FUJITSU

shaping tomorrow with you

SPDX with Yocto Project

June 2th, 2015

Bian Naimeng, Fujitsu

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

LINUX 4.0 anniversary T-shirt

FUJITSU supports KAWASAKI FRONTALE football club,
FUJITSU supports LINUX 4.0!

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

whoami

- Working for Fujitsu from 2007
- 2 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

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

Agenda

FUJITSU

Introduction of SPDX

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

A Case of study about FOSSology-SPDX&Yocto+SPDX

- FOSSology Website
- Generate SPDX File from Command Line
- Construct Private FOSSology-SPDX
- Yocto+SPDX works with FOSSology-SPDX
- SPDX Tools

Contribution to Yocto+SPDX Project

- What we have done
- Plan of Next-step

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

Introduction of SPDX

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

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

What SPDX is

What SPDX is

- 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 a OSS is a **License-Mixed one.**
- It's will be a big project to determine **lots of OSS** what we provided.

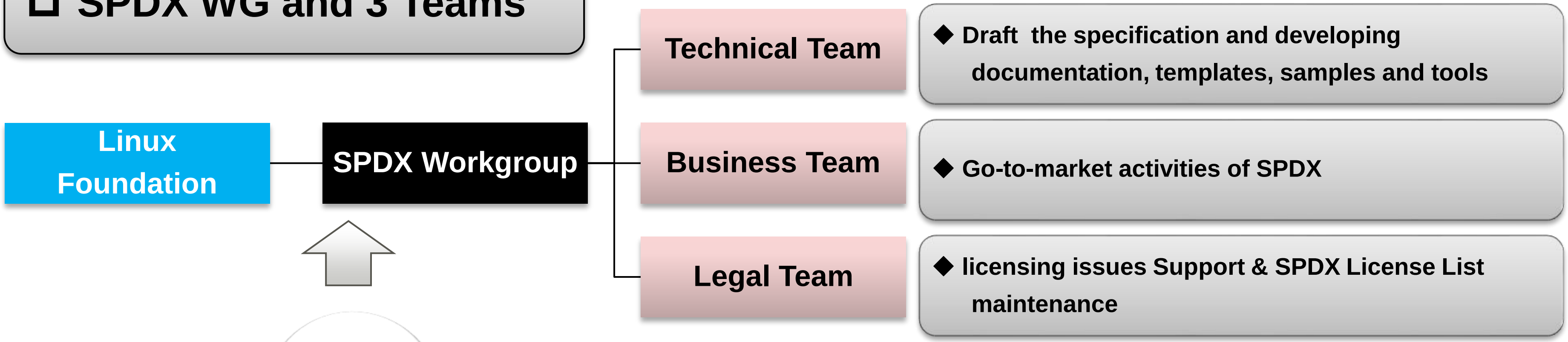
Yocto Project provides the recipe including license information, **but** it's still not enough, because it's hard to maintain license information while the license of whole or part of OSS is changed.

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

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

Who are working for SPDX

□ SPDX WG and 3 Teams



Linux Foundation

SPDX Workgroup

Technical Team

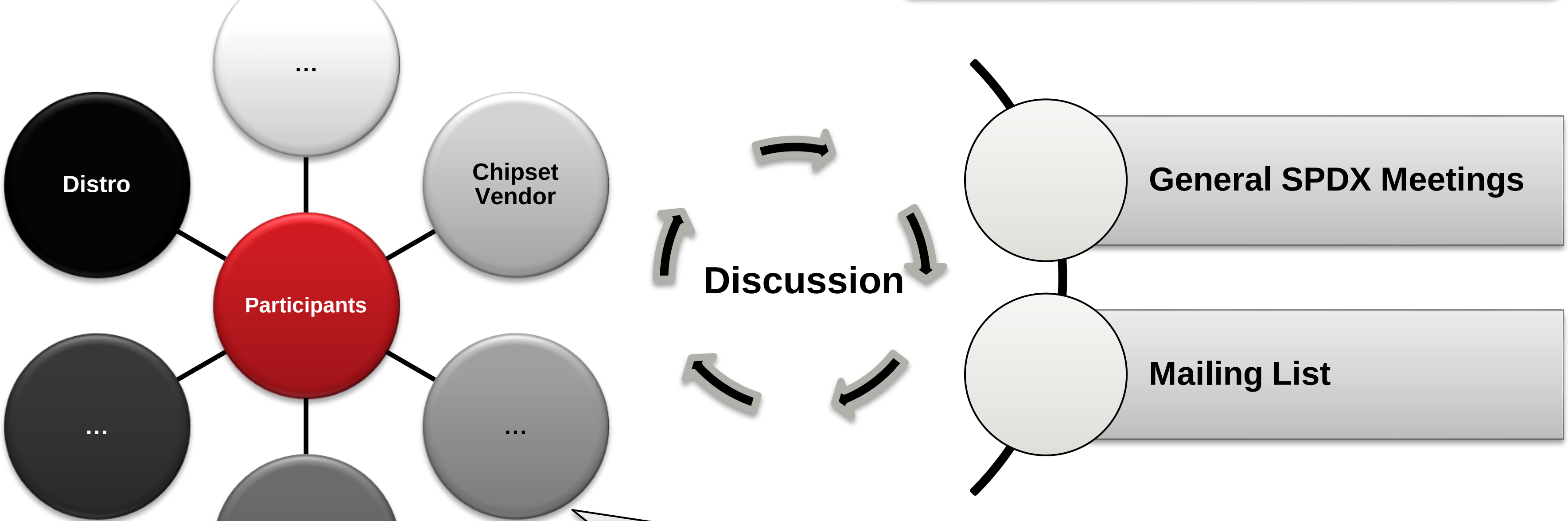
◆ Draft the specification and developing documentation, templates, samples and tools

