

# A complete compliance toolchain for Yocto projects

Alberto Pianon, Carlo Piana – **Array**

 Fosdem2023 - SBOM DevRoom - Feb 5, 2023

# Context



- Eclipse Foundation project
- a Yocto-based all-scenario OS platform project...
- ...supporting 12 target machines, 2 build toolchains, 2 different kernels (**tens of build targets, all CI'd**)...
- ...with an integrated Continuous Compliance process...
- ...managed through a dedicated toolchain

# A Toolchain For Compliance

---

NOI Techpark <https://noi.bz.it/en>

---

Array <https://array.eu>

- an **Eclipse Foundation project**, too
- based on existing OSS tools (Fossology, Scancode)
- + a set of custom tools (aliens4friends, tinfoilhat, a4f dashboard)
- it can be implemented in any other Yocto-based project
- with latest Oniro release, we reached **100% coverage** on source components
  - also by automatically reusing Debian community work

sca.software.bz.it

Aliens4Friends Dashboard 138/138 PACKAGES Filter...

### FOSSology audit progress

Total audit files

62% Audit done 38% Audit not required

### Provenance

Upstream source total: 720290

913352 Known provenance

### License types scanned

Results from automated scanners such as scancode, monk, nomos, ojo

### Main license types

Accumulated main licenses

### License types audited

Results by human auditor analysis

Main Licenses accumulated

31

Files total

914041

Distros accumulated

7

Images accumulated

12

Machines accumulated

20

Releases accumulated

6

ABOUT THIS TOOL

# sca.software.bz.it

Aliens4Friends Dashboard
138/138 PACKAGES
Filter...

