What is SSL?

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard that is used by millions of websites in the protection of their online transactions with their customers. Basically, SSL is used is to keep sensitive information sent across the Internet encrypted so that only the intended recipient can understand it. Any computer in between you and the server can see your credit card numbers, usernames and passwords, and other sensitive information if it is not encrypted with an SSL certificate. When an SSL certificate is used, the information becomes unreadable to everyone except for the server you are sending the information to.

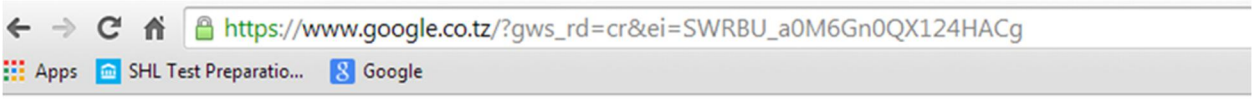
How SSL Works

To be able to create an SSL connection a web server requires an SSL Certificate. When SSL is activated on a web server the user will be prompted to complete a number of questions about the identity of his/her website and the company. Your web server then creates two cryptographic keys - a Private Key and a Public Key.

The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) a data file also containing your details. You should then submit the CSR. During the SSL Certificate application process, the Certification Authority will validate your details and issue an SSL Certificate containing your details and allowing you to use SSL. Your web server will match your issued SSL Certificate to your Private Key. Your web server will then be able to establish an encrypted link between the website and your customer's web browser. All SSL Certificates are issued to either companies or legally accountable individuals. When a browser

connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL.

When a browser attempts to access a website that is secured by SSL, the browser and the web server establish an SSL connection using a process called an SSL Handshake. Figure below shows a secure connection between web server and client computer with padlock and green color on it.

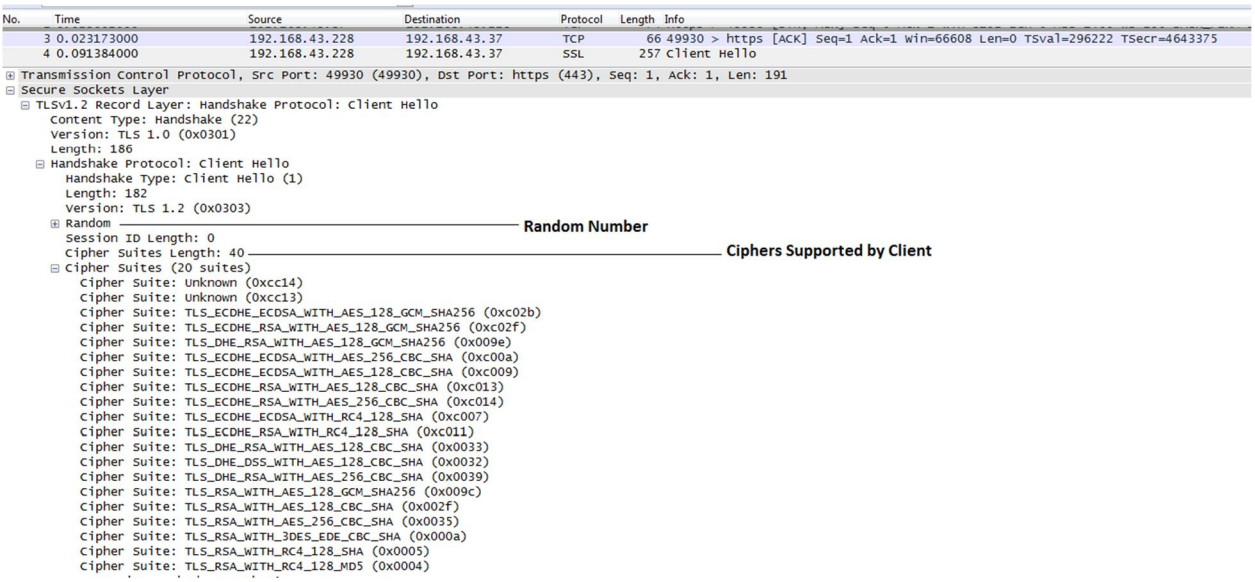


For the purpose of demonstration on how SSL works in this context Wireshark network analysis tool used to capture and analyze communication packets between server (web-server: 192.168.43.37) and the client (Web-browser: 192.168.46.228).

The SSL Handshake mechanism initiated involves several steps as follows.

