WLUG
COMMUNITY | KNOWLEDGE | SHARE

SSH

THE SECURE SHELL

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Flow of Session

- Introduction
- SSH
- History & Uses of SSH
- SSH Keys
- Encryption & Authentication
- SFTP & Basic Commands
- Configuring SSH
- SSH & Security
- SSH Agent & Tunneling
- Conclusion

WLUG
COMMUNITY | KNOWLEDGE | SHARE

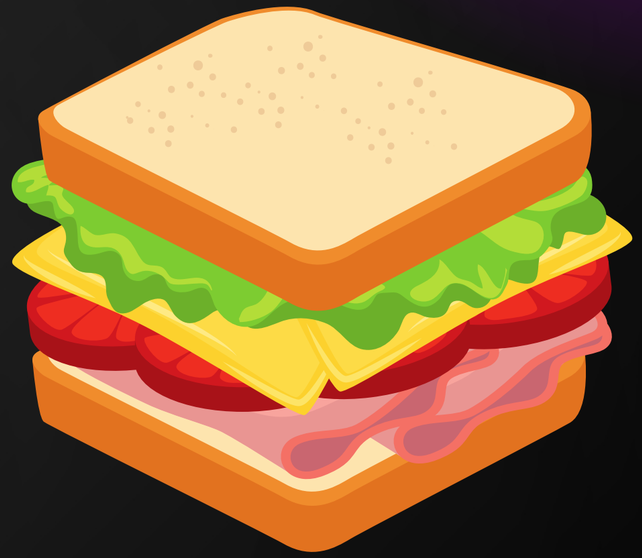
WHAT IS A PROTOCOL?

- A protocol refers to a set of rules, such as how should devices connect to each other
- Protocols are often used to ensure that activities or processes are carried out in an orderly manner

WLUG
COMMUNITY | KNOWLEDGE | SHARE

WHAT IS A PROTOCOL?

DATA

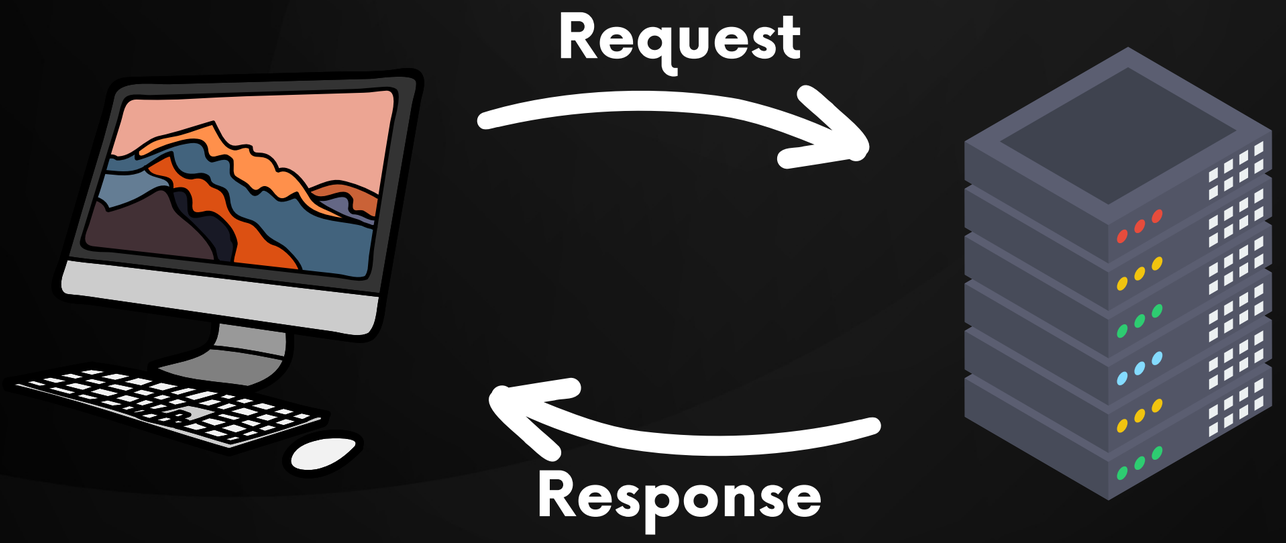


PRODUCT

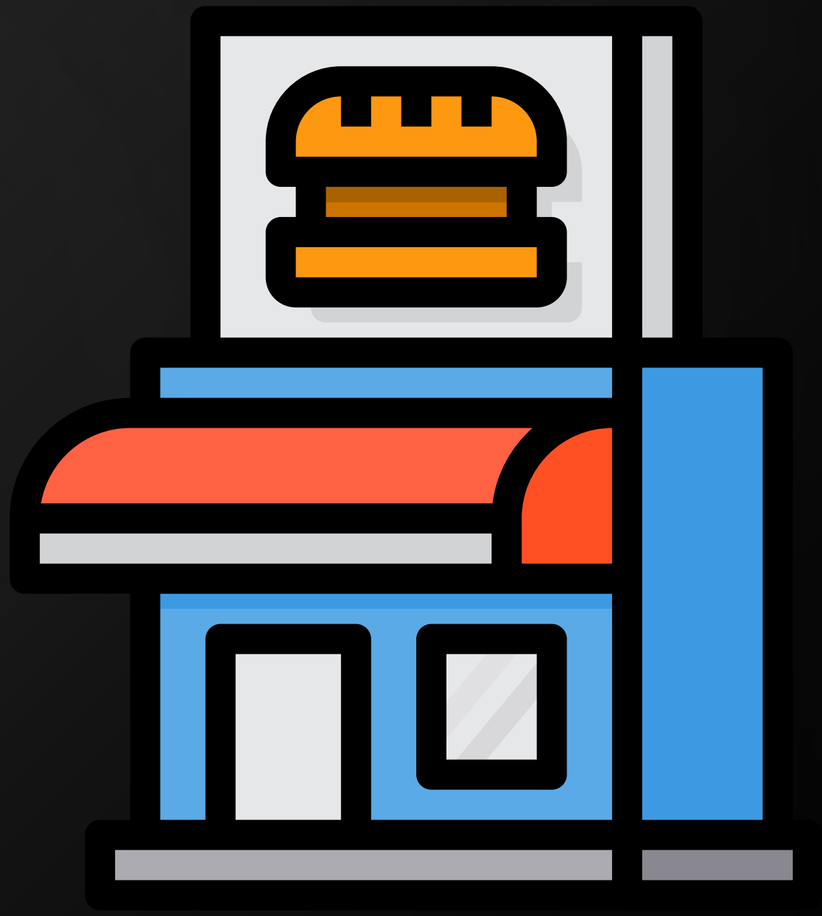
WLUG
COMMUNITY | KNOWLEDGE | SHARE

WHAT IS SERVER AND CLIENT?

