MENDER
by Northern.tech

Building open source management and SBOM process for embedded software - learn from Yocto Project

Josef Holzmayr

Developer Enablement Expert, Mender.io & Yocto Project Community Manager

OpenChain and friends, 08.04.2025

That's not a presentation title, its a novel.🤯

Let’s try again, shall we?

MENDER
by Northern.tech

Yocto does cool stuff and tells you about it.

Josef Holzmayr

Developer Enablement Expert, Mender.io & Yocto Project Community Manager

OpenChain and friends, 08.04.2025

Hello, my name is Josef.

I am a recovering embedded developer.

Photo by the awesome Tiana Lea

Some technical details

Street credibility

Yocto Project Community Manager & Ambassador

OpenEmbedded Social Media Manager

Kernel contributor (yup, really!)

Fame

https://www.linkedin.com/in/josef-holzmayr

josef.holzmayr@northern.tech

https://fosstodon.org/@theyoctojester

Photo by the awesome Tiana Lea

Who has seen me live before?

About you

Hardware Developer?

Firmware Developer?

Embedded Linux?

Yocto?

About this presentation

Every form of interaction will be rewarded
… until I run out of chocolate.

Some ideas:

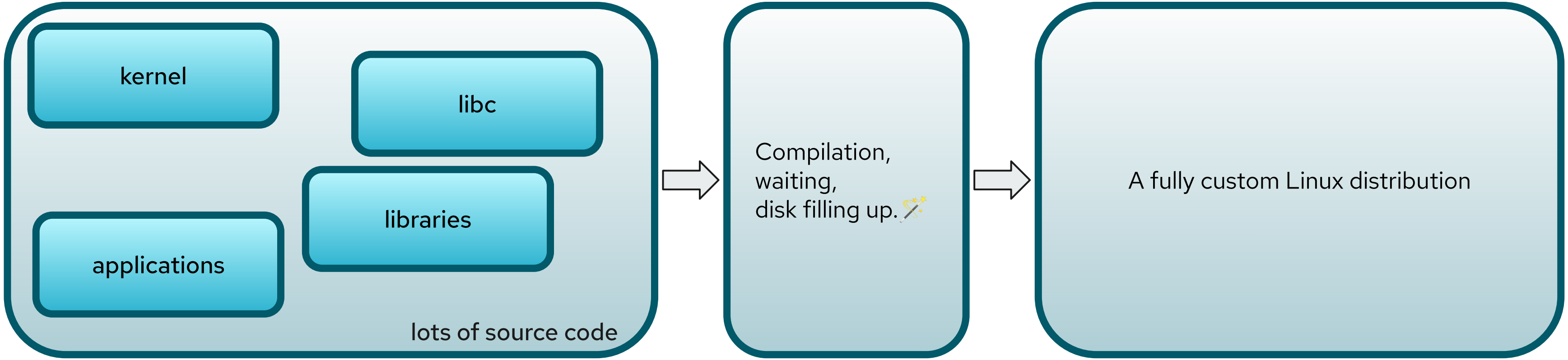
- Good: Tell me what you like.
- Better: Tell me what you don’t like.
- Best: Tell me where I am wrong.
- Helpful: Ask for a clarification.
- Practical: Ask for chocolate.

Image attribution: User:-donald- - Wikimedia Commons

MENDER
by Northern.tech

So what is this Yocto?

Yocto on one slide



If you need a mental model, think of Yocto as a form of Linux from scratch with full automation on a lot of steroids.

Insider joke: whenever you hear that something runs “Yocto Linux”, it is wrong by definition.

Yocto knows what it builds.

We’re had “manifests” for a long time.

```
acl cortexa57 2.3.2
at cortexa57 3.2.5
attr cortexa57 2.5.2
base-files qemuarm64 3.0.14
base-passwd cortexa57 3.6.6
bash cortexa57 5.2.37
bc cortexa57 1.08.1
busybox cortexa57 1.37.0
busybox-hwclock cortexa57 1.37.0
busybox-udhcpc cortexa57 1.37.0
…
```

(`core-image-full-cmdline.bb`, for `qemuarm64`, current `walnascar` tip as of 2025-04-07)

What about SBOMs?

We’ve got you covered!

