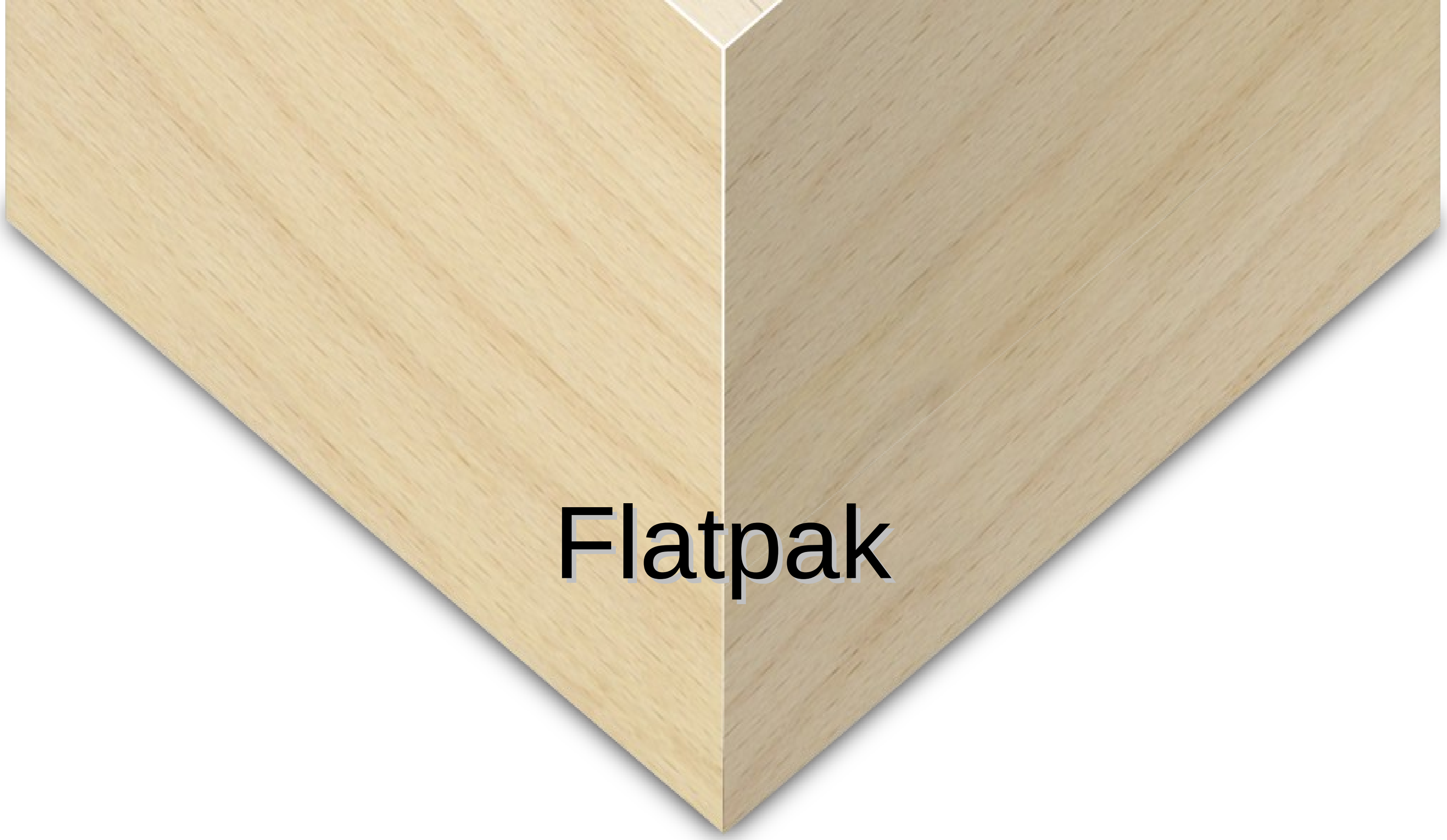


Flatpak

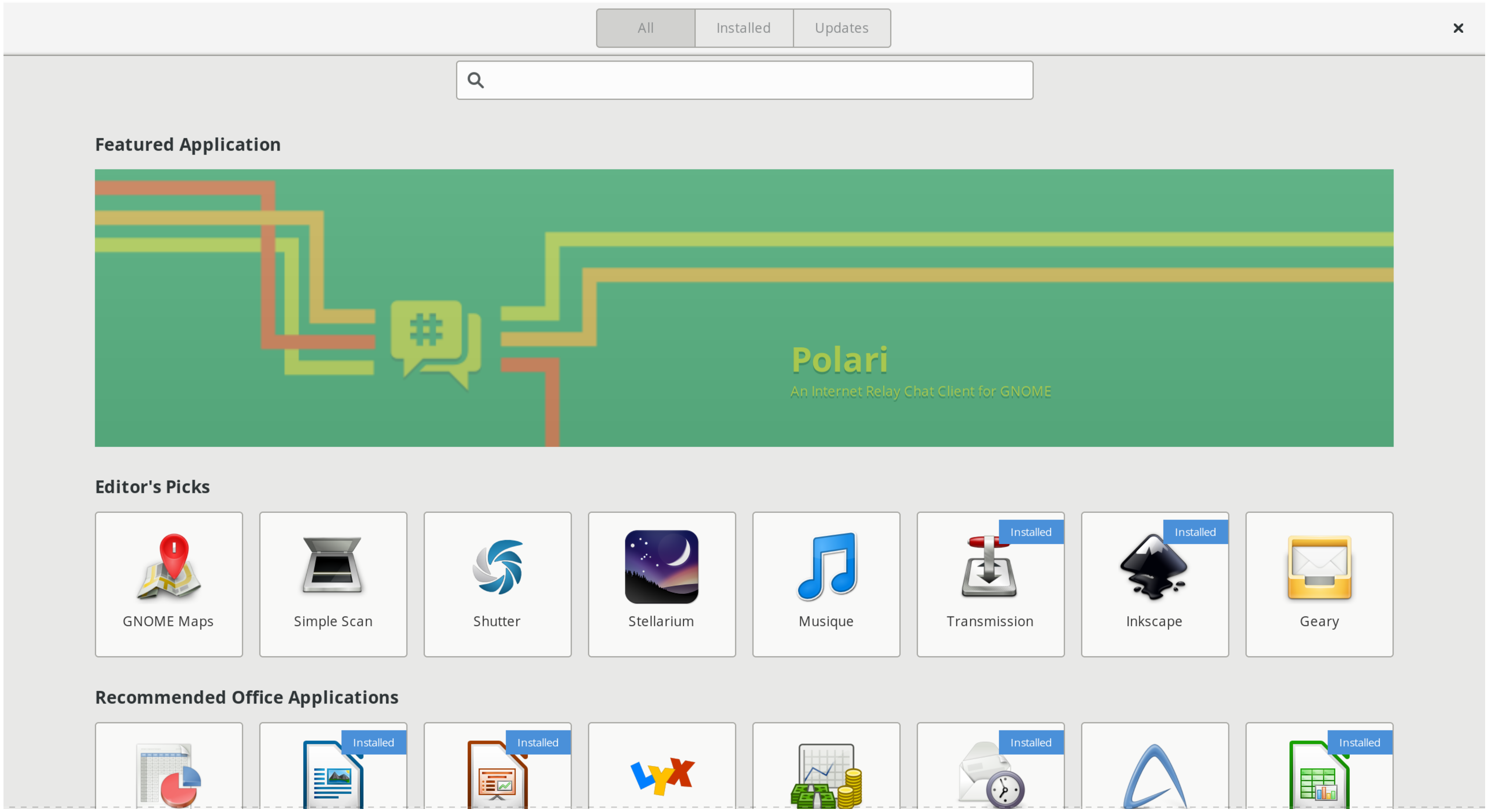
“Apps” on the Linux desktop

