Intro to *nix and Shells

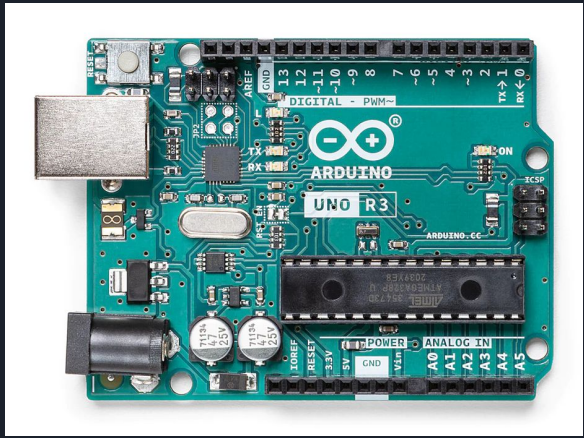
Level 0x00: The Shell

Quick Overview

- Basic Programming
  - C (and C++)
  - Python
  - Scripting (bash)
- Operating system concepts
  - User privileges
  - Networking
  - Memory
- Software Security Concepts
  - Crypto / Hashing
  - Disassembly / Reverse Engineering
  - How are bugs in software turned into exploits

Bare-metal / Embedded

- ATMEGA 328P Processor (AVR)
  - 32KB Flash (programmable memory)
  - 1 KB EEPROM
  - 2 KB SRAM
  - 1 MHz Clock
- No operating system
- Runs 1 program at a time
  - Assembly
  - C



This picture is 160 KB

Trivia

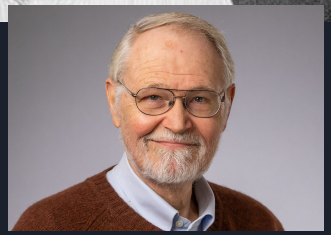
What is the highest selling single computer model of all time?

Interactive Kernel / DOS

- Commodore 64
  - 64 KB RAM
  - 8 KB Kernal
  - 4 KB Character Graphics
  - 8 KB Basic
- Microsoft DOS
- 1 Process at a time

```
A>dir command.com

 Volume in drive A is MS-DOS 3_30
 Directory of  A:\

COMMAND  COM     25276  12-23-90   2:37p
       1 File(s)     254976 bytes free

A>ver

MS-DOS Version 3.30

A>
```

Operating Systems - UNIX-like



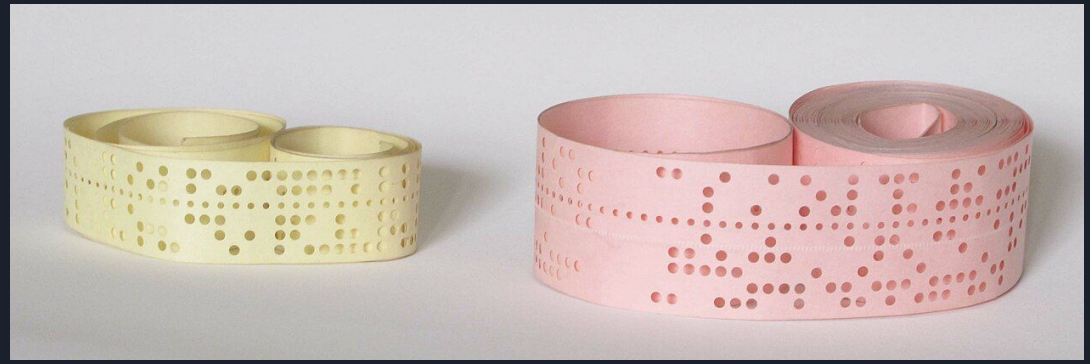
- Unix
  - AT&T Bell Labs in 1970s by Ken Thompson, Dennis Ritchie, Brian Kernighan
  - Examples include: BSD, HP-UX, Solaris, SGI Irix
  - Multi-tasking, multi-user, programming tools included
  - Unix philosophy: “Write programs that do one thing and do it well”
- OpenBSD / FreeBSD
  - University of California Berkeley open sources their Unix - permissive license
  - Also used by Mac OS, iOS, Playstation 3 (and newer)
- Linux
  - Created by Linus Torvalds, first posted to Usenet in 1991
  - RedHat, Suse, Debian, Ubuntu, Android
  - “I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones.”