Business Team

◆ Go-to-market activities of SPDX

Legal Team

◆ licensing issues Support & SPDX License List maintenance



□ 20 Organizations from wide area

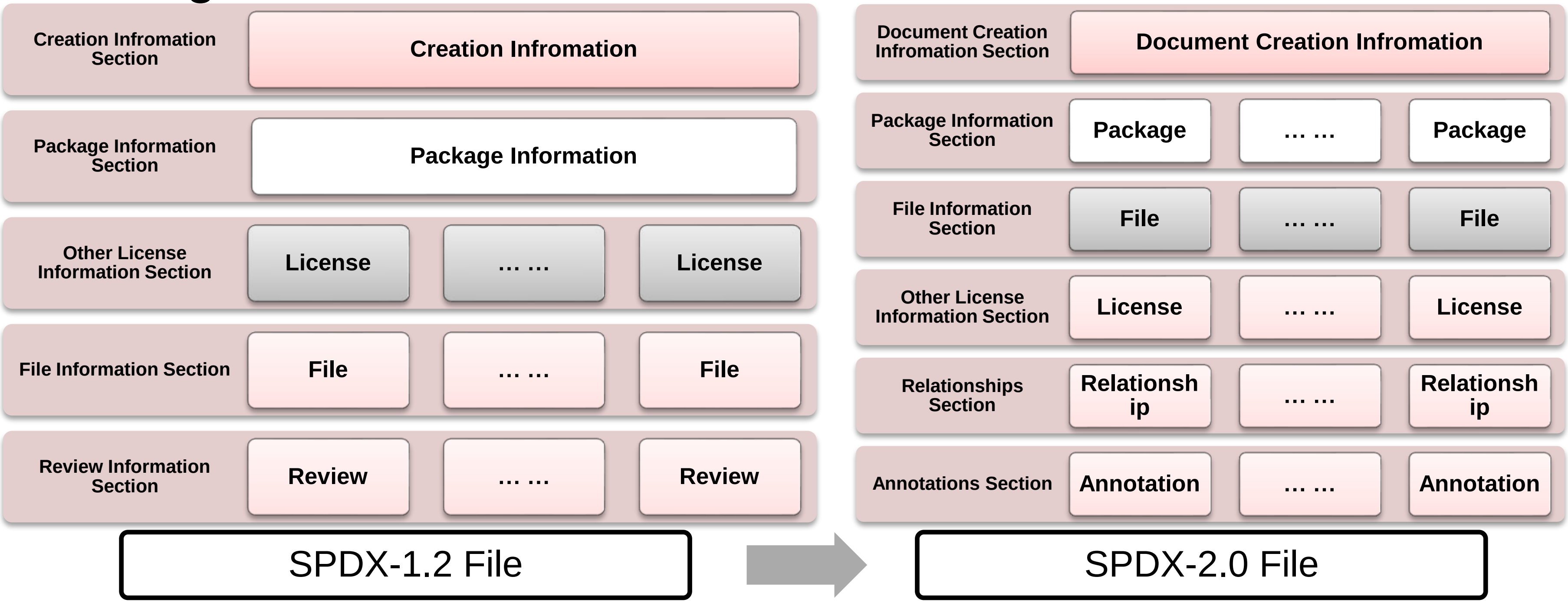
- Obtain details from http://spdx.org/participate

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

The current status of SPDX Specification

- Specification 2.0 Released

- Changed from 1.2



Creation Infromation Section	Creation Infromation		
Package Information Section	Package Information		
Other License Information Section	License	… …	License
File Information Section	File	… …	File
Review Information Section	Review	… …	Review

SPDX-1.2 File

Document Creation Infromation Section	Document Creation Infromation		
Package Information Section	Package	… …	Package
File Information Section	File	… …	File
Other License Information Section	License	… …	License
Relationships Section	Relationsh ip	… …	Relationsh ip
Annotations Section	Annotation	… …	Annotation

SPDX-2.0 File

- Multiple packages can be merged into one SPDX document
- Relationships section describes what’s relationship between two SPDX elements

Obtain details from

- http://spdx.org/SPDX-specifications/spdx-version-2.0

A Case of study about FOSSology-SPDX&Yocto+SPDX

- FOSSology Website
- Generate SPDX File from Command Line
- Construct Private FOSSology-SPDX
- Yocto+SPDX works with FOSSology-SPDX
- SPDX Tools

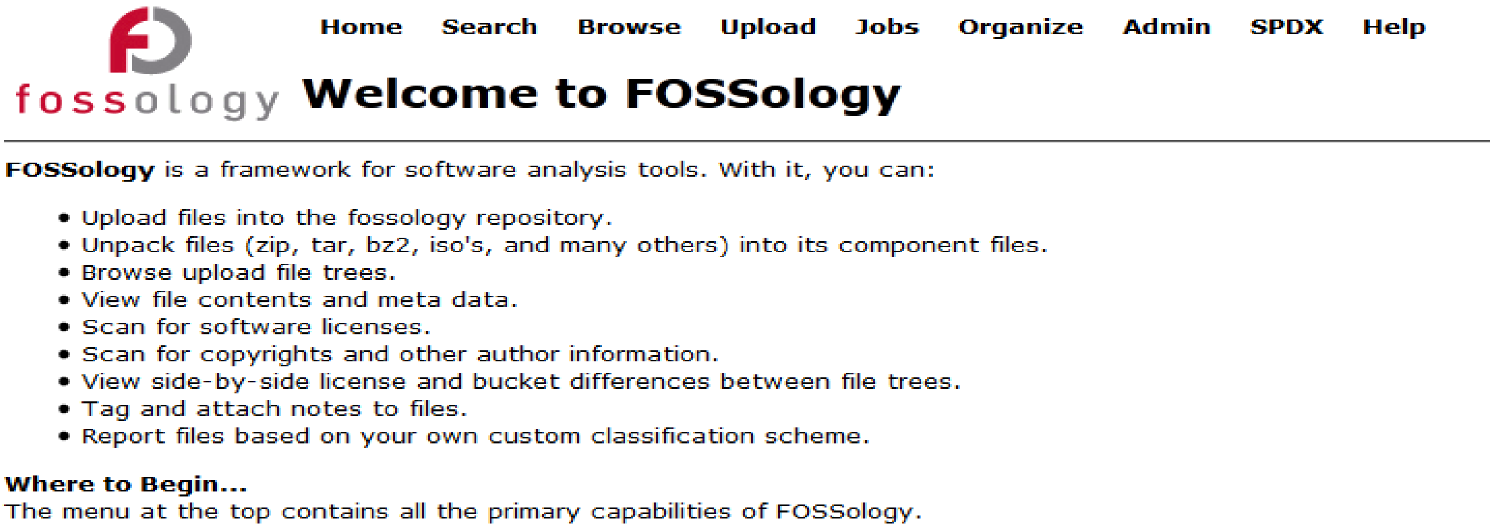
Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

FOSSology Website

- FOSSlogy is a framework for software analysis tools, and FOSSology-SPDX is a module of FOSSology, used as a SPDX implementation.

- You can study FOSSology from Website

HomePage



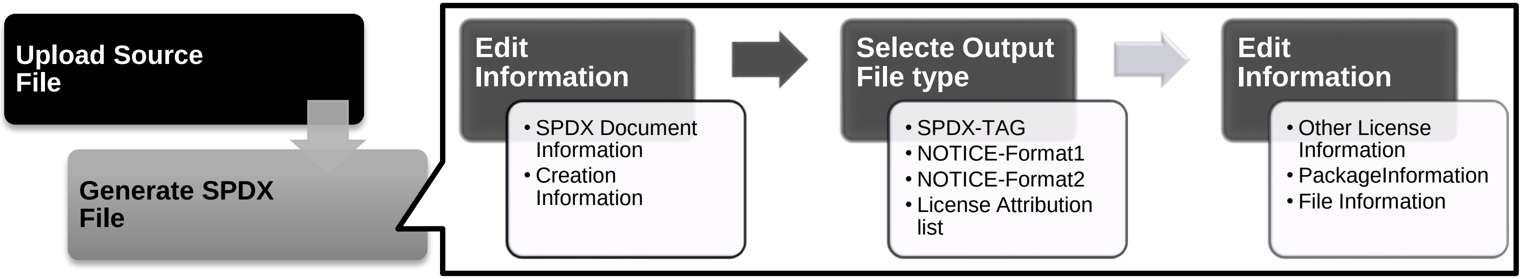
Welcome to FOSSology

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



Demo

https://fossologyspdx.ist.unomaha.edu/?mod=Default

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

Generate SPDX File from Command Line(1/2)

- Create a project including two files with different license.