### Package Explorer

State	ID	Aud. Progress	Aud. Workload	Main licenses	Distros	Images	Machines	Releases	Scan	Audit All
	ac1-2.3.1-r0-963c29b5+a4f	<div style="width: 100%; height: 10px; background-color: green;"></div> 100% 166 Files done / 166 Files total	166 Files total	<div style="border: 1px solid gray; padding: 2px;">             LGPL-2.1-only           </div>	<div style="border: 1px solid gray; padding: 2px;">linux</div> <div style="border: 1px solid gray; padding: 2px;">linux-clang</div> <div style="border: 1px solid gray; padding: 2px;">linux-gcc</div>	<div style="border: 1px solid gray; padding: 2px;">image-base</div> <div style="border: 1px solid gray; padding: 2px;">image-base-dev</div> <div style="border: 1px solid gray; padding: 2px;">image-base-seco-px30-d23-emmc.manifest</div> <div style="border: 1px solid gray; padding: 2px;">image-base-tests</div> <div style="border: 1px solid gray; padding: 2px;">image-base-tests-seco-px30-d23-emmc.manifest</div> <div style="border: 1px solid gray; padding: 2px;">image-extra</div> <div style="border: 1px solid gray; padding: 2px;">image-extra-dev</div> <div style="border: 1px solid gray; padding: 2px;">image-extra-seco-px30-d23-emmc.manifest</div> <div style="border: 1px solid gray; padding: 2px;">image-extra-tests</div> <div style="border: 1px solid gray; padding: 2px;">image-extra-tests-seco-px30-d23-emmc.manifest</div>	<div style="border: 1px solid gray; padding: 2px;">qemuarm-efi</div> <div style="border: 1px solid gray; padding: 2px;">qemuarm64-efi</div> <div style="border: 1px solid gray; padding: 2px;">qemuarm64</div> <div style="border: 1px solid gray; padding: 2px;">qemuarm64-64</div> <div style="border: 1px solid gray; padding: 2px;">raspberrypi4-64</div> <div style="border: 1px solid gray; padding: 2px;">seco-imx8mm-c61-2gb</div> <div style="border: 1px solid gray; padding: 2px;">seco-imx8mm-c61-4gb</div> <div style="border: 1px solid gray; padding: 2px;">seco-intel-b68</div> <div style="border: 1px solid gray; padding: 2px;">seco-px30-d23</div>	<div style="border: 1px solid gray; padding: 2px;">kirkstone-v2.0.0-beta</div> <div style="border: 1px solid gray; padding: 2px;">kirkstone-v2.0.0-beta-109-g2f5fa92</div>	<div style="text-align: center;"> <div style="font-weight: bold; font-size: 1.2em;">32</div> </div>	<div style="text-align: center;"> <div style="font-weight: bold; font-size: 1.2em;">32</div> </div>
	acpid-2.0.33-r0-c931e98d+a4f	<div style="width: 100%; height: 10px; background-color: green;"></div> 100% 49 Files done / 49 Files total	49 Files total	<div style="border: 1px solid gray; padding: 2px;">             GPL-2.0-only           </div>	<div style="border: 1px solid gray; padding: 2px;">linux</div> <div style="border: 1px solid gray; padding: 2px;">linux-clang</div> <div style="border: 1px solid gray; padding: 2px;">linux-gcc</div>	<div style="border: 1px solid gray; padding: 2px;">image-base</div> <div style="border: 1px solid gray; padding: 2px;">image-base-dev</div> <div style="border: 1px solid gray; padding: 2px;">image-base-tests</div> <div style="border: 1px solid gray; padding: 2px;">image-extra</div> <div style="border: 1px solid gray; padding: 2px;">image-extra-dev</div> <div style="border: 1px solid gray; padding: 2px;">image-extra-tests</div>	<div style="border: 1px solid gray; padding: 2px;">seco-intel-b68</div>	<div style="border: 1px solid gray; padding: 2px;">kirkstone-v2.0.0-beta</div> <div style="border: 1px solid gray; padding: 2px;">kirkstone-v2.0.0-beta-109-g2f5fa92</div>	<div style="text-align: center;"> <div style="font-weight: bold; font-size: 1.2em;">7</div> </div>	<div style="text-align: center;"> <div style="font-weight: bold; font-size: 1.2em;">11</div> </div>
