

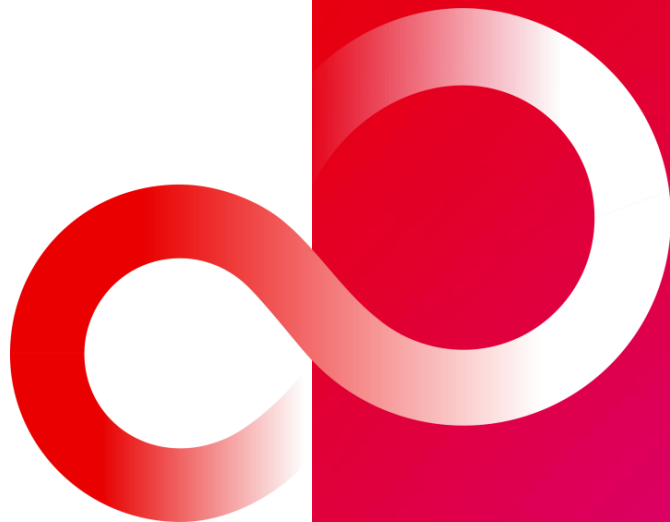
How to enhance compliance for Linux ecosystem

强化Linux生态合规性

OCT 22nd, 2022

Lei Maohui, Fujitsu

leimaohui@fujitsu.com



- Working for Fujitsu from 2011
- 9 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.



View of SPDX

- What is SPDX
- Features of SPDX
- Adopted by more and more OSS

SPDX Create Tools

- fossology
- ScanCode
- Meta-spdxscanner

Our work to enhance compliance

- Work with OpenChain
- Manage SPDX files by dnf-plugin-tui in our Linux ecosystem

View of SPDX

- ❑ What is SPDX
- ❑ Features of SPDX
- ❑ Adopted by more and more OSS
- ❑ SPDX Supporters

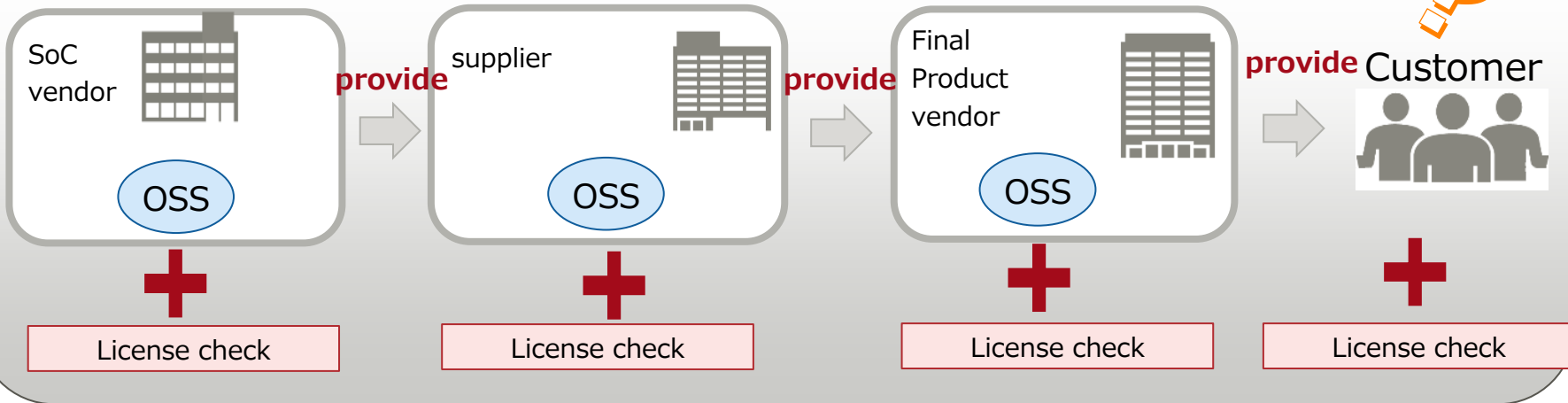
What is SPDX

- OSS developers, Distro Vendors, OSS users must know the license of the OSS software clearly. Maybe we have problems as below.