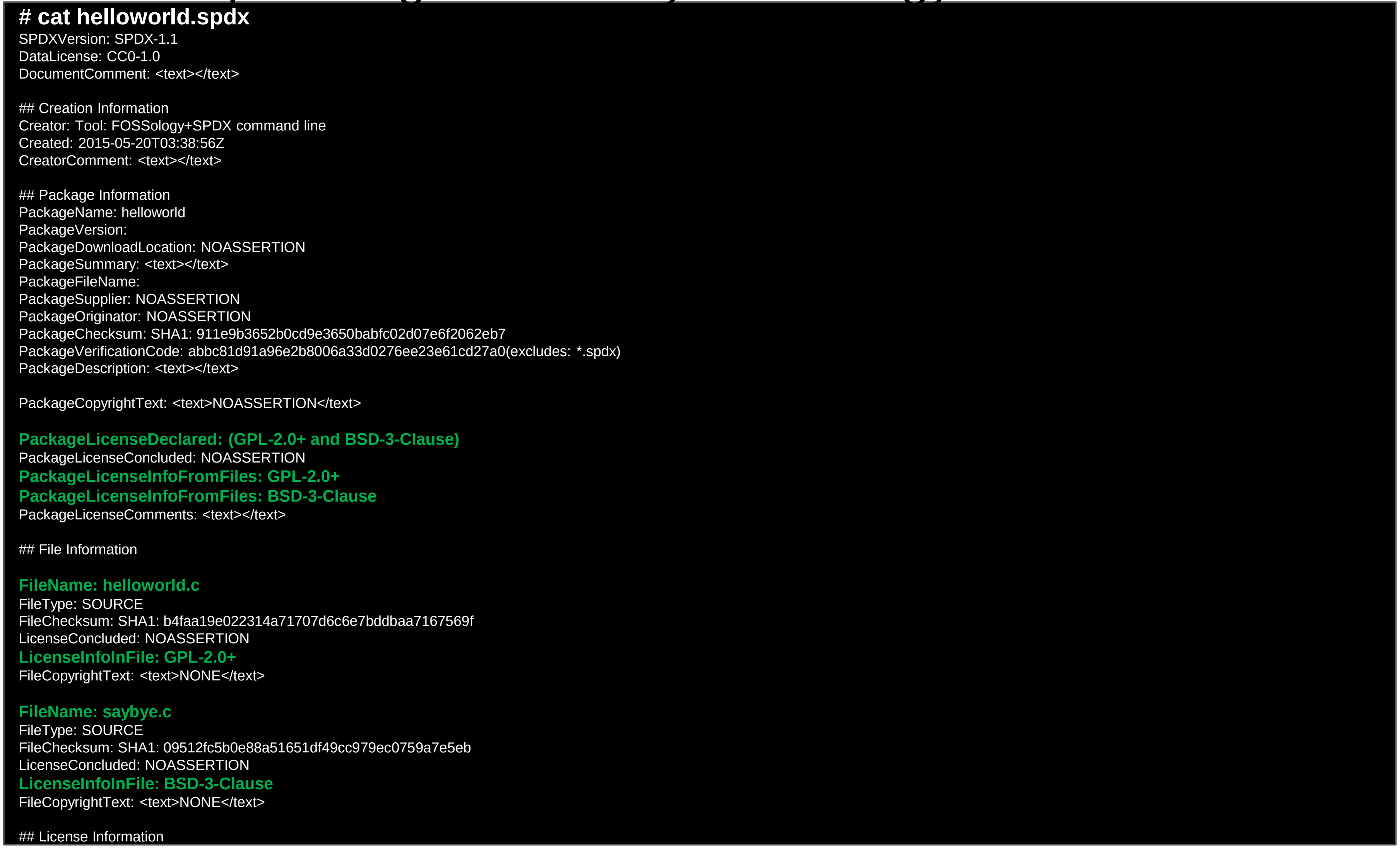
```
# cat helloworld.c
   /* This program is free software; you can redistribute it and/or modify it under the  terms of the GNU General Public License
    * as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later ersion. */
    #include <stdio.h>
    extern void saybye();
    int main(int argc, char *argv[])
    {
        printf(“Hello World¥n”);
        saybye();
        return 0;
    }
# cat saybye.c
   /*Copyright (c) The Regents of the University of California.
    *All rights reserved.
    *Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following
     * conditions are met:
    *1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    *2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the
    *    documentation and/or other materials provided with the distribution.
    *3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from
    *    this software without specific prior written permission. */
    #include <stdio.h>
    void saybye()
    {
        printf(“Good bye!¥n”);
    }
# tar cvf helloworld.tar helloworld.c saybye.c
# curl https://fossologyspdx.ist.unomaha.edu/ -k -F "mod=spdx_license_once" -F "jsonOutput=false"  ¥
   -F "fullSPDXFlag=true“ -F "packageNameInLog=helloworld" -F "file=@helloworld.tar" -o helloworld.spdx
```

Obtain detail from

- https://github.com/spdx-tools/fossology-spdx/wiki/Fossology-SPDX-Web-API#web-api
- http://www.fossology.org/projects/fossology/wiki/Using_FOSSology_from_the_Command_Line

Generate SPDX File from Command Line(2/2)

- Check spdx file generated by FOSSology-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
FileCopyrightText: <text>NONE</text>