Alexander Larsson
Red Hat

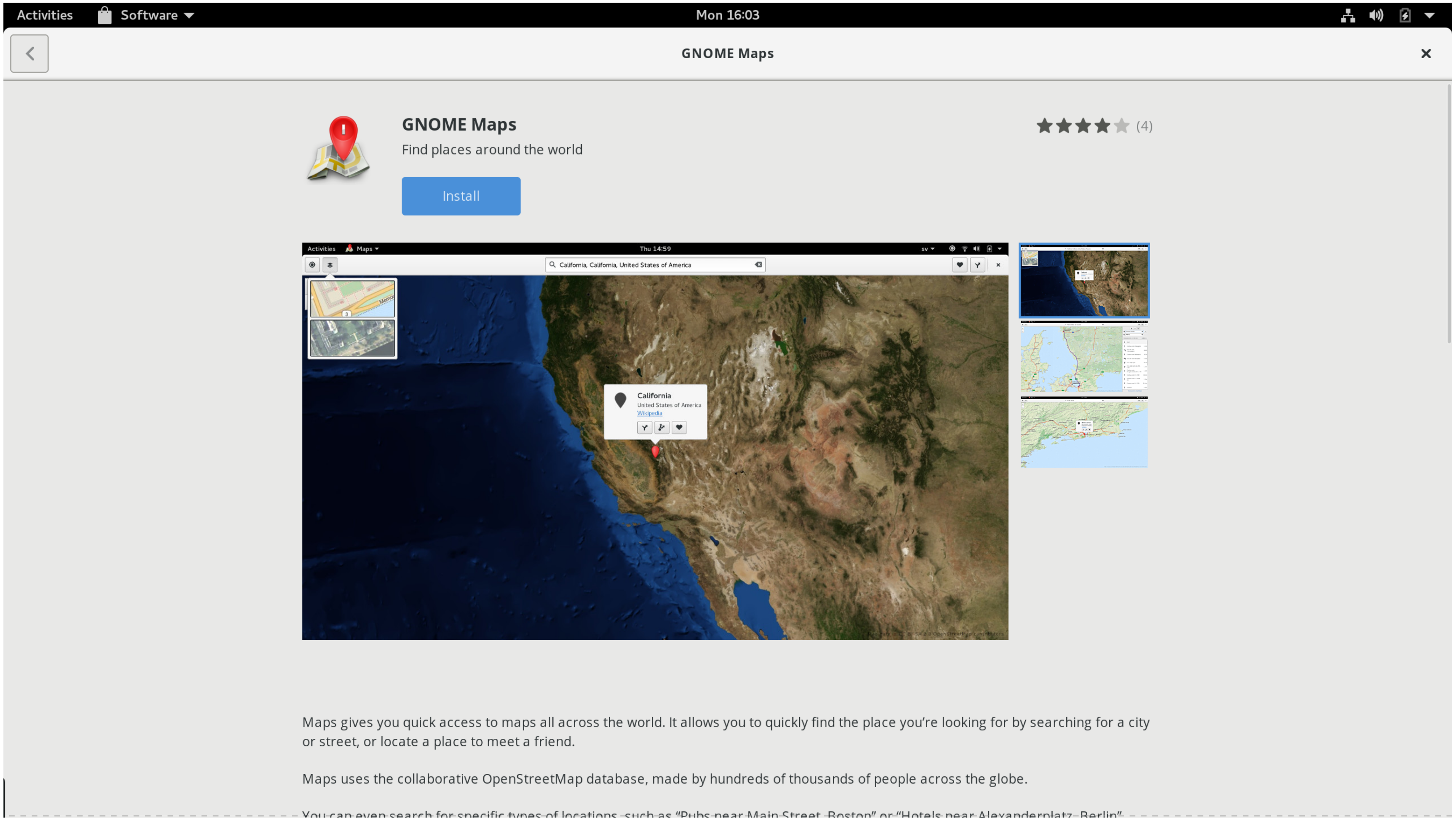
Flatpak Major Goals

- Cross-distro deployment and distribution
- Sandboxing applications
- Shorter distance between developers and users

Using Flatpak



Using Flatpak (cont)