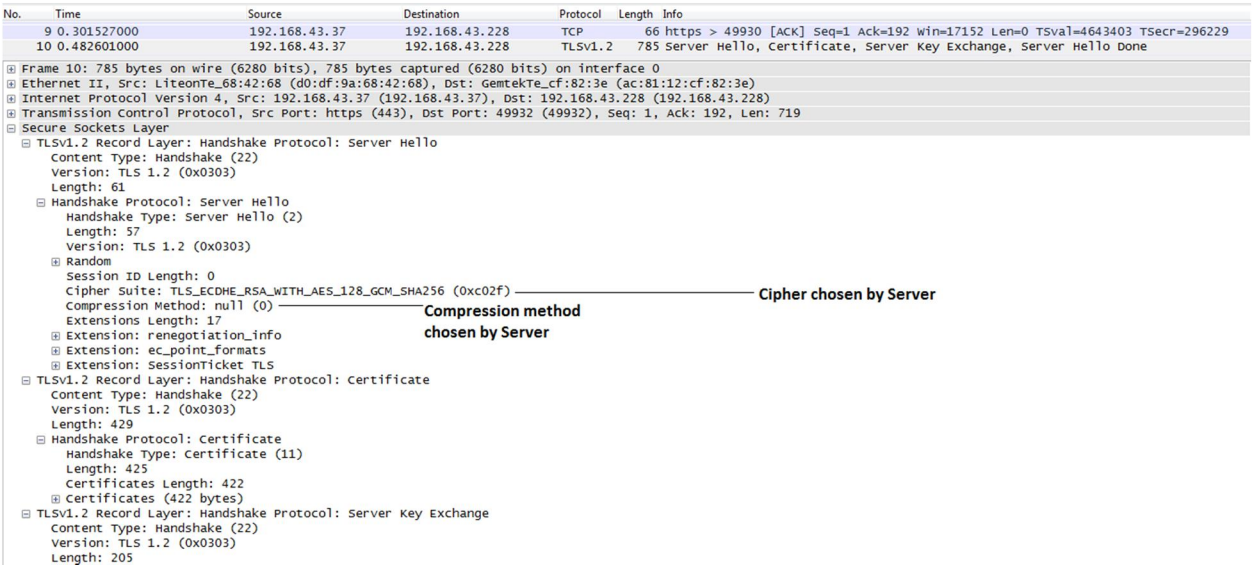
a) Client hello

First the client computer (web browser) sends hello message to the server, the hello message contains key exchange methods, cipher as the way to encrypt data between server and client, hash methods for data integrity and authentication of data, SSL version used on the client computer and random number used for computing master secrete that used to calculate encryption keys.



b) Server hello

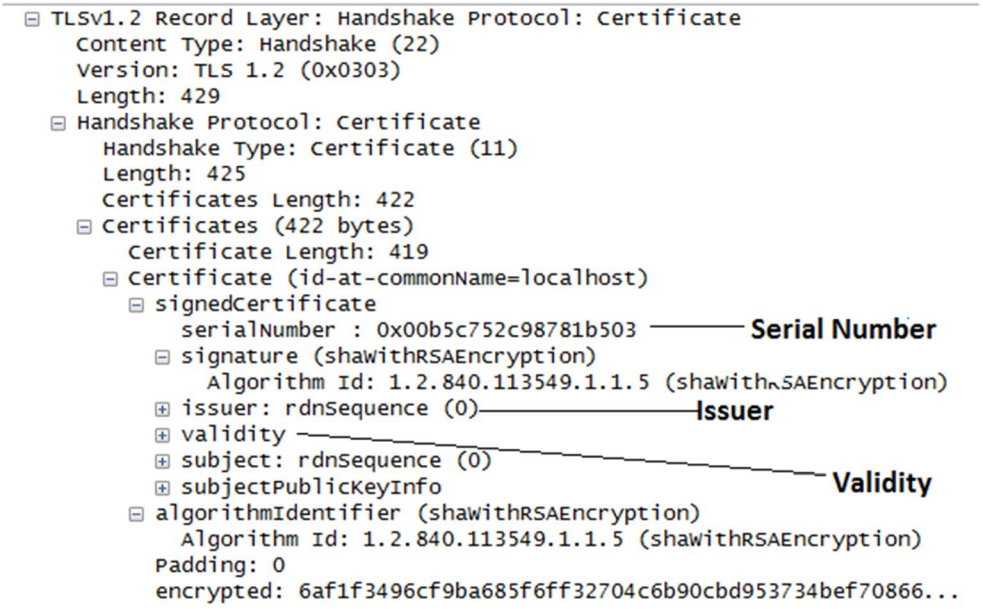
Then server sends hello message back to the client with the list of chosen key exchange methods, cipher as the way to encrypt data between server and client, hash methods from the one suggested by the client hello message