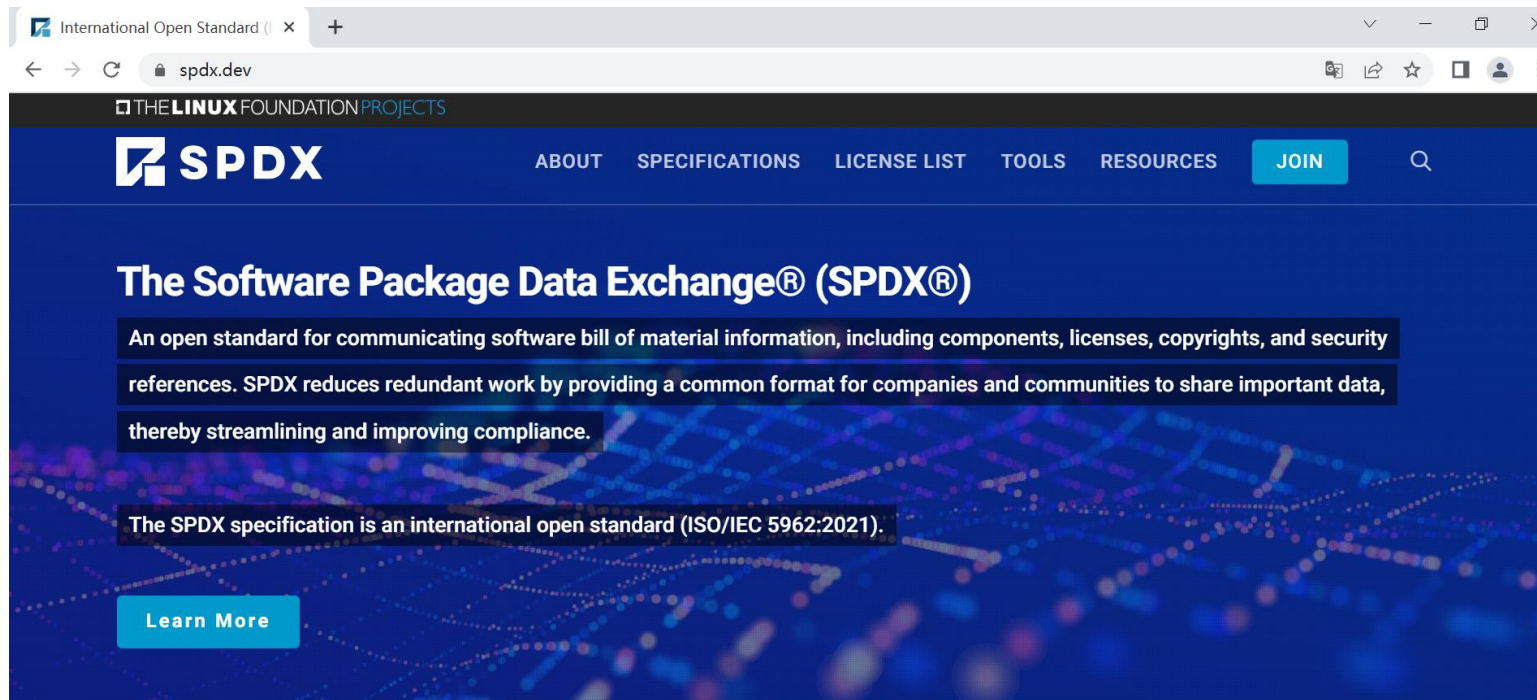
- How to determine whether an OSS is a **License-Mixing one**.
- It's a big project to determine **lots of OSS** what we provided.



- Too many redundant work in a supply chain to check license.



What is SPDX

A screenshot of the SPDX website in a web browser. The browser's address bar shows 'spdx.dev'. The website header includes 'THE LINUX FOUNDATION PROJECTS' and the 'SPDX' logo. Navigation links include 'ABOUT', 'SPECIFICATIONS', 'LICENSE LIST', 'TOOLS', 'RESOURCES', and a 'JOIN' button. The main content area features the title 'The Software Package Data Exchange® (SPDX®)' followed by a descriptive paragraph: 'An open standard for communicating software bill of material information, including components, licenses, copyrights, and security references. SPDX reduces redundant work by providing a common format for companies and communities to share important data, thereby streamlining and improving compliance.' Below this is another line of text: 'The SPDX specification is an international open standard (ISO/IEC 5962:2021).' and a 'Learn More' button. The background of the main content area is a blue abstract pattern of dots and lines.

International Open Standard (x +

spdx.dev

THE LINUX FOUNDATION PROJECTS

SPDX

ABOUT SPECIFICATIONS LICENSE LIST TOOLS RESOURCES JOIN

The Software Package Data Exchange® (SPDX®)

An open standard for communicating software bill of material information, including components, licenses, copyrights, and security references. SPDX reduces redundant work by providing a common format for companies and communities to share important data, thereby streamlining and improving compliance.

The SPDX specification is an international open standard (ISO/IEC 5962:2021).