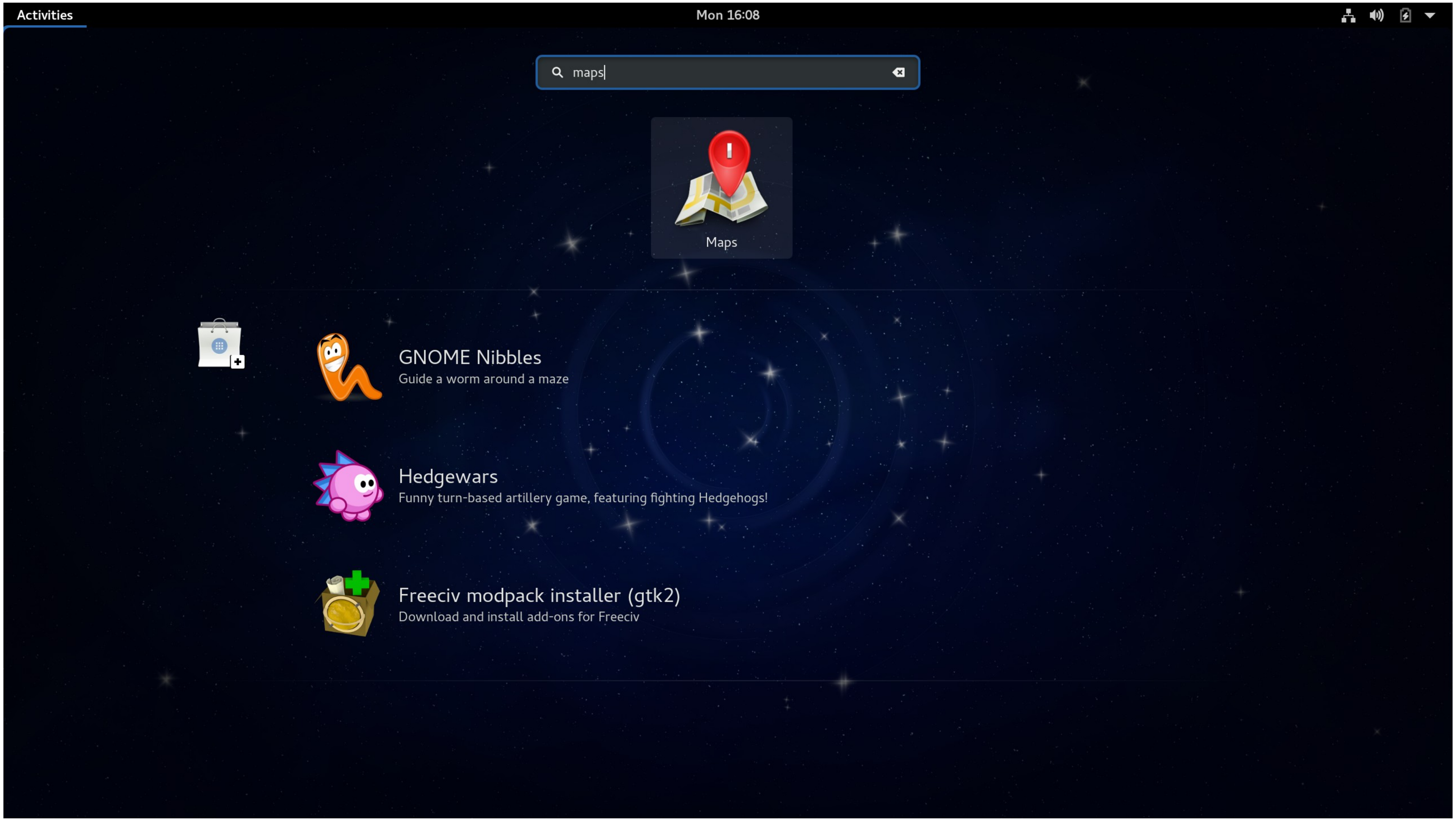


Maps gives you quick access to maps all across the world. It allows you to quickly find the place you're looking for by searching for a city or street, or locate a place to meet a friend.

Maps uses the collaborative OpenStreetMap database, made by hundreds of thousands of people across the globe.

You can even search for specific types of locations, such as "Pubs near Main Street, Boston" or "Hotels near Alexanderplatz, Berlin".

Using Flatpak (cont)



GNOME Nibbles
Guide a worm around a maze

Hedgewars
Funny turn-based artillery game, featuring fighting Hedgehogs!

Freeciv modpack installer (gtk2)
Download and install add-ons for Freeciv

Command line

```
$ flatpak remote-add gnome \
   https://sdk.gnome.org/gnome.flatpakrepo
$ flatpak remote-add gnome-apps \
   https://sdk.gnome.org/gnome-apps.flatpakrepo
$ flatpak install gnome-apps org.gnome.Maps
$ flatpak run org.gnome.Maps
$ flatpak update org.gnome.Maps

Alt:
$ flatpak install \
  https://sdk.gnome.org/gnome-maps.flatpakref
```

How did this work?

- OSTree repo on web server
- Very similar to git
- One branch per app
- One branch with metadata (AppStream) for all branches

Installation

- Pull application branch to local repo
- Check out the result to a regular directory
- Extract “exports” from the app to a global directory:
  - .desktop files
  - Icons
  - DBus service files
- This is how the app integrates with the desktop

OSTree Advantages

- Deduplication
  - On disk
  - In filesystem cache
  - Checkouts are hardlinked
- Atomic updates
  - On disk
  - While running

Example application

Files:

```
├── metadata
├── files/
│   ├── bin/hello-world
│   ├── lib/libbundled.so.1
│   └── share/helloworld/hello.txt
└── export/
    ├── share/applications/com.example.helloworld.desktop
    ├── share/dbus-1/services/com.example.helloworld.service
    └── share/icons/hicolor/48x48/apps/com.example.helloworld.png
```

Metadata:

```
[Application]
name=com.example.helloworld
command=hello-world
runtime=com.example.Platform/x86_64/1.0
```

Running

- Application runs in a contained environment
- Uses bubblewrap
- Application files are always in /app
- No need for relocation, just build application with `./configure --prefix=/app`
- `Runtime in /usr`
- Files are readonly
- App can access ~/.var/app/$appid/

What is a runtime?