- A server is a powerful device that stores and shares information or services with other computers over a network
- A client is a device that requests and receives information from server



SERVER AND CLIENT



WLUG
COMMUNITY | KNOWLEDGE | SHARE

WHAT IS USER-INTERFACE?

A user interface (UI) is how you communicate with a computer or device

WLUG
COMMUNITY | KNOWLEDGE | SHARE

CLI

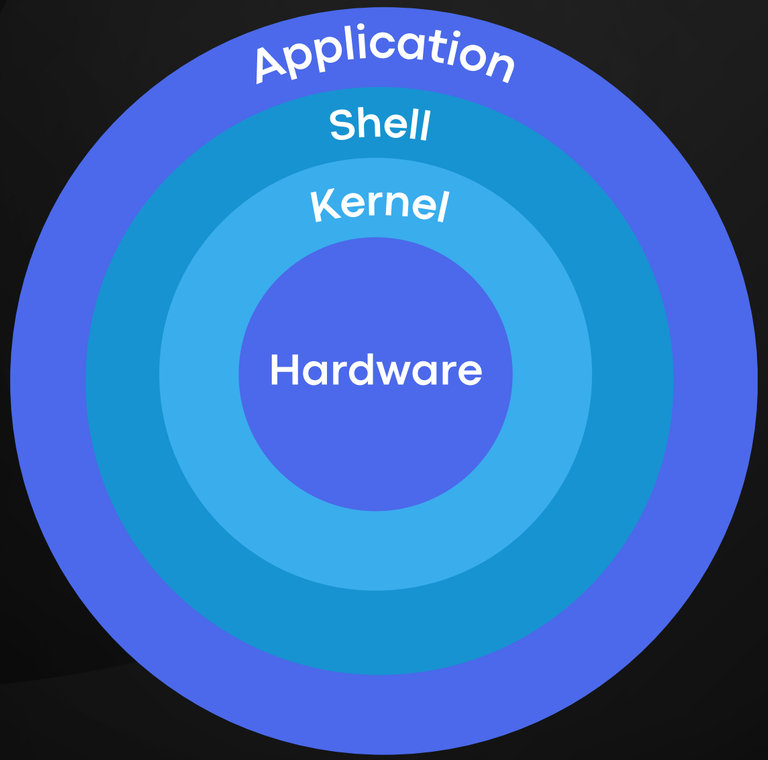
- Text-based interface
- Users type commands into a terminal
- In CLI, the information is shown or presented to the user in plain text and files

GUI

- Visual elements such as windows, buttons, and menus
- Users interact with software or devices through clickable icons
- Easier to use than CLI, especially for novice users

WHAT IS A SHELL?

- A Shell refers to a command-line interface or a text-based user interface that allows a user to interact with an operating system or a computer system by typing commands



Introduction to SSH

- SSH stands for Secure Shell
- SSH is a protocol, not a product. It is a specification of how to conduct secure communication over a network

Introduction to SSH

- Protocols are denoted with dashes: SSH-1, SSH-2, etc.
- Client programs are in lowercase: ssh, ssh1, ssh2, etc.
- SSH-based products: Products that implement the SSH protocol

HISTORY

Tatu Ylönen

1995

1996

SSH-1

SSH-2

1998

2000

2M+ USERS

WLUG

COMMUNITY | KNOWLEDGE | SHARE

WLUG
COMMUNITY | KNOWLEDGE | SHARE

USES OF SSH

Secure Remote Login

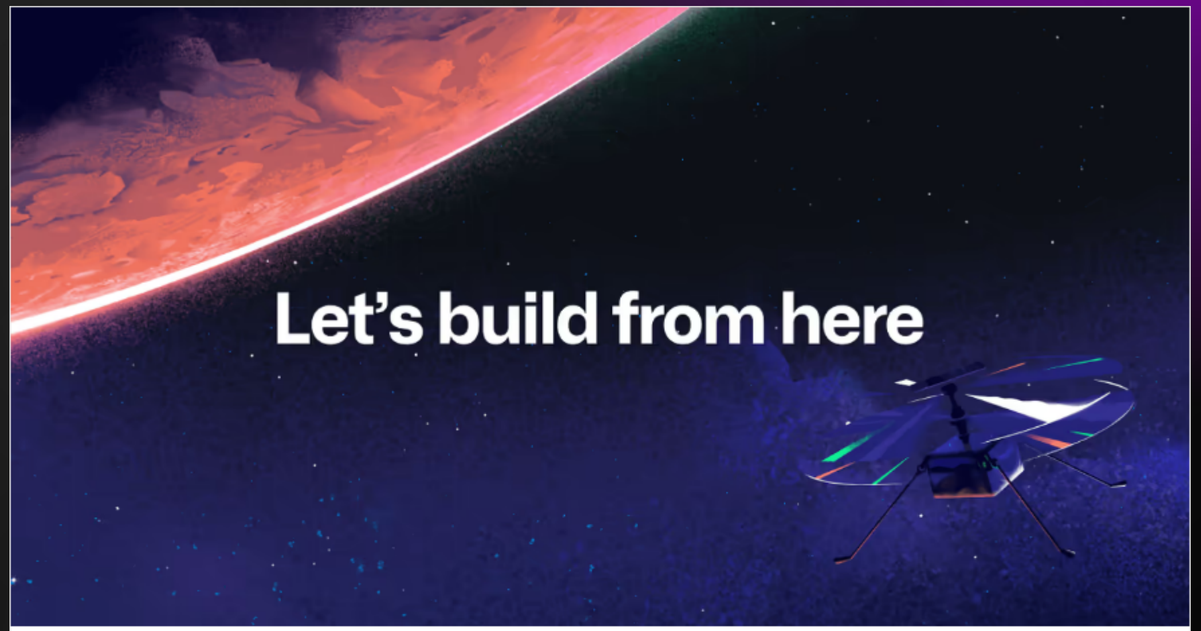
Secure File Transfer

USES OF SSH

Remote Command Execution

Tunneling and Port Forwarding

USES OF SSH



Let’s build from here

GitHub is where over 100 million developers shape the future of software, together. Contribute to the open source community, manage your Git repositories, review code like a pro, track bugs and fea...