Learn More



What is SPDX

History

Origin

- The "SPDX" name was adopted

2010/02

SPDX v1.0

- Specification 1.0 released

2011/08

SPDX 2.0

- Specification 2.0 released

2015/05

SPDX v2.1

- Specification 2.1 released

2016/10

SPDX v2.2

- Specification 2.2 released

2020/05

SPDX v2.3

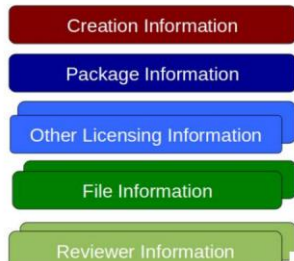
- Specification 2.3 released

2022/08

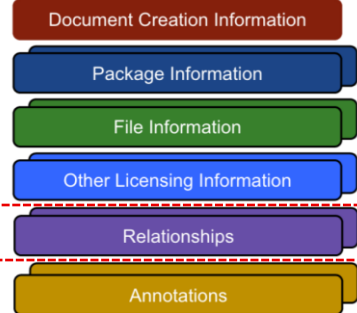
ISO/IEC
5962:2021
2022/09

Features in SPDX

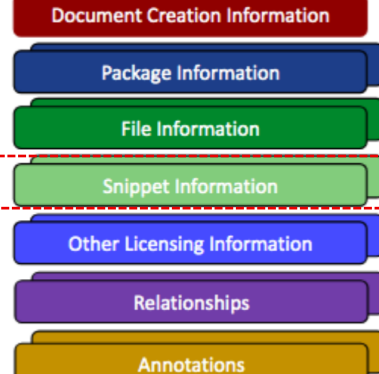
SPDX File v1.0



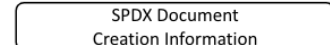
SPDX v2.0 File



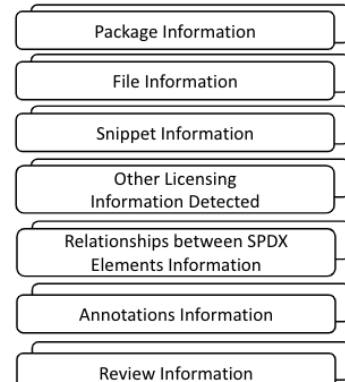
SPDX v2.2 Document contains:



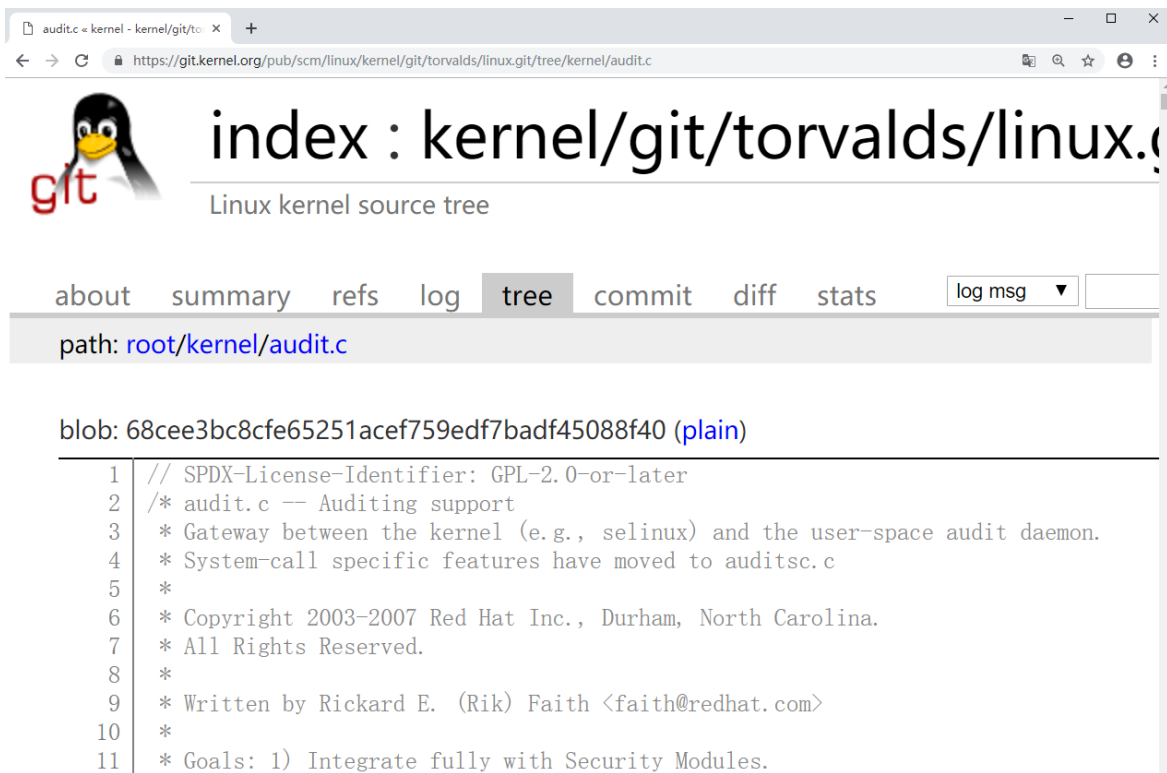
SPDX v2.3 Document shall contain:



SPDX v2.3 Document may contain:



Adopted by more and more OSS



The screenshot shows a web browser displaying the GitHub repository for the Linux kernel source tree. The URL is `https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/tree/kernel/audit.c`. The page title is "index : kernel/git/torvalds/linux.c" and the subtitle is "Linux kernel source tree". The navigation bar includes links for "about", "summary", "refs", "log", "tree" (which is selected), "commit", "diff", and "stats". Below the navigation bar, the path is shown as "path: [root/kernel/audit.c](#)". The blob ID is "blob: 68cee3bc8cfe65251acef759edf7badf45088f40 (plain)". The code content is displayed in a monospaced font, showing the SPDX license identifier and the purpose of the file.

```
1 // SPDX-License-Identifier: GPL-2.0-or-later
2 /* audit.c -- Auditing support
3  * Gateway between the kernel (e.g., selinux) and the user-space audit daemon.
4  * System-call specific features have moved to auditd.c
5  *
6  * Copyright 2003-2007 Red Hat Inc., Durham, North Carolina.
7  * All Rights Reserved.
8  *
9  * Written by Rickard E. (Rik) Faith <faith@redhat.com>
10 *
11 * Goals: 1) Integrate fully with Security Modules.
```


