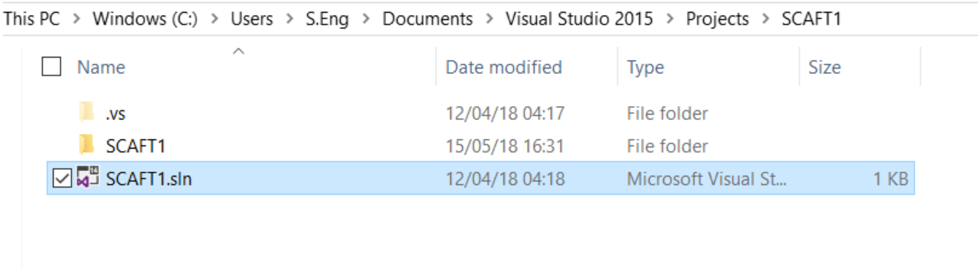
README – SCAFT.2

Loay Naser, ID: 204436042

Work hours: ~ 20

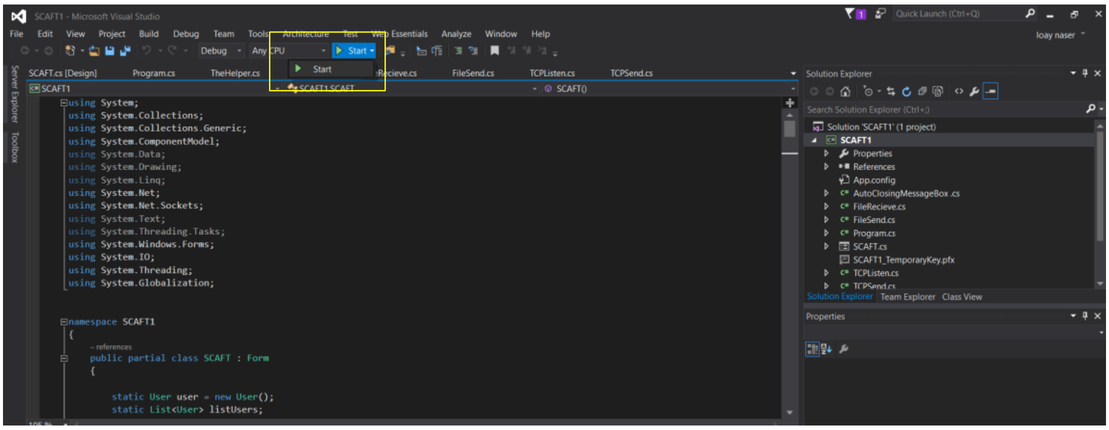
Instructions for compiling the source code for SCAFT:

After loading the code from the project folder to the Visual Studio, you only need to press the "start" button, as shown in the pictures below.



This PC > Windows (C:) > Users > S.Eng > Documents > Visual Studio 2015 > Projects > SCAFT1

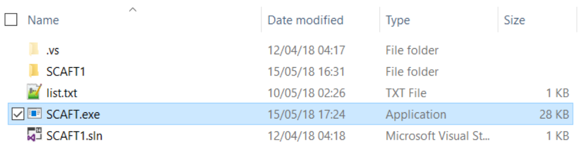
□ Name	Date modified	Type	Size
.vs	12/04/18 04:17	File folder	
SCAFT1	15/05/18 16:31	File folder	
☑ SCAFT1.sln	12/04/18 04:18	Microsoft Visual St...	1 KB



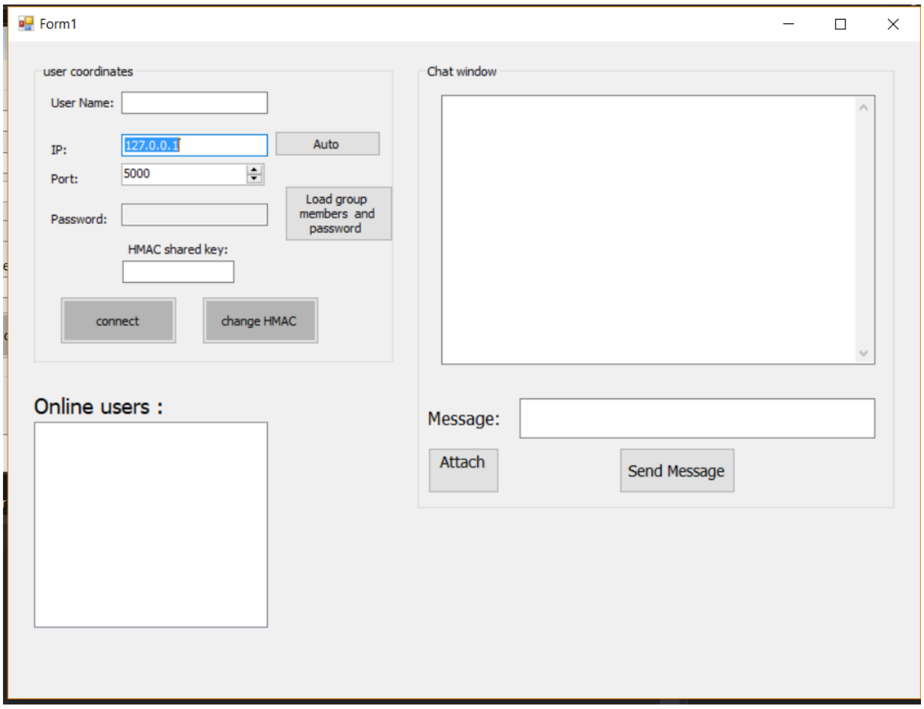
```
using System;
using System.Collections;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.IO;
using System.Threading;
using System.Globalization;


namespace SCAFT1
{
    public partial class SCAFT : Form
    {

        static User user = new User();
        static List<User> listUsers;
```

Instructions for running the SCAFT programs:

To start the program, you can run the SCAFT.exe from the project file or via visual studio as explained in the first section.



Name	Date modified	Type	Size
.vs	12/04/18 04:17	File folder	
SCAFT1	15/05/18 16:31	File folder	
list.txt	10/05/18 02:26	TXT File	1 KB
☑ SCAFT.exe	15/05/18 17:24	Application	28 KB
SCAFT1.sln	12/04/18 04:18	Microsoft Visual St...	1 KB



IP: 127.0.0.1

Port: 5000

In order to start chatting you need to insert the following parameters before connecting:

- username.
- Ip.
- Port.
- Write/Load password.
- Write/Load HMAC password

Once the needed parameters had been entered you can connect, a list of all online users will appear in "online users" box after the connection.

In case you want to change the HMAC password after connection, siply enter the new password in the textbox and press "change HMAC" button.

To send a message -> type whatever in the message box and hit "send message" button.

in order to send a file you must select a user from the list, otherwise the scaft will show a reminder to make sure you select a user.

After selecting a user you can send file by hitting the "attach" button and selecting a file.

HMAC:

In the messages the way of encryption, IV and password didn’t change, after encryption we will have a message of byte[32] then we compute the hash for the encrypted message ->

```
byte[] hashedMsg = new byte[32];
HMACSHA256 hmac = new HMACSHA256(Encoding.UTF8.GetBytes(hmacSharedkey));
var vhashedMsg = hmac.ComputeHash(encryptedmessage);
```

for the files, I compute the hash for the whole file before encryption. The hash arrive to the receiver with the "SENDFILE" message to compare it with the computed hash after.