	alsa-lib-1.2.6.1-r0-b83ad896+a4f	<div style="width: 100%; height: 10px; background-color: green;"></div> 100% 244 Files done / 244 Files total	244 Files total	<div style="border: 1px solid gray; padding: 2px;">             LGPL-2.1-only           </div>	<div style="border: 1px solid gray; padding: 2px;">linux</div> <div style="border: 1px solid gray; padding: 2px;">linux-clang</div> <div style="border: 1px solid gray; padding: 2px;">linux-gcc</div>	<div style="border: 1px solid gray; padding: 2px;">image-base</div> <div style="border: 1px solid gray; padding: 2px;">image-base-dev</div> <div style="border: 1px solid gray; padding: 2px;">image-base-seco-px30-d23-emmc.manifest</div> <div style="border: 1px solid gray; padding: 2px;">image-base-tests</div> <div style="border: 1px solid gray; padding: 2px;">image-extra</div> <div style="border: 1px solid gray; padding: 2px;">image-extra-dev</div> <div style="border: 1px solid gray; padding: 2px;">image-extra-tests</div>	<div style="border: 1px solid gray; padding: 2px;">qemuarm-efi</div> <div style="border: 1px solid gray; padding: 2px;">qemuarm64-efi</div> <div style="border: 1px solid gray; padding: 2px;">raspberrypi4-64</div> <div style="border: 1px solid gray; padding: 2px;">seco-imx8mm-c61-2gb</div> <div style="border: 1px solid gray; padding: 2px;">seco-imx8mm-c61-4gb</div> <div style="border: 1px solid gray; padding: 2px;">seco-intel-b68</div> <div style="border: 1px solid gray; padding: 2px;">seco-px30-d23</div>	<div style="border: 1px solid gray; padding: 2px;">kirkstone-v2.0.0-beta</div> <div style="border: 1px solid gray; padding: 2px;">kirkstone-v2.0.0-beta-109-g2f5fa92</div>	<div style="text-align: center;"> <div style="font-weight: bold; font-size: 1.2em;">15</div> </div>	<div style="text-align: center;"> <div style="font-weight: bold; font-size: 1.2em;">23</div> </div>
	alsa-plugins-1.2.6-r0-47385cc5+a4f	<div style="width: 100%; height: 10px; background-color: green;"></div> 100% 68 Files done / 68 Files total	68 Files total	<div style="border: 1px solid gray; padding: 2px;">             LGPL-2.1-only           </div>	<div style="border: 1px solid gray; padding: 2px;">linux</div> <div style="border: 1px solid gray; padding: 2px;">linux-gcc</div>	<div style="border: 1px solid gray; padding: 2px;">image-base</div> <div style="border: 1px solid gray; padding: 2px;">image-base-dev</div> <div style="border: 1px solid gray; padding: 2px;">image-base-tests</div> <div style="border: 1px solid gray; padding: 2px;">image-extra</div>	<div style="border: 1px solid gray; padding: 2px;">seco-imx8mm-c61-2gb</div> <div style="border: 1px solid gray; padding: 2px;">seco-imx8mm-c61-4gb</div>	<div style="border: 1px solid gray; padding: 2px;">kirkstone-v2.0.0-beta</div> <div style="border: 1px solid gray; padding: 2px;">kirkstone-v2.0.0-beta-109-g2f5fa92</div>	<div style="text-align: center;"> <div style="font-weight: bold; font-size: 1.2em;">17</div> </div>	<div style="text-align: center;"> <div style="font-weight: bold; font-size: 1.2em;">27</div> </div>

