FUJITSU

shaping tomorrow with you

How to reduce on your OSS compliance work

Jul 18th, 2019
Lei Maohui, Fujitsu
leimaohui@cn.fujitsu.com

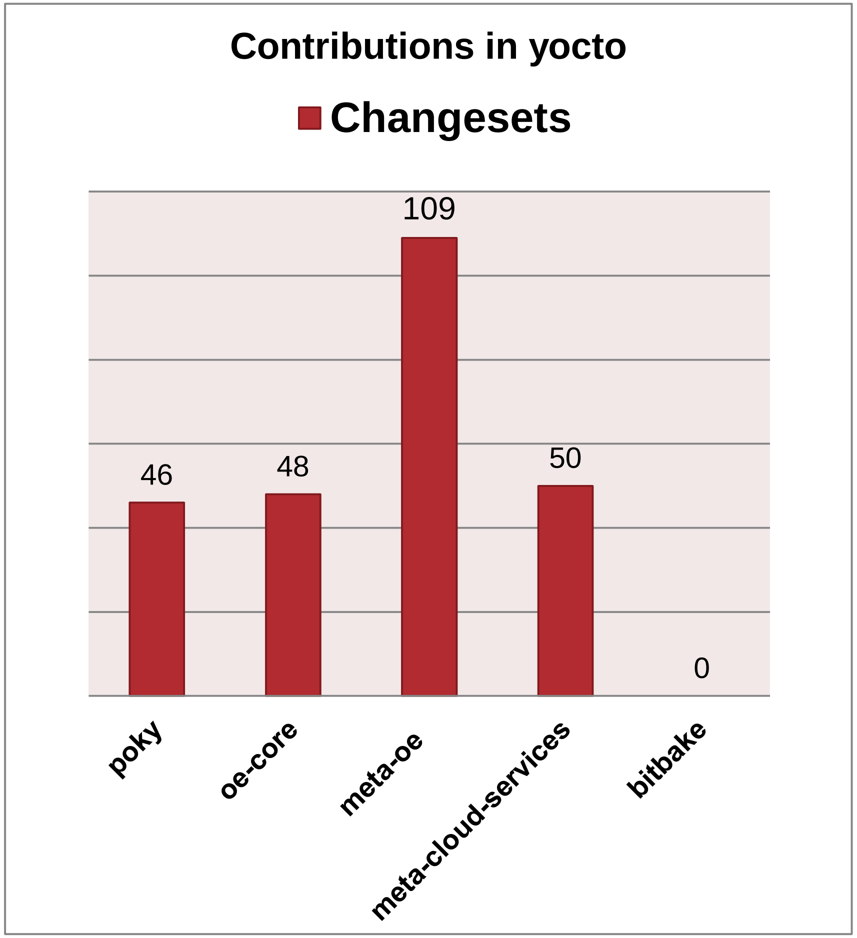
whoami

- Working for Fujitsu from 2011
- 7 years experience in Yocto related development

- In-House Embedded Linux Distributor of Fujitsu
- Our Distribution is used for
  - IVI
  - Server System Controller
  - Storage System
  - Network Equipment
  - Printer
  - etc.

Fujitsu's contributions to Yocto community

- Data comes from yocto (2018-07-01 ~ 2019-07-01)



	Layers	Changesets
1	poky	46
2	oe-core	48
3	meta-oe	109
4	meta-cloud-services	50
5	bitbake	0

- Maintain meta-spdxscanner

Fujitsu’s contributions to Yocto community

- Data comes from yocto (2018-07-01 ~ 2019-07-01)

Developers with the most changesets

No.	Our Developer	Changesets
poky		
30	Zang Ruochen	25 (0.6%)
40	Hong Liu	11 (0.3%)
71	Lei Maohui	7 (0.2%)
oe-core		
30	Zang Ruochen	25 (0.4%)
50	Hong Liu	12 (0.2%)
63	Lei Maohui	7 (0.1%)
Meta-oe		
8	Zang Ruochen	72 (3.7%)
17	Hong Liu	23 (1.2%)
29	Lei Maohui	11 (0.6%)
meta-cloud-services		
1	Zang Ruochen	26 (22.6%)
2	Hong Liu	20 (17.4%)

Agenda

FUJITSU

Yocto+SPDX

- What is SPDX
- What is Yocto
- Overview of Yocto+SPDX

Meta-spdxscanner

- What is Meta-spdxscanner
- How to use
- What we have done for Meta-spdxscanner
- Features of fossdriver-host.bbclass

Manage SPDX

- Work with ClearlyDefined
- Work with OpenChain
- Manage SPDX files by dnf-plugin-tui
- Future work

Yocto+SPDX

- What is SPDX
- What is Yocto
- Overview of Yocto+SPDX
  - Spdx.bbclass
  - Meta-spdxscanner

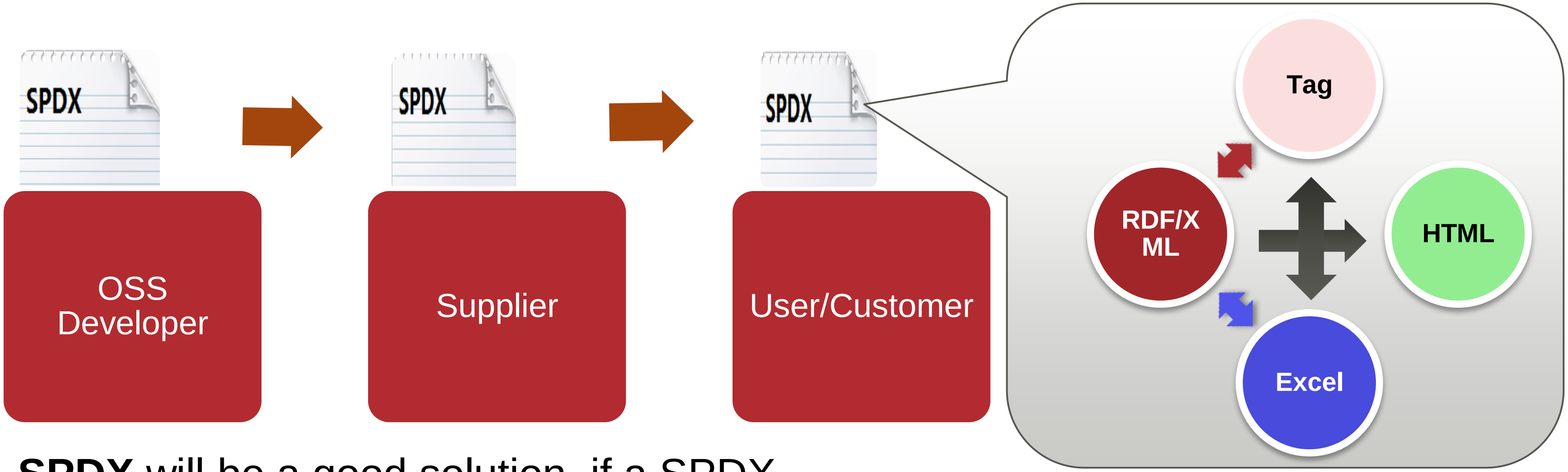
What is SPDX (1/2)

What is SPDX

- The full name of SPDX is **S**oftware **P**ackage **D**ata **Ex**change, which is a standard format for communicating the components, licenses and copyrights associated with a software package.

Vision of SPDX

- achieve license compliance with minimal cost across the supply chain.



SPDX Integrated Tool

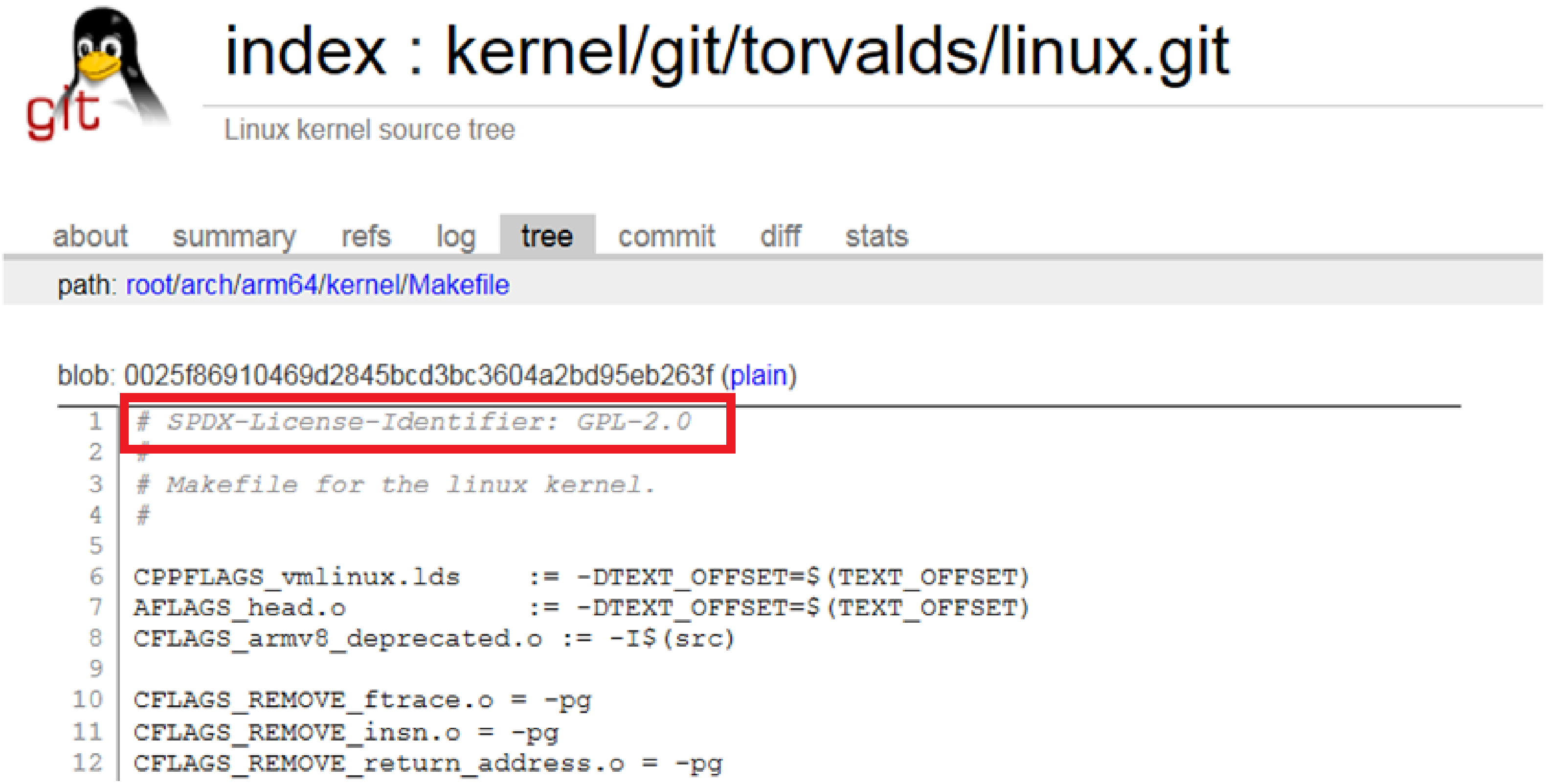
SPDX will be a good solution, if a SPDX implementation can generate SPDX file including license information automatically.