## License Information
```

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

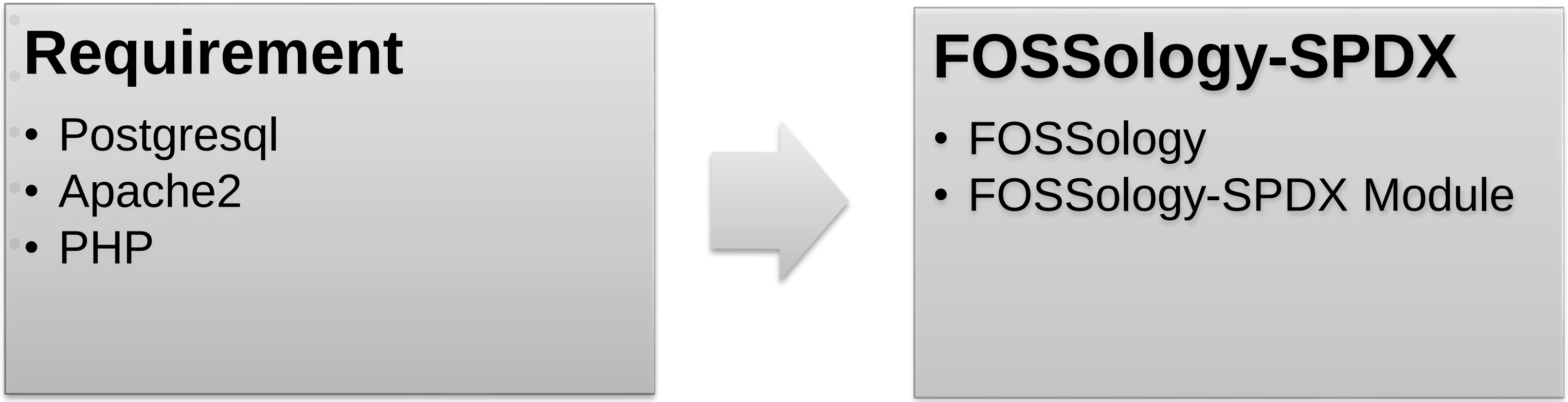
Construct Private FOSSology-SPDX

- Construct your private FOSSology Server

Prerequisites

- **Supported OS**
  - **Debian, Ubuntu, Fedora, RHEL/CentOS**
- **Disk space**
  - **A filesystem with enough disk space（300M for a Distro）**

Install & Configure



Requirement

- Postgresql
- Apache2
- PHP

FOSSology-SPDX

- FOSSology
- FOSSology-SPDX Module

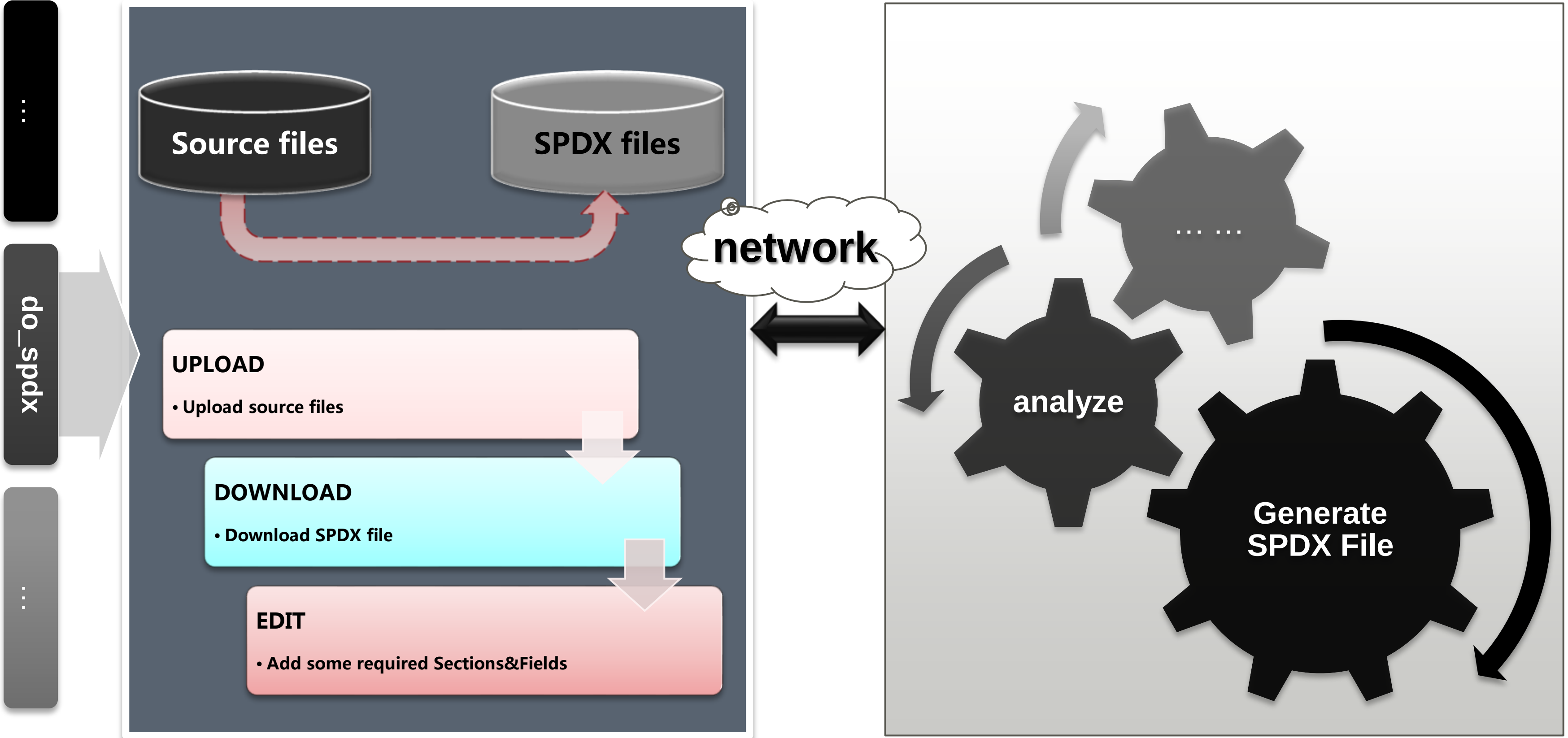
Obtain detail from

- http://www.fossology.org/projects/fossology/wiki/Sysadmin_Documentation

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

Yocto+SPDX works with FOSSology-SPDX(1/3)

- Yocto+SPDX is a module of Yocto Project. It is implemented based on FOSSology-SPDX.



Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

Yocto+SPDX works with FOSSology-SPDX(2/3)

- Configure Yocto+SPDX

Filesystem

- **SPDX_MANIFEST_DIR**
  - SPDX file will be stored here, so make sure the disk space is enough. It will be overwrited by local.conf

SPDX Format information

- **SPDX_VERSION**
  - SPDX Specification Version. Please obtain detail from SPDX Specification.
- **DATA_LICENSE**
  - Data license. Please obtain detail from SPDX Specification.

FOSSOLOGY-SPDX

- **FOSS_COPYRIGHT**
  - Option of FOSSOLOGY Command **noCopyright**. Obtain detail from: **https://github.com/spdx-tools/fossology-spdx/wiki/Fossology-SPDX-Web-API#web-api**
