Abstract
TOR network aims to ensure the privacy of families, businessmen, activists, media world. Every client who joins the TOR network becomes a part of this network and surfs over the internet privately. Although TOR network provides a secure internet experience, because of its nature every client needs to be a server. TOR network cannot be used because of the network prohibitions in companies, universities and commonly used networks.

Aim of this project is to develop a TOR-enabled proxy server between the client which is within an insecure network and TOR network and let the users make private web access over the internet. The server receives the request from client, originates it to TOR Network, evaluates the response and forward it to the client. The client side can operate on different platforms. It sends the request to the server. TOR is chosen because it is open source and supported by the community.

When using Proxy Server, the bandwidth of the client is limited by the performance of slowest node in the TOR network’s route. Overhead of using Proxy Server depends on this limit. The performance penalty of privacy is hence limited by individual performances in the TOR network route. We show the typical limits by experimentation.

Motivation
Our motivation is to implement an Interface which connects to TOR Network, handles the requests got from the client and originates it to TOR Network. In this architecture, the user does not directly become a node of the TOR network. The user host is not a server for the requests in the TOR network which means, the port which is used between the interface and the end-user can be changed to a permitted port such as HTTP (80), FTP (21), SFTP (22) and the user can indirectly access to TOR Network. Since the user is not a server, the bandwidth of the other requests does not affect the bandwidth usage of the end-user. By using the Proxy Server, users can easily join to TOR network without software installation.

Results
Our results show that we have successfully provided privacy of the users using the proxy. As indicated in Section 5.1 we have achieved to hide the identity of the users. We also show that the users can achieve this using a proxy independent of their locations.

The Onion Router (TOR)
TOR is an open-source software which provides online anonymity. TOR network is a volunteer network consisting of thousands of volunteer relays. The network makes it difficult to trace personal operations like surfing over the internet. Every client in the TOR network is also a server who originates the traffic to the final destinations.

Information of the clients in the TOR network is stored in authorized directory servers. TOR software builds a virtual circuit through the TOR network and when a request starts the request is made from the final destination by the end point. Since there is encryption inside of the circuit, the requester client cannot be detected by

Future Work
Our architecture is based on a client and a proxy server which connects to TOR Network and respond to clients requests. In order to make a secure connection between Proxy Server and client, we should make a client application which will encrypt UDP / TCP packages before sending to the server. The server should also be changed in a way that will be able to decrypt the packages received from the client application.

Contact: ozanakcora@gmail.com