Obtain details from

- https://spdx.org/tools

What is SPDX (2/2)

Kernel v4.14 added one-liners come from SPDX



index : kernel/git/torvalds/linux.git

Linux kernel source tree

path: root/arch/arm64/kernel/Makefile

blob: 0025f86910469d2845bcd3bc3604a2bd95eb263f (plain)

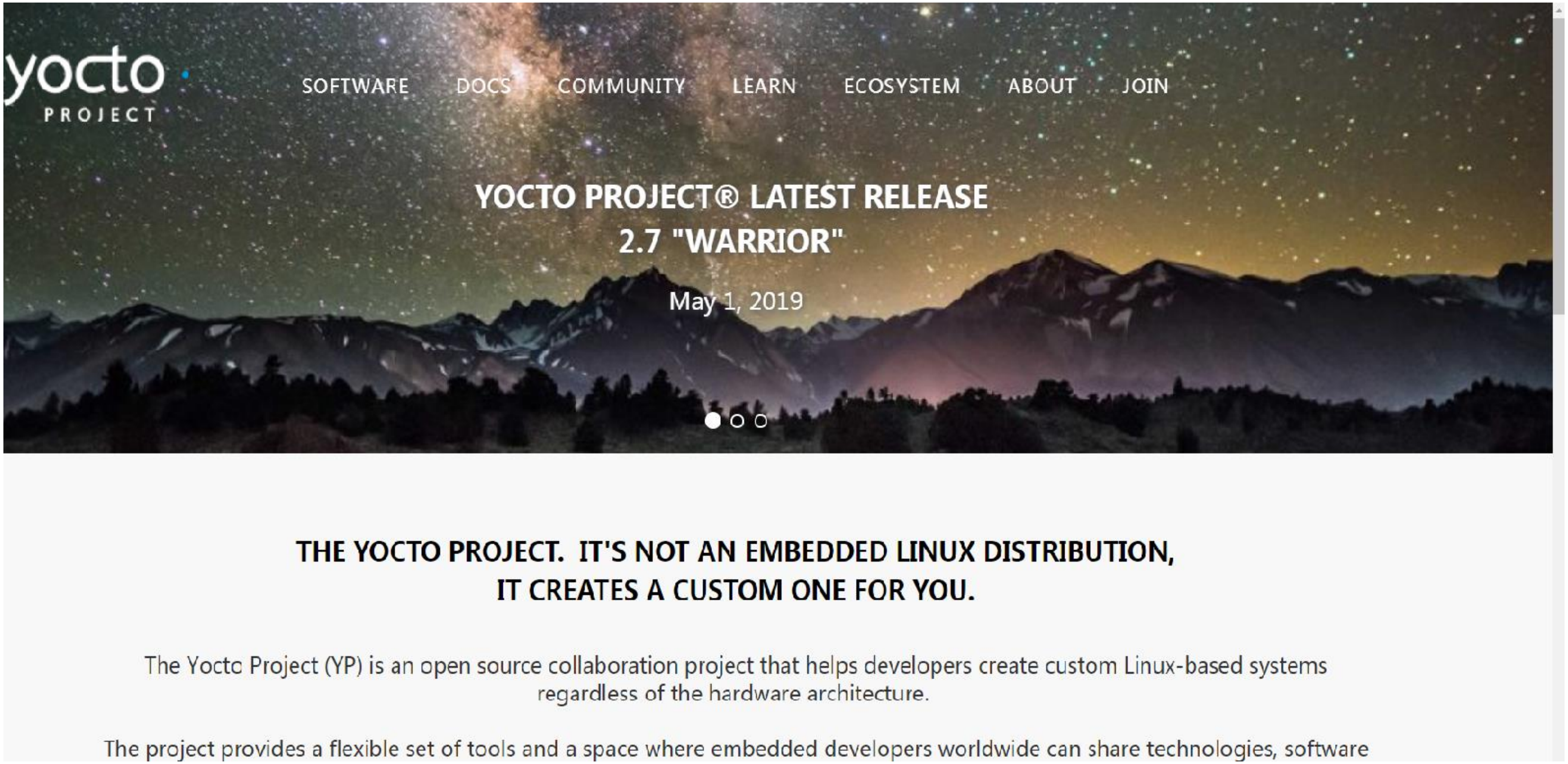
```
# SPDX-License-Identifier: GPL-2.0
#
# Makefile for the linux kernel.
#

CPPFLAGS_vmlinux.lds    := -DTEXT_OFFSET=$(TEXT_OFFSET)
AFLAGS_head.o           := -DTEXT_OFFSET=$(TEXT_OFFSET)
CFLAGS_armv8_deprecated.o := -I$(src)

CFLAGS_REMOVE_ftrace.o = -pg
CFLAGS_REMOVE_insn.o = -pg
CFLAGS_REMOVE_return_address.o = -pg
```

Play an important role

OPENCHAIN

ClearlyDefined

What is Yocto



YOCTO PROJECT® LATEST RELEASE
2.7 "WARRIOR"

May 1, 2019

THE YOCTO PROJECT. IT'S NOT AN EMBEDDED LINUX DISTRIBUTION,
IT CREATES A CUSTOM ONE FOR YOU.

The Yocto Project (YP) is an open source collaboration project that helps developers create custom Linux-based systems regardless of the hardware architecture.

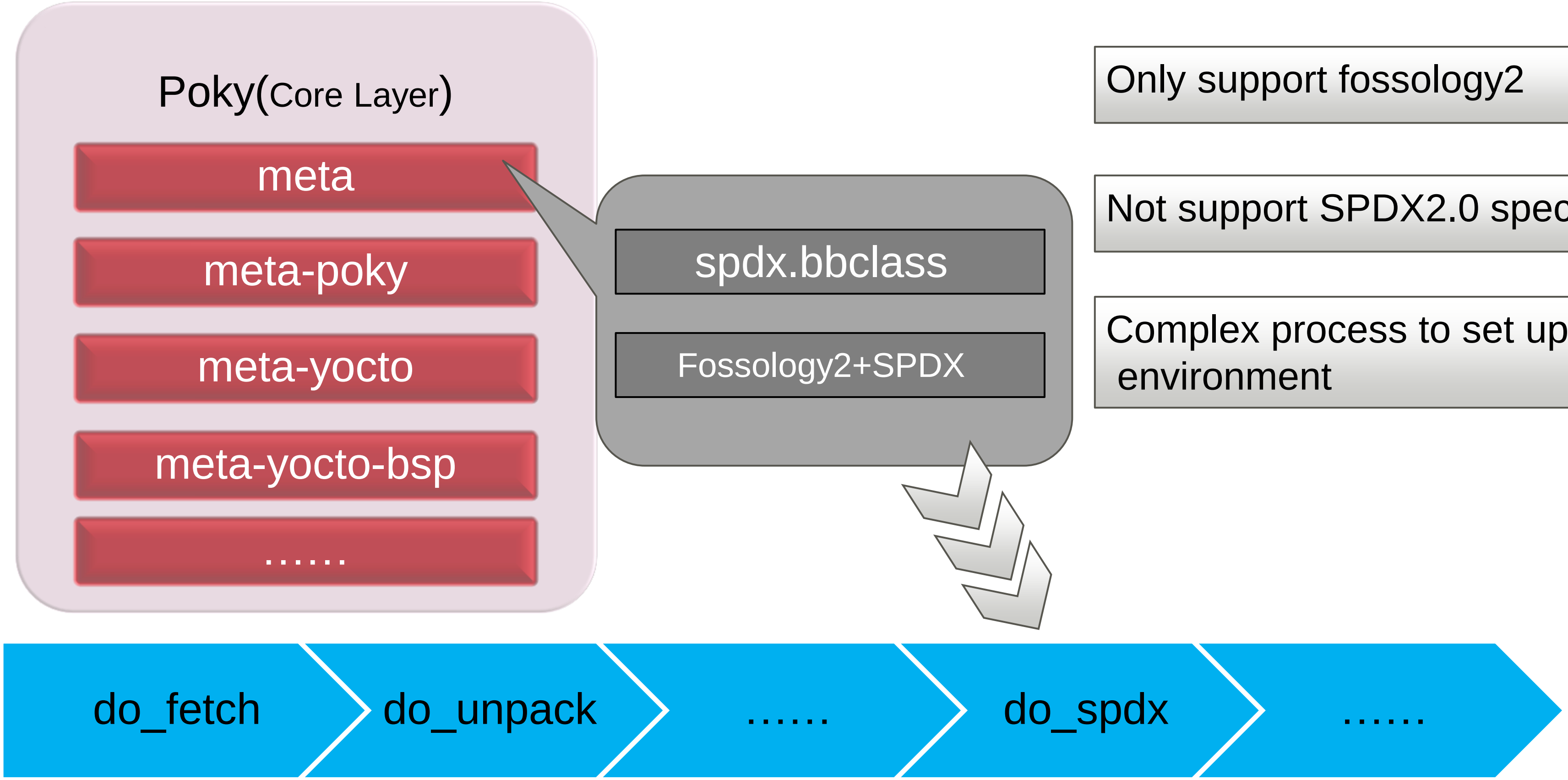
The project provides a flexible set of tools and a space where embedded developers worldwide can share technologies, software

The Yocto Project is an open source collaboration project that help you create custom Linux-based systems for embedded products

https://www.yoctoproject.org/

Overview of Yocto+SPDX (1/2)