GitHub

SSH COMPONENTS

Keys

- Public Key
- Private Key

Encryption

- Asymmetric
- Symmetric

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Encryption

- Encryption is like turning your message into a scrambled text
- It is an essential tool for protecting sensitive data and preventing unauthorized access

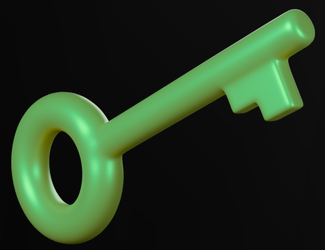
ENCRYPTION

- Encryption provides:
  - **Authentication:** Proving identity before granting access or permissions securely
  - **Integrity:** Ensuring data remains unchanged
  - **Confidentiality:** Keeping information private and restricted to authorized individuals securely

SYMMETRIC ENCRYPTION

WLUG
COMMUNITY | KNOWLEDGE | SHARE

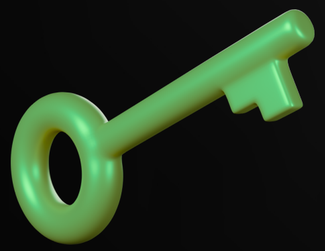
Jim



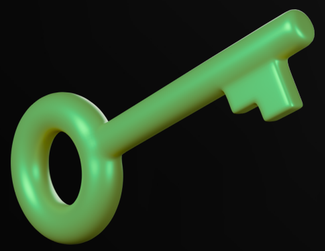
Emma

WLUG
COMMUNITY | KNOWLEDGE | SHARE

WLUG
COMMUNITY | KNOWLEDGE | SHARE