c) Server sends certificate

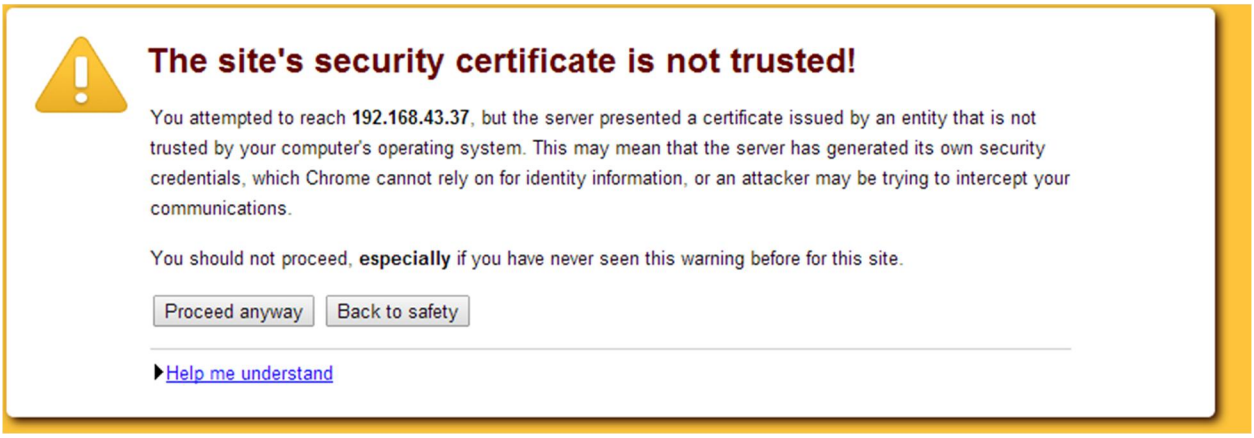
The next step is server sends a copy of its SSL Certificate to the client that contains serial number, server's public key, certificate issuer, validity period of the certificate and other relevant information.

Figure below shows some information included on SSL certificate.



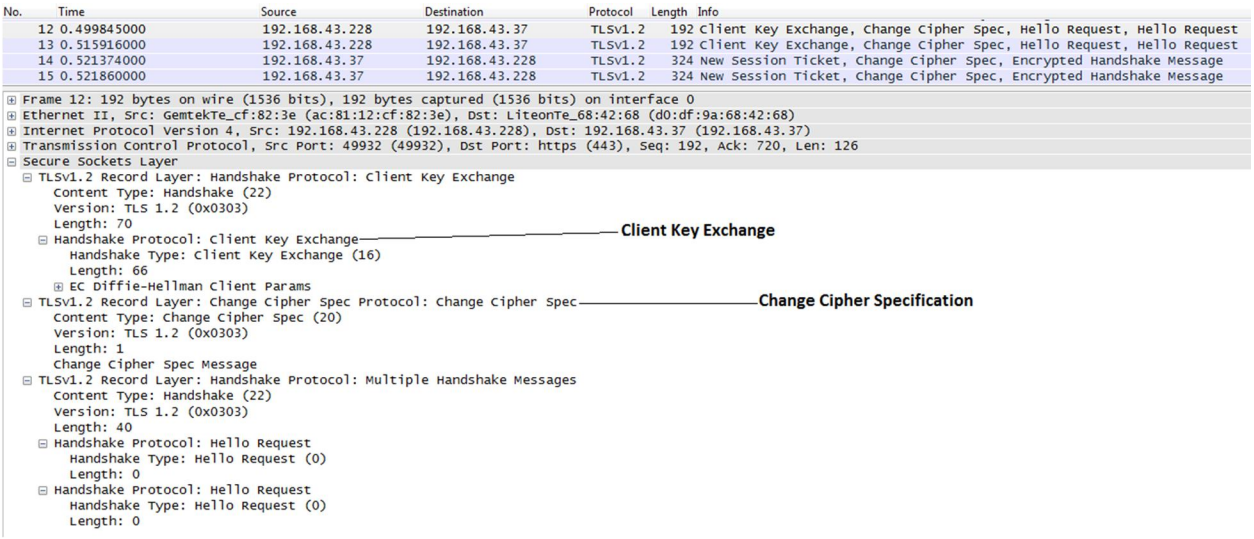
d) Browser checks the certificate

Browser checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to If the certificate is not signed by a verified issuer the client might prompt the user to proceed with an unsigned verification. In a Chrome browser the user would get a notification such as the one shown below.



