FUJITSU

shaping tomorrow with you

SPDX with Yocto Project

Nov 11th, 2015

Lei Maohui, Fujitsu

whoami

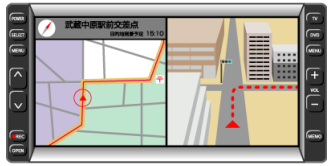
- Working for Fujitsu from 2011
- 3 years experience in Yocto related development

- In-House Embedded Linux Distributor of Fujitsu
- Our Distribution includes LTSI Kernel and is built with Yocto Project
- Our Distribution is used for
  - IVI
  - Server System Controller
  - Storage System
  - Network Equipment
  - Printer
  - etc.







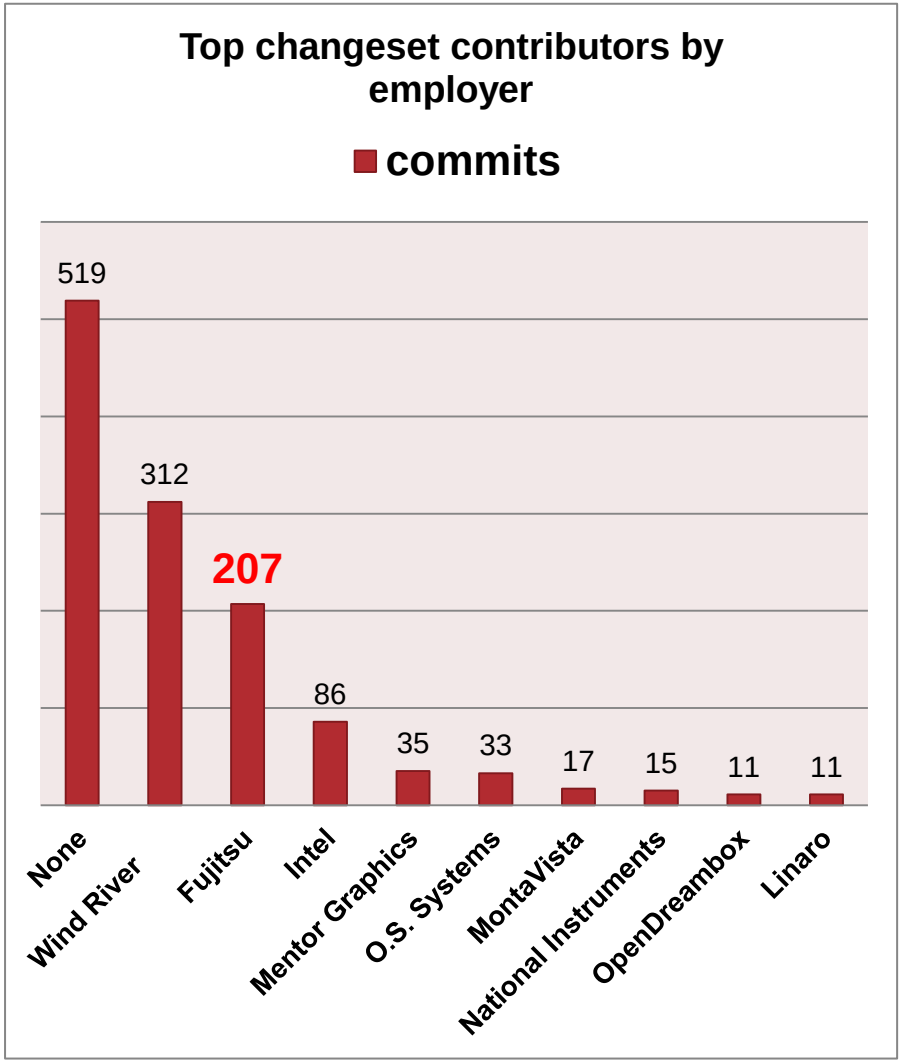



IVI : In-Vehicle Infotainment

Our contributions to Yocto community

FUJITSU

- Data comes from meta-openembedded.git (2014-11-01 ~ 2015-10-31)



	Developer	Changesets
1	Andreas Müller	155 (11.3%)
2	Martin Jansa	120 (8.8%)
3	**Li Xin (Fujitsu)**	**91 (6.7%)**
4	Roy Li	71 (5.2%)
5	Armin Kuster	67 (4.9%)
6	Yi Zhao	54 (4.0%)
7	**Bian Naimeng (Fujitsu)**	**46 (3.4%)**
8	Kai Kang	46 (3.4%)
9	Jackie Huang	38 (2.8%)
10	**Qian Lei(Fujitsu)**	**34 (2.5%)**
11	Paul Eggleton	33 (2.1%)
12	**Maohui Lei (Fujitsu)**	**32 (2.3%)**
13	Tim Orling	29 (2.1%)
14	Khem Raj	27 (2.0%)
15	Otavio Salvador	25 (1.8%)

Developers with the most changesets

Agenda

FUJITSU

Introduction of SPDX

- What is SPDX
- Who are working for SPDX
- The status of SPDX specification

SPDX Create Tools

- TripleCheck Reporter
- FOSSology-SPDX
- DoSOCSv2
- Contrast

Yocto-SPDX

- Current state
- Generate SPDX file from Yocto building
- Current problems of Yocto-SPDX

Contribution to Yocto-SPDX project

- What we have done
- Plan of Next-step

FUJITSU

Introduction of SPDX

- What is SPDX
- Who are working for SPDX
- The current status of SPDX Specification

What is SPDX

FUJITSU

What is SPDX

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

Vision

- To help reduce redundant work in determining software license information and facilitate compliance.