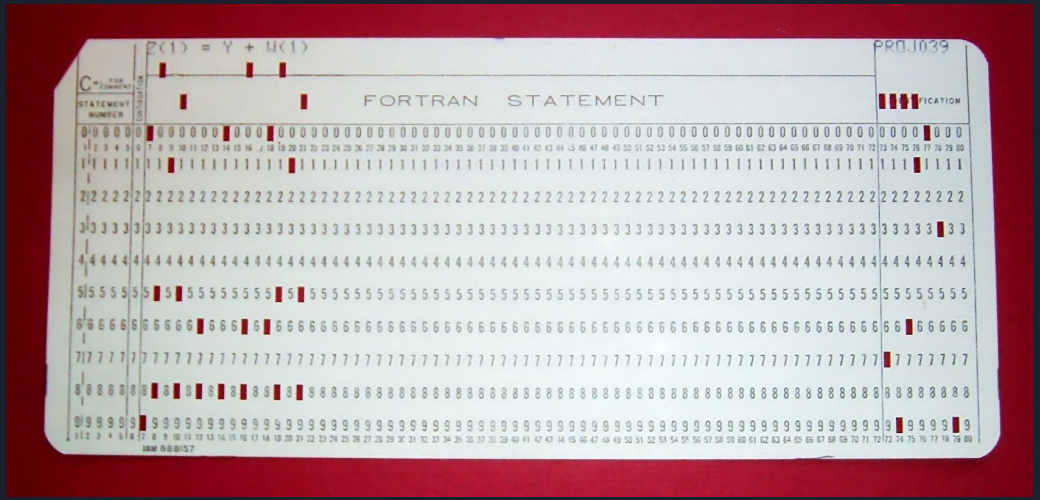
Early Interfaces

- Serial terminal / Teletype
- No graphics, just characters
- No mouse

Early Storage

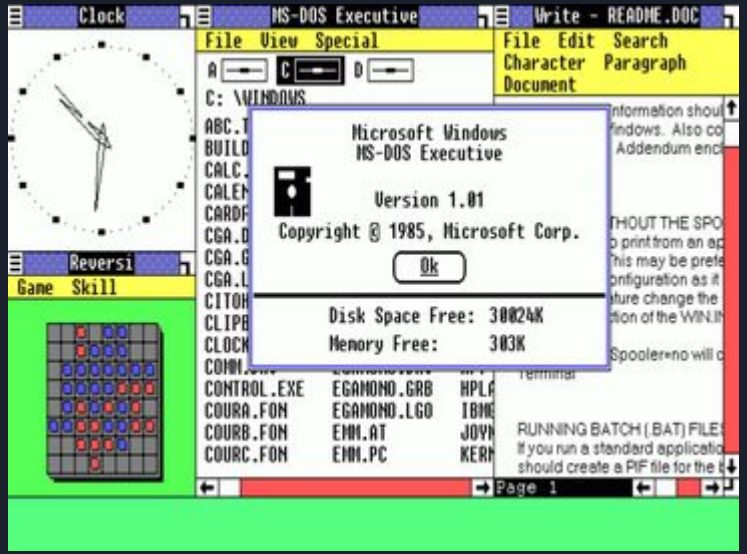
- Paper tape
- Punch card
- Analog magnetic tape
- Magnetic disks
- Optical disk