spdx.bbclass



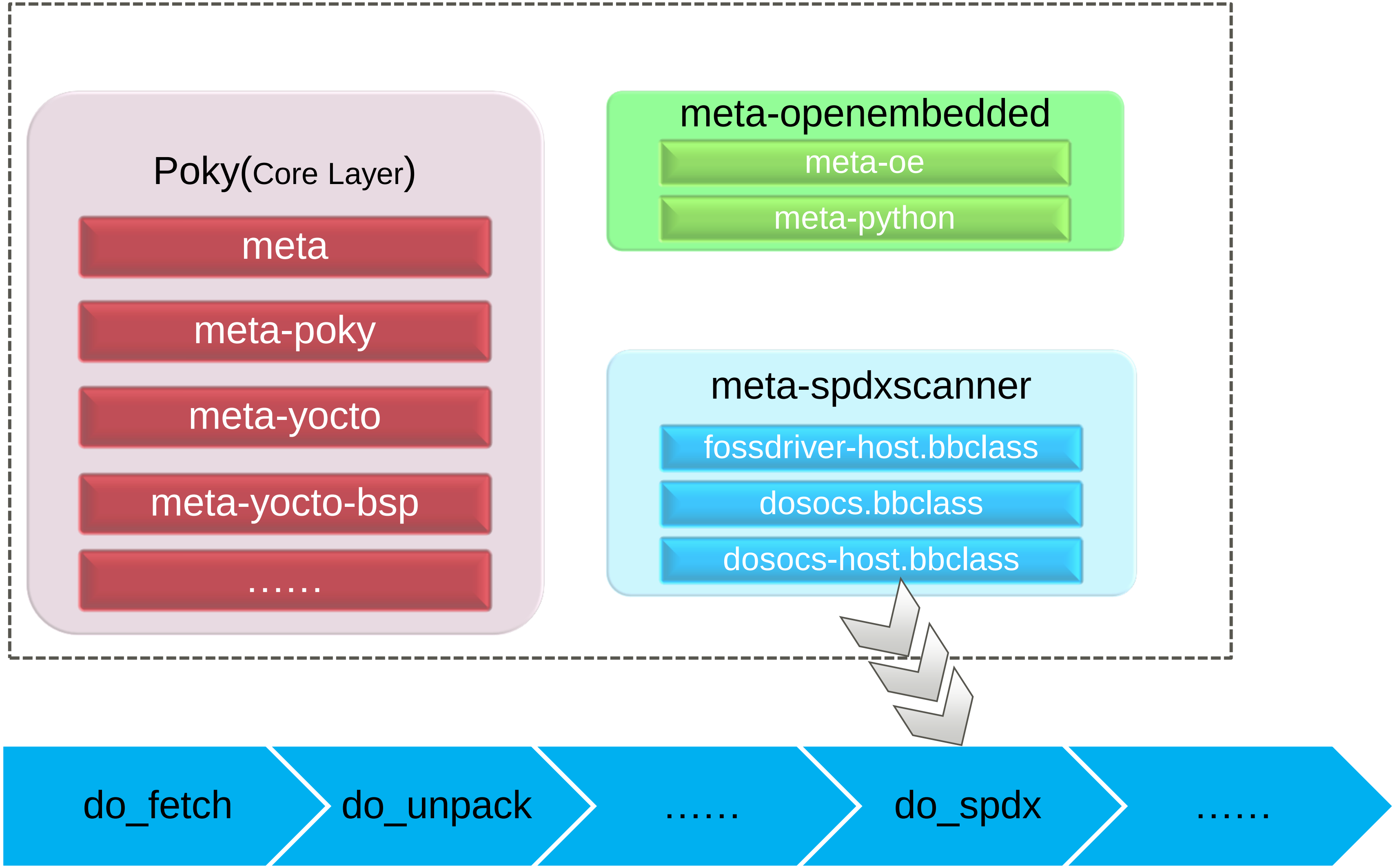
Only support fossology2

Not support SPDX2.0 spec

Complex process to set up environment

Overview of Yocto+SPDX (2/2)

Meta-spdxscanner


Poky(Core Layer)

meta

meta-poky

meta-yocto

meta-yocto-bsp

……

meta-openembedded

meta-oe

meta-python

meta-spdxscanner

fossdriver-host.bbclass

dosocs.bbclass

dosocs-host.bbclass

do_fetch

do_unpack

……

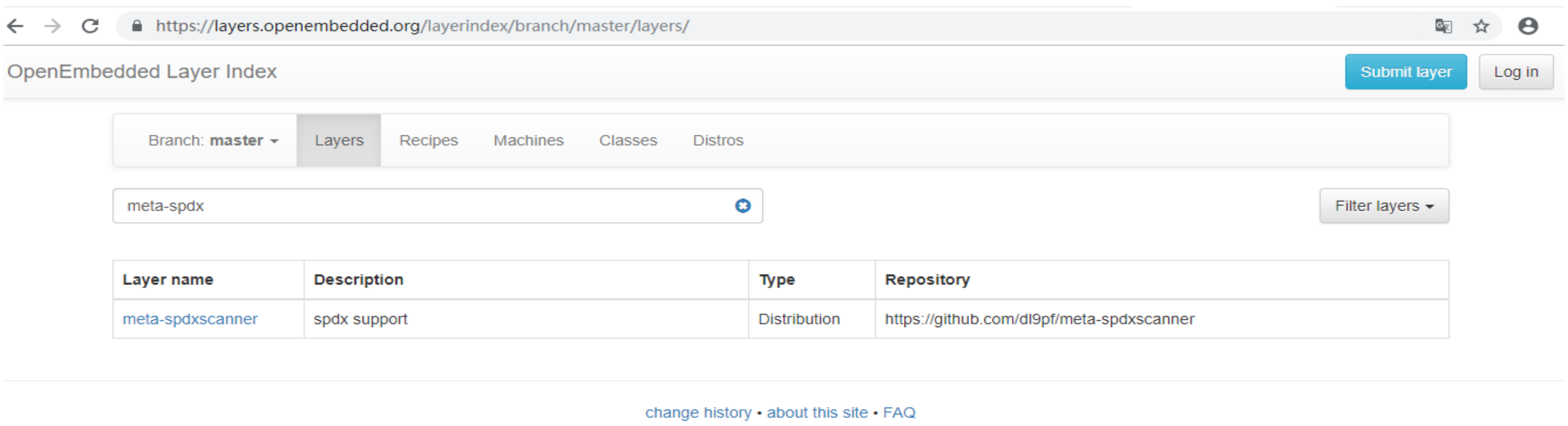
do_spdx

……

Meta-spdxscanner

- What is Meta-spdxscanner
- How to use
- What we have done for Meta-spdxscanner
- Features of fossdriver-host.bbclass
  - Reduce this layer's work time
  - Easier to use
  - More credible

What is Meta-spdxscanner

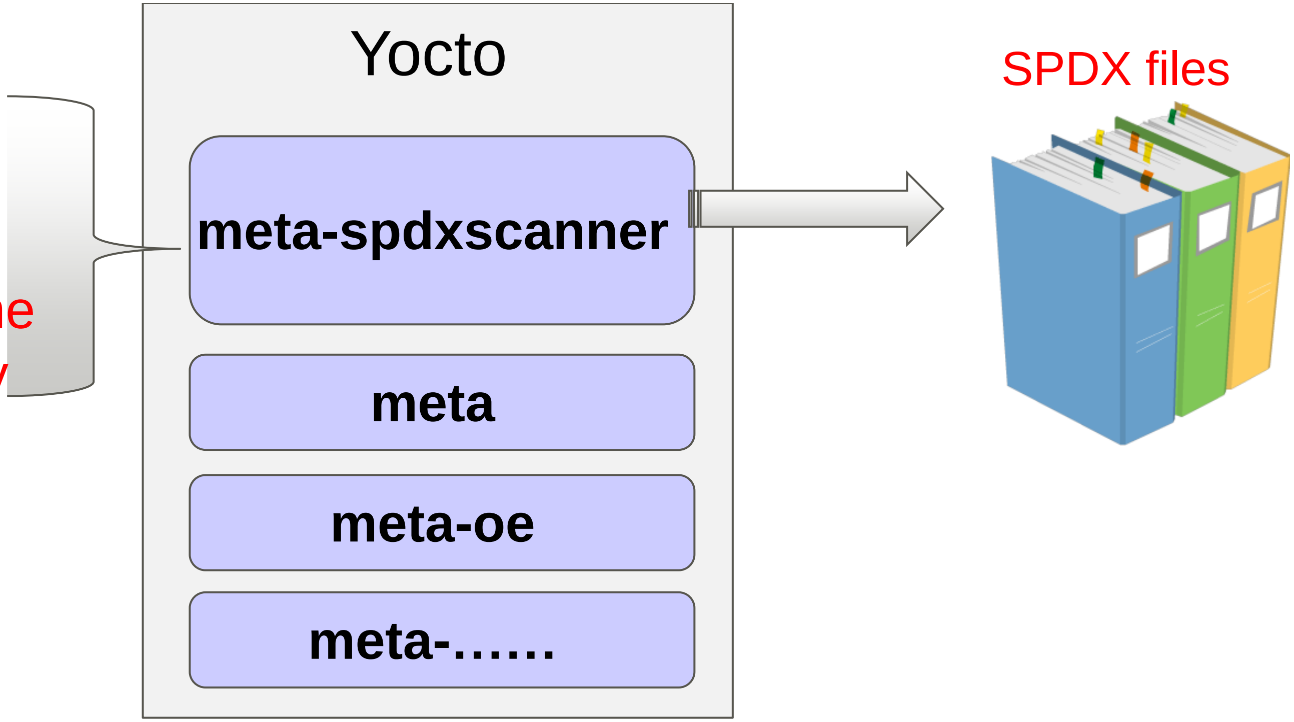


https://layers.openembedded.org/layerindex/branch/master/layers/

OpenEmbedded Layer Index

Layer name	Description	Type	Repository
meta-spdxscanner	spdx support	Distribution	https://github.com/dl9pf/meta-spdxscanner

- ■ FOSS
- □ Patches come from 3rd party



How to use

Deploy

- # ls /yocto/spdx-outdir-warrior
- acl-2.2.52.spdx   libusb-compat-0.1.5.spdx   python-manilaclient-1.4.0+gitAUTOINC+0bbd2144f7.spdx
  acpid-2.0.31.spdx libuser-0.62.spdx   python-markupsafe-1.0.spdx adcli-0.8.2.spdx
  libutempter-1.1.6-alt2+gitAUTOINC+3ef74fff31.spdx python-mccabe-0.4.0.spdx ……

⑤ Start building

- # cd [build_dir]
- # bitbake recipe/image

④ Edit local.conf

- # cd [build_dir]
- # tail –n 2 conf/local.conf

```
INHERIT += "fossdriver-host“
SPDX_DEPLOY_DIR = "/yocto/spdx-outdir-warrior"
```

③ Setup Yocto Build Environment

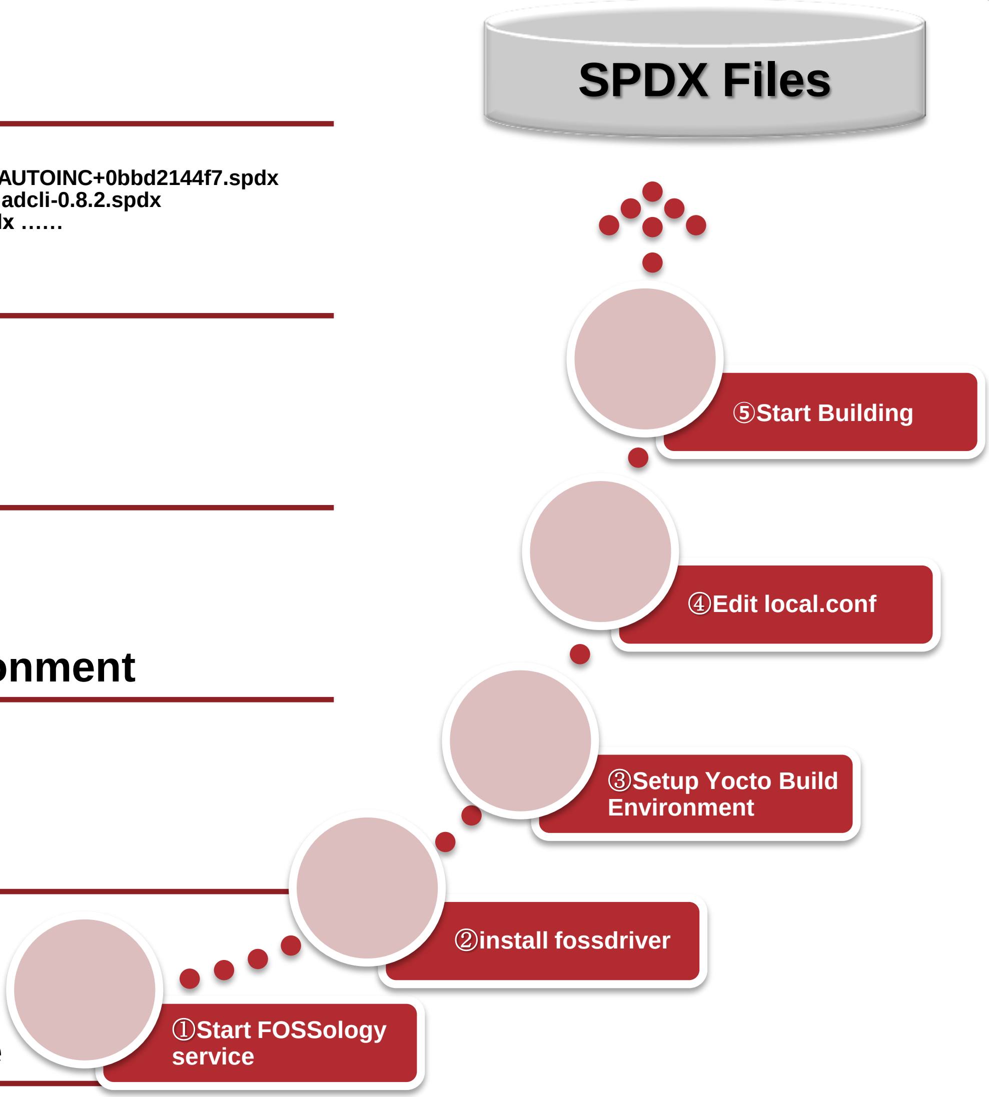
- # cd [yocto_dir]
- # source oe-init-build-env [build_dir]