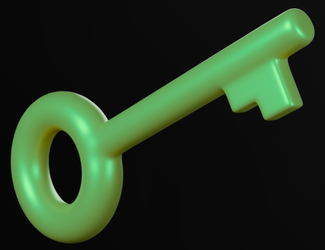


WLUG
COMMUNITY | KNOWLEDGE | SHARE



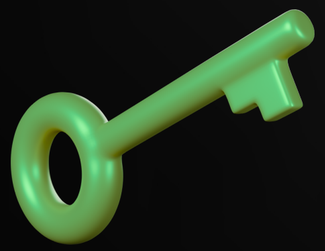
WLUG

COMMUNITY | KNOWLEDGE | SHARE

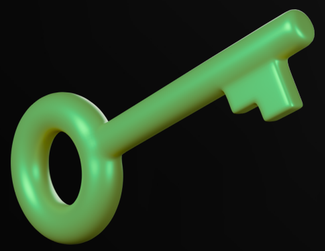


WLUG
COMMUNITY | KNOWLEDGE | SHARE

WLUG
COMMUNITY | KNOWLEDGE | SHARE

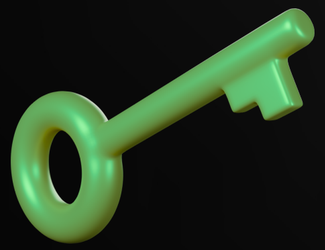


WLUG
COMMUNITY | KNOWLEDGE | SHARE

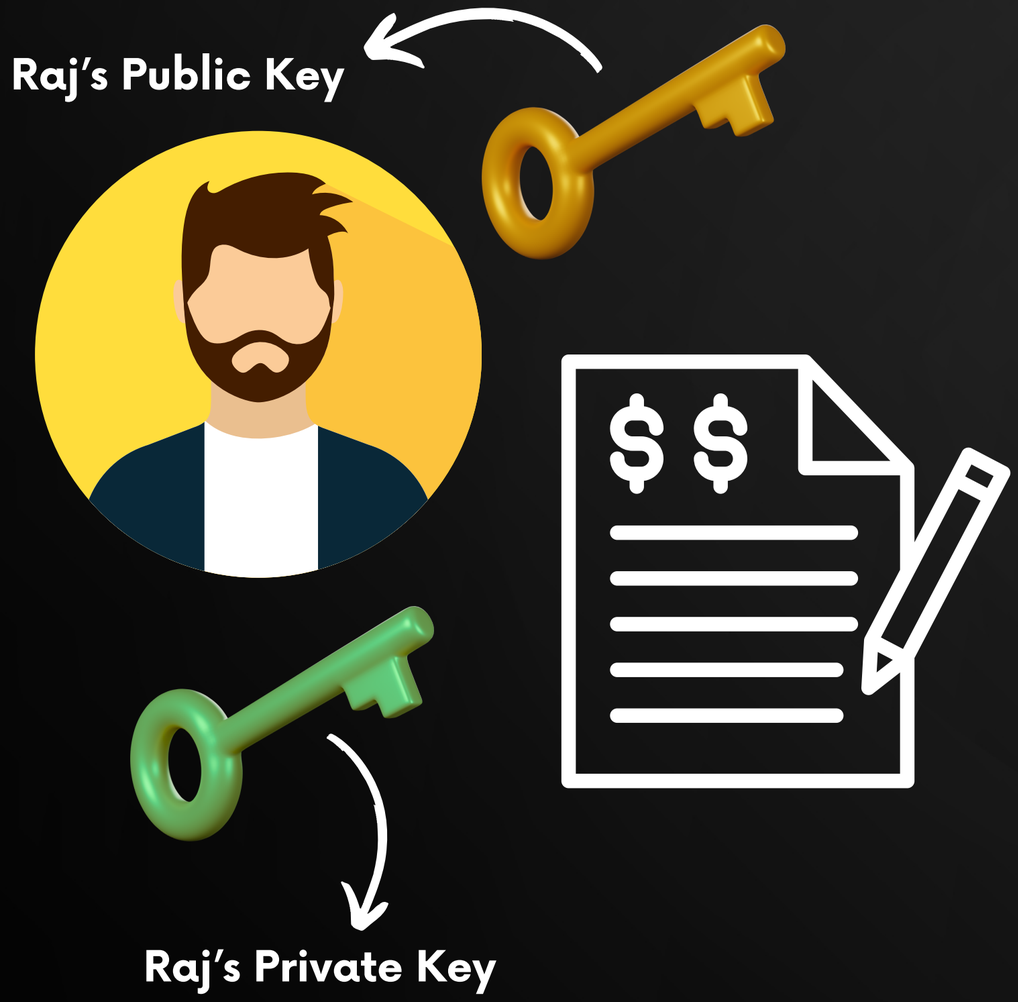


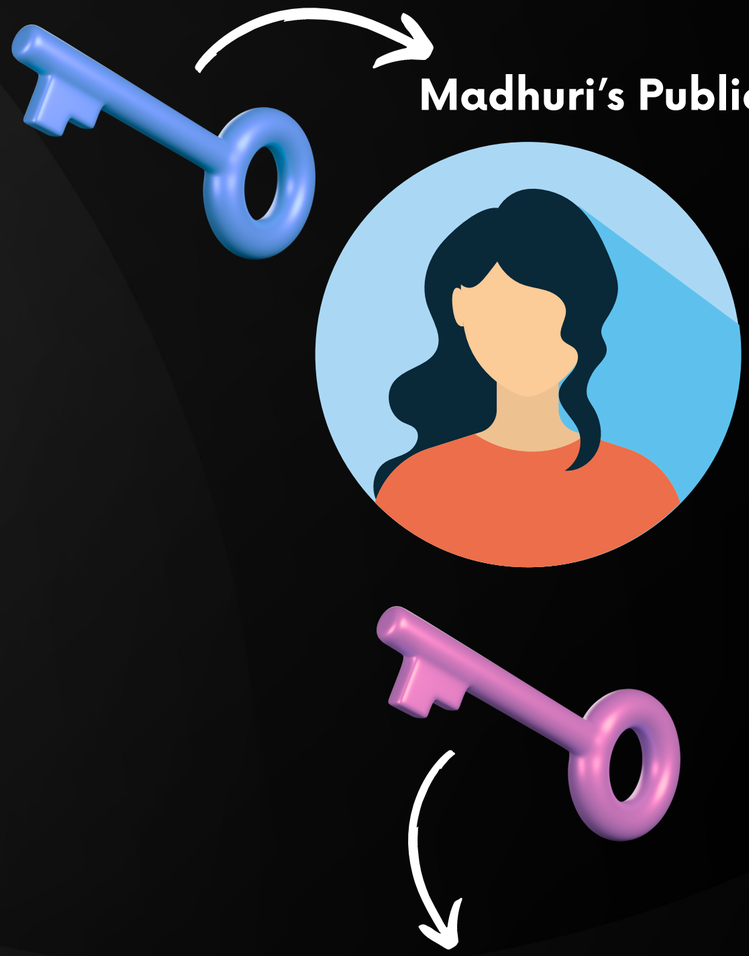
WLUG
COMMUNITY | KNOWLEDGE | SHARE

SYMMETRIC ENCRYPTION



ASYMMETRIC ENCRYPTION





PUBLIC AND PRIVATE KEYS

PUBLIC AND PRIVATE KEYS

PUBLIC AND PRIVATE KEYS

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PUBLIC AND PRIVATE KEYS

This is **Authentication!**

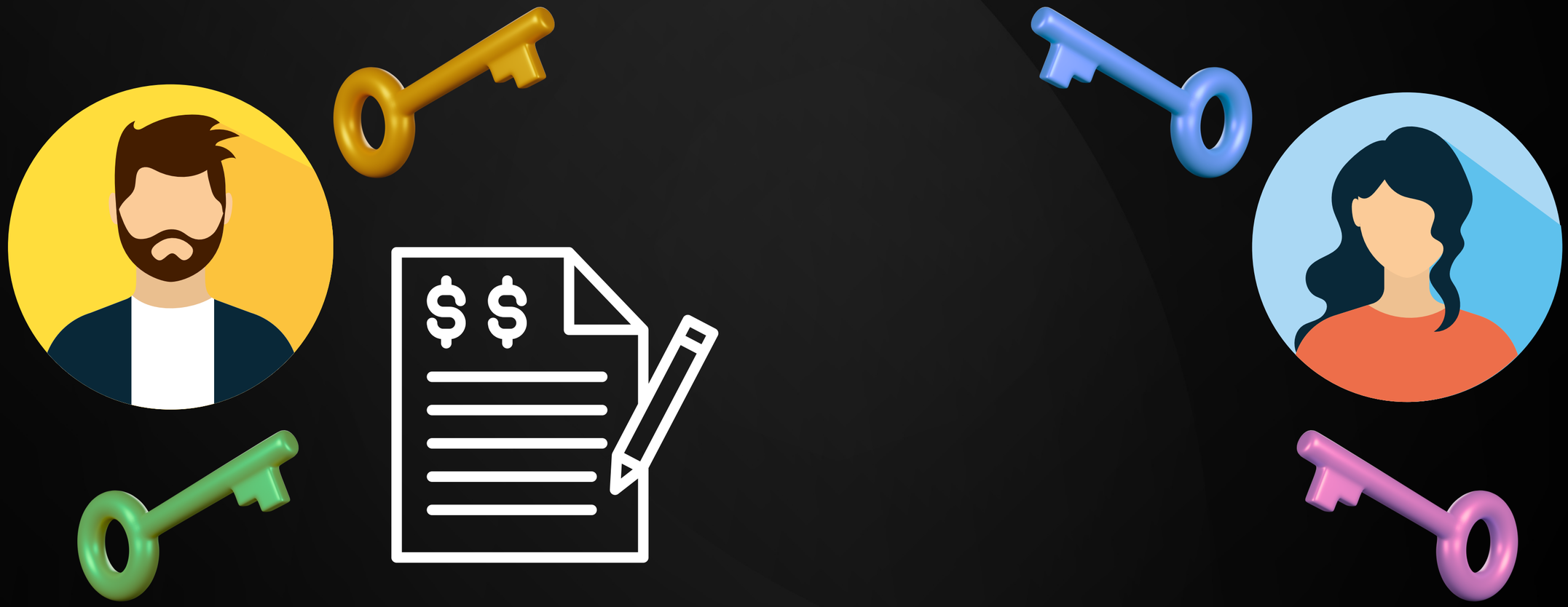
PUBLIC AND PRIVATE KEYS

The message was not modified
in transit

This is Integrity!

