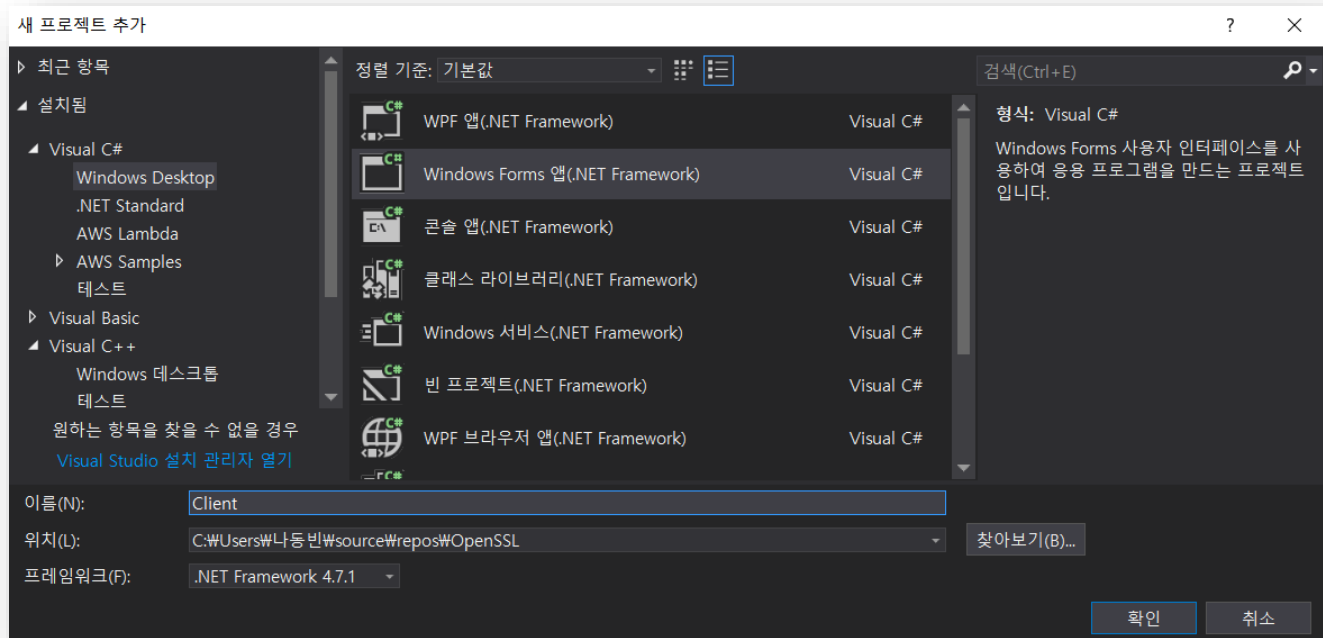
서버 인증서 준비하기



이름	수정한 날짜	유형	크기
 cert.pem	2019-01-15 오전 3...	PEM 파일	1KB
 key.pem	2019-01-15 오전 3...	PEM 파일	1KB
 Server.exe	2019-01-15 오전 3...	응용 프로그램	40KB
 Server.ilc	2019-01-15 오전 3...	Incremental Linke...	389KB
 Server.pdb	2019-01-15 오전 3...	Program Debug ...	516KB