[ABOUT THIS TOOL](#)

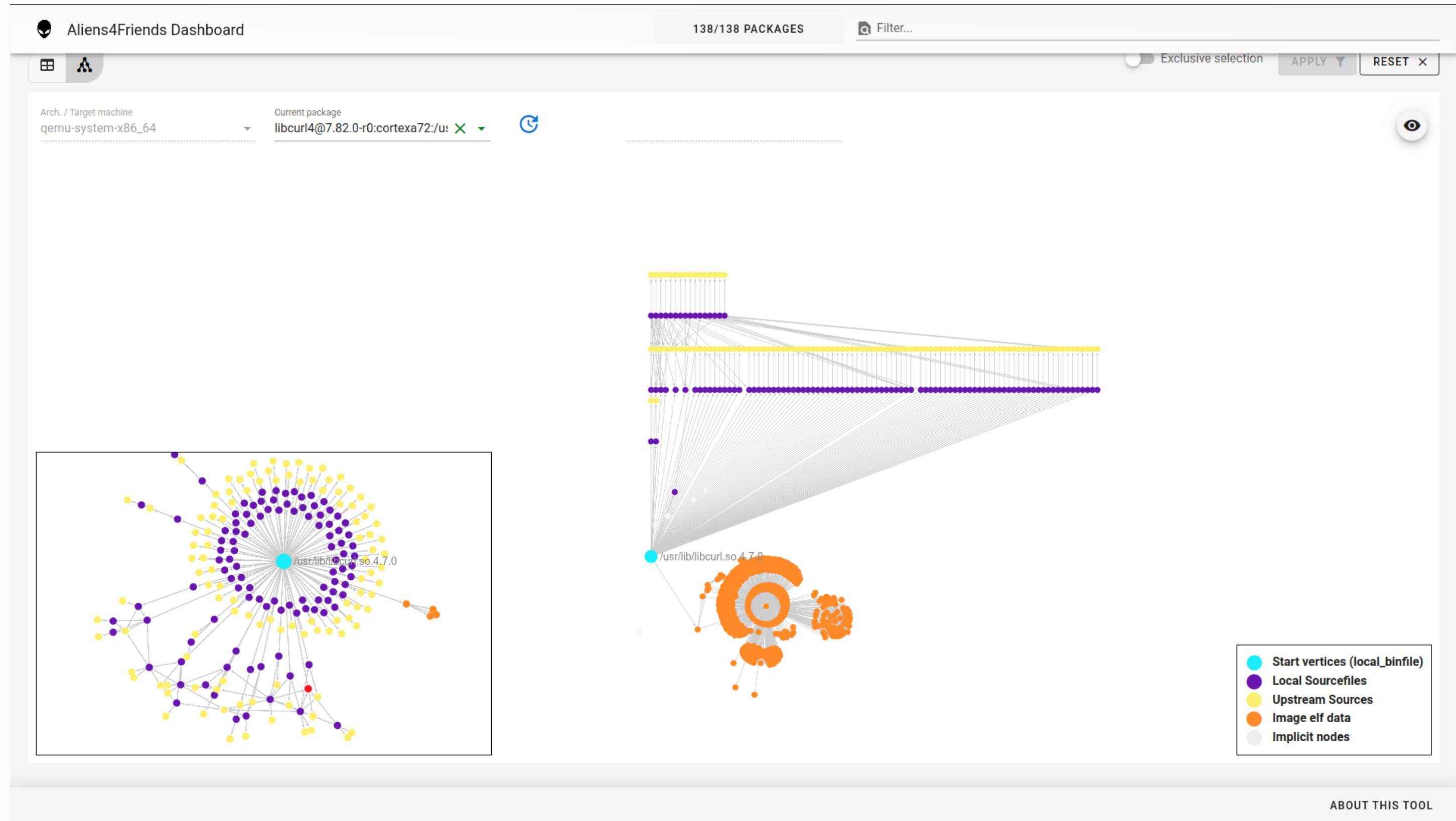
**but now we want more!**

# R&D for Oniro Compliance Toolchain v2.0

- A **graph** database
- Software composition analysis, dependency analysis, automated license incompatibility checks
- To do that, we need to:
  - map all **license metadata**\* on upstream source files down to binary files (**file-level mapping**)
    - (\*) coming from our Audit Team, Debian community, possibly ClearlyDefined and other shared data sources
  - find a way to automatically combine **different inbound-outbound licenses** and check their **compatibility**