- **FOSS_RECURSIVE_UNPACK**
  - Option of FOSSOLOGY Command **recursiveUnpack** . Obtain detail from: **https://github.com/spdx-tools/fossology-spdx/wiki/Fossology-SPDX-Web-API#web-api**
- **FOSS_SERVER**
  - FOSSologySPDX instance server . E.g., using a private FOSSology server in localhost.
    FOSS_SERVER ?= "http://127.0.0.1/repo//?mod=spdx_license_once"
- **FOSS_WGET_FLAGS**
  - Parameter of wget. E.g. ,
    FOSS_WGET_FLAGS = "-qO - --no-check-certificate --timeout=0"

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

Yocto+SPDX works with FOSSology-SPDX(3/3)

- Generate SPDX File from Yocto building.

④ Start building

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

③ Edit local.conf

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

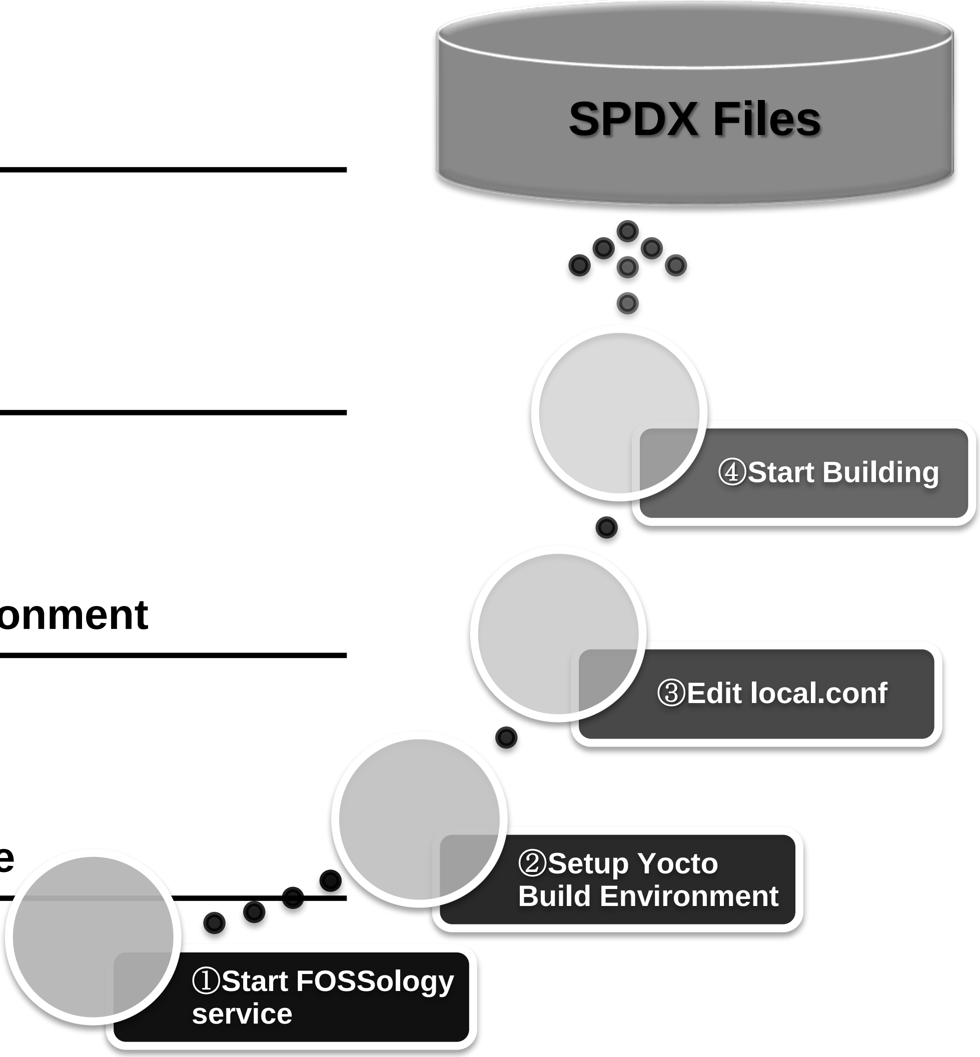
```
SPDX_MANIFEST_DIR ?= "/yocto/spdx/fossology/xxx“
INHERIT += "spdx“
```

② Setup Yocto Build Environment

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

① Start FOSSology Service

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



SPDX Tools

- Using the SPDX Workgroup TOOLS

Translator

- Translate SPDX file between four types

Viewer

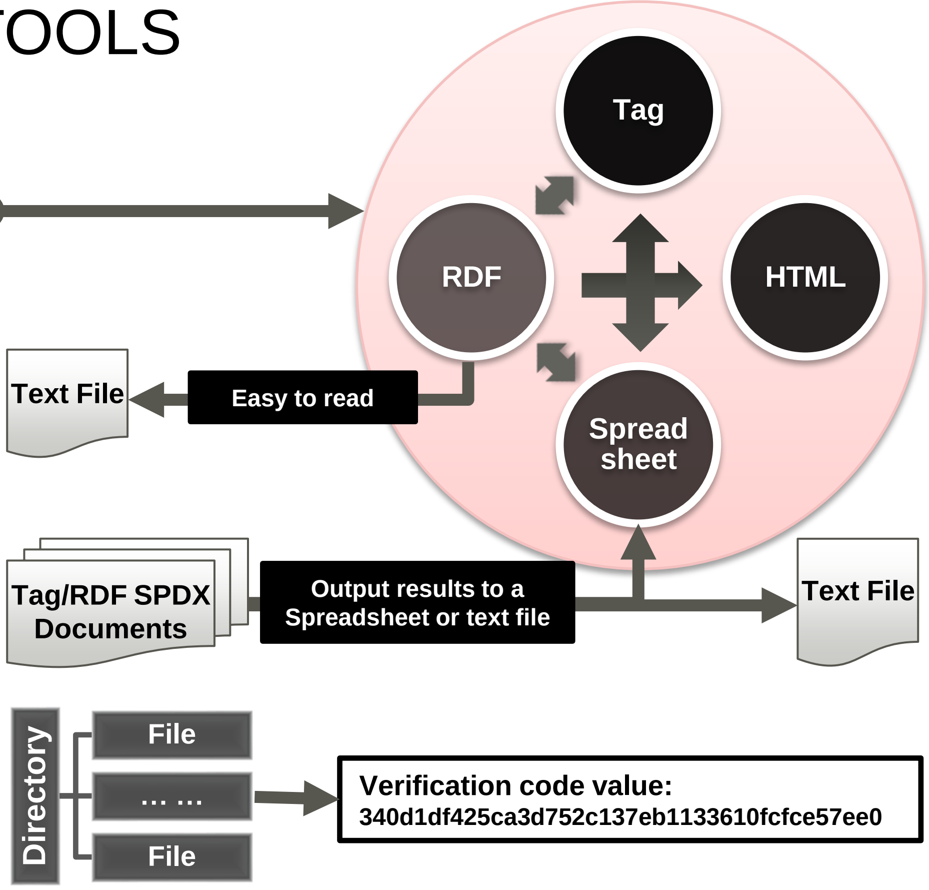
- Format RDF into a Text file

Comparer

- Compare SPDX documents

Verification

- Compute&Display a Verification Code for a directory of source files



Obtain detail from

- http://spdx.org/sites/spdx/files/spdx_tools-draft-20140314.pdf
- http://spdx.org/sites/spdx/files/SPDXTools-v2.0.0.zip