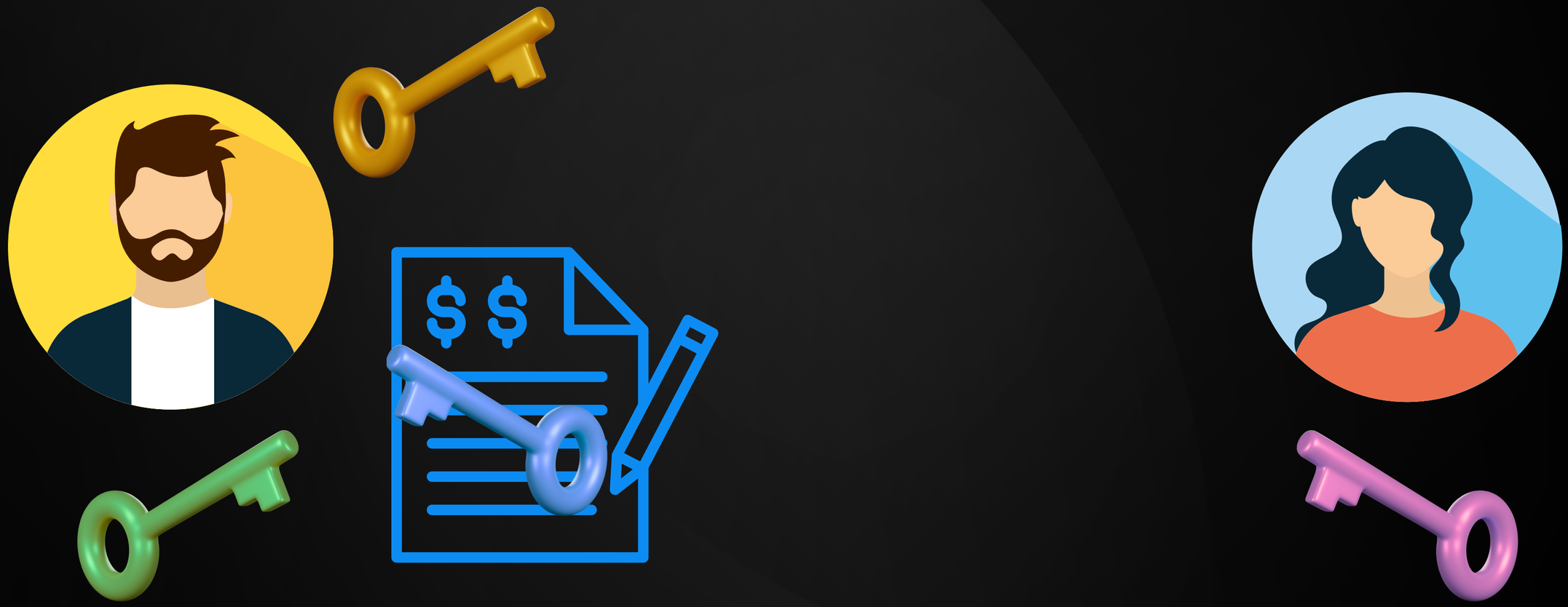
WLUG
COMMUNITY | KNOWLEDGE | SHARE

PUBLIC AND PRIVATE KEYS



WLUG
COMMUNITY | KNOWLEDGE | SHARE

PUBLIC AND PRIVATE KEYS



PUBLIC AND PRIVATE KEYS

WLUG
COMMUNITY | KNOWLEDGE | SHARE

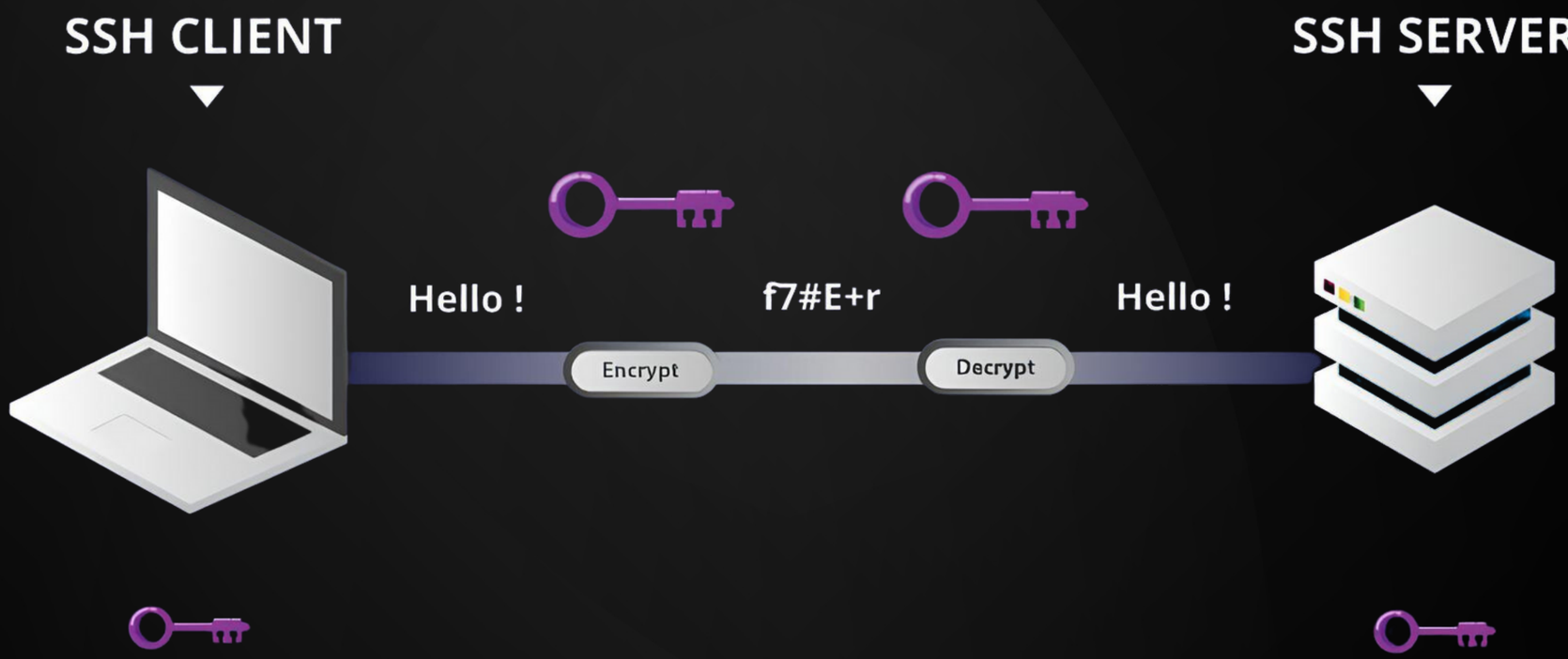
PUBLIC AND PRIVATE KEYS

PUBLIC AND PRIVATE KEYS

This is Confidentiality!

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SSH COMPONENTS



WLUG
COMMUNITY | KNOWLEDGE | SHARE

WHY OPENSSH?

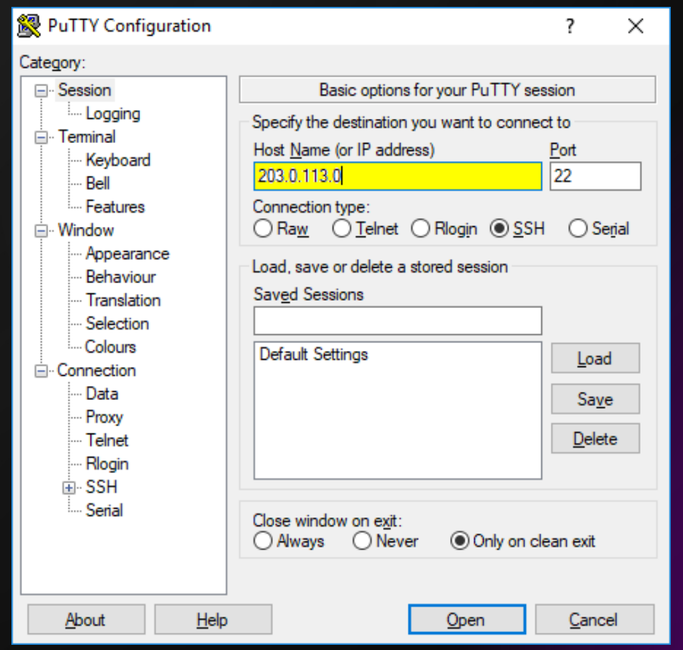
Open Source and Community-Driven

Cross-Platform Compatibility

Ease of Use

OTHER SSH IMPLEMENTATIONS

- **Dropbear:** Lightweight and efficient SSH server and client
- **PuTTY:** Popular and free SSH client for Windows
- **Tectia SSH:** Commercial SSH implementation



WLUG
COMMUNITY | KNOWLEDGE | SHARE

INSTALLING OPENSSH

SSH `sudo apt update`

SSH `sudo apt install openssh-client -y`

SSH `sudo apt install openssh-server -y`

SSH `sudo systemctl status sshd`

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Let's Connect !

Connection using SSH

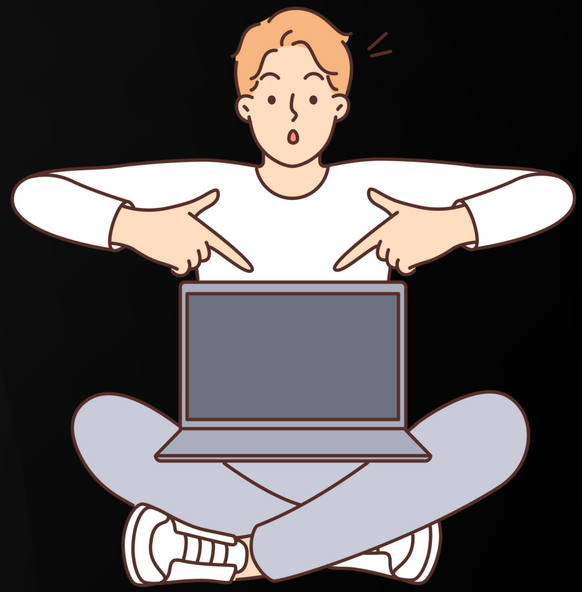
```
ssh server_user_name_@server_ip_address
```

To know user of your device

```
whoami
```

To get IP address

```
hostname -I
```



WLUG
COMMUNITY | KNOWLEDGE | SHARE

SECURE FILE TRANSFER

- Secure transfer of files between two computers using the SSH protocol
- Provides confidentiality