OSS developers, Distro Vendors, OSS users must know the license of the OSS software clearly. So 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.

Yocto Project provides the recipe including license information, **but** it's still not enough, because it's hard to maintain license information while the license of whole or part of OSS is changed.

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

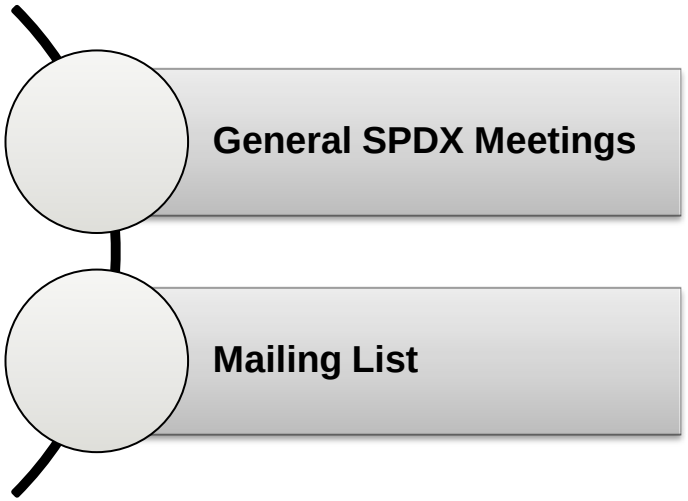
Who are working for SPDX

FUJITSU

☐ SPDX WG and 3 Teams

Linux Foundation — SPDX Workgroup

- Technical Team
  - ◆ Draft the specification and developing documentation, templates, samples and tools
- Business Team
  - ◆ Go-to-market activities of SPDX
- Legal Team
  - ◆ licensing issues Support & SPDX License List maintenance



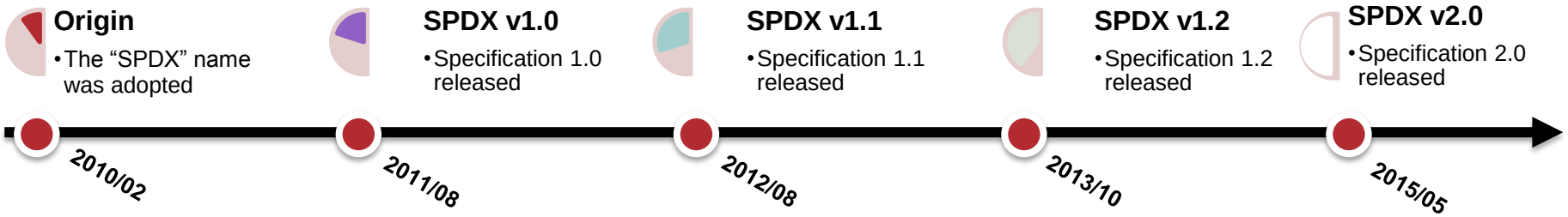
☐ More than 20 organizations

- Obtain details from http://spdx.org/participate

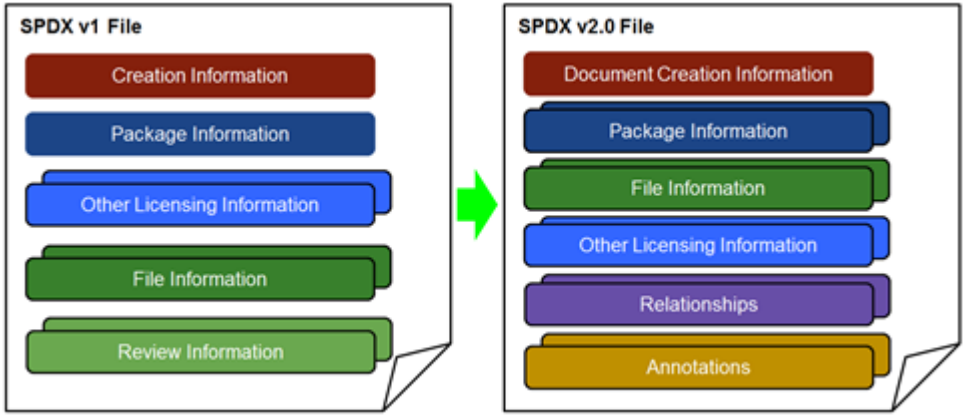
The status of SPDX Specification

FUJITSU

- The latest version is SPDX 2.0



- New features within SPDX v2.0



Obtain details from

- https://spdx.org/about-spdx/what-is-spdx
- http://wiki.spdx.org/view/Technical_Team/SPDX_Specification_Versions
- http://spdx.org/sites/spdx/files/publications/SPDX_2.0_Collab_2015.pdf