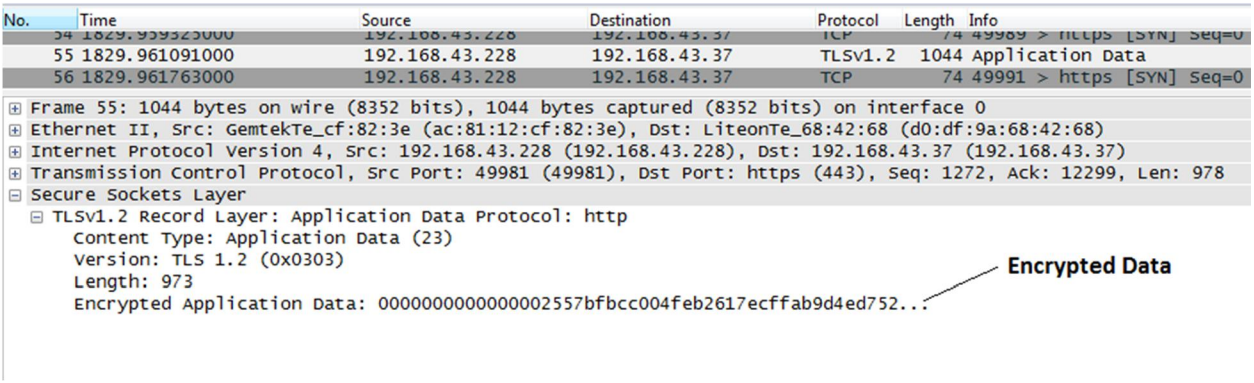
e) Client and server agree to start encryption

When browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key through hello packets. **Server** decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session through hello packets.

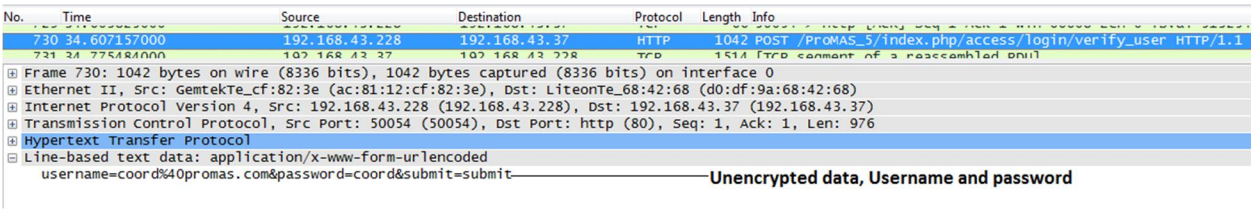


f) All communication between server and client is now encrypted

Server and Browser now encrypt all transmitted data with the session key. Because encrypting and decrypting with private and public key takes a lot of processing power, they are only used during the SSL Handshake to create a symmetric session key. After the secure connection is made, the session key is used to encrypt all transmitted data. Therefore server and client exchange data using the encryption specifications agreed until the SSL session expires after the validity period is reached.



As opposed to browser communication over SSL (https), http send unencrypted data. See example below where an attacker could intercept sensitive information.



How SSL is used in practice

- To secure online credit card transactions.
- To secure system logins and any sensitive information exchanged online.
- To secure webmail and applications like Outlook Web Access, Exchange and Office Communications Server.
- To secure workflow and virtualization applications like Citrix Delivery Platforms or cloud-based computing platforms.
- To secure the connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.
- To secure the transfer of files over https and FTP(s) services such as website owners updating new pages to their websites or transferring large files.
- To secure hosting control panel logins and activity like Parallels, cPanel, and others.
- To secure intranet based traffic such as internal networks, file sharing, extranets, and database connections.
- To secure network logins and other network traffic with SSL VPNs such as VPN Access Servers or applications like the Citrix Access Gateway.

Why we use SSL

Confidentiality

The data being transmitted over the Internet or network needs confidentiality. In other words, people do not want their credit card number, account login, passwords or personal information to be exposed over the Internet.