- Provides better security by protecting from tampering

SECURE COPY PROTOCOL

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SCP (Secure Copy Protocol):

SCP is a protocol that allows you to securely copy files and directories between two systems

SCP

```
scp localfile.txt username@remote_server:/destination
```

SECURE FILE TRANFER

SFTP (SSH File Transfer Protocol): SFTP is a more feature-rich protocol than SCP. It allows users to browse directories, upload, download, rename, and delete files on remote servers

SFTP `sftp username@hostname`

SFTP `put localfile.txt`

SFTP `get remotefile.txt`

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Configuring SSH

What is Configuration?

- Process of setting up and customizing the Secure Shell (SSH) protocol settings on a computer to control remote access and secure communication

Why do we need it?

- To easily work with ssh
- Managing multiple servers

Config file

- How to use it ?

Best Practices

WLUG
COMMUNITY | KNOWLEDGE | SHARE

- **Key Management**
  - Copying public key to remote server before logging in

```
ssh-copy-id -i path_to_pubKey root@ip_addr
```

  - Changing the type of key

```
ssh-keygen -t key_type
```

  - Adding the comment to key

```
ssh-keygen -t ed25519 -C "Your_comment"
```

- **Host Verification**
  - known_hosts

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SSH Agent

>>> Why do we need SSH Agent?