FUJITSU

SPDX Create Tools

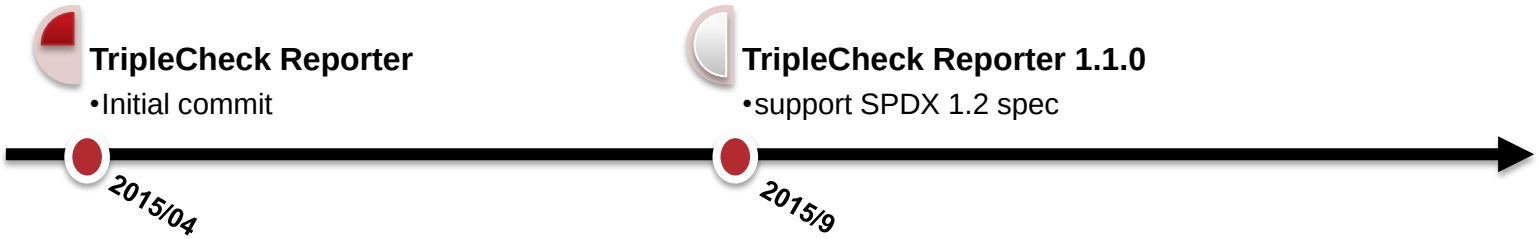
- TripleCheck Reporter
- FOSSology-SPDX
- DoSOCSv2
- Contrast

TripleCheck Reporter

• What is TripleCheck Reporter

- The TripleCheck reporter is the ideal tool for a quick overlook of the licensing compliance status for a given set of source code files in your desktop computer (Linux, Windows and Mac OS X).

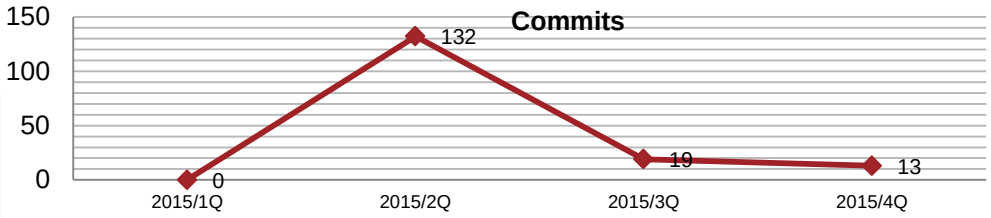
• History

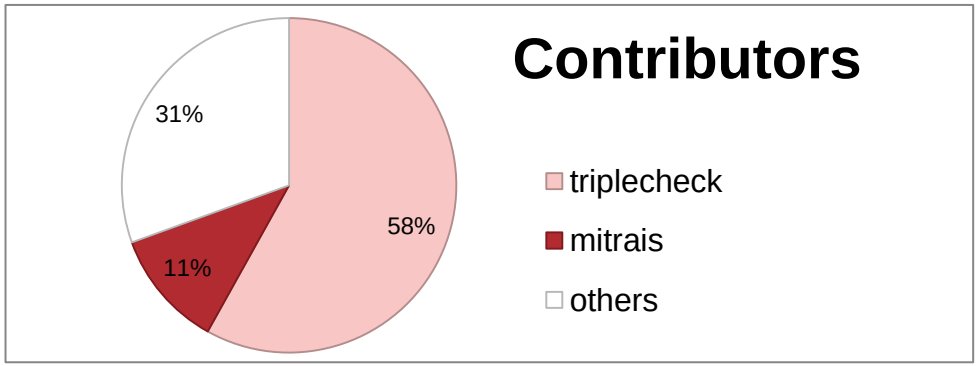


• Project Activity

Item		TripleCheck
Last release		2015/09
Contributors	All Time	5
	Past 12 Months	5
Commits	All Time	164
	Past 12 Months	164
Activity level		New

(1) Data comes from OpenHub - www.openhub.net.
(2) Git Repository:
https://github.com/triplecheck/triplecheck.github.io





TripleCheck Reporter


```
[leimh@localhost spdx-test]$ cat ~/tc/reports/helloworld.spdx
##------------------------
## SPDX Document Information
##------------------------
SPDXVersion: SPDX-1.2
DataLicense: CC-BY-4.0

##------------------------
## Creation Information
##------------------------
Creator: leimh
Creator: Tool: TripleCheck 1.1.0
Created: 2015-11-06T15:15:02Z

##------------------------
## Package Information
##------------------------
PackageName: helloworld
PackageLicenseDeclared: NOASSERTION

##------------------------
## File Information
##------------------------
FileName: ./helloworld.c
FileType: SOURCE
FileChecksum: SHA1: 7ef5ffdf92714113d433781e1d9c7ad2024c259f
FileChecksum: SHA256: 6db977e3835870796a532684be552df01f877292d0a2ce63bd771154a7
1710a
FileChecksum: MD5: 9ae4858662f0eb5770d3fdf348a440e1
FileSize: 388 bytes
FileLOC: 10
LicenseInfoInFile: GPL-2.0+

FileName: ./saybye.c
FileType: SOURCE
FileChecksum: SHA1: 20e202b299e750bcbb0cc7d5482e17ba822d5434
FileChecksum: SHA256: cebad6672603a61fad9570829b64b66bb7cbf65c9f154e83cc99fc7acc
5d552
FileChecksum: MD5: e29e77459b2b71ee6d99e8ec8ceda70f
FileSize: 849 bytes
FileLOC: 14
FileCopyrightText: <text>Copyright (c) The Regents of the University of Californ
a </text>
```