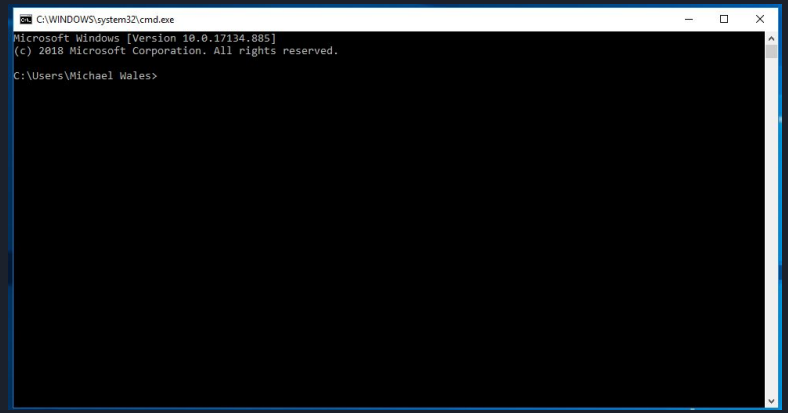
Operating Systems - GUI

- Xerox / PARC / Apple
  - Mouse, Window Systems, GUI conventions
  - Steve Jobs
- Windows (DOS Application)
  - Multiple applications
  - Resizable GUIs, Networking
- Windows 95/NT
  - Became core operating system
  - Long filenames
  - Start menu
  - 32-bit Only



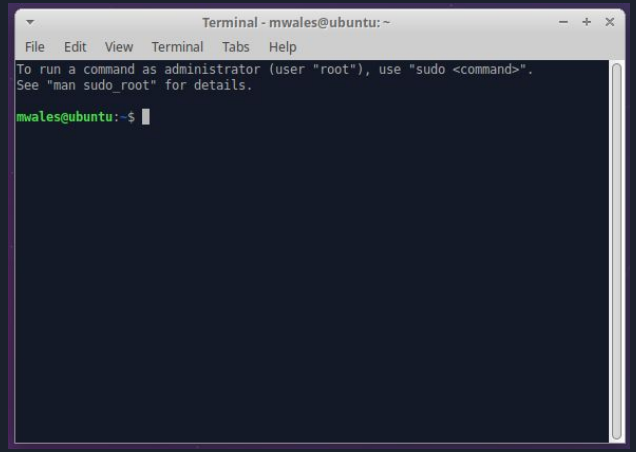
Windows Shell Basics

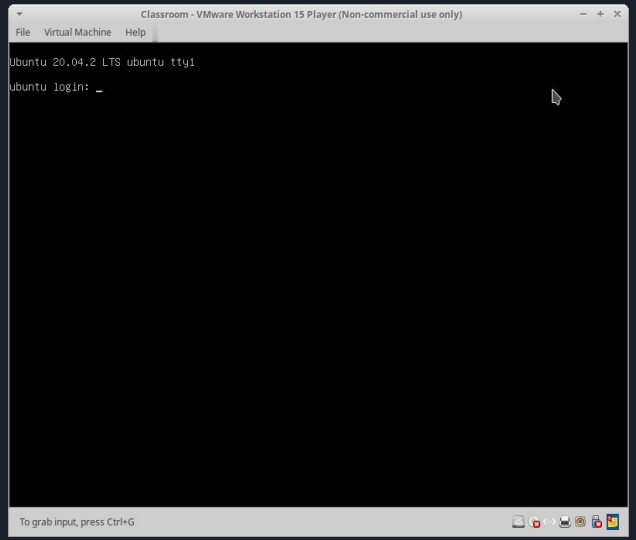
- Windows Basic Shell
  - Press Win+R to bring up Run dialog
  - Type cmd to open shell
  - Functional, but very basic
- Windows Alternative Shells
  - Powershell
  - WSL (Windows Subsystem for Linux)
  - WSL2



Linux Shell Basics

- Bourne Shell (sh) and Bash (Bourne Again Shell)
  - There are many many others
- Many ways to access the shell
  - GUI Shell Program (Terminal)
  - `/dev/tty1` text console
    - CTRL+ALT+F1 (through F6 typically)
    - CTRL+ALT+F7 restores GUI
  - Serial port
  - Remotely via SSH (or Telnet)





Filesystem

- Filesystem is usually a directory of files on your SSD / hard disk
  - Windows: C: D: (drive letters)
  - *nix: / /mnt /media/cdrom
- Each directory can have thousands of files and other directories