- Like a minimal distribution
- Only app dependencies
- An application specifies the runtime to use
- Multiple runtimes can be used in parallel

Example Minimal Runtime

Files:

```
├── metadata
└── files/
    ├── bin/bash
    ├── etc/ld.so.conf
    └── lib
        ├── ld-linux.so.2
        ├── libc.so.6
        └── libdl.so.6
```

Metadata:

```
[Runtime]
name=com.example.Platform/x86_64/1.0
```

May also contain shared data like:

Locales, Fonts, icons

What is in a runtime?

- libc
- Basic library dependencies
- Basic unix tools
- Security update critical modules

What is a runtime not?

- Another name for packages
- Something most people should create
- A way to avoid bundling dependencies

How do I chose a runtime?

- Depends on your application
- Generally
  - Smaller runtime
    - Longer supported lifespan
    - May need to bundle more
  - Larger runtime
    - Shorter supported lifespan
    - Need to bundle less
- Freedesktop.org runtime
- Gnome/KDE runtime
- Re-packaging distro packages: Fedora, Debian, etc
  - Allows making flatpaks from existing app packages

Sandboxing

- Protect users data from apps
- Protect apps from each others
- Require less trust from app source
  - Don’t run arbitrary code as root
- Atomic, easily uninstalled apps
- Don't make machine a botnet node, spam sender, bitcoin miner, etc