- **Install SSH Agent**

```
eval $(ssh-agent -s)
```

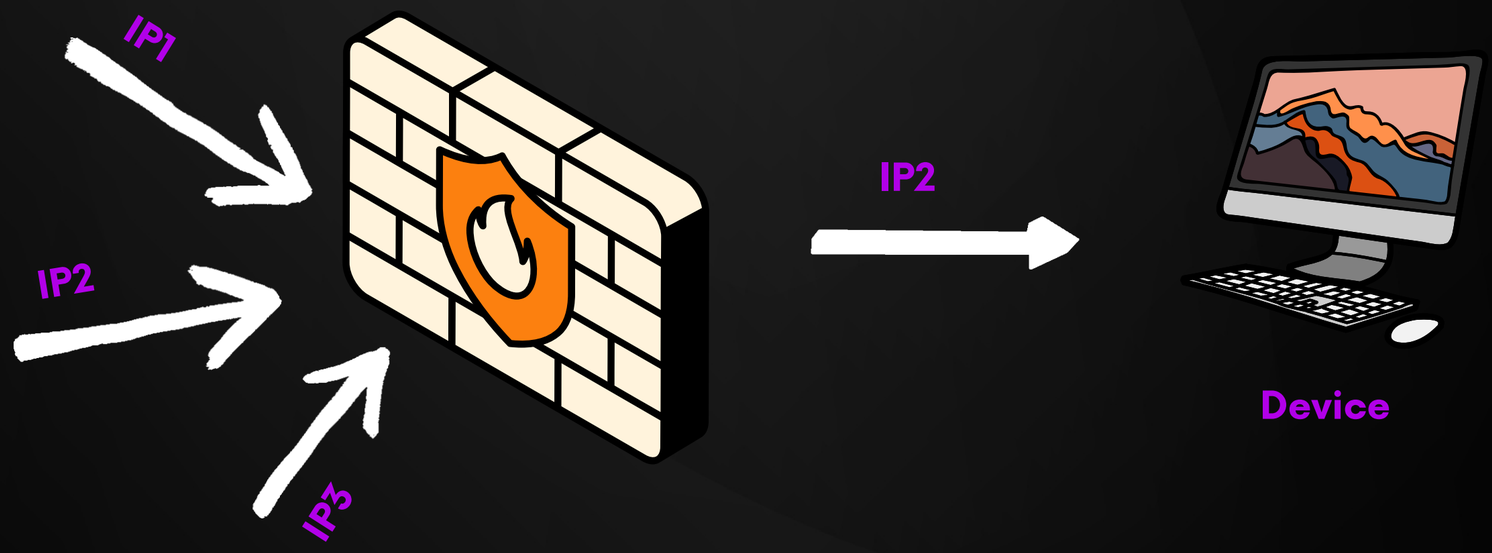
- **Add Private key to SSH Agent**

```
ssh-add ~/.ssh/your-key-file
```

SSH & Security

- **What is Firewall?**

  Digital security guard that blocks unauthorized access to your computer or network while allowing approved data to pass through



SSH & Security

- **Fail2Ban**
  - Tool to prevent Brute-Force attacks on server
- **Installing Fail2Ban**

```
sudo apt-get install fail2ban
```

- **Check status and configure fail2ban**
- Configuration consists of majorly 3 parts:
  - **maxretry** - Number of allowed failed attempts to login server
  - **findtime** - Given Time in which attempts are allowed
  - **bantime** - The time for which we want to ban the user