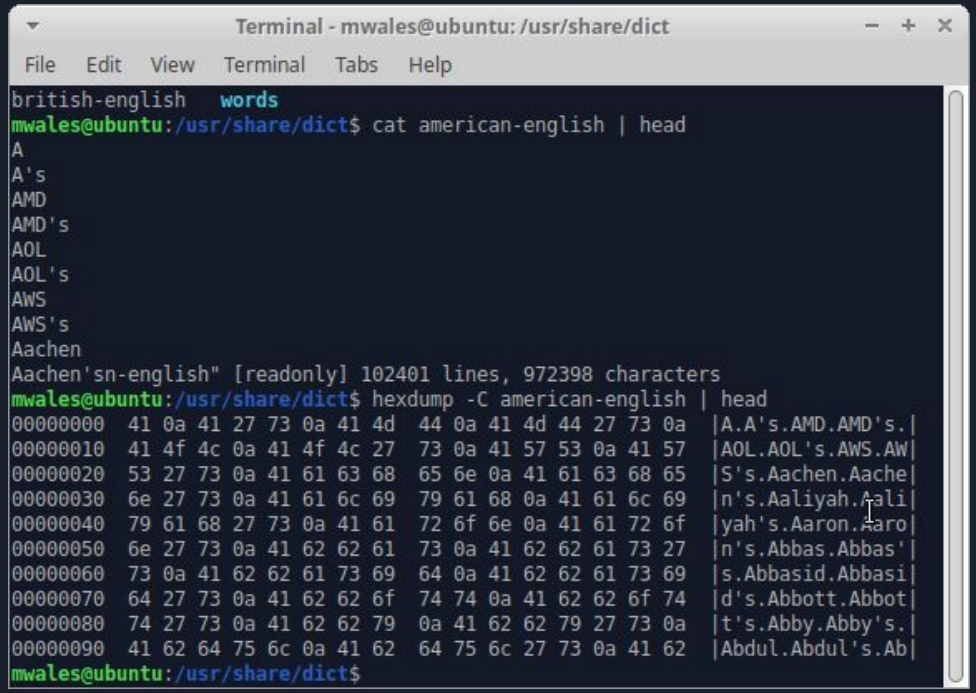
Linux Command	Windows/DOS Command	Explanation
`pwd`	`cwd`	Present working directory
`ls`	`dir`	List contents of a directory

Directory Commands

Linux	Windows / DOS	Explanation
`mkdir DIRECTORY`	`mkdir`	Makes a new directory
`cd DIRECTORY`	`cd`	Changes to a subdirectory
`cd ..`	`cd ..`	Changes to the parent directory
`rmdir DIRECTORY`	`rmdir`	Removes a directory (must be empty)
`tree`	`dirtree`	Lists all files / subdirectories

Files

- Common contents of a file
  - Text
  - Executable Programs
  - Databases (SQL)
  - Compressed Archive
  - Images
  - Word document
    - Compressed Archive
    - Text
    - Images

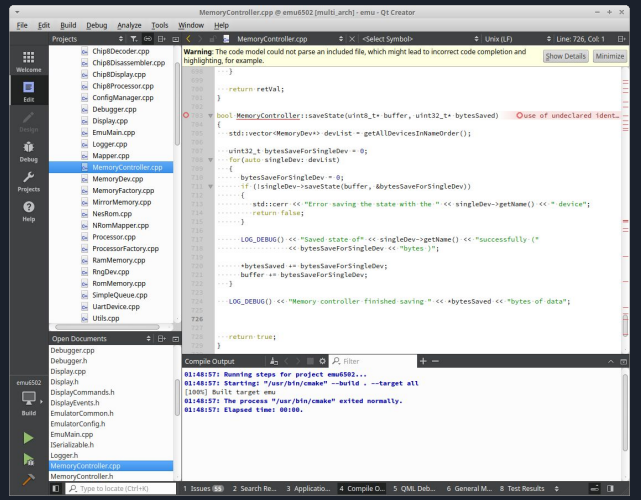


File Commands

Linux	Windows / DOS	Explanation
`touch FILE`	`copy con FILE`	Creates a blank file
`cat FILE`	`type FILE`	Displays contents of a file
`head FILE`		Displays beginning of a file
`tail FILE`		Displays ending of a file
`hexdump -C FILE`		Displays contents of a binary
`file FILE`		Tells you what type of a file