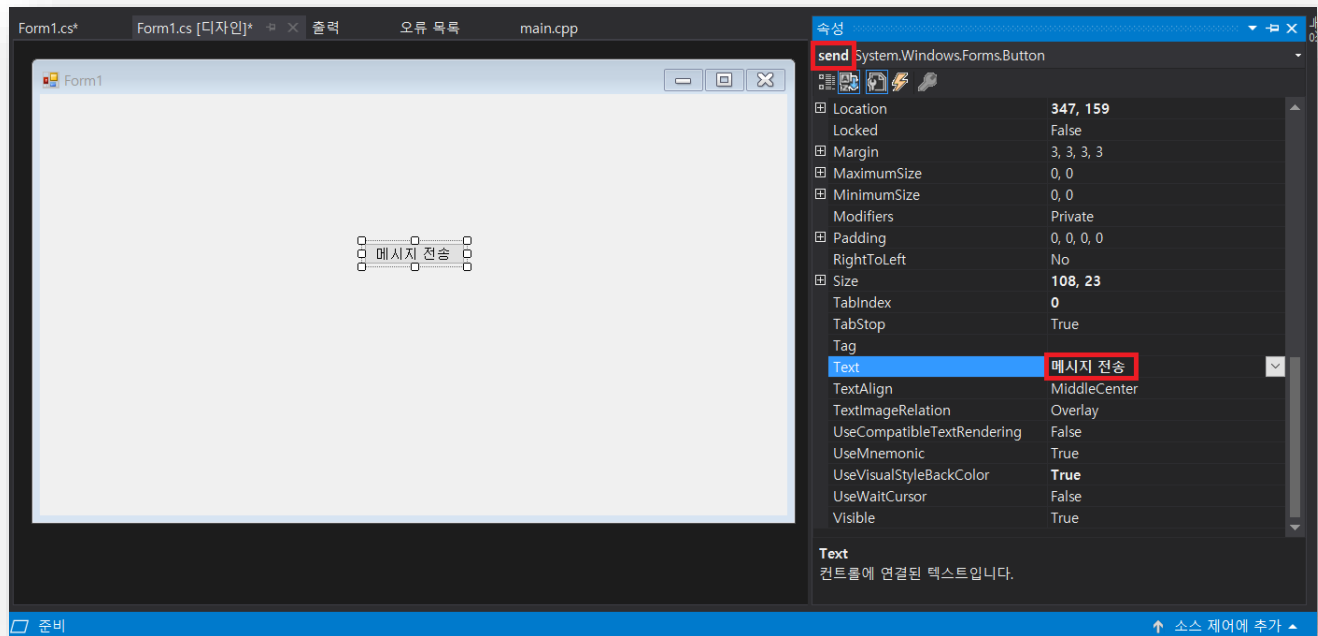
OpenSSL 설치하기

클라이언트 프로젝트 추가하기



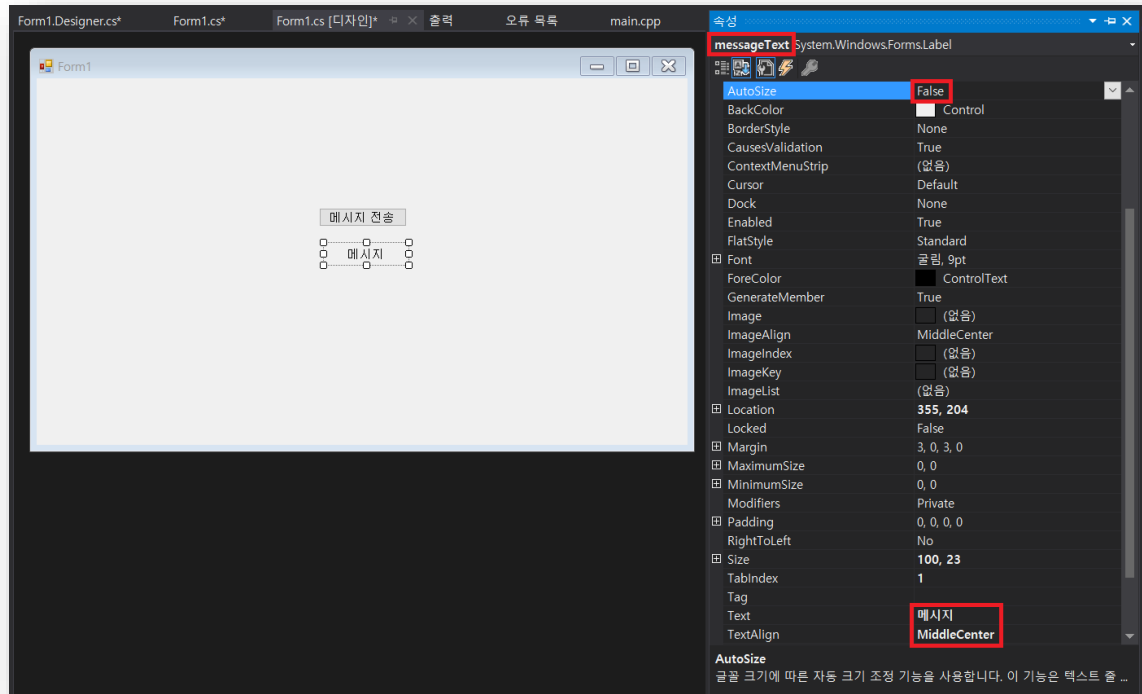
OpenSSL 설치하기

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);