FOSSology-SPDX

FUJITSU

- What is FOSSology-SPDX
  - The FOSSology-SPDX Project is a Free Open Source Software (FOSS) project built from FOSSology project. (Website)

- History

FOSSology-SPDX (2013/01)
- Initial commit

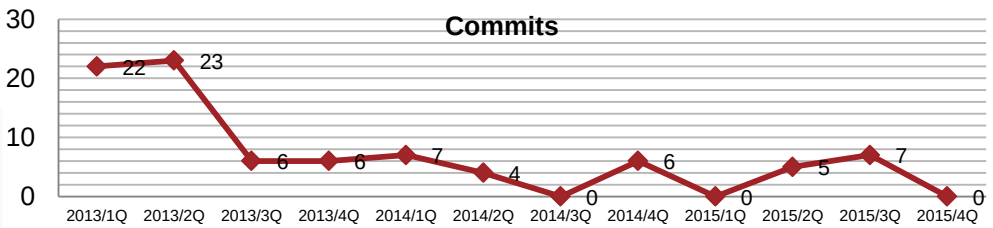
FOSSology-SPDX (2014/12)
- Latest commit
- Support fossology 2.6.2

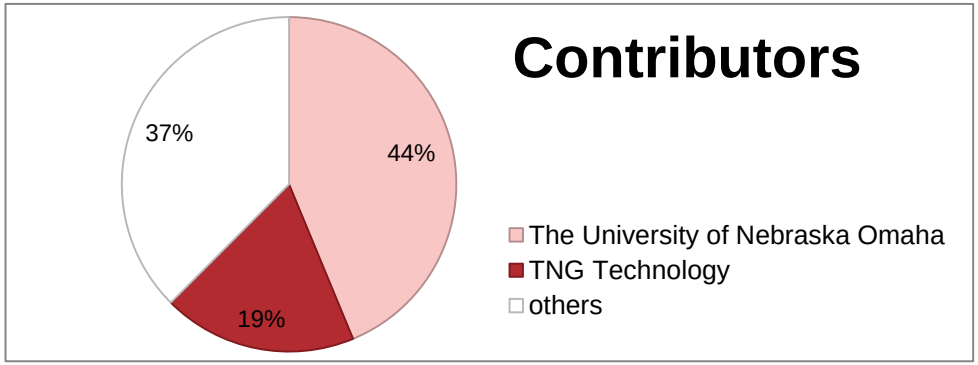
FOSSology (2015/05)
- SPDX module is integrated into FOSSology

FOSSology 3.0 (Coming soon)
- support SPDX 2.0

- Project Activity

Item		FOSSology-SPDX/FOSSology
Last release		2014-12/Coming soon
Contributors	All Time	8/1
	Past 12 Months	2/1
Commits	All Time	74/12
	Past 12 Months	6/12
Activity level		Very Low/New



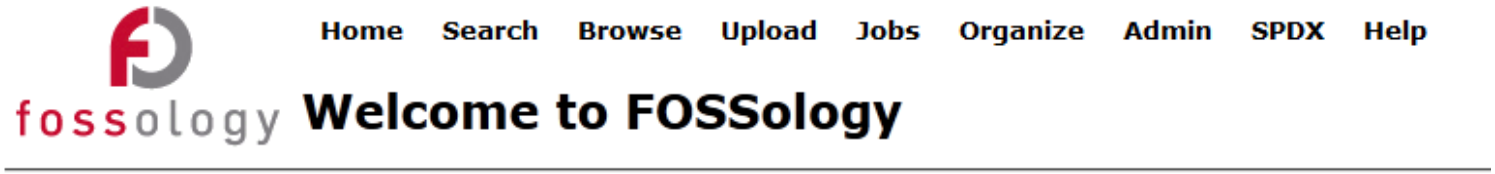


(1) Data comes from OpenHub - www.openhub.net.
(2) Git Repository: https://github.com/fossology/fossology
https://github.com/FOSSology-SPDX/fossology-spdx

Get SPDX file by browser

- You can get a spdx file from the public fossology server or your private server

HomePage

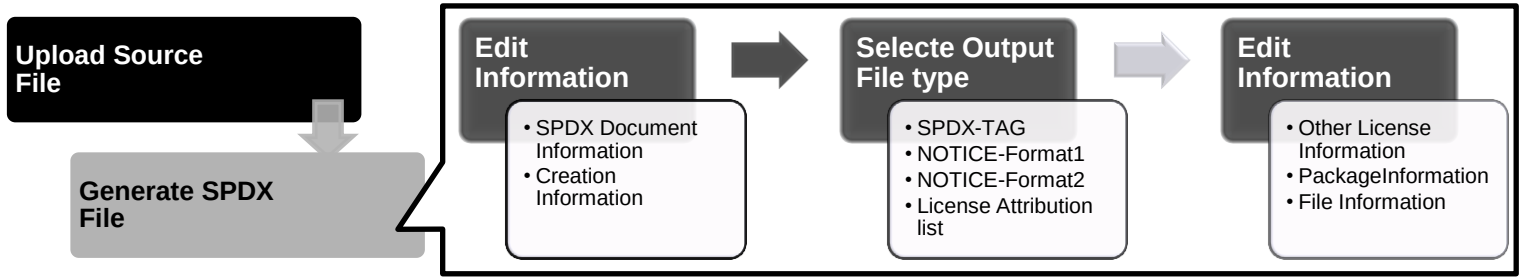


FOSSology is a framework for software analysis tools. With it, you can:

- Upload files into the fossology repository.
- Unpack files (zip, tar, bz2, iso's, and many others) into its component files.
- Browse upload file trees.
- View file contents and meta data.
- Scan for software licenses.
- Scan for copyrights and other author information.
- View side-by-side license and bucket differences between file trees.
- Tag and attach notes to files.
- Report files based on your own custom classification scheme.