Editors

- GUI
  - Simple: write text, save to a file
    - Gedit, Mousepad, Notepad
  - Coding: automatic coloring, auto-complete
    - Geany
    - Sublime ($)
    - Atom
  - IDE: integrated development environment
    - Qt Creator
    - Visual Studio
    - CLion
- Command Line
  - nano, pico
  - vi / vim, emacs



File Commands

Command	Explanation
`strings FILE`	Prints out printable strings of a binary file
`sort [FILE]`	Prints lines in alphabetical order
`uniq [FILE]`	Removes redundant lines out output
`wc [FILE]`	Counts number of words in a file
`dos2unix / unix2dos [FILE]`	Converts file line endings
`more / less [FILE]`	Shows output 1 page at a time
`grep needle [FILEs]`	Searches for a string

Standard Input / Output

- 3 file descriptors open by CLI application
  - 0 = stdin (standard input)
  - 1 = stdout (standard output)
  - 2 = stderr (standard error)
- Pipes (|) can be used to connect output from one application to input of another application

```
strings somefile | grep -i password

cat logfile | sort | unique
```

I/O Redirection

- Using "`> file.txt`" after a command causes output from stdout to be redirected into a file
  - You won't be able to see it on screen
  - stderr will still be displayed
- Using "`2> file.txt`" after a command causes stderr to be redirected into file
- Using "`> file.txt 2>&1`" causes both to be redirected
  - Order matters!
- `tee` will write standard output to a file and also write it to the screen
  - Ex: `./myprogram arg1 arg2 | tee logfile.txt`
- >> will append to existing file, > overwrites it

Shell scripts

- A series of commands in a text file
  - Linux
    - Can start text file with #! (shebang) and make executable
    - Can call interpreter directly
  - Windows
    - .bat (batch) files
    - Windows Power Shell
- Can take arguments ($1, $2)
- Number of arguments ($#)
- Command Substitution (not just for scripts)
  - `echo “There are `ls *.txt | wc -l` files in this directory”`
  - `echo “There are $(ls *.txt | wc -l) files in this directory”`

Executable Files

- Linux - permissions bits
  - Permission bits for user, then group, then others
  - r = read, w = write, x = executable
  - `$ ls -l`

```
-rwxrwxr-x 1 mwales mwales 16784 Feb  1  2023 a.out
-rw-rw-r-- 1 mwales mwales    26 Feb  1  2023 flag.txt
-rwxrwxr-x 1 mwales mwales  3969 Feb  3  2023 judge.py
-rw-rw-r-- 1 mwales mwales   330 Feb  2  2023 solution.c
```

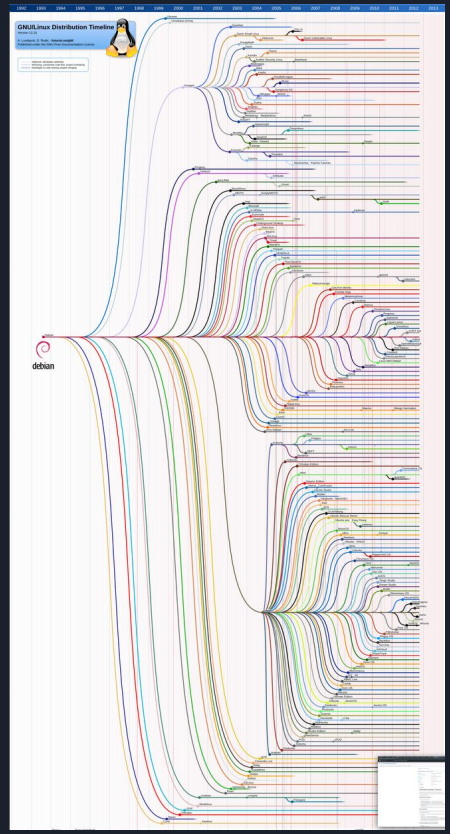
  - `chmod` can change file permissions
- Windows - file extension
  - .bat (batch) and .cmd (command) script files
  - .exe and .com binary files
  - Many others
-