Adopted by more and more OSS



U-Boot

*full abbreviated
different indentation
line wrapping*

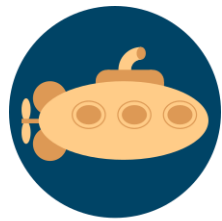
```
# See the CREDITS for list of people who contributed to this
# project.
#
# This program is free software; you can redistribute it and/or
# modify it under the terms of the GNU General Public License as
# published by the Free Software Foundation; either version 2 of
# the License, or (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place, Suite 330, Boston,
# MA 02111-1307 USA
```



```
# SPDX-License-Identifier: GPL-2.0+
```

<https://gitlab.denx.de/u-boot/u-boot/commit/eca3aeb352c964bdb28b8e191d6326370245e03f>

Adopted by more and more OSS



U-Boot



POCO
C++ LIBRARIES

Linux kernel



arm
MBED



Zephyr™ Project



➤ REUSE.software

<https://github.com/fsfe/reuse-tool>

➤ SPDX tutorial

<https://github.com/david-a-wheeler/spdx-tutorial#spdx-tutorial>

SPDX Supporters

anchore

apiiro

arm

Bitergia

CAICT
中国信通院

CANVASS LABS

CHAIN GUARD

cisco

dynatrace

ECLIPSE
FOUNDATION

FOSSA

FOUNDRIES.IO

Google

GUIDE-RAILS

here

HITACHI
Inspire the Next

intel

Laird
CONNECTIVITY

Microsoft

MITRE

nexB

paloalto

Rezilion

SAP

SCANIA

SHEBASH

SIEMENS

snyk

sonatype

SOURCE

synopsys

TEXAS INSTRUMENTS

TIDELIFT

TNG
TECHNOLOGY
CONSULTING

vmware

WDRVR

wipro


XILINX


yocto
PROJECT

SPDX Create Tools

- ❑ fossology
- ❑ ScanCode
- ❑ Meta-spdxscanner

THE **LINUX** FOUNDATION PROJECTS

 **SPDX**

ABOUT SPECIFICATIONS LICENSE LIST **TOOLS** RESOURCES [JOIN](#) 

Open Source Tools

This page lists Open Source tools that support SPDX.

