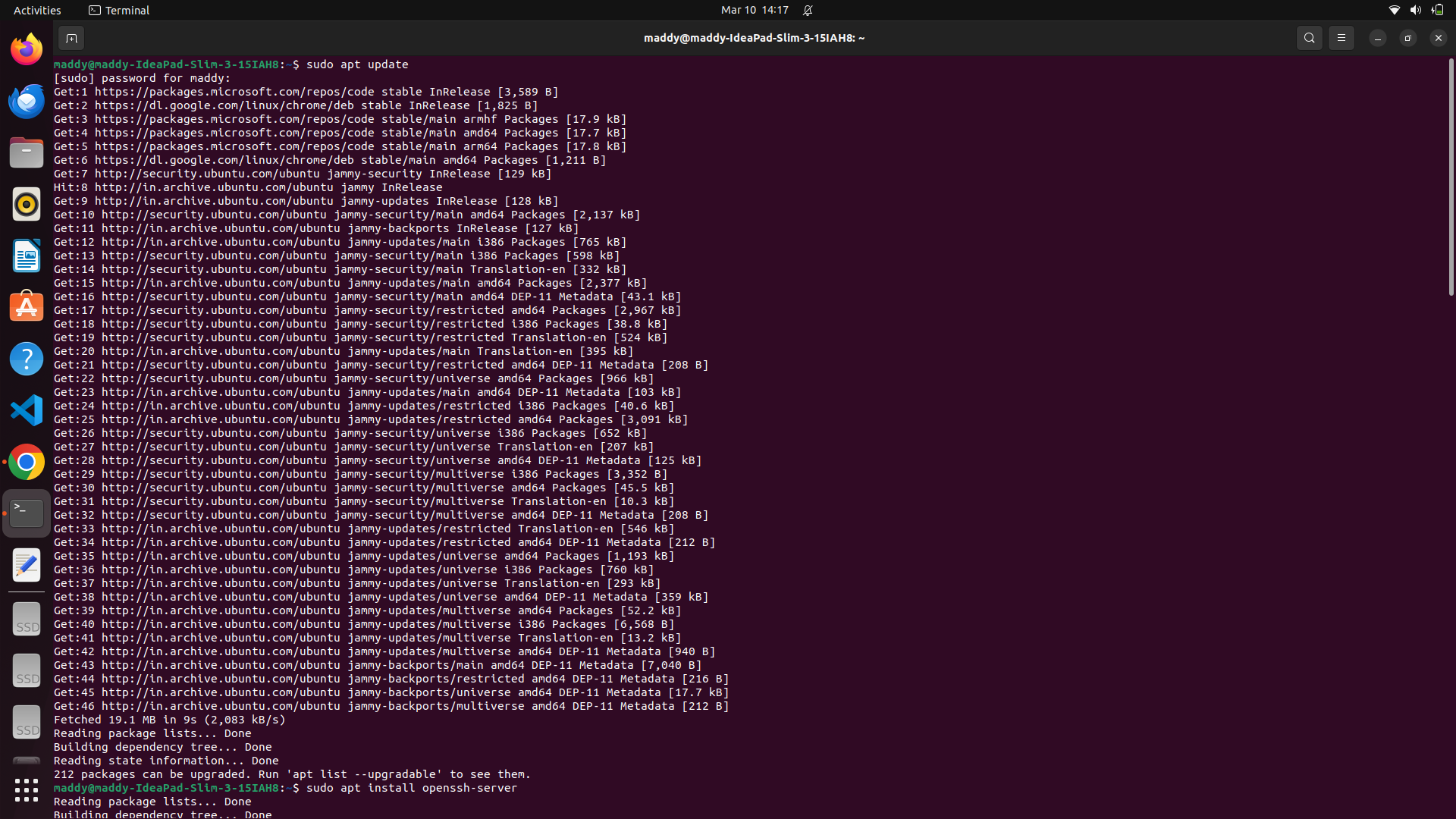
SECURE SHELL (SSH):

INTRODUCTION :

