SSL Mardshale P.	grotocol
------------------	----------

4) Host complex past of SSL to authoriticate each tolker and Heres seemen regoticies 13 encouption Ly MAC XIQ sai HAMS 13 Guy ptogosphie Reys +) This is used before an application data is sent. reavege

1) SSL TLS VOILION Helle 2) Our ptogoraphic algorithms 3) Data Composision Methods) Gurtogeosphie Agorithm Harament Nelle a) lession ID 3) source & Digital Costificate 1) soon vog Public Key L) Bith contificate Authority) contificate vosification TE(should secont bey with]

1) client bey exchange 2) outificate voisfication

(intelligence of the property of the property

dient

bert

2) finished

) E (firested) with stared second bay 2) finished

SSL Powtocal Stack

highen _	55L Kardshake Protocol	SSL Change Cipter Spec Protocol Protocol	SSL About Protocol	кттР
Davel	551	TCP		
		IP		

SSL Clarge Ciples? Notifies the receiver that all the spectated subsequent prehats are to be protected based on negotiated ciphon suite I bay

SSL XBod ? protose y

- 4) Stands Sends the about messages to the socaring pasety.
- +) Hast Hessage √ contains these security level & a description

SSL paroad Protocol Message Integrity Confidentiality HAC Address Convertional Method