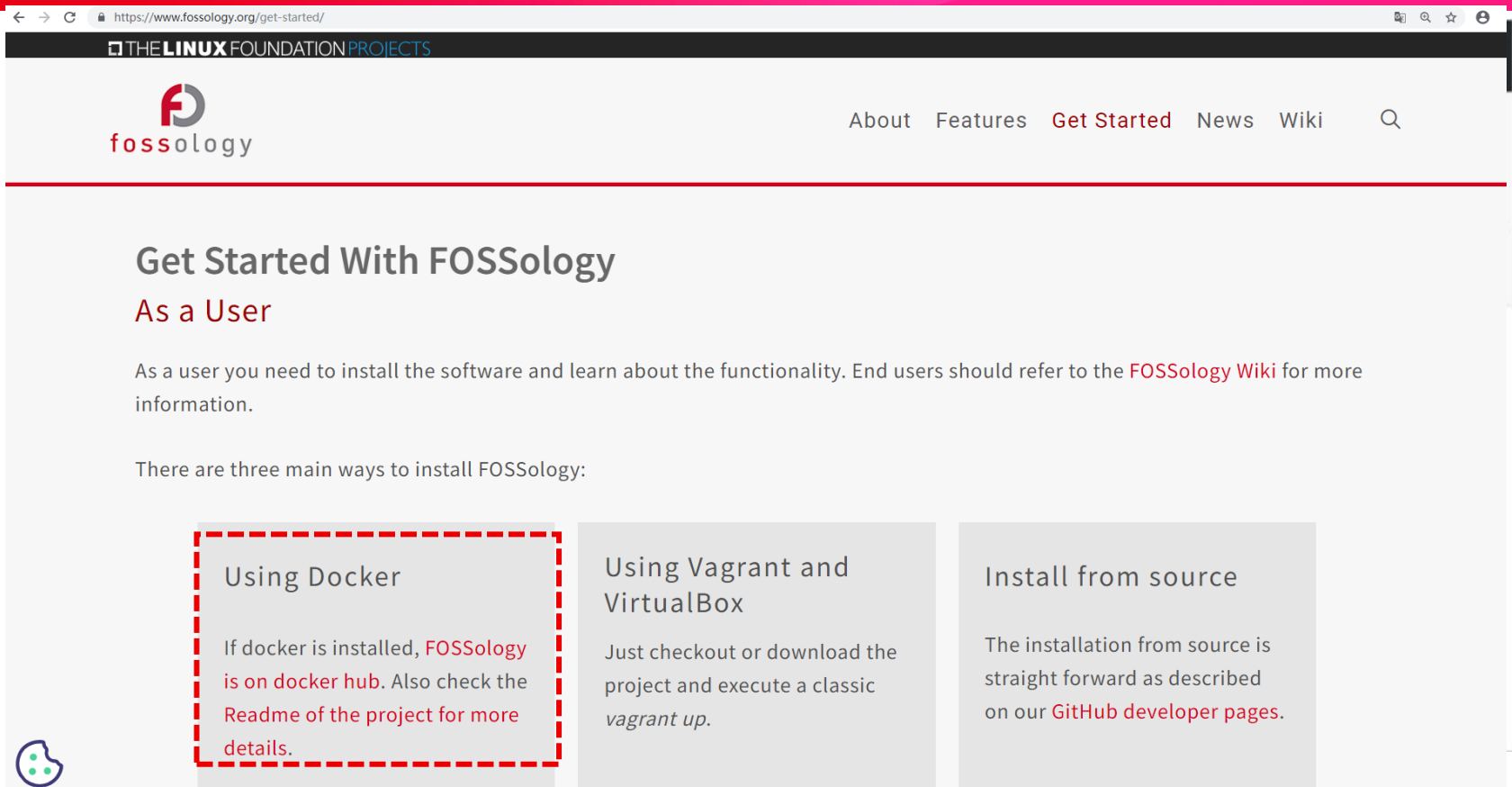
Augur

Classification	Produce (Audit tool)
Functionality	<p>Augur is a tool for consumption of open source software health and Sustainability metrics & data collection. One of the functionalities of a standard Augur implementation is to scan projects to collect license information and create SPDX Documents with the resulting information. Augur APIs and web UI are available for the creation of SPDX documents.</p> <p>See the primary Augur instance at http://augur.osshealth.io/ for demonstration.</p>
Location	<p>Website: http://www.augurlabs.io/</p> <p>Source: https://github.com/chaoss/augur/</p>
Installation instructions	https://oss-augur.readthedocs.io/en/master/getting-started/installation.html
How to use	https://oss-augur.readthedocs.io/en/master/getting-started/create-a-metric/overview.html
Versions supported	SPDX 2.1

FOSSology

Classification	Author after Creation (Audit tool, Manual), Consume(View,Diff,Analyze), Transform(Translate,
----------------	--

<https://spdx.dev/tools-community/>



← → ↻ 🔒 https://www.fossology.org/get-started/ THE LINUX FOUNDATION PROJECTS

fossology About Features **Get Started** News Wiki 🔍

Get Started With FOSSology

As a User

As a user you need to install the software and learn about the functionality. End users should refer to the [FOSSology Wiki](#) for more information.

There are three main ways to install FOSSology:

Using Docker

If docker is installed, [FOSSology is on docker hub](#). Also check the [Readme of the project for more details](#).

Using Vagrant and VirtualBox

Just checkout or download the project and execute a classic *vagrant up*.

Install from source

The installation from source is straight forward as described on our [GitHub developer pages](#).



Folder: Software Repository/ ubinux202207/
 nativesdk-glibc-2.36-r0-patched.tar.gz/nativesdk-glibc-2.36-r0-patched.tar/spdx_temp

[Software Heritage](#) | [License Browser](#) | [File Browser](#) | [Spasht](#) | [Copyright](#) | [ECC](#) | [Email/URL/Author](#) | [Keyword](#) | [Browse](#) | [Export List](#) | [Search](#) | [Bucket](#) • [View](#) | [Conf](#) | [Info](#) • [Refresh](#)

Display files (tree view or flat)

	-- filter for scan results --	-- filter for edited results --	<input type="checkbox"/> Open		MarkAsIrrelevant
Files	Scanner Results (N: nomos, M: monk, Nk: ninka, I: reportImport, O: ojo, Sp: spasht, Rs: reso)	Edited Results	Clearing Status	Cleared / Open / Total	Actions
build-x86_64-ubinuxsdk-linux				0 / 0 / 0	[Tag][Edit][Bulk]
etc/ld.so.conf	No_license_found [N]			0 / 0 / 1	[View][Info] [Download][Tag] [Edit]
git	0BSD, Artistic-1.0, Autoconf-exception, BSD-2-Clause-FreeBSD, BSD-2-Clause-Views, BSD-3-Clause, BSL-1.0, CMU, FSF, FSFAP, FSFUL, Freeware, GCC-exception-2.0, GFDL, GFDL-1.3, GNU-style.EXECUTE, GPL, GPL-2.0, GPL-2.0+, GPL-2.0-with-GCC-exception, GPL-3.0+, HPND, IBM-dhcop, IBM-possibility, ISC, InnerNet-2.00, LGPL, LGPL-2.0+, LGPL-2.1, LGPL-2.1+, LGPL-3.0+, LGPL-possibility, MIT, MIT-CMU-style, MIT-style, No_license_found, Public-domain, Public-domain-ref, Same-license-as, See-URL, See-doc.OTHER, See-file, Spencer-86, Spencer-94, TeX-exception, Unicode, Unicode-DFS-2015, Unicode-TOU, Unlicense, WebM, X11, linking-exception			0 / 13168 / 19258	[Tag][Edit][Bulk]
0003-nativesdk-glibc-Look-for-host-system-ld.so.cache-as-.patch	No_license_found [N]			0 / 0 / 1	[View][Info] [Download][Tag] [Edit]
0004-nativesdk-glibc-Fix-buffer-overflow-with-a-relocated-.patch	No_license_found [N]			0 / 0 / 1	[View][Info] [Download][Tag] [Edit]
0005-nativesdk-glibc-Raise-the-size-of-arrays-containing-.patch	No_license_found [N]			0 / 0 / 1	[View][Info] [Download][Tag] [Edit]
0006-nativesdk-glibc-Allow-64-bit-					[View][Info]