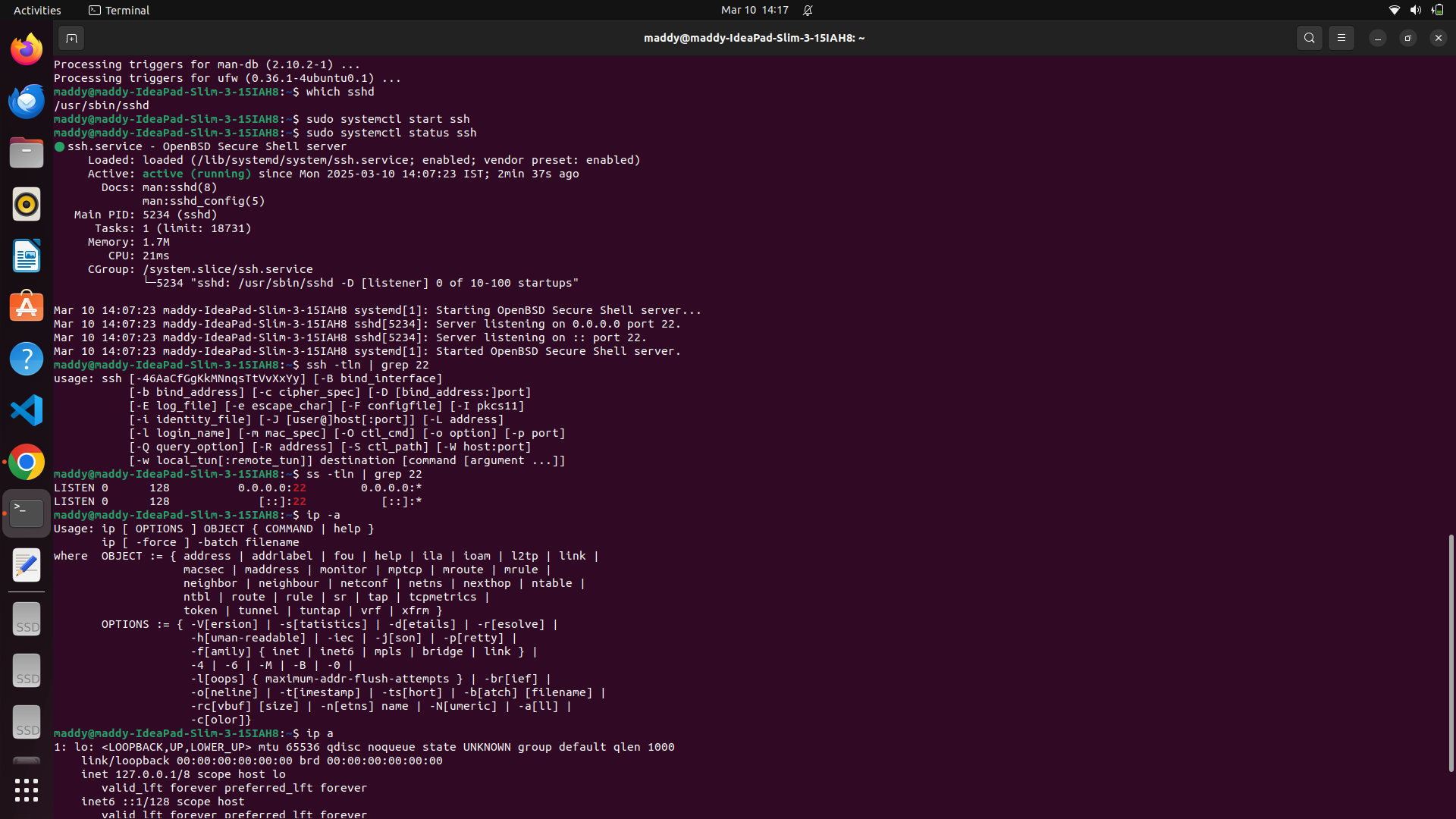
1. SSH (Secure Shell) is a cryptographic network protocol used for securely connecting to remote systems, executing commands, and transferring files.
2. SSH operates on the **client-server model**, where an SSH client initiates a connection to an SSH server. The connection is secured using encryption (AES etc.) and authentication mechanisms (HMAC and diffie hellman algorithms etc.).
3. Offers both password based and public key based authentication methods. (in public key based, client will generate two keys using RSA like algorithms and places the public key in server side and accepts request from server and signs it using public key and sends back to server while logging in . this acts as alternative to password based signing in).
4. By default, SSH works on port 22. (but port can be customized)
5. In OSI model , it works on all the layers above Data link layer.

DEMONSTRATION :

1. Requires installing open ssh server package in linux as follows:



1. To enable the machine to be ssh server, Server should be manually or automatically (from boot) to be started. Followed by, the status can be checked to ensure it is “active (running)” and then, the port can be confirmed by using netstat with grep command to filter the results as follows: (ssh folder can be verified after installation by using which sshd command)



1. To connect to any ssh server , ensure the above steps are made ready (including specifying the IP address of the current working network interface with host name -> using whoami in server side). SYNTAX : ssh hostname@IP address (if password is enabled, it asks for password, if not key verification after one time setup will take place automatically )