Linux Strengths

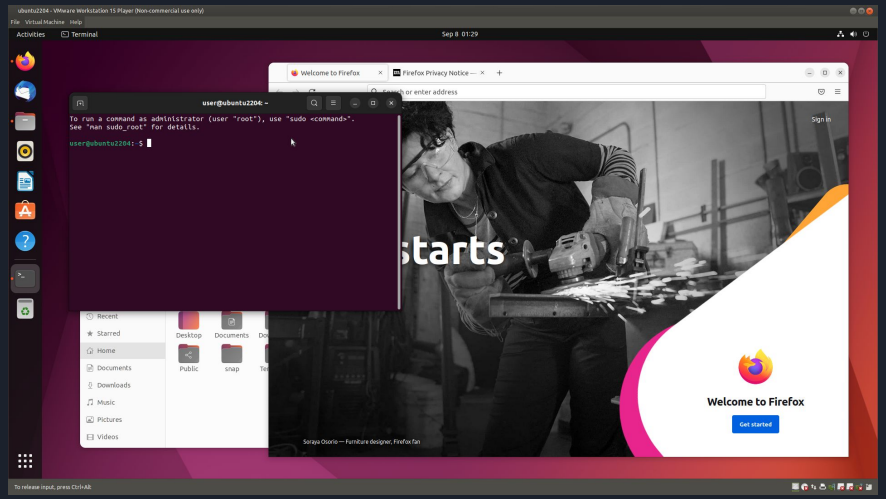
- Command Line First
  - Everything can be done via command line
  - Easy to automate
  - Remote access
- Live Versions
  - Knoppix / Tails
- Customization / Open Source
  - Kernel is fully transparent
  - Easy for anyone to add to kernel
  - User space is fully customizable (Steam Deck)
- Package Managers
  - Easy / fast to add other open source tools / development packages

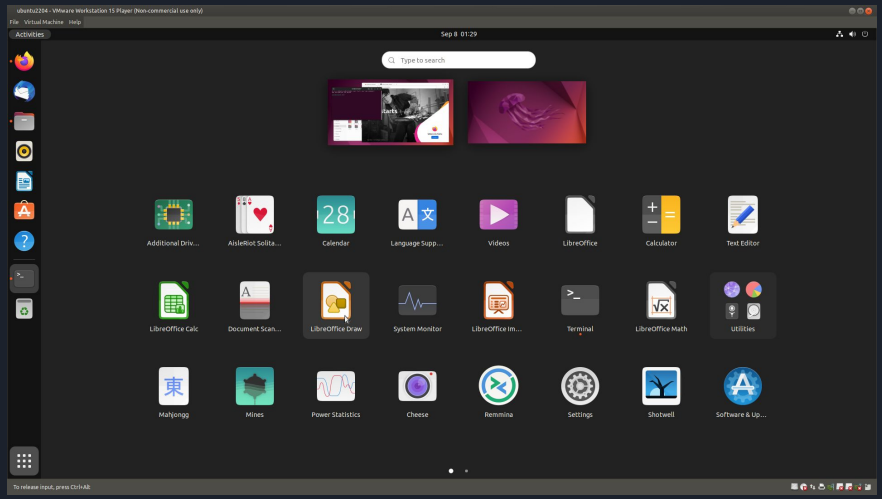
Ubuntu

- Child / Fork of Debian Linux
- Ubuntu provides:
  - Software repository with > 20,000 packages (apps, libraries)
  - Apt package manager
    - Installs new packages
    - Updates packages
    - Removes packages
- Ubuntu has many flavors
  - Which desktop manager used by default
  - Which applications used by default
  - Custom theming
- Releases every 6 months
  - LTS every 2 years. 22.04 is current LTS