Display licenses

Scanner Count	Concluded License Count	License Name
11880	0	LGPL-2.1+
383	0	Public-domain
324	0	BSD-3-Clause
242	0	WebM
192	0	Freeware
174	0	GCC-exception-2.0
138	0	GPL-2.0+
104	0	GPL-2.0-with-GCC-exception
85	0	Public-domain-ref
70	0	linking-exception
57	0	IBM-possibility
54	0	ISC
33	0	0BSD
32	0	Same-license-as
25	0	LGPL-2.0+
18	0	CMU
11	0	LGPL-2.1
10	0	See-doc.OTHER
7	0	LGPL
6	0	GPL

☰ README.rst

Quick Start

Note the [commands variation](#) across installation methods and platforms.

You can run an example scan printed on screen as JSON:

```
./scancode -clip --json-pp - samples
```

Follow the [How to Run a Scan](#) tutorial to perform a basic scan on the `samples` directory distributed by default with Scancode.

See more command examples:

```
./scancode --examples
```

See [How to select what will be detected in a scan](#) and [How to specify the output format](#) for more information.

You can also refer to the [command line options synopsis](#) and an exhaustive list of [all available command line](#)

https://spdx.dev/tools-community/

[ABOUT](#)[SPECIFICATIONS](#)[LICENSE LIST](#)[TOOLS](#)[RESOURCES](#)[JOIN](#)

\$ term report -f spdxtagvalue -d <Dockerfile> -o spdx.txt

Versions supported

SPDX 2.1, SPDX 2.2 (WIP)

Yocto Project / OpenEmbedded

Classification	Author during Build
Functionality	Yocto project through the OpenEmbedded build system supports creation of embedded system distros, including Linux and other RTOSes. By combining build debug information with source code licensing, a precise understanding of the relevant licensing for a binary can be created during builds.
Location	Website: https://www.yoctoproject.org/ Source: https://git.yoctoproject.org/cgit/cgit.cgi/meta-spdxscanner/
Installation instructions	See: https://git.yoctoproject.org/cgit/cgit.cgi/meta-spdxscanner/tree/README.md
How to use	See README in installation instructions. Questions can go to: https://lists.yoctoproject.org/g/licensing
Versions supported	SPDX 2.1, SPDX 2.2 (WIP)

← → ↺ https://git.yoctoproject.org/?q=meta-spdxscanner

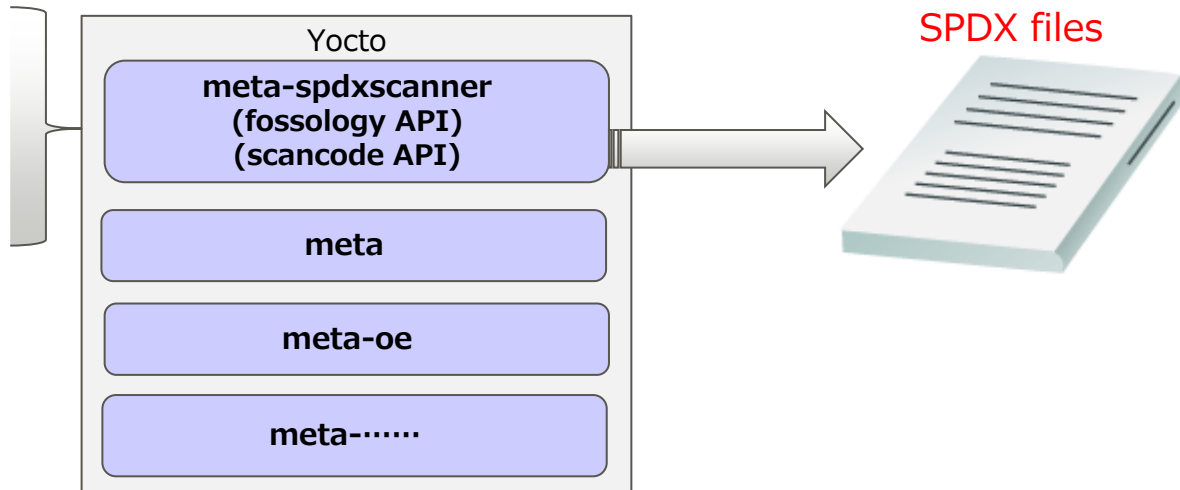
yocto PROJECT Source Repositories Yocto Project