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

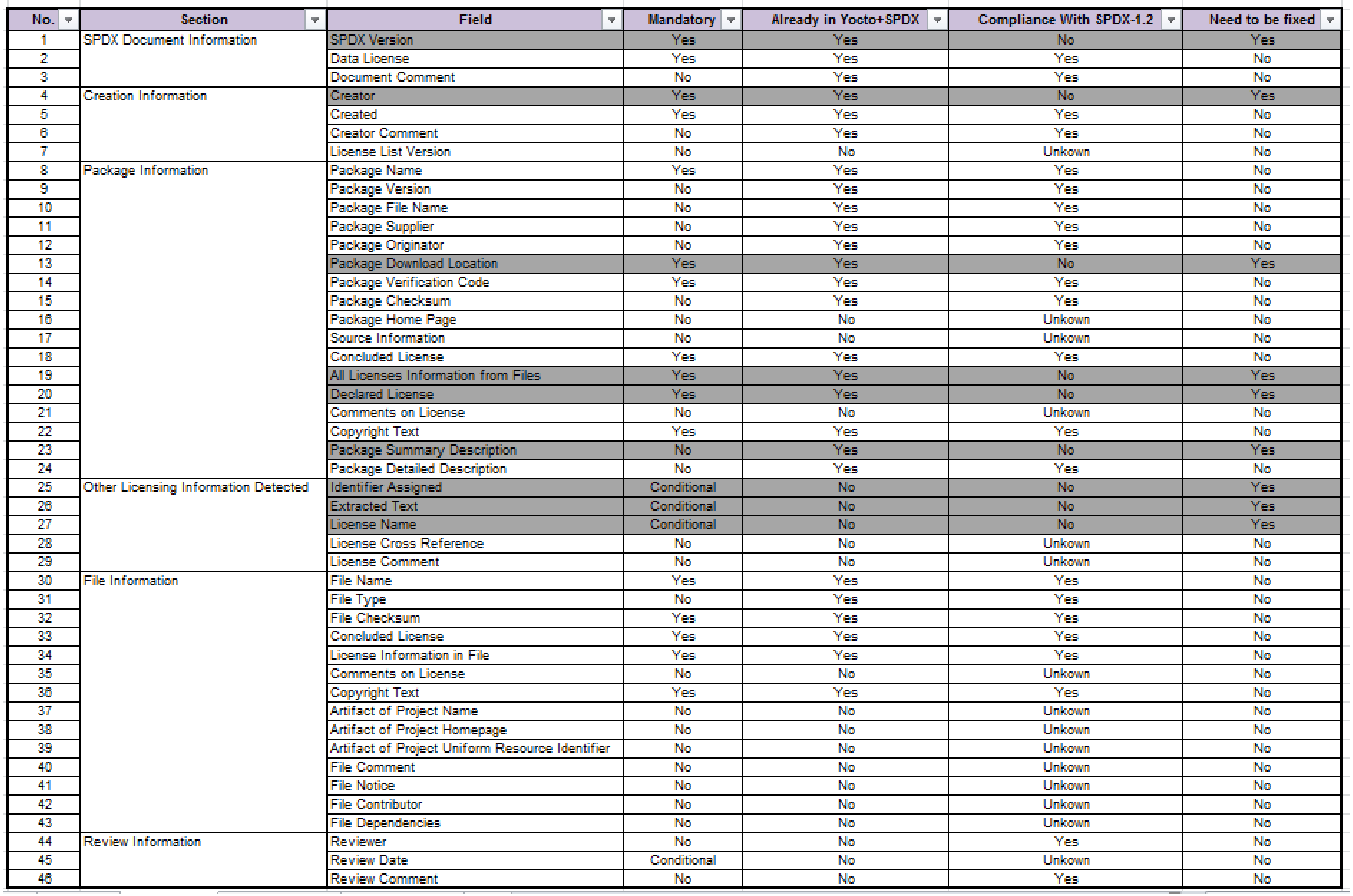
Contribution to Yocto+SPDX Project

- What we have done
- Plan of Next-step

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

What we have done(1/2)

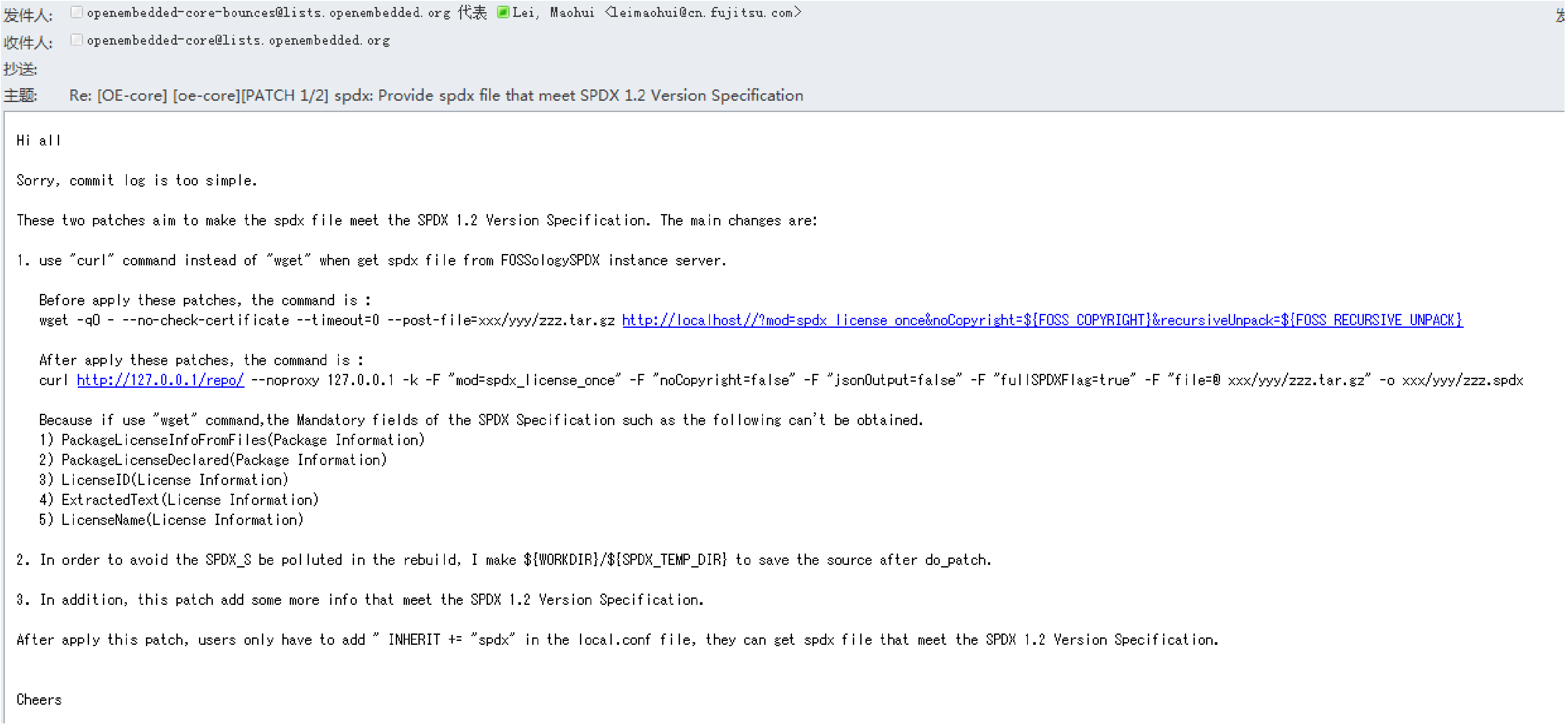
- Yocto+SPDX is not compliant with SPDX Specification.



No.	Section	Field	Mandatory	Already in Yocto+SPDX	Compliance With SPDX-1.2	Need to be fixed
1	SPDX Document Information	SPDX Version	Yes	Yes	No	Yes
2		Data License	Yes	Yes	Yes	No
3		Document Comment	No	Yes	Yes	No
4	Creation Information	Creator	Yes	Yes	No	Yes
5		Created	Yes	Yes	Yes	No
6		Creator Comment	No	Yes	Yes	No
7		License List Version	No	No	Unkown	No
8	Package Information	Package Name	Yes	Yes	Yes	No
9		Package Version	No	Yes	Yes	No
10		Package File Name	No	Yes	Yes	No
11		Package Supplier	No	Yes	Yes	No
12		Package Originator	No	Yes	Yes	No
13		Package Download Location	Yes	Yes	No	Yes
14		Package Verification Code	Yes	Yes	Yes	No
15		Package Checksum	No	Yes	Yes	No
16		Package Home Page	No	No	Unkown	No
17		Source Information	No	No	Unkown	No
18		Concluded License	Yes	Yes	Yes	No
19		All Licenses Information from Files	Yes	Yes	No	Yes
20		Declared License	Yes	Yes	No	Yes
21		Comments on License	No	No	Unkown	No
22		Copyright Text	Yes	Yes	Yes	No
23		Package Summary Description	No	Yes	No	Yes
24		Package Detailed Description	No	Yes	Yes	No
25	Other Licensing Information Detected	Identifier Assigned	Conditional	No	No	Yes