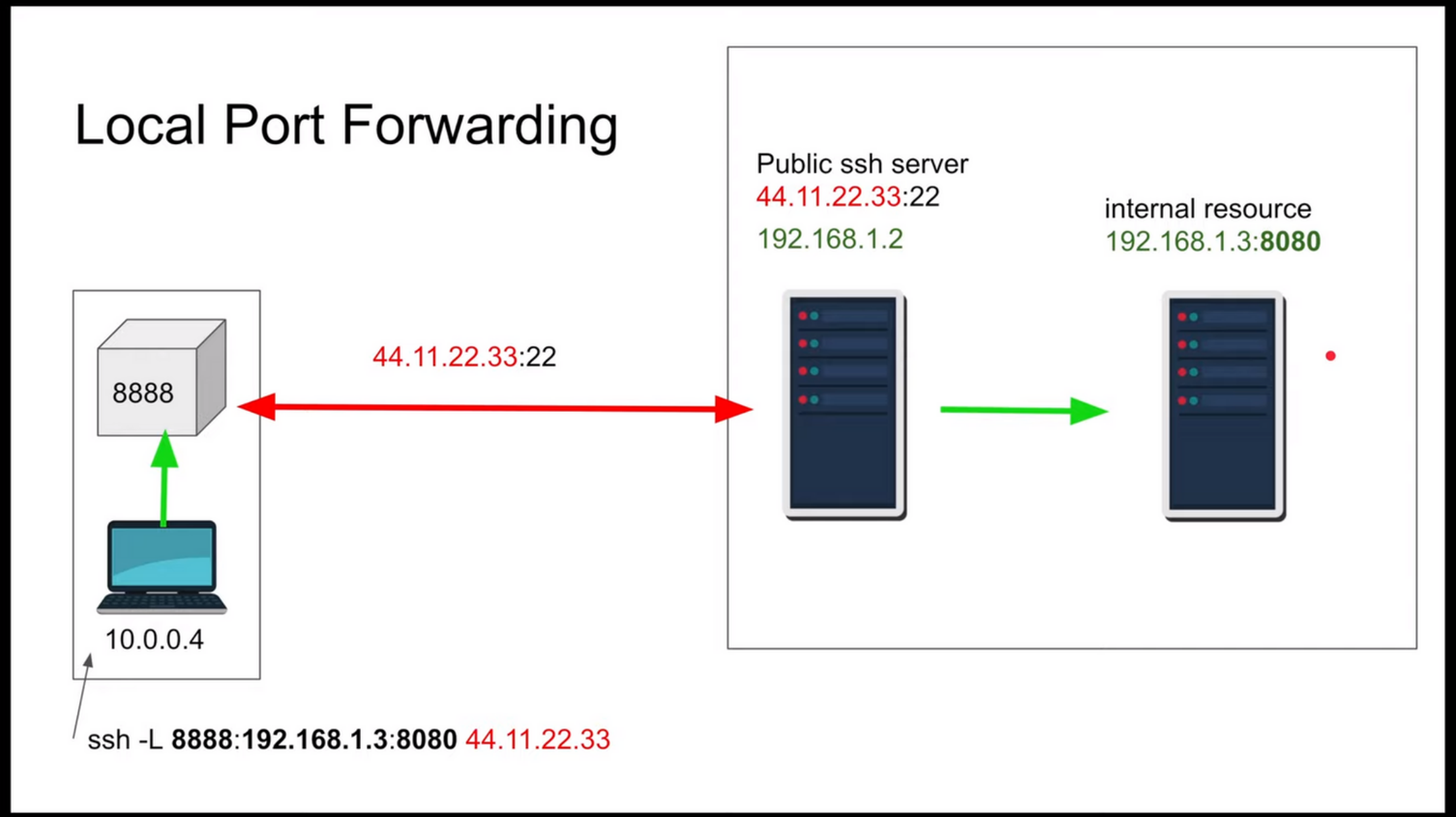
WLUG
COMMUNITY | KNOWLEDGE | SHARE

SSH Tunneling

- **What is Tunneling ?**
  - Bypassing through blocked port and and smuggling content
- **Local Port Forwarding**
  - I want to access the resources that I am not allowed to access
- **Dynamic Port Forwarding**
  - I want people to access the resources that they don’t have access to

SSH Tunneling

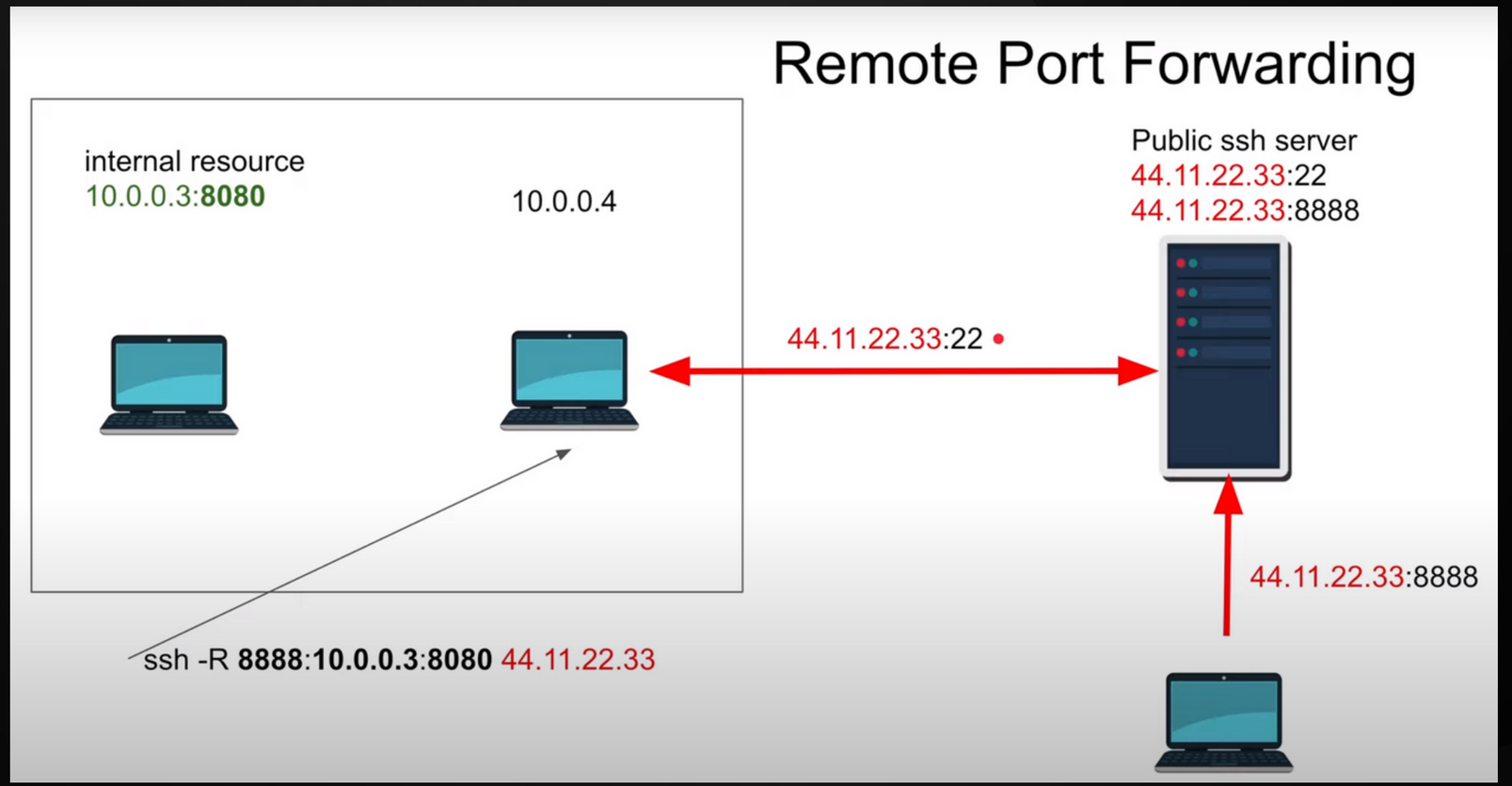
- **Local Port Forwarding**



WLUG
COMMUNITY | KNOWLEDGE | SHARE

SSH Tunneling

- **Dynamic Port Forwarding**



WLUG
COMMUNITY | KNOWLEDGE | SHARE

CONCLUSION

- SSH (Secure Shell) is a secure protocol for remote communication
- Encryption, public key, private key
- SSH configuration to improve security
- Remote server administration
- Secure file transfer
- Port forwarding

WLUG
COMMUNITY | KNOWLEDGE | SHARE

CONCLUSION

"Where secure connections are forged and data travels in the shadows of encryption, keeping the digital world safe"

WLUG

COMMUNITY | KNOWLEDGE | SHARE

THANK YOU

COMMUNITY | KNOWLEDGE | SHARE