index meta-spdxsca search


Name	Description	Idle
-Yocto Metadata Layers - Other Layers meta-spdxscanner	Layer to support multiple SPDX creation tools	3 months

generated by cqit (git 2.34.1) at 2022-10-19 02:00:39 +0000

- FOSS
- Patches come from 3rd party



Manage SPDX files by dnf-plugin-tui



Home

Search

Browse

Upload

Jobs

Organize

Admin

Help

Browse

Version: [unknown], Branch: [unknown], Commit: [#unknown] unknown built @ 2022/01/24 15:44 UTC

logou

User: fossy

Group: fossy

Folder Navigation

X

Show 50 entries

Collapse All

Expand All

Search folder

Software Repository

201907

ubinux2021.10

ubinux202207

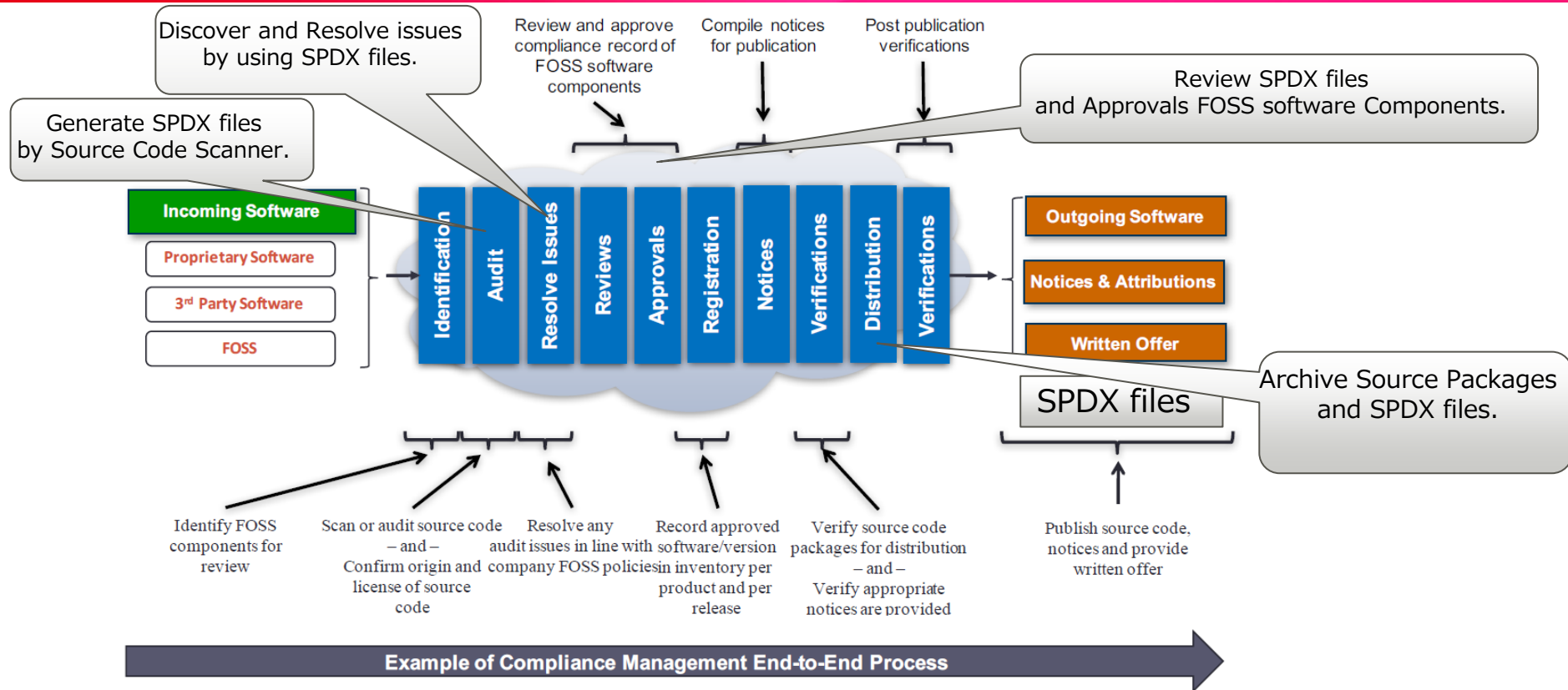
Uploads in ubinux202207

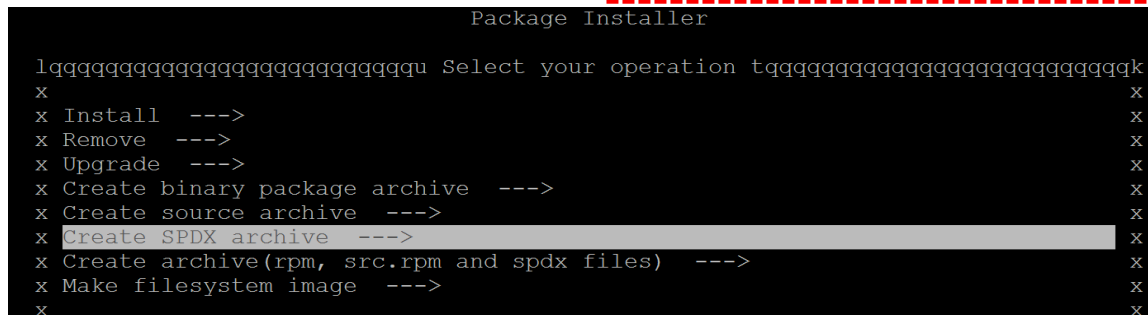
Upload Name and Description	Comment
<div><div>Search:</div><div></div></div> <div><div><div>nativesdk-glibc-2.36-r0-patched.tar.gz</div><div>le-2.36-r0-patched.tar.gz</div></div><div><div>nativesdk-glibc-2.36-r0-patched.tar.gz</div><div>nativesdk-cmake-3.24.0-r0-patched.tar.gz</div></div><div><div>nativesdk-pseudo-1.9.0+gitAUTOINC+c9670c27ff-r0-patched.tar.gz</div><div>nativesdk-gdk-pixbuf-2.42.9-r0-patched.tar.gz</div></div><div><div>nativesdk-shadow-4.1.2.1-r0-patched.tar.gz</div><div>nativesdk-meson-0.63.1-r0-patched.tar.gz</div></div><div><div>nativesdk-gpgme-1.18.0-r0-patched.tar.gz</div><div></div></div></div> <div><div>\$ ls