Where to Begin...
The menu at the top contains all the primary capabilities of FOSSology.

Generate a SPDX File



Generate SPDX File from Command Line

FUJITSU

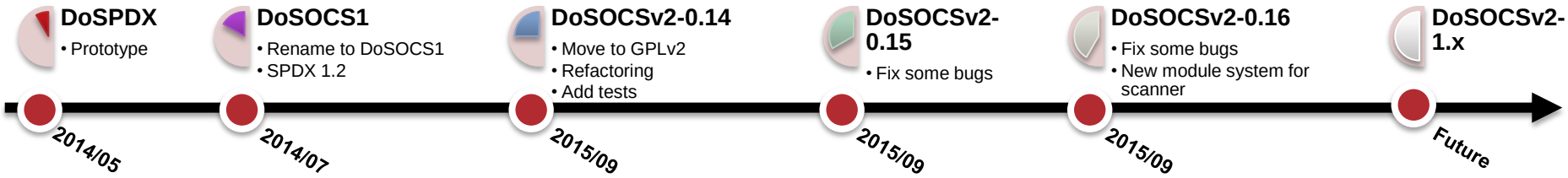
```
# curl http://localhost/repo// -k -F "mod=spdx_license_once" -F "jsonOutput=false"  ¥
        -F "fullSPDXFlag=true“ -F "packageNameInLog=helloworld" -F "file=@helloworld.tar" -o helloworld.spdx

# cat helloworld.spdx
SPDXVersion: SPDX-1.1
DataLicense: CC0-1.0
DocumentComment: <text></text>

## Creation Information
Creator: Tool: FOSSology+SPDX command line
Created: 2015-05-20T03:38:56Z
CreatorComment: <text></text>

## Package Information
PackageName: helloworld
PackageVersion:
PackageDownloadLocation: NOASSERTION
PackageSummary: <text></text>
PackageFileName:
PackageSupplier: NOASSERTION
PackageOriginator: NOASSERTION
PackageChecksum: SHA1: 911e9b3652b0cd9e3650babfc02d07e6f2062eb7
PackageVerificationCode: abbc81d91a96e2b8006a33d0276ee23e61cd27a0(excludes: *.spdx)
PackageDescription: <text></text>

PackageCopyrightText: <text>NOASSERTION</text>

PackageLicenseDeclared: (GPL-2.0+ and BSD-3-Clause)
PackageLicenseConcluded: NOASSERTION
PackageLicenseInfoFromFiles: GPL-2.0+
PackageLicenseInfoFromFiles: BSD-3-Clause
PackageLicenseComments: <text></text>

## File Information

FileName: helloworld.c
FileType: SOURCE
FileChecksum: SHA1: b4faa19e022314a71707d6c6e7bddbaa7167569f
LicenseConcluded: NOASSERTION
LicenseInfoInFile: GPL-2.0+
FileCopyrightText: <text>NONE</text>

FileName: saybye.c
FileType: SOURCE
FileChecksum: SHA1: 09512fc5b0e88a51651df49cc979ec0759a7e5eb
LicenseConcluded: NOASSERTION
LicenseInfoInFile: BSD-3-Clause
```

Obtain detail from https://github.com/spdx-tools/fossology-spdx/wiki/Fossology-SPDX-Web-API#web-api

DoSOCSv2

- What is DoSOCSv2
  - DoSOCSv2 is a command-line tool for managing SPDX 2.0 documents and data