26		Extracted Text	Conditional	No	No	Yes
27		License Name	Conditional	No	No	Yes
28		License Cross Reference	No	No	Unkown	No
29		License Comment	No	No	Unkown	No
30	File Information	File Name	Yes	Yes	Yes	No
31		File Type	No	Yes	Yes	No
32		File Checksum	Yes	Yes	Yes	No
33		Concluded License	Yes	Yes	Yes	No
34		License Information in File	Yes	Yes	Yes	No
35		Comments on License	No	No	Unkown	No
36		Copyright Text	Yes	Yes	Yes	No
37		Artifact of Project Name	No	No	Unkown	No
38		Artifact of Project Homepage	No	No	Unkown	No
39		Artifact of Project Uniform Resource Identifier	No	No	Unkown	No
40		File Comment	No	No	Unkown	No
41		File Notice	No	No	Unkown	No
42		File Contributor	No	No	Unkown	No
43		File Dependencies	No	No	Unkown	No
44	Review Information	Reviewer	No	No	Yes	No
45		Review Date	Conditional	No	Unkown	No
46		Review Comment	No	No	Yes	No

What we have done(2/2)

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



发件人: □ openembedded-core-bounces@lists.openembedded.org 代表 Lei, Maohui <leimaohui@cn.fujitsu.com>

收件人: □ openembedded-core@lists.openembedded.org

抄送:

主题: Re: [OE-core] [oe-core][PATCH 1/2] spdx: Provide spdx file that meet SPDX 1.2 Version Specification

Hi all

Sorry, commit log is too simple.

These two patches aim to make the spdx file meet the SPDX 1.2 Version Specification. The main changes are:

1. use "curl" command instead of "wget" when get spdx file from FOSSologySPDX instance server.

   Before apply these patches, the command is :