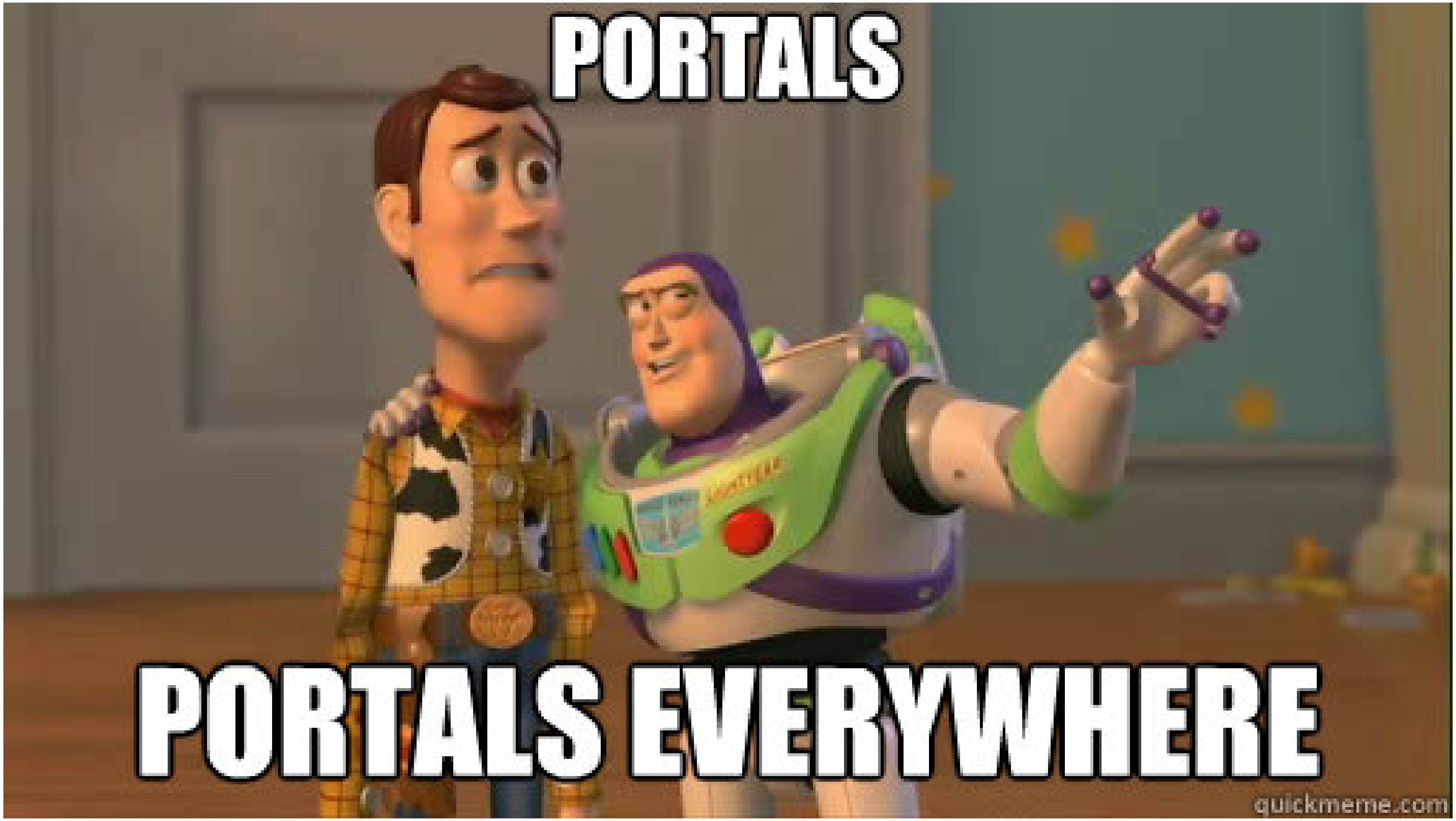
Container technologies

- Namespaces
- Limited filesystem visiblity
- PR_SET_NO_NEW_PRIVS
- Seccomp
- (Optional) cgroups

So, how does an app actually do something?

Optionally disable limits

- Network namespace
- IPC namespace
- DRI device nodes
- File access (all or partial)
- Grant access to host services
  - X11
  - Wayland
  - PulseAudio
  - Filtered DBus


PORTALS
PORTALS EVERYWHERE
quickmeme.com

What is a portal

- Service running in the session
- Typically accessed via dbus
- Designed to be “safely” accessed from sandbox
  - Safe due to user interaction
  - App permission checks
- Extends what a sandboxed app can do

Current portals

- Document portal
- Desktop portal
  - File chooser
  - Show URI
  - Print
  - HTTP Proxy config
  - Network status
  - Backends: Gtk+, KDE

Building flatpaks

- Two approaches
  - Pre-existing contents
  - Build in Flatpak with SDKs
    - “flatpak build”

Flatpak-builder

- Layered above the lowlevel commands
- Json manifest describing build steps
- Nice features
  - Source downloading and verification
  - Build cache
  - Runs with limited fs access, no network access, etc
  - Repeatable build paths (/run/build)
  - Creates debug-info and locale extensions
  - Built-in ccache support

Example manifest

```
{
    ”id”: ”org.gnome.Characters”,
    ”runtime”: ”org.gnome.Platform”,
    ”runtime-version”: ”3.22”,
    ”sdk”: ”org.gnome.Sdk”,
    ”finish-args”: [ ”--socket=x11” ],
    ”cleanup”: [”/include”, ”*.a” ],
    ”modules”: [
      …
    ]
}
```

```
{
  "name": "gnome-desktop",
  "config-opts": ["--disable-debug-tools", "--disable-udev"],
  "cleanup": ["/bin" ],
  "sources": [
    {
      "type": "archive",
      "url": "https://download.gnome.org/.../gnome-desktop-3.22.0.tar.xz",
      "sha256": "cff36ccd8d0a62177a4c1513ec70d13ead3b84fdc208ba54199cf7616f05644d"
    }
  ]
},
{
  "name": "gnome-characters",
  "sources": [
    {
      "type": "archive",
      "url": "https://download.gnome.org/.../gnome-characters-3.22.0.tar.xz",
      "sha256": "0778b625646d6d934cf252d58a2e16403889da6bfc237bdca1d3cb3258f63d4e"
    }
  ]
}
```

Community uptake

- Ships in most distros
  - Fedora, Debian, Ubuntu, Arch, ClearLinux, OpenSuse, Mageira
  - COPR for Centos/RHEL
- 3rd parties using flatpak
  - Gnome
  - KDE
  - Endless Mobile
  - LibreOffice
  - Microsoft/Xamarin
  - VMWare
- Flathub
  - Work in progress

Questions

More info at:

http://flatpak.org

Code:

http://github.org/flatpak

Talk to us:

#flatpak on freenode

https://lists.freedesktop.org/mailman/listinfo/xdg-app