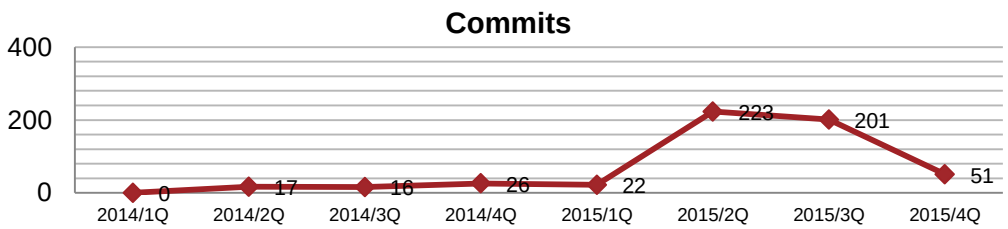
- History

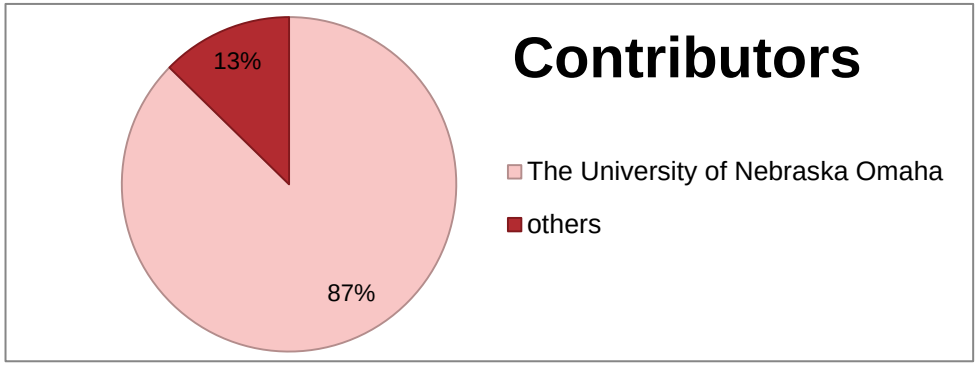


- Project Activity

Item		DoSOCSv2
Last Release		2015/11
Contributors	All Time	9
	Past 12 Months	7
Commits	All Time	545
	Past 12 Months	496
Activity Level		High

(1) Data comes from OpenHub - www.openhub.net.
(2) Git Repository: https://github.com/DoSOCSv2/DoSOCSv2





How to use DoSOCSv2

FUJITSU

 # dosocs2 oneshot ./helloworld.tar > helloworld.spdx

 # cat helloworld.spdx

```
SPDXVersion: SPDX-2.0
DataLicense: CC0-1.0
DocumentNamespace: sqlite:////home/leimh/.config/dosocs2/dosocs2.sqlite3/helloworld-9c4ac292-36e1-434c-a1cb-53174b221034
DocumentName: helloworld
SPDXID: SPDXRef-DOCUMENT
DocumentComment: <text></text>

## External Document References

## Creation Information
.....
LicenseListVersion: 2.0

## Document Annotations

## Document Relationships
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-package-helloworld_tar-262e-69134790
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-file-helloworld_c-7ef5-b3e17d72
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-file-saybye_c-20e2-1b812729

## Package Information
PackageName: helloworld
SPDXID: SPDXRef-package-helloworld_tar-262e-69134790
.....
PackageLicenseInfoFromFiles: BSD-3-Clause
PackageLicenseInfoFromFiles: GPL-2.0+
.....
## Relationships
Relationship: SPDXRef-package-helloworld_tar-262e-69134790 CONTAINS SPDXRef-file-helloworld_c-7ef5-b3e17d72
……

## File Information
FileName: ./saybye.c
SPDXID: SPDXRef-file-saybye_c-20e2-1b812729
……
LicenseInfoInFile: BSD-3-Clause
.....
## Relationships
Relationship: SPDXRef-file-saybye_c-20e2-1b812729 CONTAINED_BY SPDXRef-package-helloworld_tar-262e-69134790
Relationship: SPDXRef-file-saybye_c-20e2-1b812729 DESCRIBED_BY SPDXRef-DOCUMENT

FileName: ./helloworld.c
SPDXID: SPDXRef-file-helloworld_c-7ef5-b3e17d72
……
LicenseInfoInFile: GPL-2.0+
```

Obtain detail from https://github.com/DoSOCSv2/DoSOCSv2

DoSOCSv2

FUJITSU

- DoSOCSv2 is under heavy development
- Current deviations from SPDX 2.0 specification

  - Exactly one package per document is required. (SPDX 2.0 allows zero or more packages per document.)
  - Files in a document can only exist within a package. (SPDX 2.0 allows files to exist outside of a package.)
  - Checksums are always assumed to be SHA-1. (SPDX 2.0 permits SHA-1, SHA-256, and MD5)
  - A file may be an artifact of only one project.
  - License expression syntax is not parsed; license expressions are interpreted as license names that are not on the SPDX license list.
  - Deprecated fields from SPDX 1.2 (reviewer info and file dependencies) are not supported.

Obtain detail from

- https://github.com/DoSOCSv2/DoSOCSv2

The contrast of three tools

FUJITSU

- These three spdx tools have their features as following.

item		TripleCheck Reporter	FOSSology+SPDX	DoSOCSv2
Last Release		2015/09	2014/12	2015/10
DataLicense		CC-BY-4.0	CC0-1.0	CC0-1.0
support SPDX spec	1.1		√	
	1.2	√	√	
	2.0			√
Supported Platform	Linux	√	√	√
	Others (Windows/Mac OS X)	√		
UI	Command Line		√	√
	Graphics	√	√	
Difficulty of build environment		Easy	Complex	Easy
Can work with Yocto			√	
Project Activity (1)		New Project	Very Low Activity	High Activity

(1) Data comes from www.openhub.net.

- Yocto has supported spdx
  - Yocto has supported from Yocto-1.5

FUJITSU

Yocto-SPDX

- Current state
- Generate SPDX File from Yocto building
- Current problems of Yocto-SPDX

Current state

FUJITSU

- The status of the Yocto-SPDX

Original Version

- Yocto-SPDX was supported from yocto 1.5.

SPDX Specification

- Yocto-SPDX supports SPDX v1.1 specification

SPDX Implementation

- Yocto-SPDX generates spdx files by using fossology-spdx server.