② install fossdriver

- # pip install -e /WHEREVER/fossdriver
- # Create and edit a config file. E.g. .fossdriverrc

① Start FOSSology Service

- # docker pull fossology/fossology
- # docker run -p 8081:80 fossology/fossology



SPDX Files

⑤Start Building

④Edit local.conf

③Setup Yocto Build Environment

②install fossdriver

①Start FOSSology service

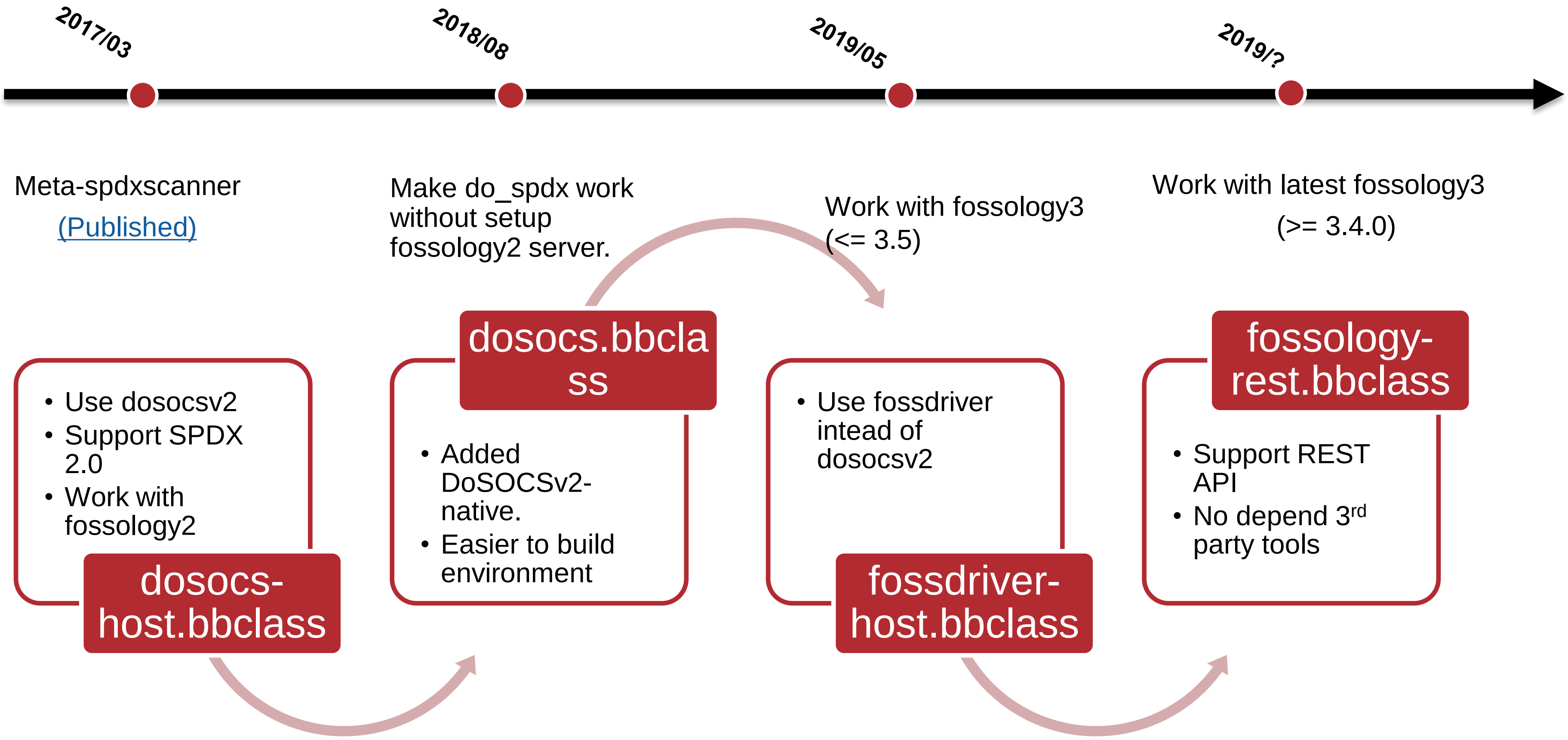
What we have done for Meta-spdxscanner(1/2)

History of SPDX create tools

Item	FOSSology+ SPDX	dosocsv2	fossdriver	Fossology REST API
URL	https://github.com/FOSSology-SPDX/fossology-spdx	https://github.com/DoSOCSv2/DoSOCSv2	https://github.com/fossology/fossdriver	https://www.fossology.org/
maintainer	University of Nebraska	University of Nebraska	Swinslow of linuxfoudation	fossology
License	Apache-2.0	GPLv2	BSD-3-Clause OR MIT	GPL-2.0
Support SPDX version	1.2	2.0	2.1	2.1
Support fosslogy	Fossology 2	Fossology3	Fossology3 <=3.5	Fossology3 >=3.4.0
Support multitask	√			√
Reuse prior results		√	√	√

Now

What we have done for Meta-spdxscanner(2/2)



2017/03

Meta-spdxscanner

(Published)

- Use dosocsv2
- Support SPDX 2.0
- Work with fossology2

dosocs-host.bbclass

2018/08

Make do_spdx work without setup fossology2 server.

dosocs.bbclass

- Added DoSOCSv2-native.
- Easier to build environment

2019/05

Work with fossology3 (<= 3.5)

- Use fossdriver intead of dosocsv2

fossdriver-host.bbclass

2019/?

Work with latest fossology3

(>= 3.4.0)

fossology-rest.bbclass

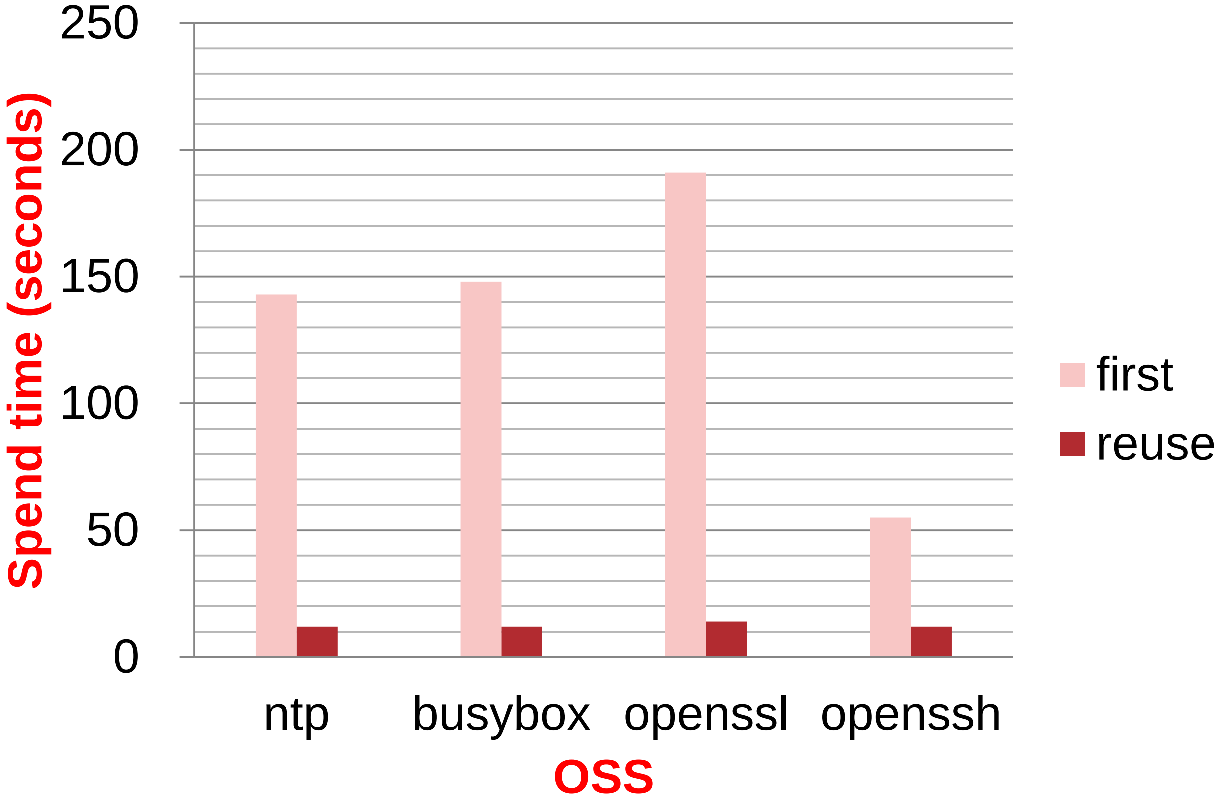
- Support REST API
- No depend 3rd party tools

Features of fossdriver-host.bbclass (1/3)

Reduce this layer's work time

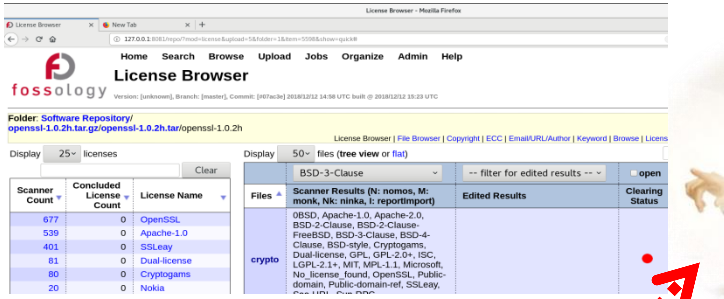
- Support multitask do_spdx

- Can reuse prior results



Features of fossdriver-host.bbclass (2/3)