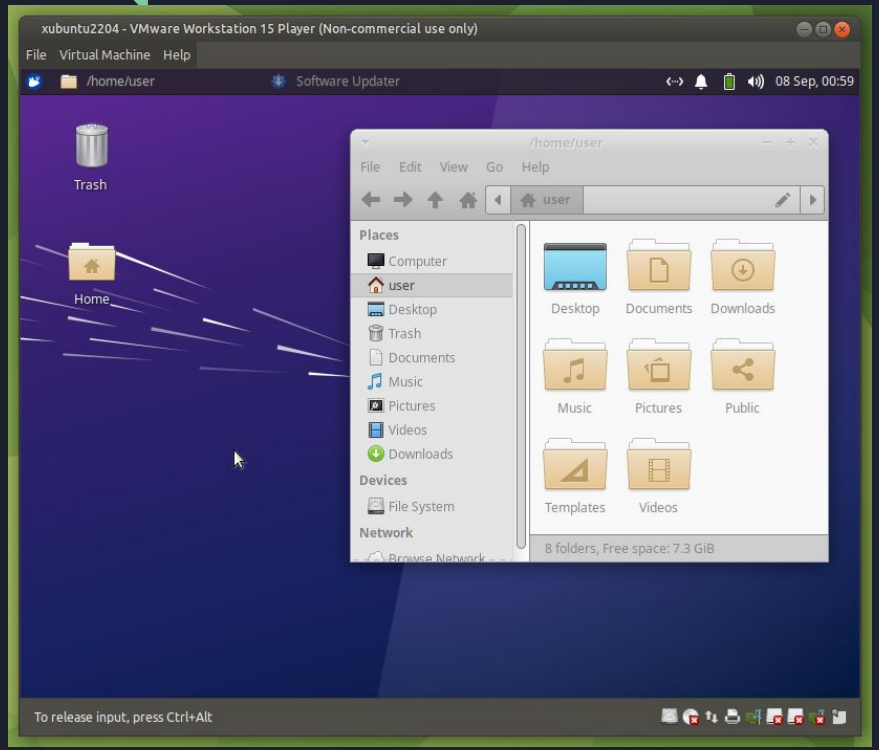


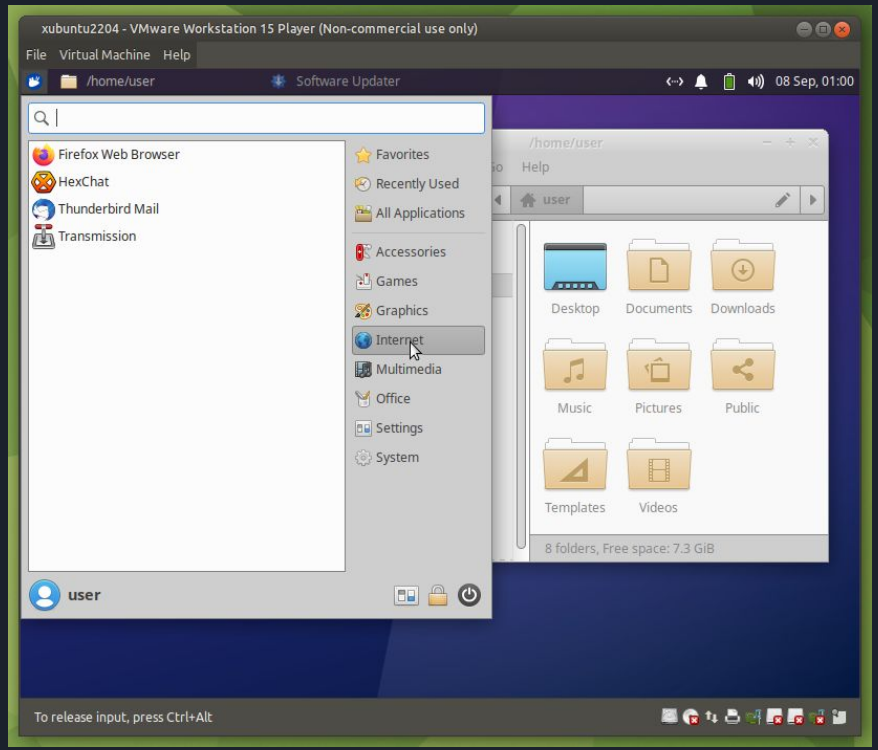
“Vanilla” Ubuntu



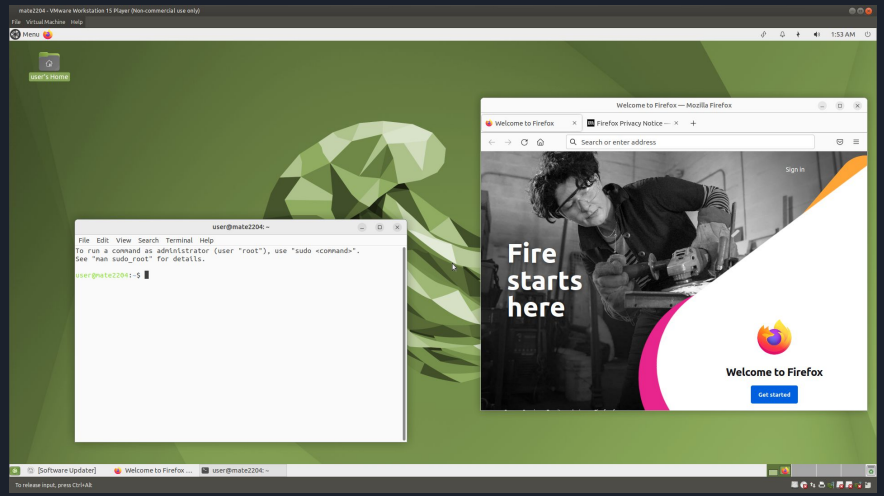


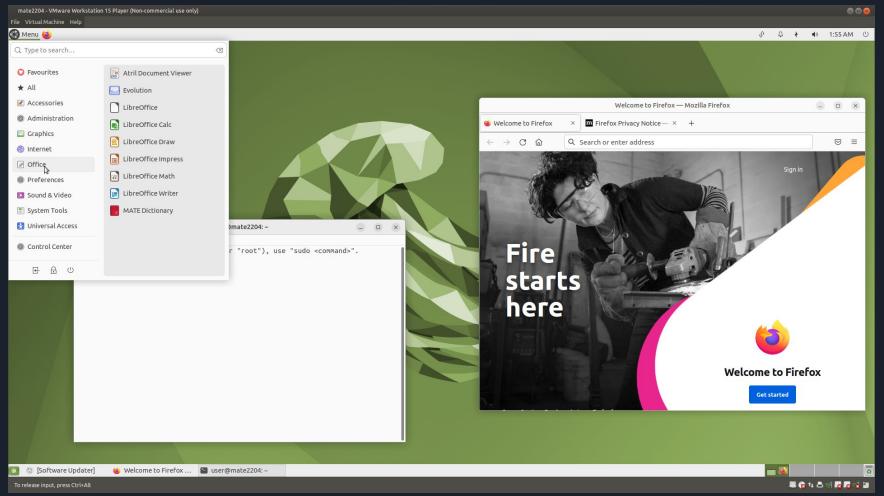
Xubuntu


xubuntu2204 - VMware Workstation 15 Player (Non-commercial use only)
File Virtual Machine Help
/home/user
Software Updater
08 Sep, 00:59
Trash
Home
/home/user
File Edit View Go Help
user
Places
Computer
user
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
8 folders, Free space: 7.3 GiB
To release input, press Ctrl+Alt


xubuntu2204 - VMware Workstation 15 Player (Non-commercial use only)
File Virtual Machine Help
/home/user
Software Updater
08 Sep, 01:00
Firefox Web Browser
HexChat
Thunderbird Mail
Transmission
Favorites
Recently Used
All Applications
Accessories
Games
Graphics
Internet
Multimedia
Office
Settings
System
user
/home/user
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
8 folders, Free space: 7.3 GiB
To release input, press Ctrl+Alt

Ubuntu MATE


Fire starts here
Welcome to Firefox
Get started


Fire starts here
Welcome to Firefox
Get started

Attributions

- Ken Thompson and Dennis Ritchie: from Wikipedia, public domain
- Linus Torvalds: Wikimedia Creative Commons Attribution-Share Alike 3.0
- Windows screenshot: https://en.wikipedia.org/wiki/File:Windows1.0.png
- Bits/Bytes: Frank Carmody
- Debian Family Tree: Andreas Lundqvist, Donjan Rodic from wikimedia.org