- Activity
  - Until 2015/11/03,There are only 5 commits about Yocto-SPDX.

```
[poky] $ git log --pretty=format:"%ad %s" meta/classes/spdx.bbclass
Thu Nov 13 15:49:52 2014 +0100 spdx.bbclass: improved error handling and code cleanup
Mon Oct 20 16:09:15 2014 +0200 spdx.bbclass: improved stability, fixed SPDX compliance issues. Changes are reflected in licenses.conf.
Tue Sep 23 17:48:12 2014 +0800 spdx.bbclass: Add SPDX-specific source tree variable.
Sun Sep 1 08:52:40 2013 +0100 meta: Don't use deprecated bitbake API
Fri Aug 23 14:40:35 2013 -0700 SPDX:real-time license scanning and SPDX output.
[poky] $
```

Generate SPDX File from Yocto building

FUJITSU

④ Start building

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

③ Edit local.conf

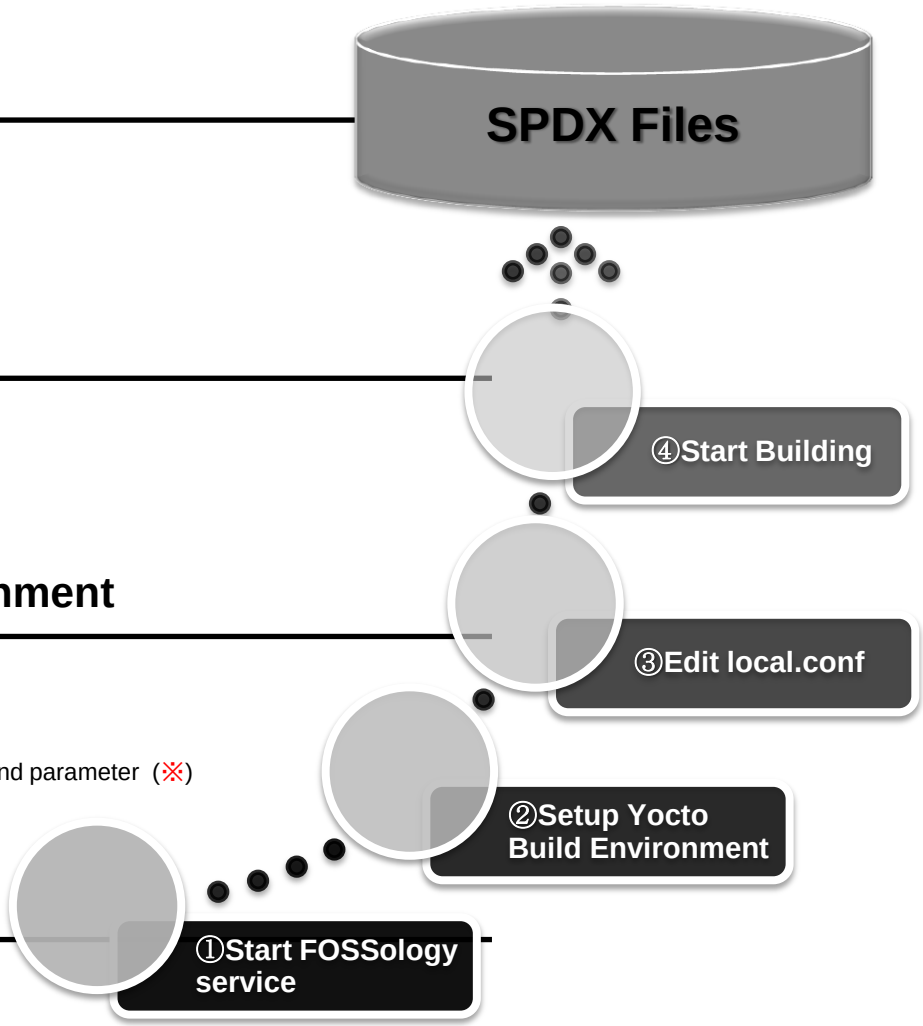
- **# cd [build_dir]**
- **# tail –n 2 conf/local.conf**
  SPDX_MANIFEST_DIR ?= "/yocto/spdx/fossology/xxx“
  INHERIT += "spdx“

② Setup Yocto Build Environment

- **# cd [yocto_dir]**
- **# vim meta/conf/licenses.conf**
  FOSS_SERVER ?= “…”
  FOSS_WGET_FLAGS = “ …“ **#**Configure your fossology-server and Command parameter (※)
- **# source oe-init-build-env [build_dir]**

① Start FOSSology Service

- **# sudo /etc/init.d/fossology start**



※ Please refer to http://events.linuxfoundation.org/sites/events/files/slides/SPDX_WITH_YOCTO_PROJECT_1.pdf

Current problems of Yocto-SPDX

FUJITSU

- Only support SPDX v1.1
  - Even SPDX v1.1, Yocto+SPDX has deviations from SPDX 1.1 specification

Section	Fields	Mandatory	Already in Yocto+SPDX
Creation Information	Creator	Yes	NO
Package Information	Package Download Location	Yes	NO
	All Licenses Information from Files	Yes	NO
	Declared License	Yes	NO
Other Licensing Information Detected	Identifier Assigned	Conditional	NO
	Extracted Text	Conditional	NO
	License Name	Conditional	NO

- Complex to build a Yocto+SPDX environment
  - If you want to use Yocto+SPDX, you have to set up a FOSSology-SPDX instance server. It is **complex**.

