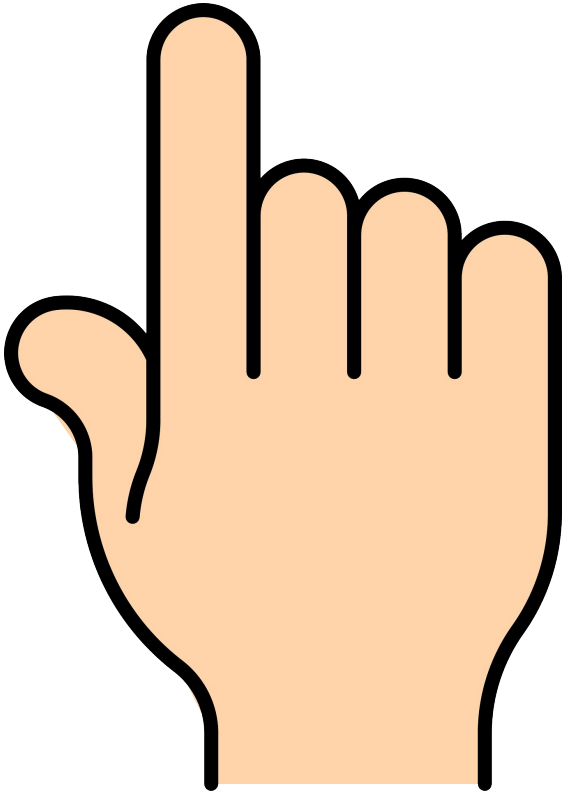
The Finger Protocol

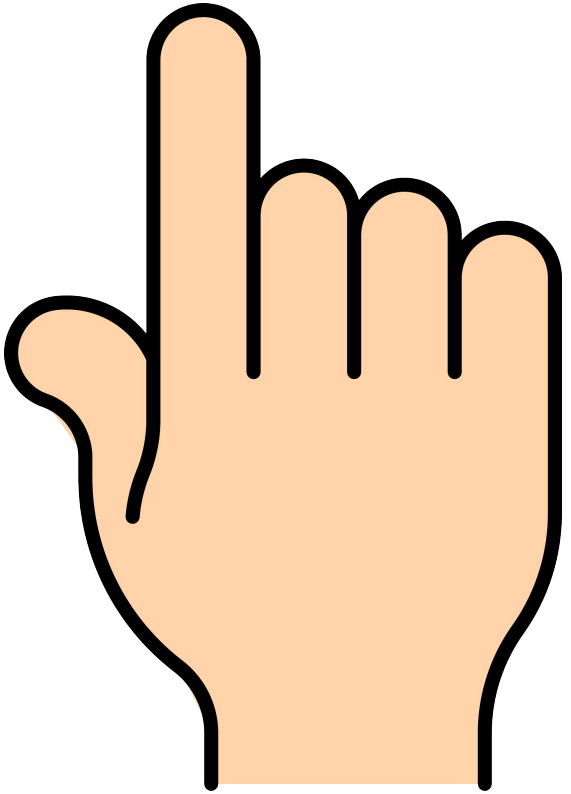
The Finger protocol is service that can be found on network servers. It can be used to retrieve user data from the server.



The Finger Protocol

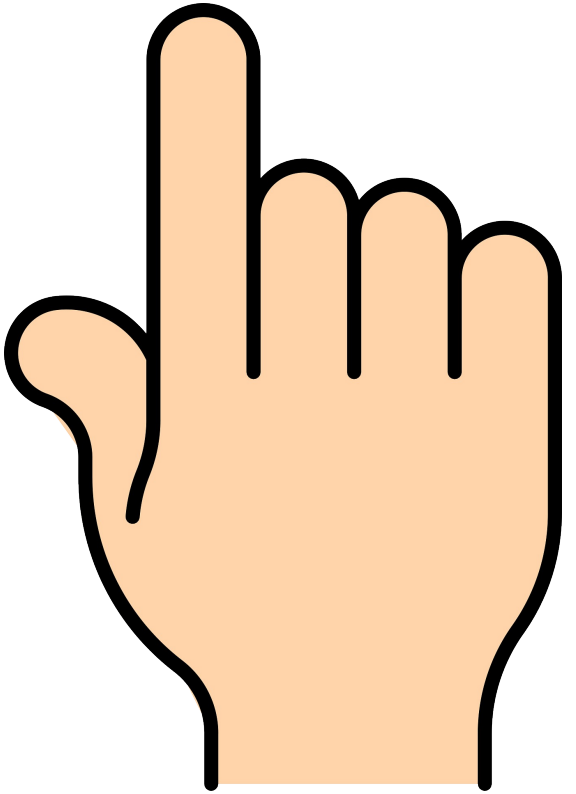
Data that can be gained from the Finger service can include:

- username and real name
- user login status
- home directory and shell
- contact info (address, email phone number, etc)
- **.plan** and **.project** files



The Finger Protocol

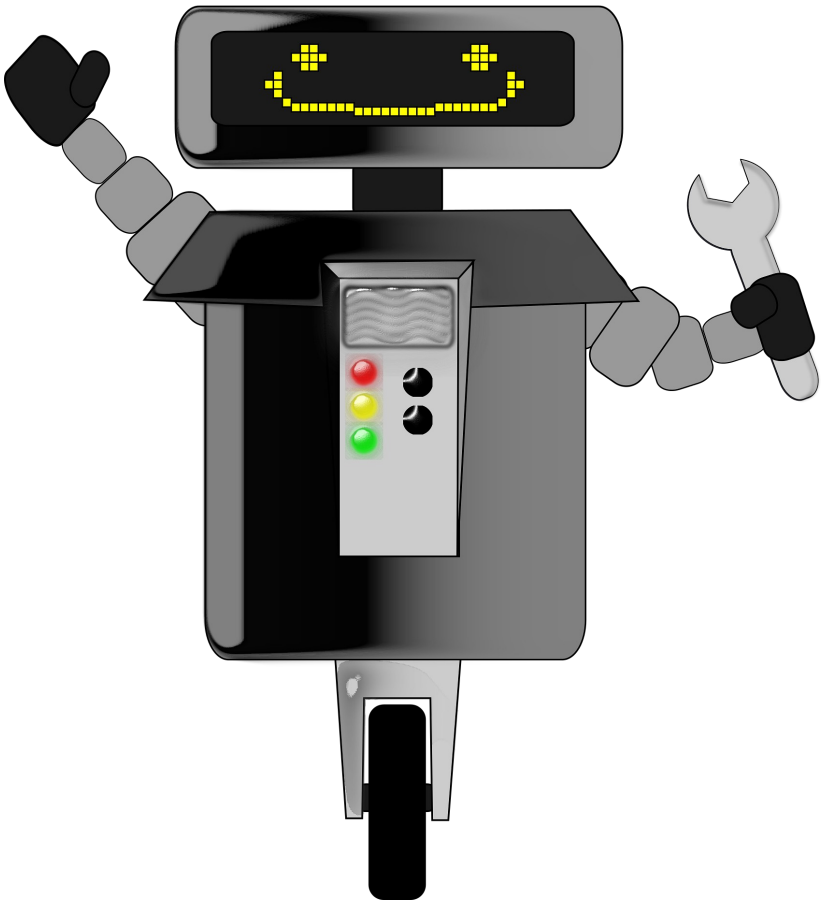
Finger is a service that was popular before the internet became popular, but it is rarely found in modern network environments, due to privacy converns.



Privilege Escalation
SUID Doas

Doas is a UNIX / Linux program that allows a user to run commands in the context of another user.

It is similar to the Sudo command, but Doas has a simpler setup process.



Privilege Escalation
SUID Doas

```
[redacted]:~$ cat /etc/doas.conf
permit nopass keepenv adam as root cmd /usr/bin/find
```

The configuration for the Doas program can be found in the /etc/doas.conf file.

Privilege Escalation
SUID Doas

```
[redacted]:~$ cat /etc/doas.conf
permit nopass keepenv adam as root cmd /usr/bin/find
```

For example, in this configuration, without providing a password, keeping the current environment variables, the **adam** user can run, as the **root** user, the **/usr/bin/find** command.

Privilege Escalation
SUID Doas

```
[redacted]:~$ cat /etc/doas.conf
permit nopass keepenv adam as root cmd /usr/bin/find
```

In this example, the user can run the Find command as root, so it can be used as a method of privilege escalation through Doas.

Privilege Escalation
Sudo Find

The Find command is used to locate files and directories on a filesystem that match specified parameters.

Privilege Escalation
Sudo Find

```
sudo find . -exec /bin/sh \; -quit
```

One feature of the Find command is the ability to run system commands on the files or directories that it finds, so if a user can run it with Sudo, it can be used to open a root shell with the above command.