Integrity

The data needs to remain integral, which means that once credit card details and the amount to be charged to the credit card have been sent, a hacker sitting in the middle cannot change the amount to b charged and where the funds should go.

Authentication

Your organization needs identity assurance to authenticate itself to customers / extranet users and ensure them they are dealing with the right organization.

Disadvantages of SSL

- **Cost**

SSL providers need to set up a trusted infrastructure and validate your identity so there is a cost involved. Because some providers are so well known, their prices can be overwhelmingly high.

- **Performance**

This is another disadvantage to SSL. Because the information that you send has to be encrypted by the server, it takes more server resources than if the information weren't encrypted. The performance difference is only noticeable for web sites with very large numbers of visitors and can be minimized with special hardware.

- Requires regular renewals
- Complex installation

What is SSH?

SSH stands for "Secure Shell". SSH commonly uses port 22 to connect your computer to another computer on the Internet. It is most often used by network administrators as a remote login / remote control way to manage their business servers. Examples would be: your email administrator needs to reboot the company email server from his home, or your network administrator needs to reset your office password while she is away at a conference.

Ssh Protocal

SSH (Secure Shell) is a network protocol that provides secure access to a computer (mostly UNIX based). When you want to connect to a remote UNIX server, SSH is one way of accessing the server. SSH is very powerful by combining both securities of the data transmitted over network and accessibility to the remote system. SSH protocol works between two computers by client-server architecture. When a client computer connects to the server, the server requires the client to authenticate itself. There are different ways a client can authenticate itself to the server. A typical authentication mode will be to enter a password when logging into a remote system. In this how to we can explore another mode of authentication in which server doesn't require a password to be entered by the user. This mode will be very useful if you are connecting to a remote system frequently and don't want to enter the password every time

Ssh Server

When you need to connect to a remote computer via SSH, that computer should have a SSH server running on it. All UNIX based distributions (Linux, Mac OSX etc.,) includes a SSH server. For Windows based systems third party software needs to be installed in order to have the SSH server capabilities.

Ssh Client

Assuming your remote computer has an SSH server running on it, to connect to that computer you would need a SSH client on the local computer. On Unix based systems, SSH clients are available as command line utilities. For Windows based systems third party

software need to be installed in order to enable SSH client capabilities, putty is an excellent SSH client.

Configuration

In order to configure SSH between two networked computer, one computer has to be configured as an SSH server and another computer has to be configured as an SSH client.