Easier to use



License Browser - Mozilla Firefox

127.0.0.1:8081/repo/?mod=license&upload=5&folder=1&item=5598&show=quick#

License Browser

Version: [unknown], Branch: [master], Commit: [#07ac3e] 2018/12/12 14:58 UTC built @ 2018/12/12 15:23 UTC

Folder: Software Repository/ openssl-1.0.2h.tar.gz/openssl-1.0.2h.tar/openssl-1.0.2h

License Browser | File Browser | Copyright | ECC | Email/URL/Author | Keyword | Browse | Licens

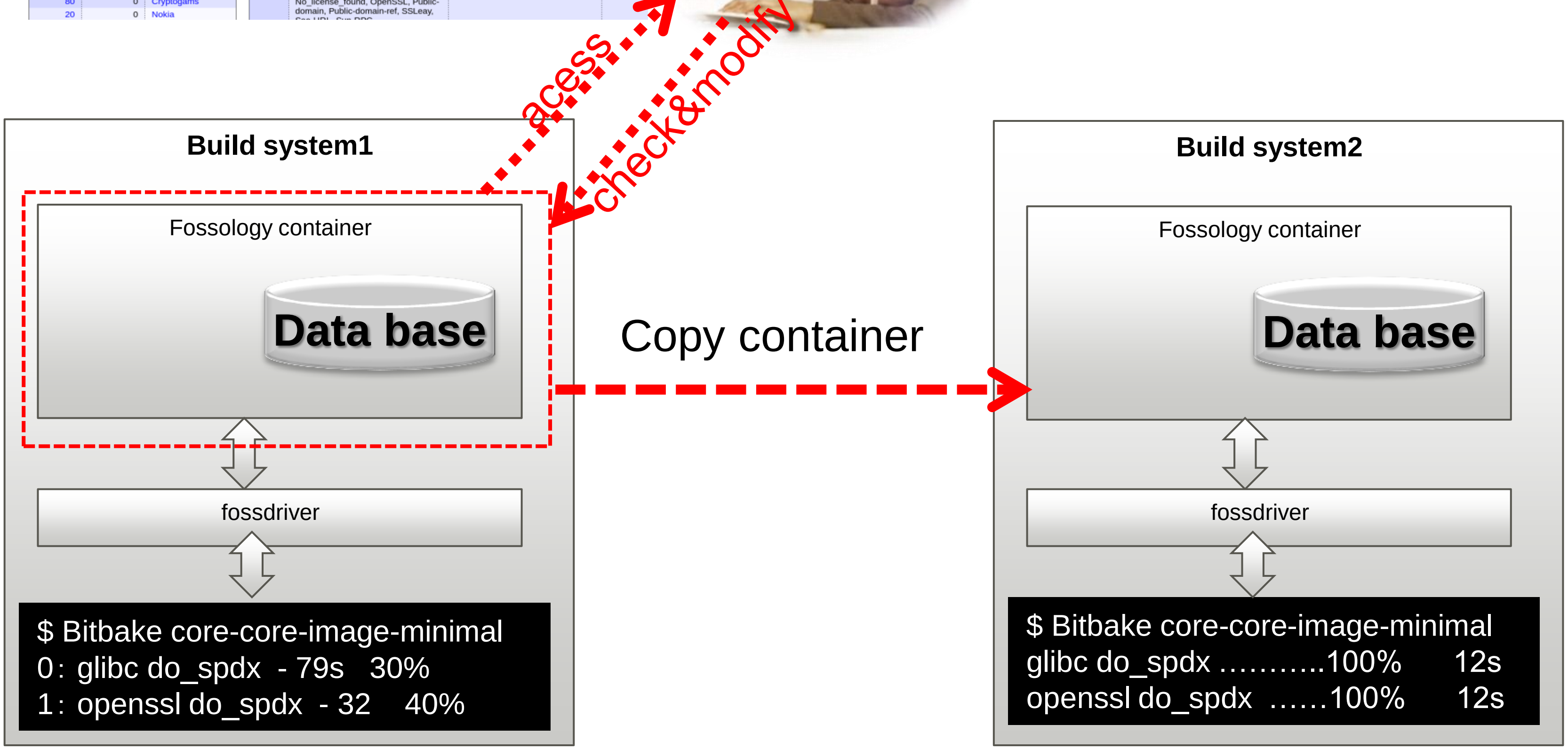
Display 25 licenses

Scanner Count	Concluded License Count	License Name
677	0	OpenSSL
539	0	Apache-1.0
401	0	SSLeay
81	0	Dual-license
80	0	Cryptogams
20	0	Nokia

Display 50 files (**tree view** or flat)

	BSD-3-Clause	-- filter for edited results --	□ open
Files	Scanner Results (N: nomos, M: monk, Nk: ninka, I: reportImport)	Edited Results	Clearing Status
crypto	0BSD, Apache-1.0, Apache-2.0, BSD-2-Clause, BSD-2-Clause-FreeBSD, BSD-3-Clause, BSD-4-Clause, BSD-style, Cryptogams, Dual-license, GPL, GPL-2.0+, ISC, LGPL-2.1+, MIT, MPL-1.1, Microsoft, No_license_found, OpenSSL, Public-domain, Public-domain-ref, SSLeay,		●

Legal team

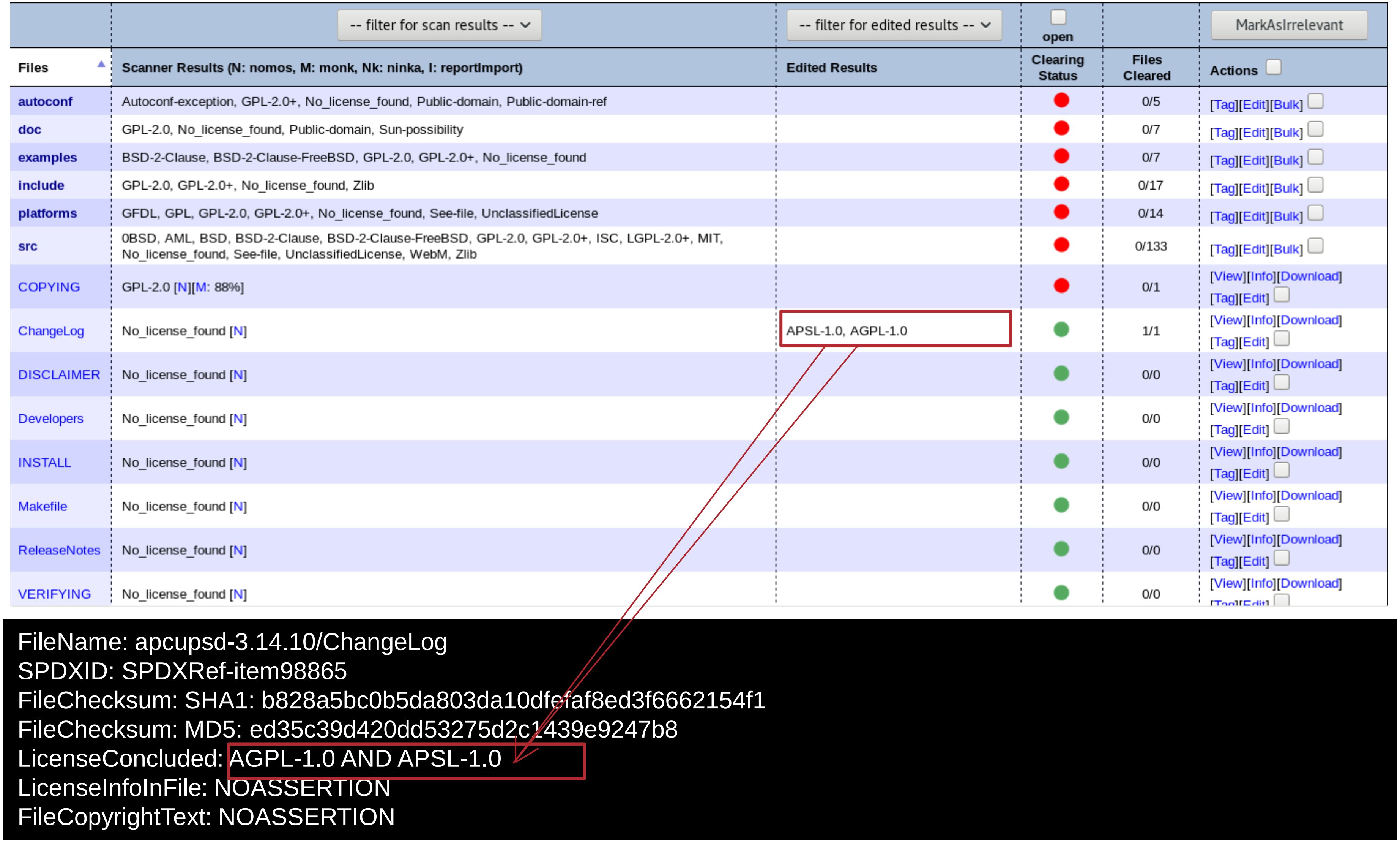


```
$ Bitbake core-core-image-minimal
0: glibc do_spdx  - 79s   30%
1: openssl do_spdx  - 32    40%
```

```
$ Bitbake core-core-image-minimal
glibc do_spdx ………..100%      12s
openssl do_spdx  ……100%      12s
```

Features of fossdriver-host.bbclass (3/3)

More credible



	-- filter for scan results --	-- filter for edited results --	□ open		MarkAsIrrelevant
Files	Scanner Results (N: nomos, M: monk, Nk: ninka, I: reportImport)	Edited Results	Clearing Status	Files Cleared	Actions □
autoconf	Autoconf-exception, GPL-2.0+, No_license_found, Public-domain, Public-domain-ref		🔴	0/5	[Tag][Edit][Bulk] □
doc	GPL-2.0, No_license_found, Public-domain, Sun-possibility		🔴	0/7	[Tag][Edit][Bulk] □
examples	BSD-2-Clause, BSD-2-Clause-FreeBSD, GPL-2.0, GPL-2.0+, No_license_found		🔴	0/7	[Tag][Edit][Bulk] □
include	GPL-2.0, GPL-2.0+, No_license_found, Zlib		🔴	0/17	[Tag][Edit][Bulk] □
platforms	GFDL, GPL, GPL-2.0, GPL-2.0+, No_license_found, See-file, UnclassifiedLicense		🔴	0/14	[Tag][Edit][Bulk] □
src	0BSD, AML, BSD, BSD-2-Clause, BSD-2-Clause-FreeBSD, GPL-2.0, GPL-2.0+, ISC, LGPL-2.0+, MIT, No_license_found, See-file, UnclassifiedLicense, WebM, Zlib		🔴	0/133	[Tag][Edit][Bulk] □
COPYING	GPL-2.0 [N][M: 88%]		🔴	0/1	[View][Info][Download] [Tag][Edit] □
ChangeLog	No_license_found [N]	APSL-1.0, AGPL-1.0	🟢	1/1	[View][Info][Download] [Tag][Edit] □
DISCLAIMER	No_license_found [N]		🟢	0/0	[View][Info][Download] [Tag][Edit] □
Developers	No_license_found [N]		🟢	0/0	[View][Info][Download] [Tag][Edit] □
INSTALL	No_license_found [N]		🟢	0/0	[View][Info][Download] [Tag][Edit] □
Makefile	No_license_found [N]		🟢	0/0	[View][Info][Download] [Tag][Edit] □
ReleaseNotes	No_license_found [N]		🟢	0/0	[View][Info][Download] [Tag][Edit] □
VERIFYING	No_license_found [N]		🟢	0/0	[View][Info][Download] [Tag][Edit] □

```
FileName: apcupsd-3.14.10/ChangeLog
SPDXID: SPDXRef-item98865
FileChecksum: SHA1: b828a5bc0b5da803da10dfefaf8ed3f6662154f1
FileChecksum: MD5: ed35c39d420dd53275d2c1439e9247b8
LicenseConcluded: AGPL-1.0 AND APSL-1.0
LicenseInfoInFile: NOASSERTION
FileCopyrightText: NOASSERTION
```