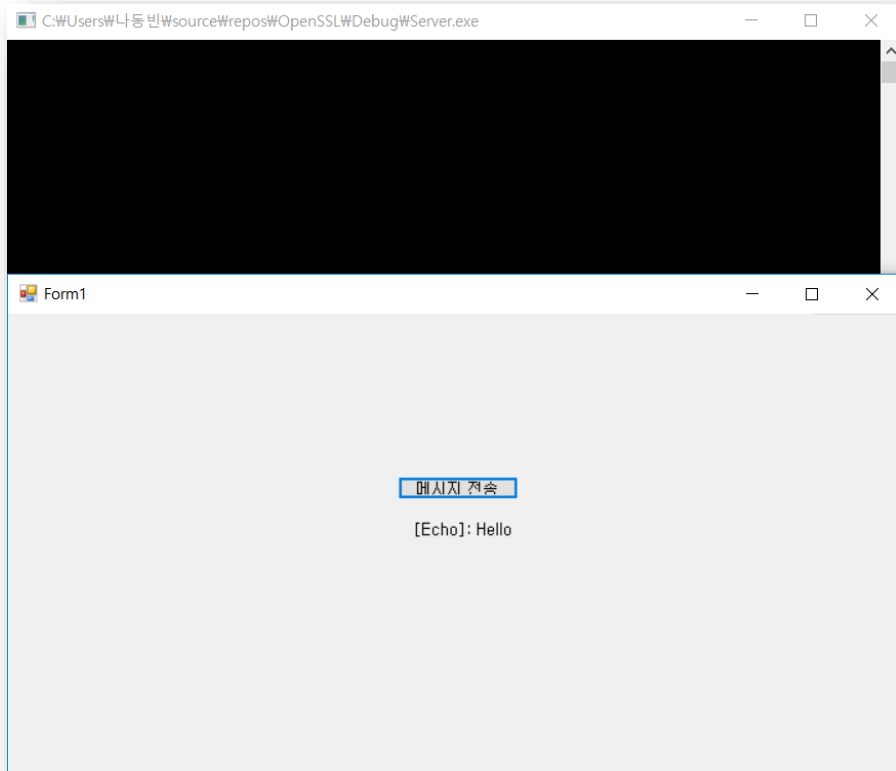
    byte[] buf = Encoding.ASCII.GetBytes("Hello SSL!");
    sslStream.Write(buf, 0, buf.Length);
    sslStream.Flush();

    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

***Npcap Loopback Adapter**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
410	43.143245	:::1	:::1	TCP	148	[TCP Retransmission] 36865 → 9229 [SYN] Seq=0
411	43.143268	:::1	:::1	TCP	124	9229 → 36865 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
412	43.143782	127.0.0.1	127.0.0.1	TCP	108	36869 → 9229 [SYN] Seq=0 Win=64240 Len=0 MSS=
413	43.143799	127.0.0.1	127.0.0.1	TCP	84	9229 → 36869 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
414	43.145217	:::1	:::1	TCP	148	[TCP Retransmission] 36864 → 9229 [SYN] Seq=0
415	43.145237	:::1	:::1	TCP	124	9229 → 36864 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
416	43.145757	127.0.0.1	127.0.0.1	TCP	108	36870 → 9229 [SYN] Seq=0 Win=64240 Len=0 MSS=
417	43.145776	127.0.0.1	127.0.0.1	TCP	84	9229 → 36870 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
418	43.174055	127.0.0.1	127.0.0.1	TCP	156	36866 → 4490 [PSH, ACK] Seq=259 Ack=1045 Win=
419	43.174092	127.0.0.1	127.0.0.1	TCP	84	4490 → 36866 [ACK] Seq=1045 Ack=295 Win=52531
420	43.174142	127.0.0.1	127.0.0.1	TCP	170	4490 → 36866 [PSH, ACK] Seq=1045 Ack=295 Win=
421	43.174163	127.0.0.1	127.0.0.1	TCP	84	36866 → 4490 [ACK] Seq=295 Ack=1088 Win=52428
422	43.174232	127.0.0.1	127.0.0.1	TCP	84	4490 → 36866 [FIN, ACK] Seq=1088 Ack=295 Win=
423	43.174250	127.0.0.1	127.0.0.1	TCP	84	36866 → 4490 [ACK] Seq=295 Ack=1088 Win=52428

> Frame 413: 84 bytes on wire (672 bits), 44 bytes captured (352 bits) on interface 0

Null/loopback

Family: IP (2)

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 9229, Dst Port: 36869, Seq: 1, Ack: 1, Len: 0

```

0000  02 00 00 00 45 00 00 28 19 8d 40 00 80 06 00 00    ....E.( ..@....
0010  7f 00 00 01 7f 00 00 01 24 0d 90 05 00 00 00 00    .....$......
0020  10 04 1b 25 50 14 00 00 d2 92 00 00              ...%P...
  
```

wireshark_70F07F14-06A1-4C8C-B74A-E296A273B5A9_20190115020834_a34732

Packets: 55118 · Displayed: 55118 (100.0%)

Profile: Default