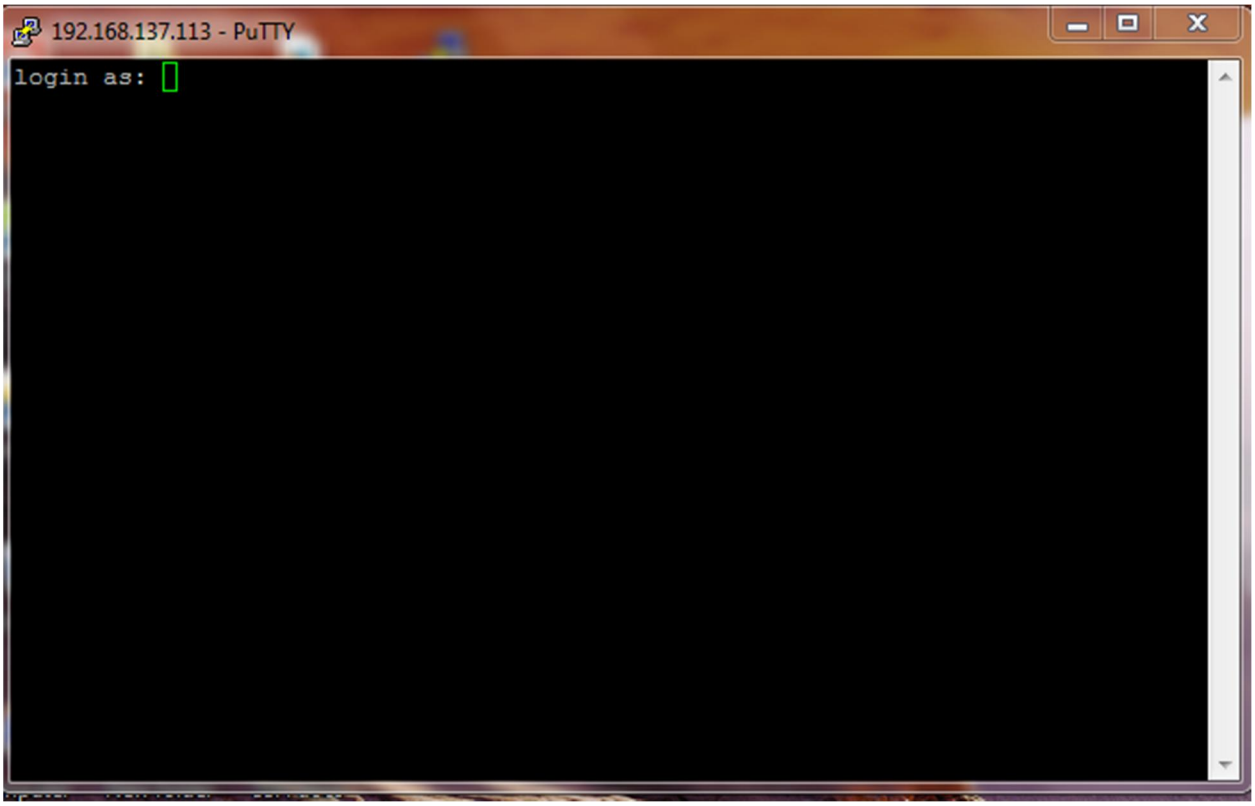
Configuring the SSH client

In UNIX based systems SSH client is available as the service in the terminal / command line interface. In window systems however you have to install the SSH client software. Putty is the most commonly used. To login to an SSH server from the SSH client simply invoke the command "*ssh username@ssh_server.*" Where "*username"* is the name of the user and "*ssh_server* is the domain name or IP address of the ssh server.