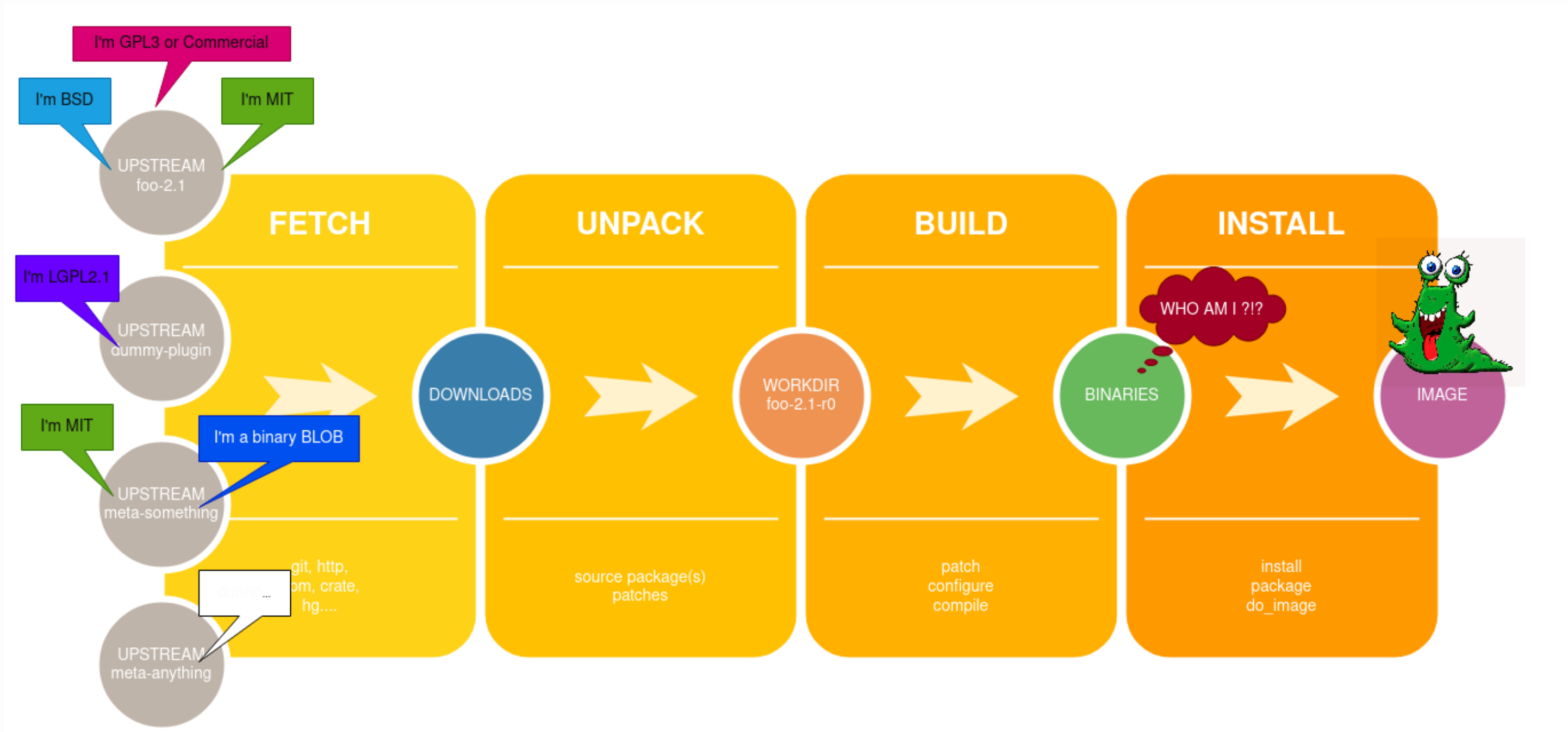


# sca-staging.software.bz.it



# Why do we need this?

# Yocto workflow (simplified)

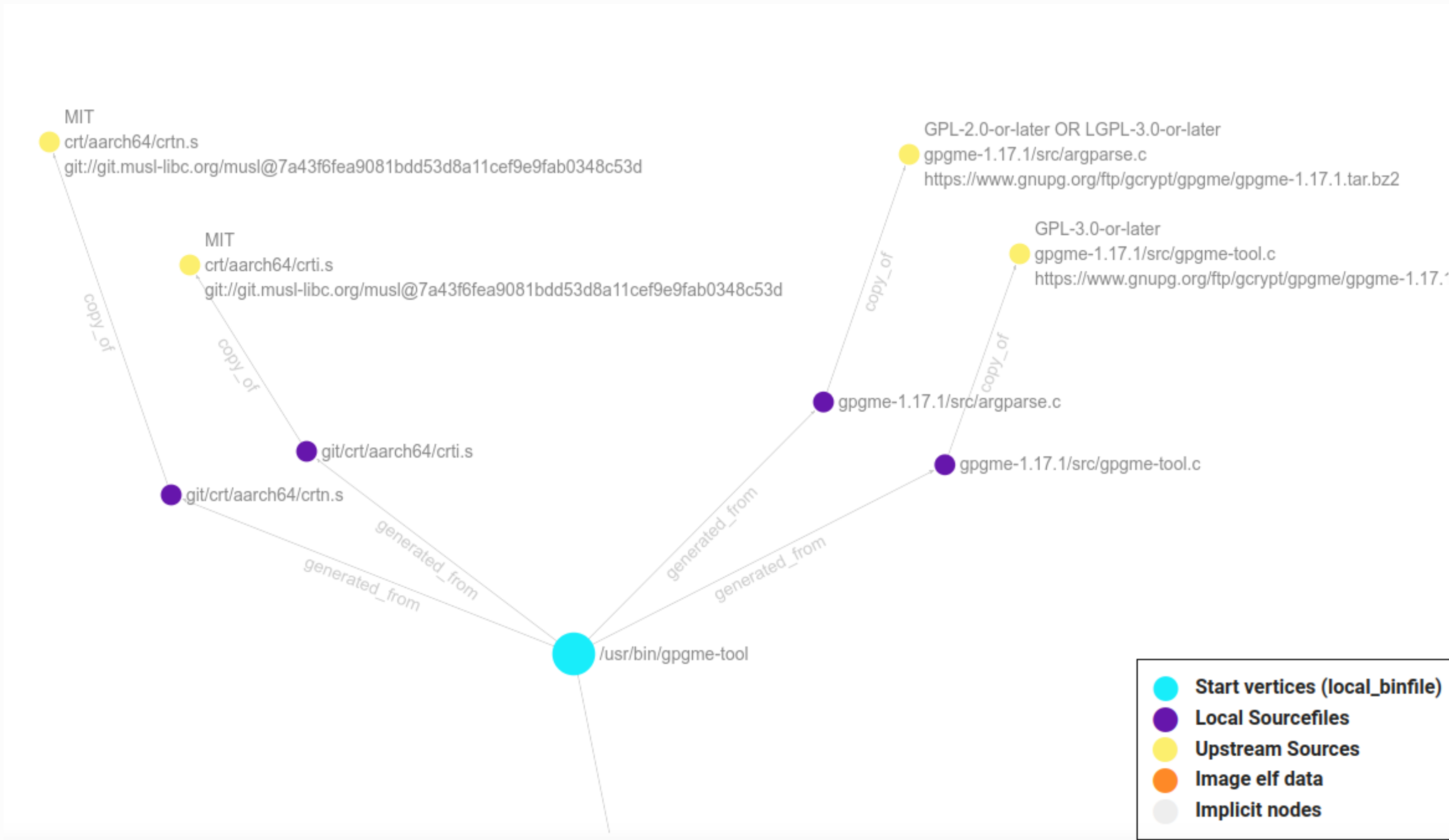


# Logic Steps

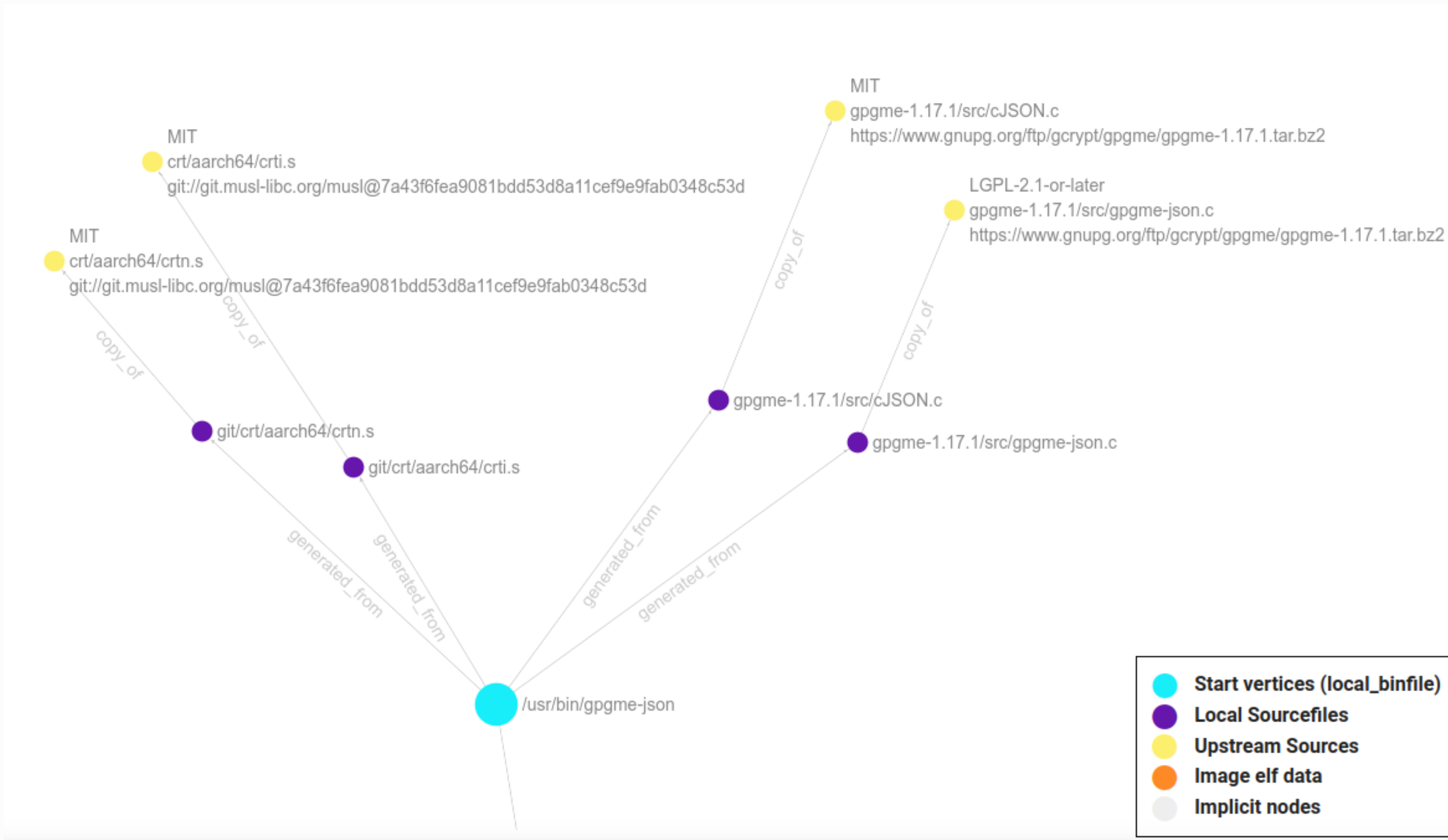
1. Find out the relationship with third party, upstream code (inbound)
2. Find out under which license(s) the inbound upstream software is, therefore the inbound Licenses
3. Find out if there is a possible combination of them
4. Match this combination with the outbound license(s).