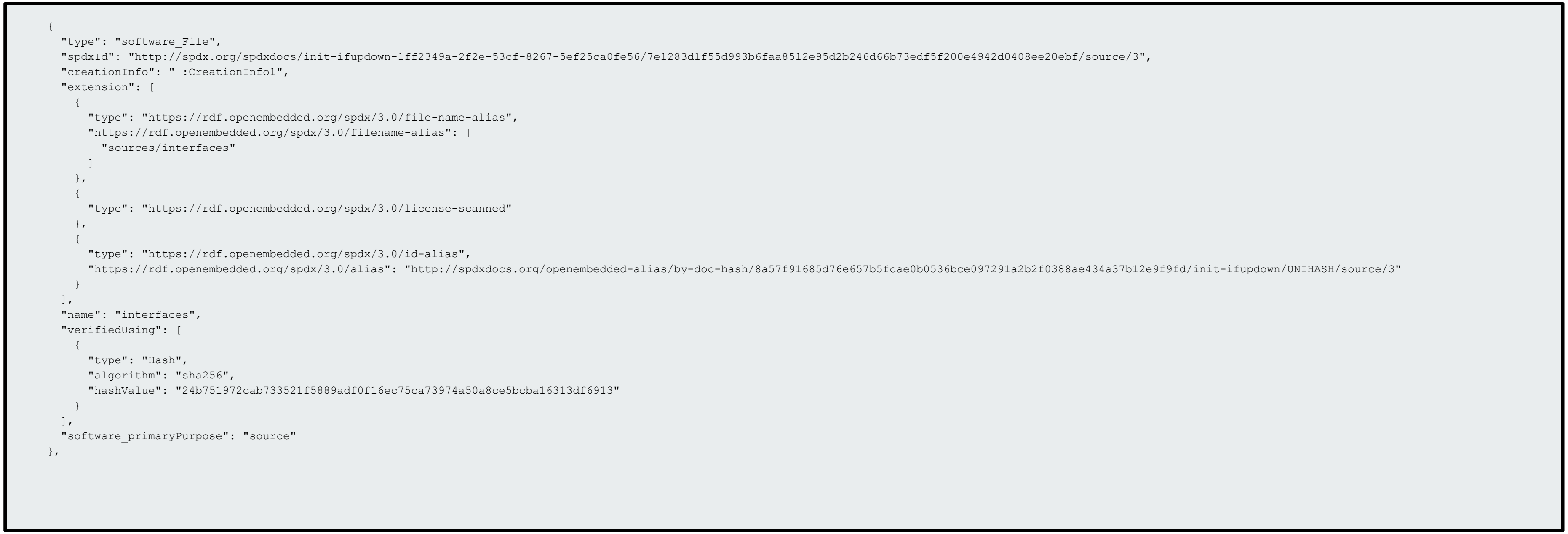
```
local.conf:


INHERIT += "create-spdx"
SPDX_PRETTY = "1"
SPDX_INCLUDE_SOURCES = "1"
```

Rundown:

- `INHERIT += "create-spdx"` enables SPDX-style SBOM generation. V 3.0.1 as of the walnascar release
- `SPDX_PRETTY = "1"` makes the generated SBOM (somewhat) human readable
- `SPDX_INCLUDE_SOURCES = "1"` adds the source code files used to the SBOM

As Yocto builds EVERYTHING from source, the data is quite exhaustive.

Example: etc/network/interfaces



```
{
  "type": "software_File",
  "spdxId": "http://spdx.org/spdxdocs/init-ifupdown-1ff2349a-2f2e-53cf-8267-5ef25ca0fe56/7e1283d1f55d993b6faa8512e95d2b246d66b73edf5f200e4942d0408ee20ebf/source/3",
  "creationInfo": "_:CreationInfo1",
  "extension": [
    {
      "type": "https://rdf.openembedded.org/spdx/3.0/file-name-alias",
      "https://rdf.openembedded.org/spdx/3.0/filename-alias": [
        "sources/interfaces"
      ]
    },
    {
      "type": "https://rdf.openembedded.org/spdx/3.0/license-scanned"
    },
    {
      "type": "https://rdf.openembedded.org/spdx/3.0/id-alias",
      "https://rdf.openembedded.org/spdx/3.0/alias": "http://spdxdocs.org/openembedded-alias/by-doc-hash/8a57f91685d76e657b5fcae0b0536bce097291a2b2f0388ae434a37b12e9f9fd/init-ifupdown/UNIHASH/source/3"
    }
  ],
  "name": "interfaces",
  "verifiedUsing": [
    {
      "type": "Hash",
      "algorithm": "sha256",
      "hashValue": "24b751972cab733521f5889adf0f16ec75ca73974a50a8ce5bcba16313df6913"
    }
  ],
  "software_primaryPurpose": "source"
},
```

(build/tmp/deploy/spdx/3.0.1/recipes/recipe-init-ifupdown.spdx.json)

And thats also the problem...

The “source” of this was:

```
SRC_URI = "file://interfaces"

do_install () {
    install -m 0644 ${S}/interfaces ${D}${sysconfdir}/network/interfaces
}
```

(leaving out non-related other files)

We need to work together to solve this in the long run.

Its not a you or me problem.

Its not a Yocto Project problem.

Its an SBOM ecosystem problem.

In the long run, we need to figure out how to make real use of this data, to provide actual value.

I’m all ears.

MENDER
by Northern.tech

Learn more

✉ contact@mender.io

mender.io

@mender_io

company/northern.tech

Get started now

docs.mender.io/getting-started

Join the Mender Hub community

hub.mender.io

Mender on Github

github.com/mendersoftware

MENDER by Northern.tech

Q & A

Josef Holzmayr
Developer Enablement Expert, Mender.io & Community Manager, The Yocto Project
https://github.com/TheYoctoJester/
https://www.linkedin.com/in/josef-holzmayr/

MENDER
by Northern.tech

Thank you

Contact us

mender.io/contact-us