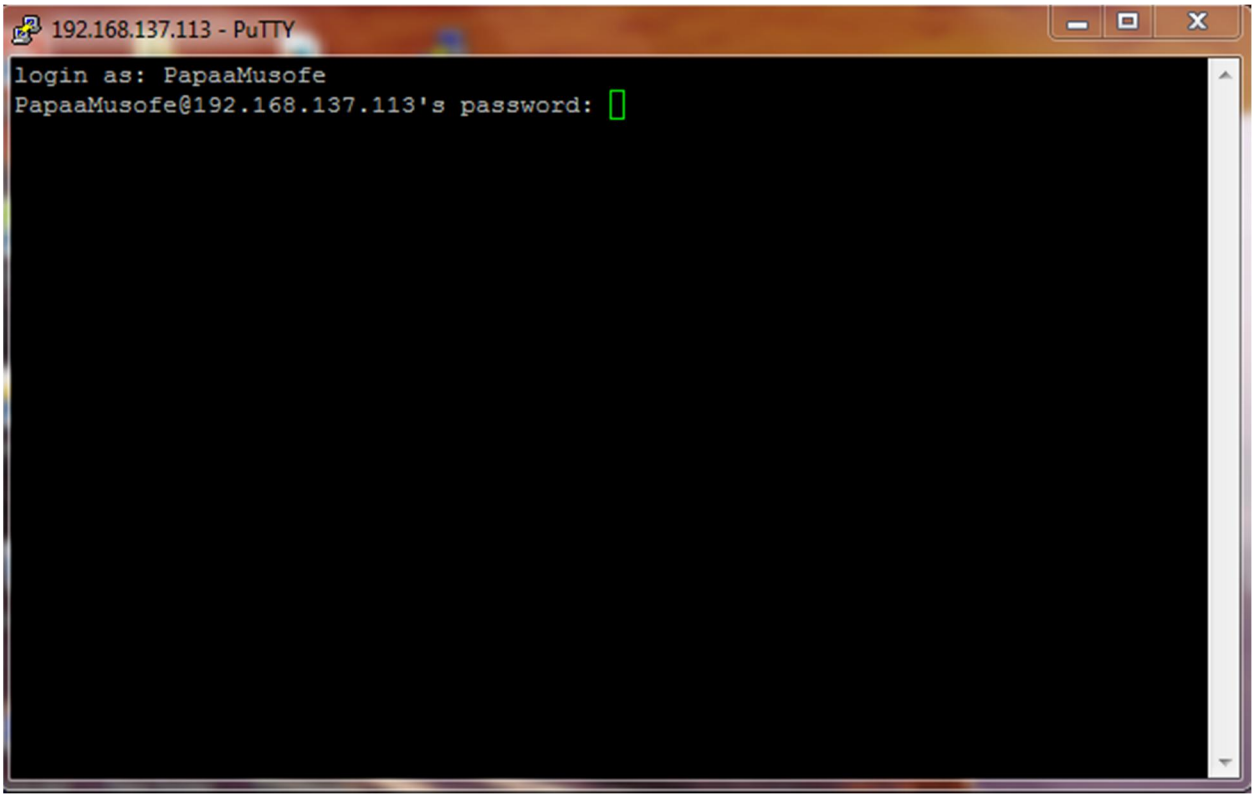
Configuring the SSH server

To configure the SSH client in windows systems, third party program has to be installed in order to have the SSH server capabilities. The SSH server program which was used in our case study is FreeSSHd. Simply install the program following the instructions given on the installation window. After the software has been installed open the software and go to settings and add the user who will access the server remotely.

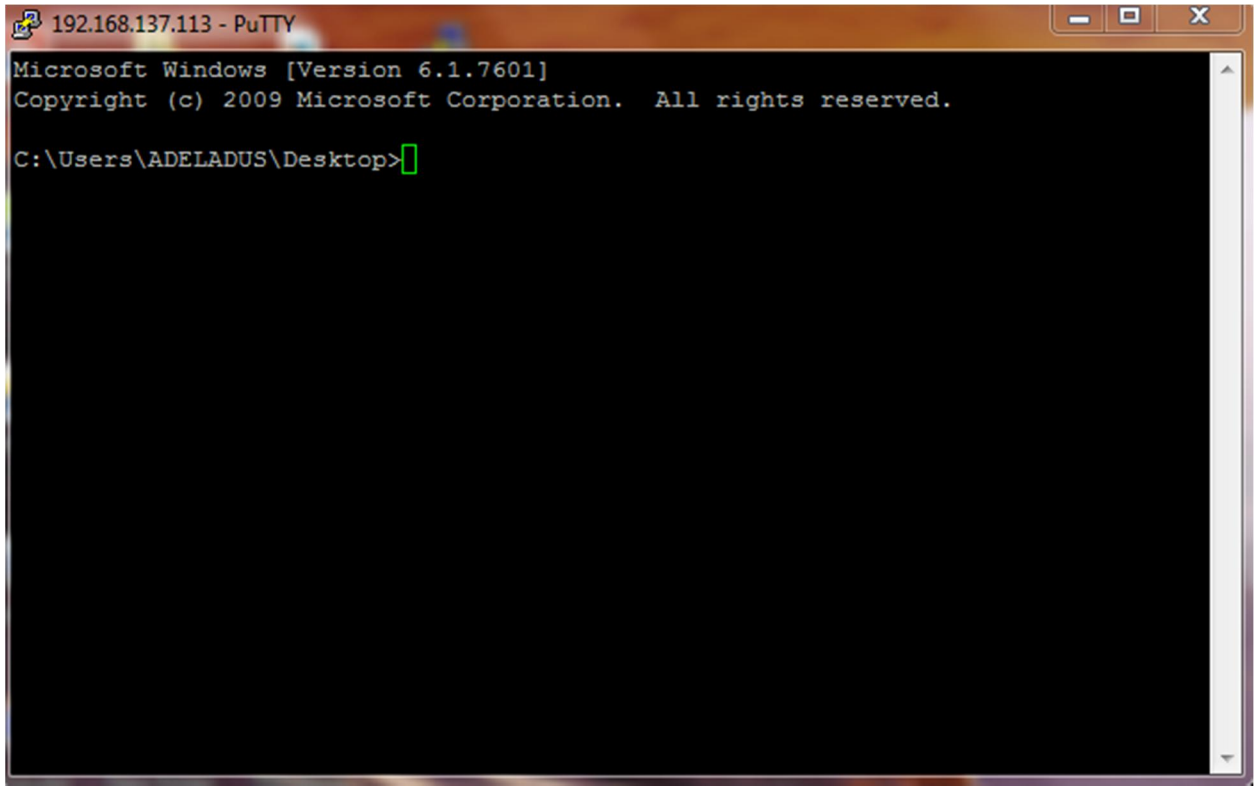
Screen shots Showing the Successful ssh remote access