For **each** artifact (**file!**)

# A simple example: GPGME (1)



# A simple example: GPGME (2)





# How can we handle that?



# A battle between License Cards!



# Proposed syntax for license battle rules (tentative)

```
GPL-3.0-or-later vs LGPL-3.0-or-later, battlefield: strong, authority: FSF, result: GPL-3.0-or-later
```

```
LGPL-3.0-only vs GPL-2.0-or-later, battlefield: strong, authority: FSF, result: GPL-3.0-only
```

```
LGPL-3.0-only vs GPL-2.0-only, battlefield: any, authority: FSF, result: INVALID
```

```
GPL-3.0-only vs Apache-2.0, battlefield: any, authority: FSF, result: GPL-3.0-only
```

```
GPL-2.0-only vs Apache-2.0, battlefield: any, authority: FSF, result: INVALID
```

```
GPL-2.0-or-later vs Apache-2.0, battlefield: any, authority: FSF, result: GPL-3.0-or-later
```

```
LGPL-3.0-only vs MPL-2.0, battlefield: weak, authority: Mozilla, result: LGPL-3.0-only OR MPL-2.0
```

```
GPL-3.0-only vs MPL-2.0, battlefield: any, authority: Mozilla, result: GPL-3.0-only
```

# Rules in action (1)

```
[
  {
    "inbound_licenses": [
      "MIT",
      "GPL-2.0-or-later OR LGPL-3.0-or-later",
      "GPL-3.0-or-later"
    ],
    "outbound_license": "GPL-3.0-or-later",
    "unhandled_licenses": [],
    "processed_license_options": [
      {
        "inbound_licenses": [
          "MIT",
          "GPL-2.0-or-later",
          "GPL-3.0-or-later"
        ],
        "results": {
          "prevailing_licenses": [
            "GPL-3.0-or-later"
          ],
          "decisions": [
            "GPL-2.0-or-later vs MIT, result: GPL-2.0-or-later",
            "GPL-3.0-or-later vs MIT, result: GPL-3.0-or-later",
            "GPL-3.0-or-later vs GPL-2.0-or-later, result: GPL-3.0-or-later"
          ]
        },
        "unhandled_licenses": []
      }
    ]
  }
]
```

## Rules in action (2)

```
{
  "processed_license_options": [
    {
      "inbound_licenses": ["MIT", "LGPL-3.0-or-later", "GPL-3.0-or-later"],
      "results": {
        "prevailing_licenses": ["GPL-3.0-or-later"],
        "decisions": [
          "GPL-3.0-or-later vs LGPL-3.0-or-later, result: GPL-3.0-or-later",
          "GPL-3.0-or-later vs MIT, result: GPL-3.0-or-later",
          "LGPL-3.0-or-later vs MIT, result: LGPL-3.0-or-later"
        ],
        "unhandled_licenses": []
      }
    }
  ]
}
```

# How we collect required data on Yocto's side

- map upstream source files to local workdir source files to binary files
  - consume metadata coming from Yocto
  - fetch upstream source packages (including Yocto layers with patches etc.) separately from each other, and then map them to local workdir source files
- in our PoC we do that with an external, post-mortem script using `bb.tinfoil`
- it may be integrated in Yocto `create-spdx.bbclass`

**Q&A: we need your feedback!**

# Thank you for your attention

<https://array.eu>

<https://projects.eclipse.org/projects/oniro.oniro-compliancetoolchain>

<https://gitlab.eclipse.org/eclipse/oniro-compliancetoolchain/toolchain>

---

  Array     Alberto Pianon     Carlo Piana



This work is licensed under a [Creative Commons - Attribution - ShareAlike 4.0](https://creativecommons.org/licenses/by-sa/4.0/)  
Presentation made using [Reveal.js](https://github.com/hakimel/reveal.js) and a [Markdown](https://github.com/leandromore/markdown-reveal) workflow with [reveal-md](https://github.com/leandromore/markdown-reveal)