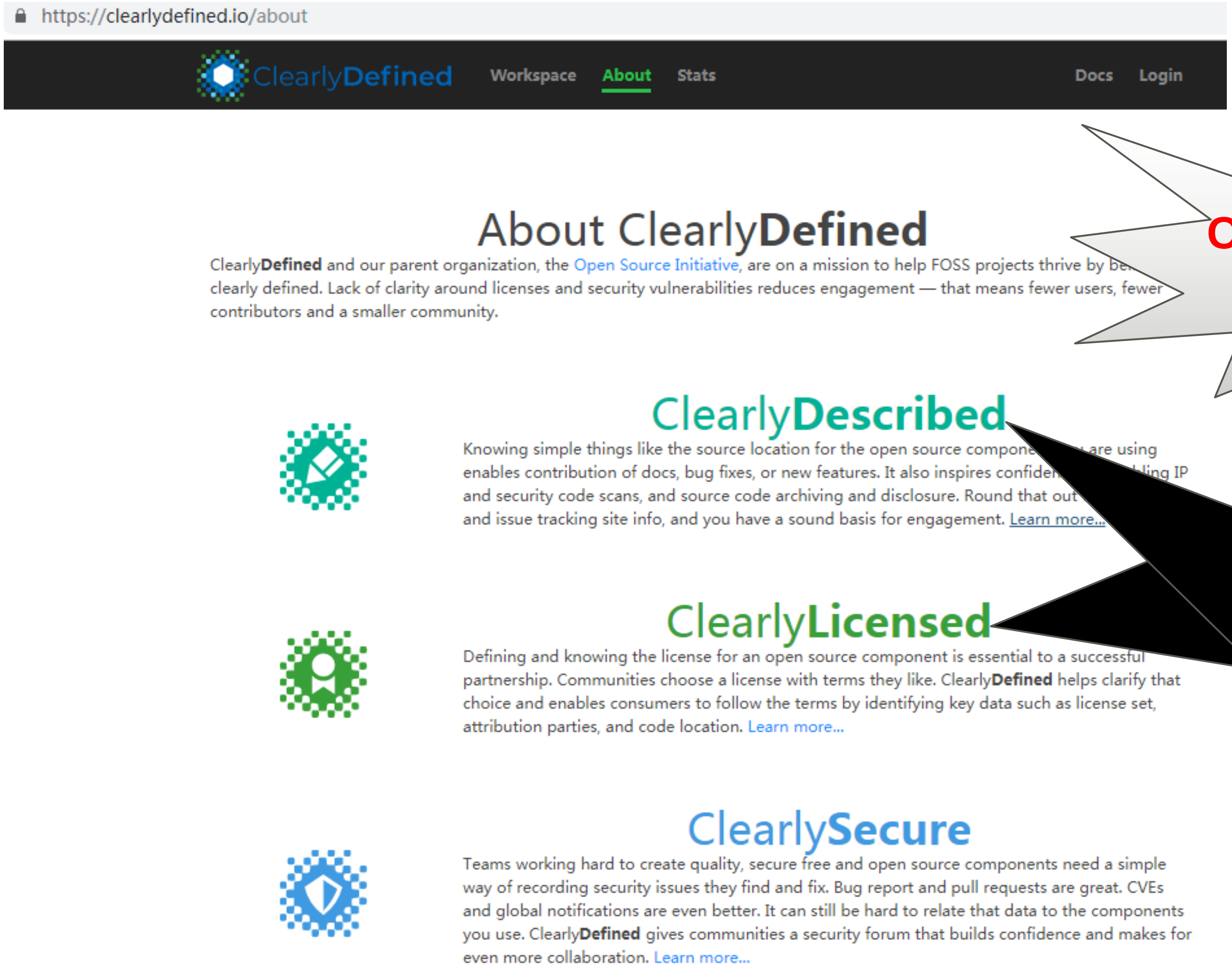
Manage SPDX

- Work with ClearlyDefined
- Work with OpenChain
- Manage SPDX files by dnf-plugin-tui
- Future work

Work with ClearlyDefined (1/2)

FUJITSU

What is ClearlyDefined



https://clearlydefined.io/about

About ClearlyDefined

ClearlyDefined and our parent organization, the Open Source Initiative, are on a mission to help FOSS projects thrive by be clearly defined. Lack of clarity around licenses and security vulnerabilities reduces engagement — that means fewer users, fewer contributors and a smaller community.

ClearlyDescribed

Knowing simple things like the source location for the open source compone are using enables contribution of docs, bug fixes, or new features. It also inspires confide ling IP and security code scans, and source code archiving and disclosure. Round that out and issue tracking site info, and you have a sound basis for engagement. Learn more...

ClearlyLicensed

Defining and knowing the license for an open source component is essential to a successful partnership. Communities choose a license with terms they like. ClearlyDefined helps clarify that choice and enables consumers to follow the terms by identifying key data such as license set, attribution parties, and code location. Learn more...

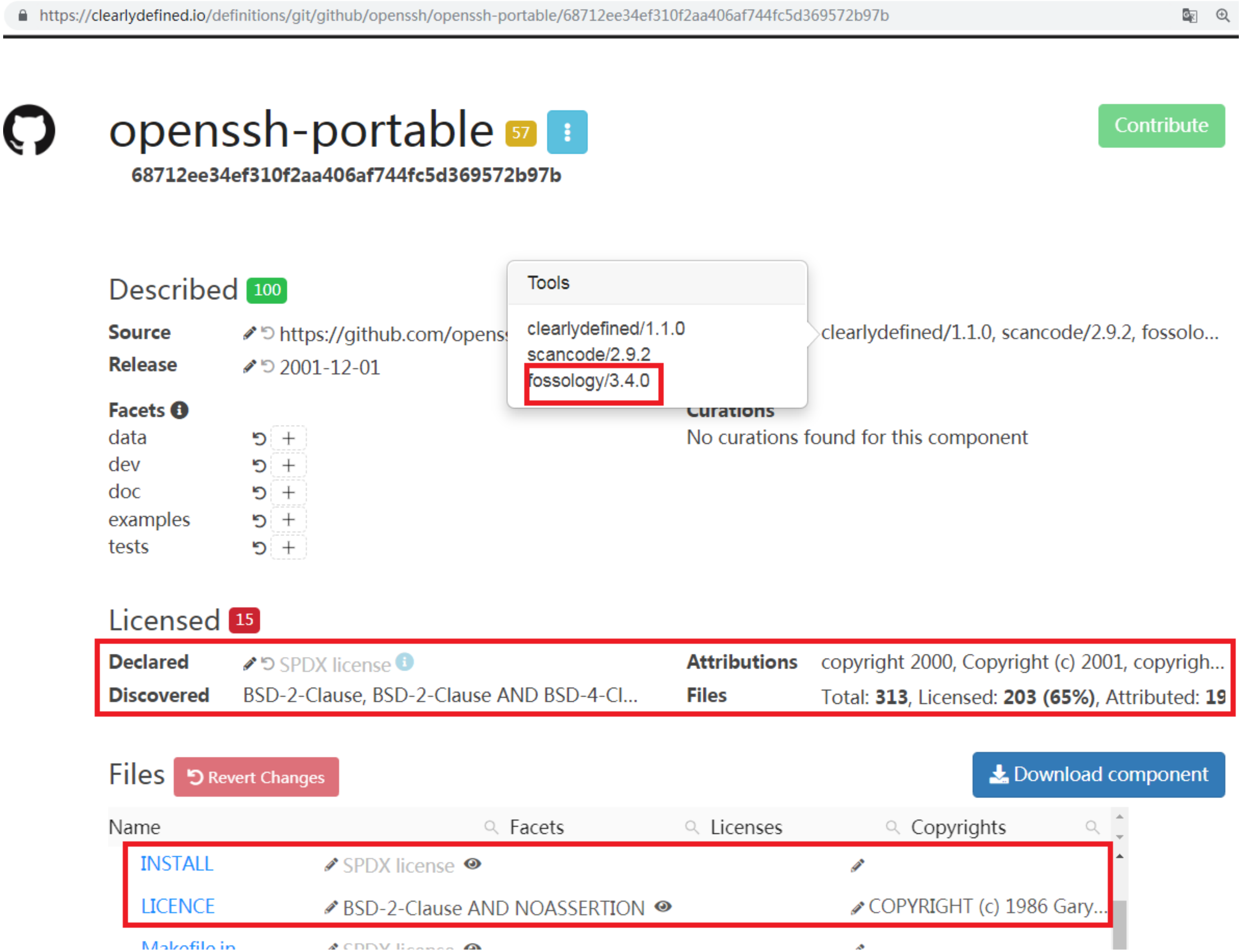
ClearlySecure

Teams working hard to create quality, secure free and open source components need a simple way of recording security issues they find and fix. Bug report and pull requests are great. CVEs and global notifications are even better. It can still be hard to relate that data to the components you use. ClearlyDefined gives communities a security forum that builds confidence and makes for even more collaboration. Learn more...

Can be get from spdx files

```
$ Les openssh-7.9p1.spdx
PackageName: openssh
PackageVersion: 7.9p1
PackageFileName: openssh-7.9p1-r0-…
SPDXID: SPDXRef-upload265
PackageDownloadLocation: http://ftp.op...
PackageHomePage: http://www.openssh.
PackageSummary: ……
……
FileName: spdx_temp/openssh-7.9p1/LICEN
SPDXID: SPDXRef-item671105
FileChecksum: SHA1: 6f569d09a2bd52b…
FileChecksum: MD5: 429658c6612f3a9b…
LicenseConcluded: NOASSERTION
LicenseInfoInFile: X11
LicenseInfoInFile: BSD-2-Clause
LicenseInfoInFile: MIT
LicenseInfoInFile: BSD-3-Clause
……
```

Work with ClearlyDefined (2/2)



https://clearlydefined.io/definitions/git/github/openssh/openssh-portable/68712ee34ef310f2aa406af744fc5d369572b97b

openssh-portable 57

68712ee34ef310f2aa406af744fc5d369572b97b

Contribute

Described 100

Source https://github.com/opens

Release 2001-12-01

Tools

clearlydefined/1.1.0
scancode/2.9.2
fossology/3.4.0

clearlydefined/1.1.0, scancode/2.9.2, fossolo...