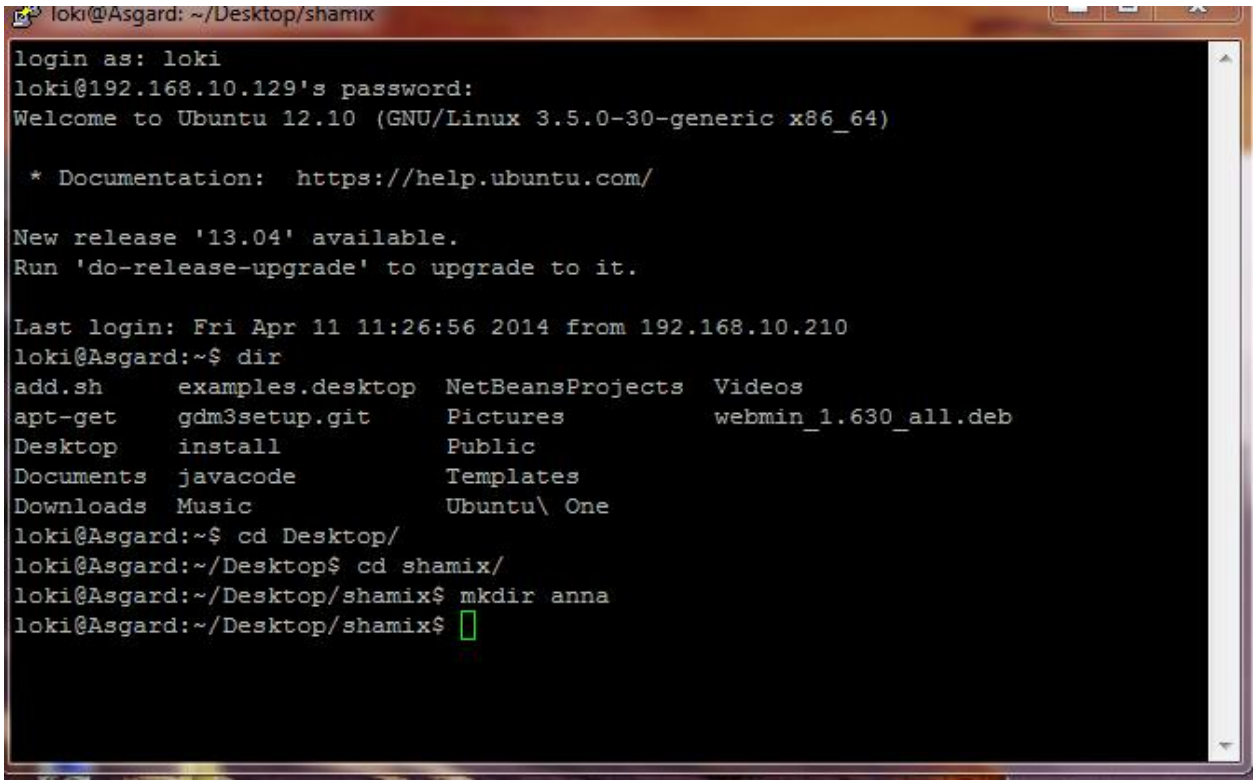


Login using putty



Entering credentials1111111111111111


192.168.137.113 - PuTTY
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\ADELADUS\Desktop>


loki@Asgard: ~/Desktop/shamix
login as: loki
loki@192.168.10.129's password:
Welcome to Ubuntu 12.10 (GNU/Linux 3.5.0-30-generic x86_64)
* Documentation: https://help.ubuntu.com/
New release '13.04' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Fri Apr 11 11:26:56 2014 from 192.168.10.210
loki@Asgard:~$ dir
add.sh examples.desktop NetBeansProjects Videos
apt-get gdm3setup.git Pictures webmin_1.630_all.deb
Desktop install Public
Documents javacode Templates
Downloads Music Ubuntu\ One
loki@Asgard:~$ cd Desktop/
loki@Asgard:~/Desktop$ cd shamix/
loki@Asgard:~/Desktop/shamix$ mkdir anna
loki@Asgard:~/Desktop/shamix$

Both SSL and SSH strive to create confidential connections across the internet. With only a very few exceptions, it is not possible for a regular hacker to break into an SSL or SSH connection.

When you are trying to transmit financial information or internal business documentation, it is highly advisable that you only do so with an SSL or SSH type of connection.

Both SSL and SSH are special encryption and protocol technologies used to connect two computers. SSL and SSH lock out eavesdroppers by encrypting (ciphering) the connection, and scrambling the transmitted data so it is meaningless to anyone outside of the two computers.