spdx-2022.07/</div><div>abseil-cpp-20220623.0.spdx</div><div>acl-2.3.1.spdx</div><div>acpid-2.0.33.spdx</div><div>adcli-0.9.0.spdx</div><div>adwaita-icon-theme-42.0.spdx</div><div>alsa-lib-1.2.7.2.spdx</div><div>alsa-plugins-1.2.7.1.spdx</div><div>alsa-state-0.2.0.spdx</div><div>alsa-topology-conf-1.2.5.1.spdx</div><div>alsa-ucm-conf-1.2.7.2.spdx</div><div>alsa-utils-1.2.7.spdx</div><div>anthy-9100h.spdx</div><div>apr-1.7.0.spdx</div><div>apr-util-1.6.1.spdx</div><div>at-3.2.5.spdx</div><div>at-spi2-atk-2.38.0.spdx</div><div>at-spi2-core-2.44.1.spdx</div><div>atk-2.38.0.spdx</div><div>attr-2.5.1.spdx</div><div>audit-3.0.8.spdx</div><div>augeas-1.12.0.spdx</div><div>.....</div></div> <div><div>SPDXVersion: SPDX-2.2</div><div>DataLicense: CC0-1.0</div><div>.....</div><div>DocumentName: openssh-8.4p1</div><div>.....</div><div>Creator: Tool: yocto+fossology-spxd</div><div>Creator: Person: fossy (y)</div><div>.....</div><div>PackageName: openssh</div><div>PackageVersion: 8.4p1</div><div>PackageFileName: openssh-8.4p1-r0-patched.tar.gz</div><div>.....</div><div>FileName: spdx_temp/openssh-8.4p1/sshbuf.c</div><div>LicenseConcluded: NOASSERTION</div><div>LicenseInfoInFile: 0BSD</div><div>LicenseInfoInFile: ISC</div><div>.....</div><div>LicenseID: LicenseRef-BSD</div><div>LicenseName: BSD</div><div>ExtractedText: <text> BSD is referenced</div><div>.....</div></div>	

Our work to enhance compliance

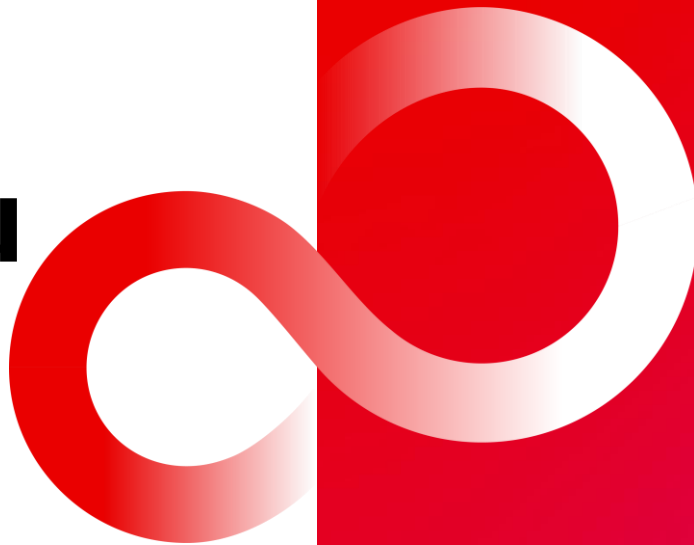
- Work with OpenChain
- Manage SPDX files by dnf-plugin-tui

Work with OpenChain





Thank you



leimaohui@fujitsu.com