Facets

data
dev
doc
examples
tests

Curations

No curations found for this component

Licensed 15

Declared SPDX license

Discovered BSD-2-Clause, BSD-2-Clause AND BSD-4-Cl...

Attributions copyright 2000, Copyright (c) 2001, copyrigh...

Files Total: **313**, Licensed: **203 (65%)**, Attributed: **19**

Files

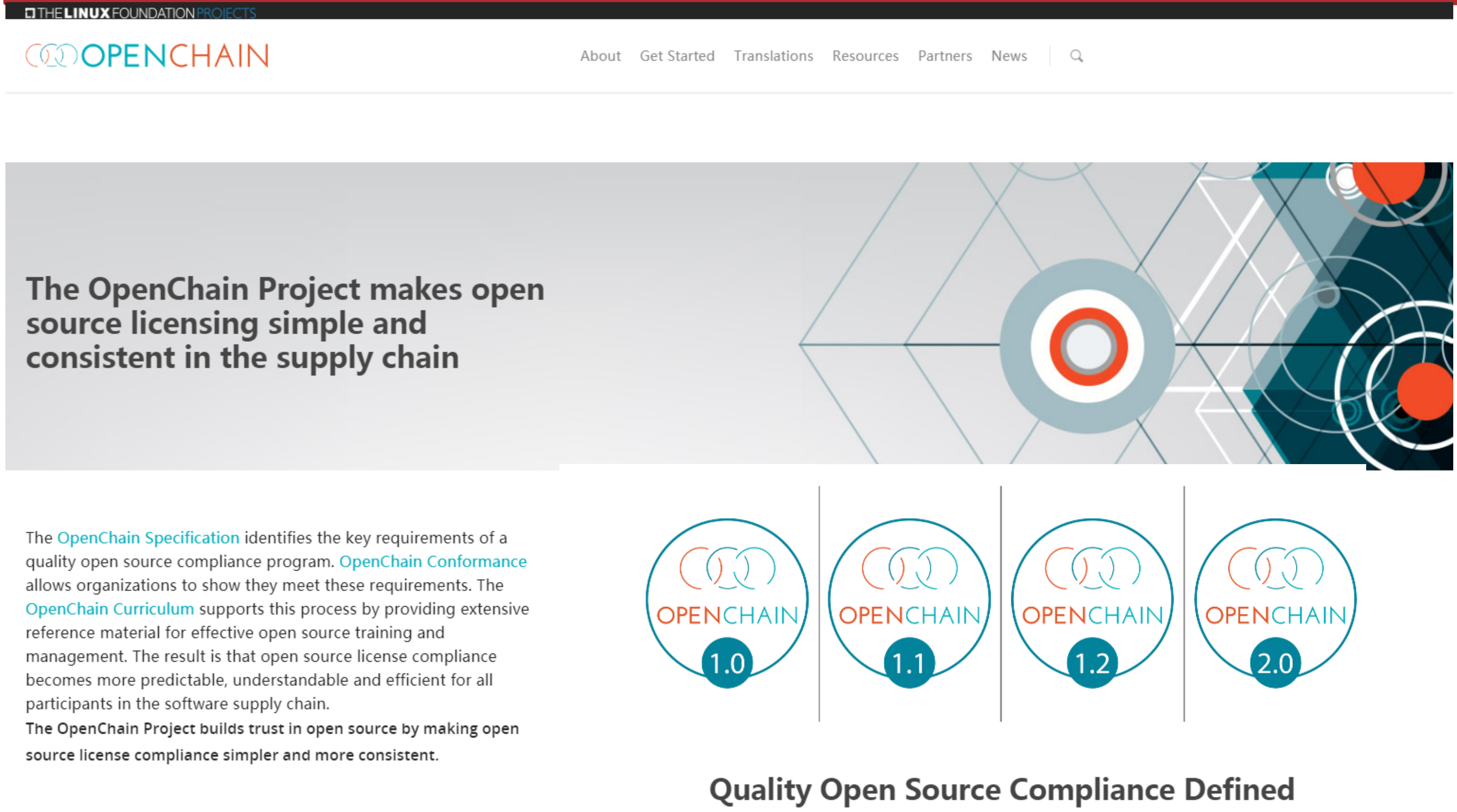
Revert Changes

Download component

Name	Facets	Licenses	Copyrights
INSTALL		SPDX license	
LICENCE		BSD-2-Clause AND NOASSERTION	COPYRIGHT (c) 1986 Gary...
Makefile.in		SPDX license	

Work with OpenChain (1/3)

What is openchain



The OpenChain Project makes open source licensing simple and consistent in the supply chain

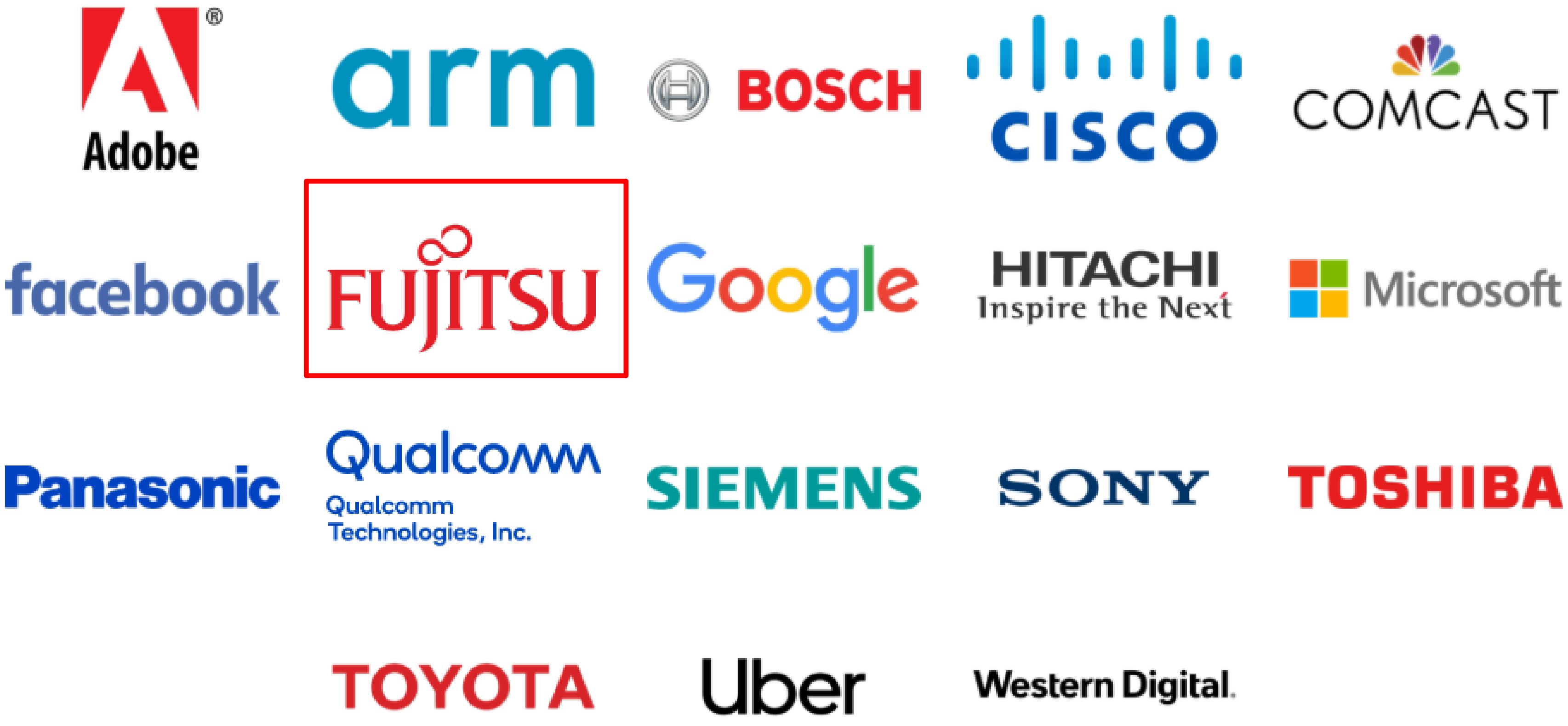
The OpenChain Specification identifies the key requirements of a quality open source compliance program. OpenChain Conformance allows organizations to show they meet these requirements. The OpenChain Curriculum supports this process by providing extensive reference material for effective open source training and management. The result is that open source license compliance becomes more predictable, understandable and efficient for all participants in the software supply chain.

The OpenChain Project builds trust in open source by making open source license compliance simpler and more consistent.

Quality Open Source Compliance Defined

Work with OpenChain (2/3)

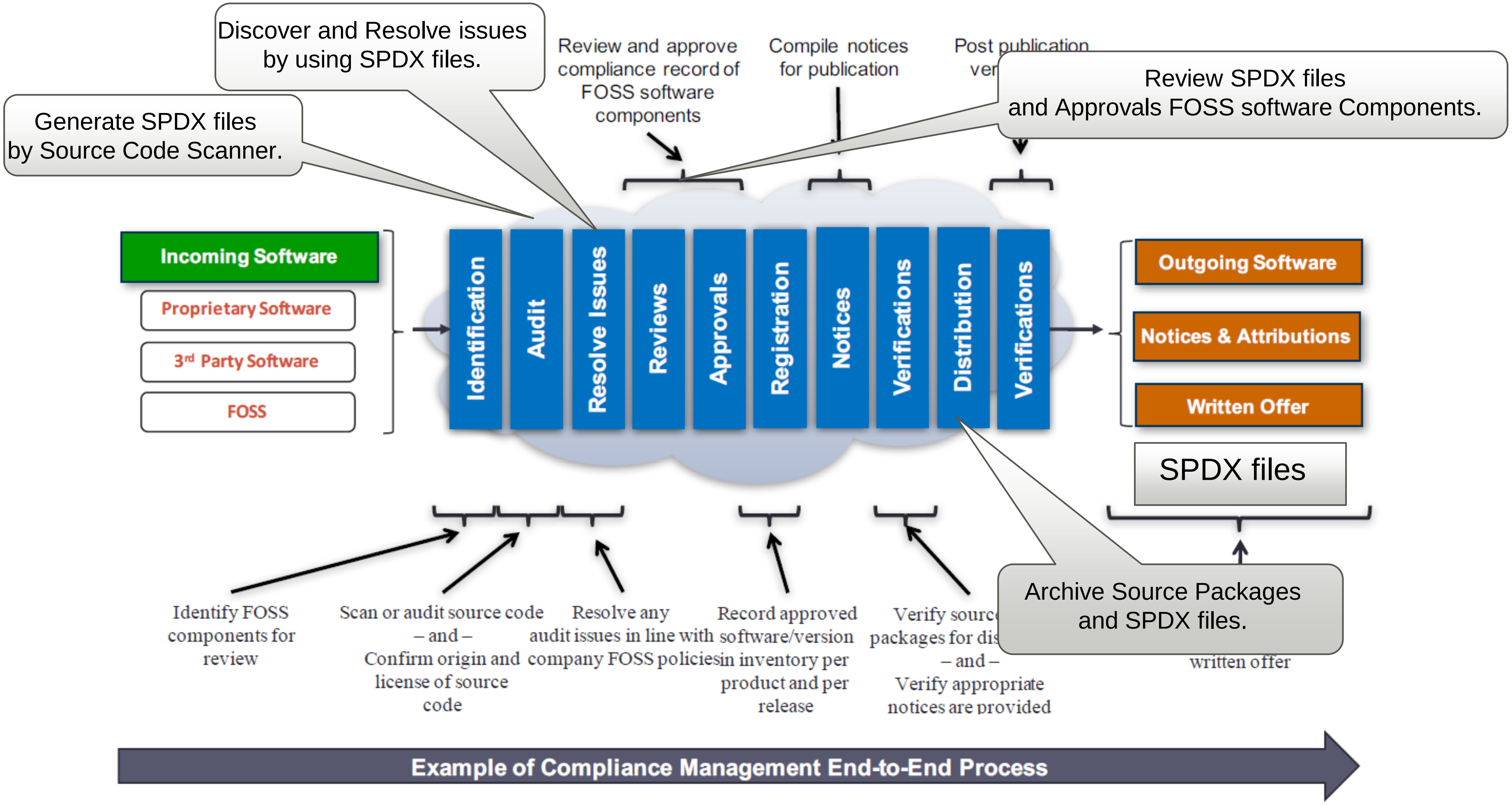
The Companies behind OpenChain



Work with OpenChain (3/3)

FUJITSU

an example of an enterprise process comes from OpenChain



Discover and Resolve issues by using SPDX files.