FUJITSU

Contribution to Yocto+SPDX Project

- What we have done
- Plan of Next-step

What we have done

FUJITSU

- Make Yocto+SPDX be compliant with SPDX-1.2 Specification

发件人: Lei, Maohui
收件人: openembedded-core@lists.openembedded.org
抄送: Lei, Maohui
主题: [PATCH v4 0/3] These patches aim to make the spdx file be compliant with the SPDX 1.2 Specification.
发送时间: 2015/6/10 (周三) 18:09

Those patches aim to make the spdx file be compliant with the SPDX 1.2 Specification.
If you want to use this feature,you need to do:
1. Make sure your fossology+spdx server works well.You can get spdx file with the following command.
curl http://127.0.0.1/repo/ --noproxy 127.0.0.1 -k -F mod=spdx_license_once -F noCopyright=false
-F jsonOutput=false -F fullSPDXFlag=true -F file=@xxx.tar.gz -o xxx.spdx

2. Add the following INHERIT statement and set the SPDX_MANIFEST_DIR at the end of your conf/local.conf file found in the Build Directory.
INHERIT += "spdx"

Lei Maohui (3):
licenses.conf: Modified parameters for new spdx.bbclass
spdx.bbclass: Create the spdx file which is compliant with SPDX
1.2 Specification
spdx: create a directory to save source code

meta/classes/spdx.bbclass | 431 ++++++++++++++++++----------------------
meta/conf/licenses.conf | 86 +++------
2 files changed, 184 insertions(+), 333 deletions(-)

--
1.8.4.2

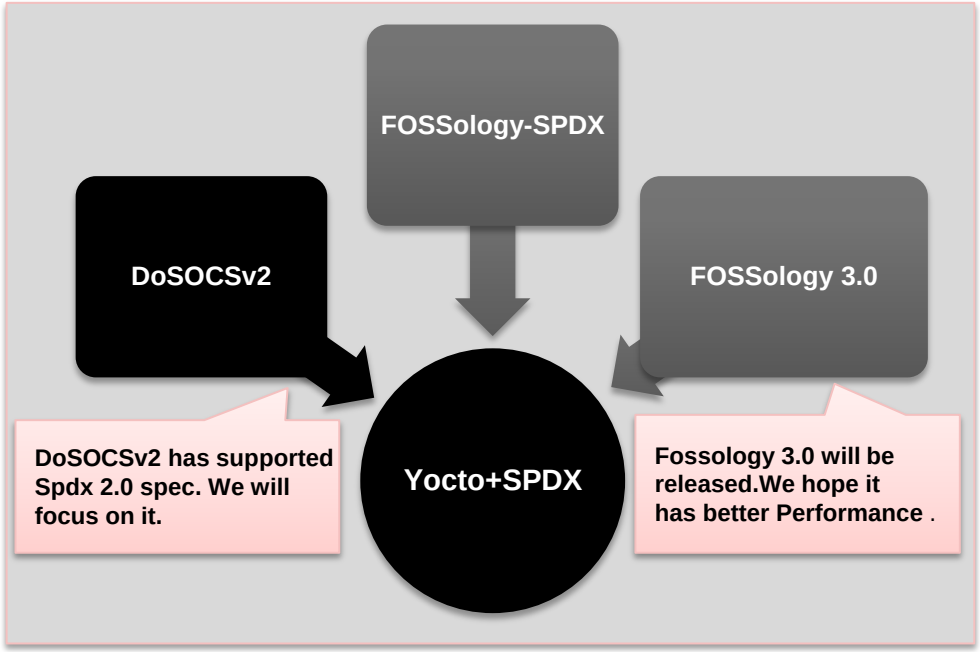
- **This Patch has not been merged into mainline tree. But already been used by some people or company.**

Plan of Next-step

- To optimize Yocto-SPDX, we have some plans.

Support SPDX 2.0 Specification

Easy to build environment



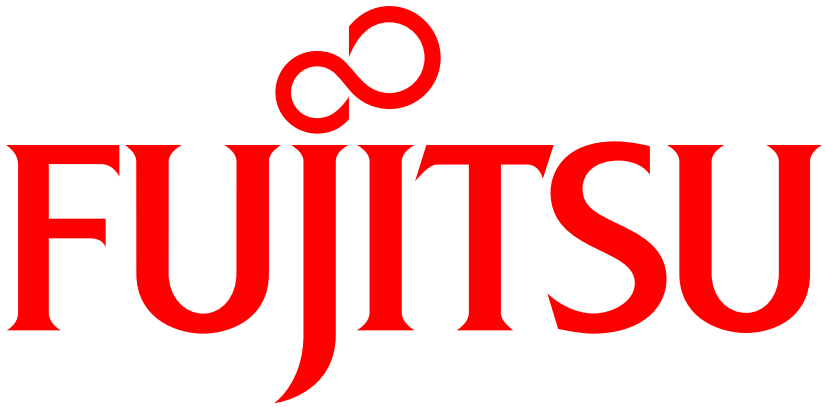
GOAL → **PLAN**

Obtain detail from

- https://github.com/DoSOCSv2/DoSOCSv2
- https://github.com/fossology/fossology
- https://github.com/FOSSology-SPDX/fossology-spdx

FUJITSU

Any Questions?



shaping tomorrow with you