Generate SPDX files by Source Code Scanner.

Review SPDX files and Approvals FOSS software Components.

Archive Source Packages and SPDX files.

Review and approve compliance record of FOSS software components
Compile notices for publication
Post publication ver
Incoming Software
Proprietary Software
3rd Party Software
FOSS
Identification
Audit
Resolve Issues
Reviews
Approvals
Registration
Notices
Verifications
Distribution
Verifications
Outgoing Software
Notices & Attributions
Written Offer
SPDX files
Identify FOSS components for review
Scan or audit source code – and – Confirm origin and license of source code
Resolve any audit issues in line with company FOSS policies
Record approved software/version in inventory per product and per release
Verify source packages for dis – and – Verify appropriate notices are provided
written offer
Example of Compliance Management End-to-End Process

https://wiki.linuxfoundation.org/_media/openchain/openchain-curriculum-for-1-1.pdf

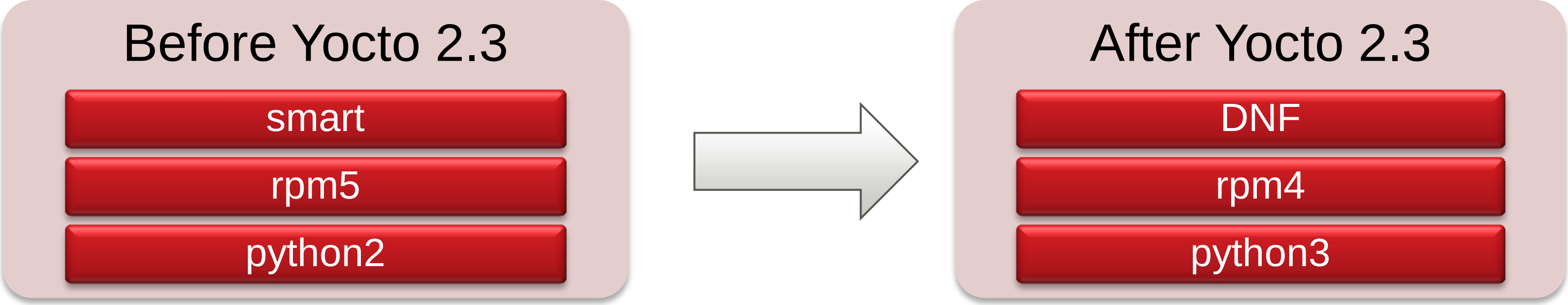
Manage SPDX files by dnf-plugin-tui(1/2)

What is dnf-plugin-tui

- A plugin of dnf that can manage packages created by YP on host.

Why we use dnf-plugin-tui

- Because rpm5 will be replaced by rpm4 from Yocto 2.3 due to the version change of python, Upstream (Yocto) pretends to use DNF from Yocto 2.3 as DNF is more suitable for rpm4.

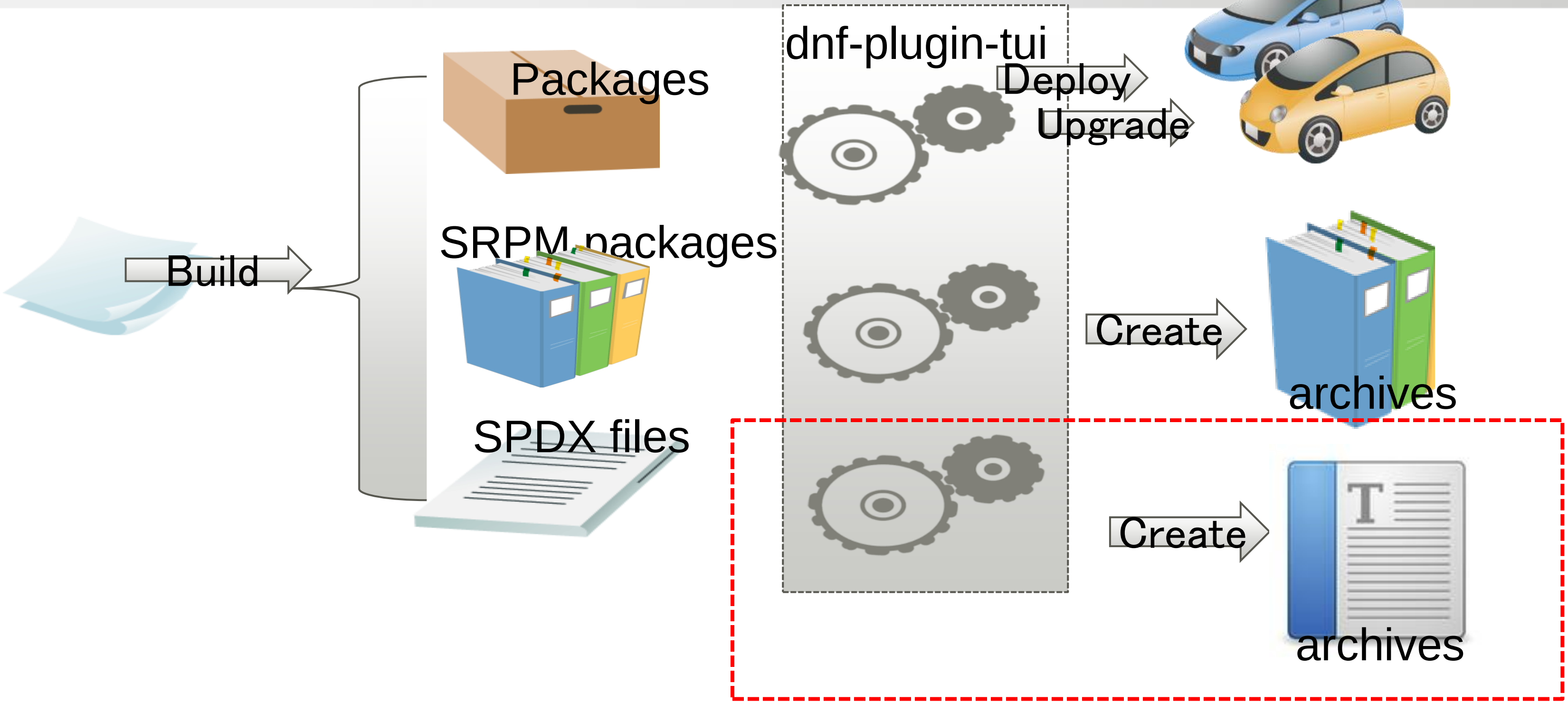


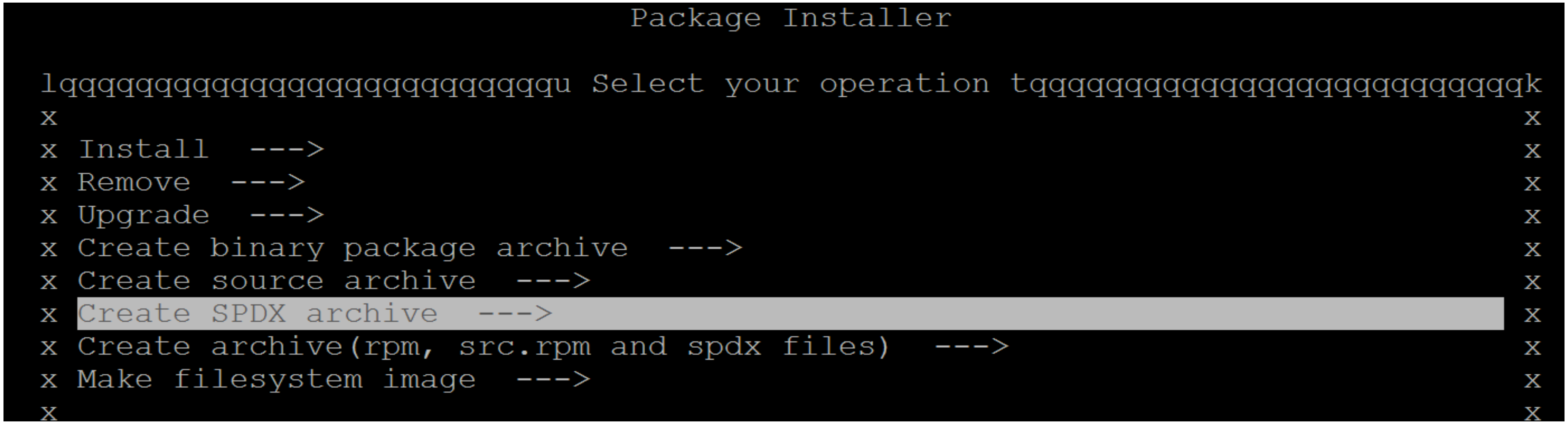
Features of dnf-plugin-tui

- Text-based user interface for dnf
- Manage SPDX files
- Manage SRPM file

https://github.com/ubinux/dnf-plugin-tui

Manage SPDX files by dnf-plugin-tui(2/2)





```
                         Package Installer

lqqqqqqqqqqqqqqqqqqqqqqqqqqqu Select your operation tqqqqqqqqqqqqqqqqqqqqqqqqqk
x                                                                              x
x Install   --->                                                               x
x Remove   --->                                                                x
x Upgrade   --->                                                               x
x Create binary package archive  --->                                          x
x Create source archive  --->                                                  x
x Create SPDX archive  --->                                                    x
x Create archive(rpm, src.rpm and spdx files)  --->                            x
x Make filesystem image  --->                                                  x
x                                                                              x
```

Future work

- Maintain meta-spdxscanner
  - Solve issues
  - Meet more user case

- Added fossology REST API support
  - There will be no necessary to install tools come from 3rd party.
  - Maintained by fosslogy, can get long-term stable technical support.

Q&A

Any Questions?

FUJITSU

shaping tomorrow with you