```
wget -qO - --no-check-certificate --timeout=0 --post-file=xxx/yyy/zzz.tar.gz http://localhost//?mod=spdx_license_once&noCopyright=${FOSS_COPYRIGHT}&recursiveUnpack=${FOSS_RECURSIVE_UNPACK}
```

   After apply these patches, the command is :

```
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/yyy/zzz.tar.gz" -o xxx/yyy/zzz.spdx
```

   Because if use "wget" command,the Mandatory fields of the SPDX Specification such as the following can't be obtained.
   1) PackageLicenseInfoFromFiles(Package Information)
   2) PackageLicenseDeclared(Package Information)
   3) LicenseID(License Information)
   4) ExtractedText(License Information)
   5) LicenseName(License Information)

2. In order to avoid the SPDX_S be polluted in the rebuild, I make ${WORKDIR}/${SPDX_TEMP_DIR} to save the source after do_patch.

3. In addition, this patch add some more info that meet the SPDX 1.2 Version Specification.

After apply this patch, users only have to add " INHERIT += "spdx" in the local.conf file, they can get spdx file that meet the SPDX 1.2 Version Specification.

Cheers

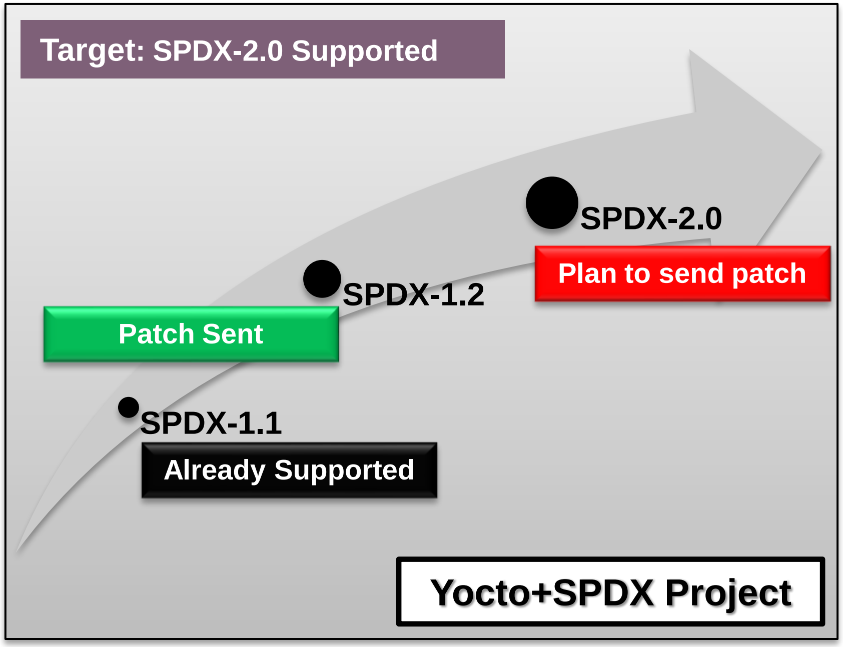
- **This Patch has not been merged into mainline tree. But already been used by some people or company.**

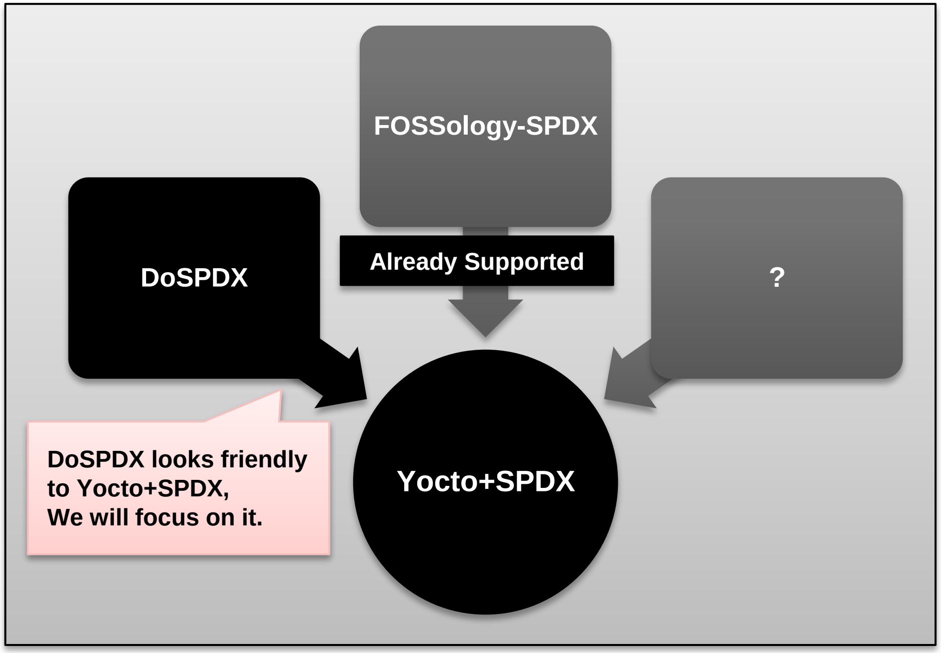
Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

Plan of Next-step(1/3)

- SPDX-2.0 supported

- Other SPDX implementations supported





DoSPDX looks friendly to Yocto+SPDX,
We will focus on it.

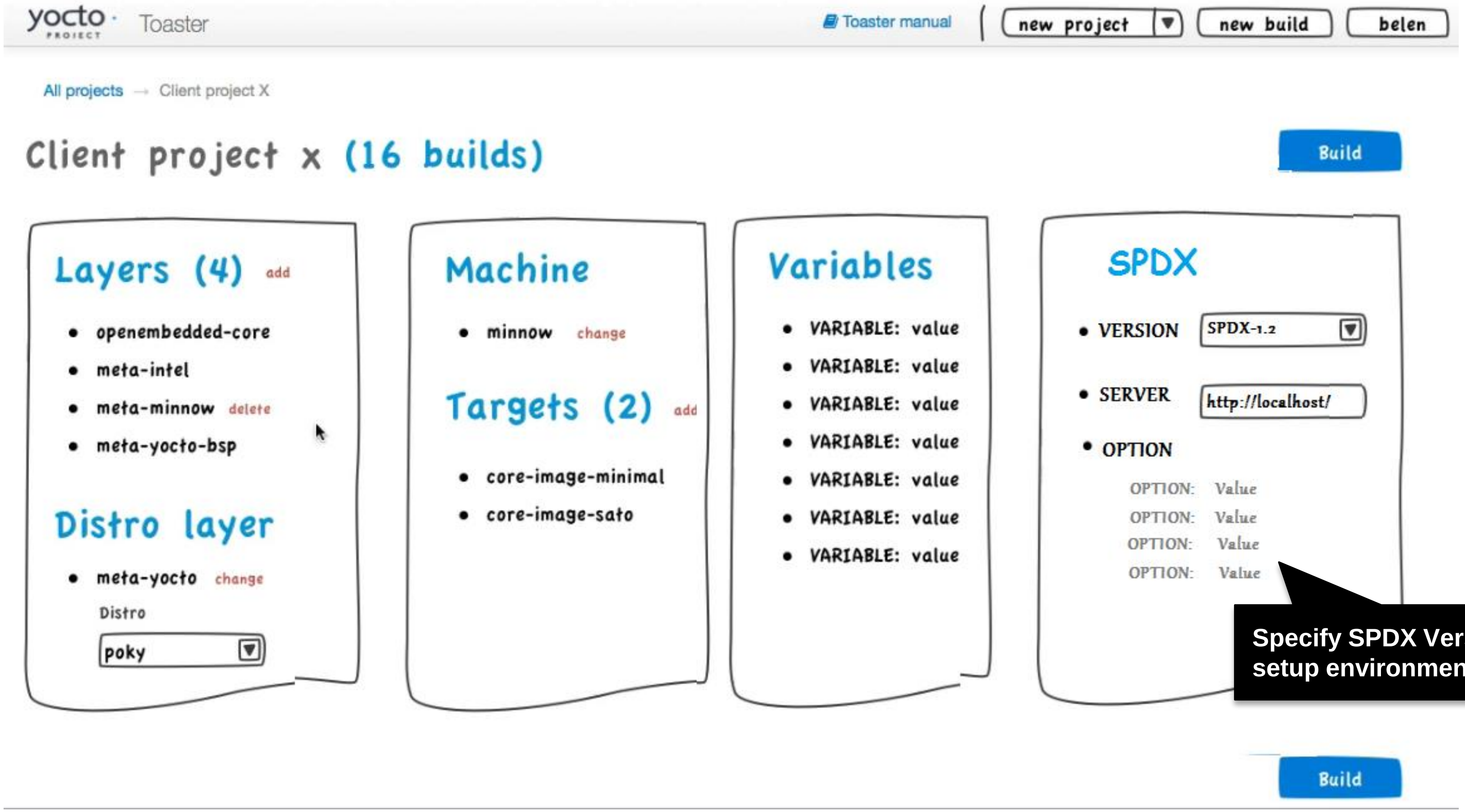
Obtain detail from

- https://github.com/spdx-tools/DoSPDX
- https://github.com/spdx-tools/SPDXDash
- https://github.com/spdx-tools/SPDXDash/blob/master/SPDX%20Tooling.pptx

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

Plan of Next-step(2/3)

- Toaster is a web-based interface to OpenEmbedded and BitBake. It is a replacement for Hob.
- Be merged into Toaster



Client project x (16 builds)

Layers (4)

- openembedded-core
- meta-intel
- meta-minnow
- meta-yocto-bsp

Distro layer

- meta-yocto

Distro: poky

Machine

- minnow

Targets (2)

- core-image-minimal
- core-image-sato

Variables

- VARIABLE: value
- VARIABLE: value
- VARIABLE: value
- VARIABLE: value
- VARIABLE: value
- VARIABLE: value
- VARIABLE: value

SPDX

- VERSION: SPDX-1.2
- SERVER: http://localhost/
- OPTION

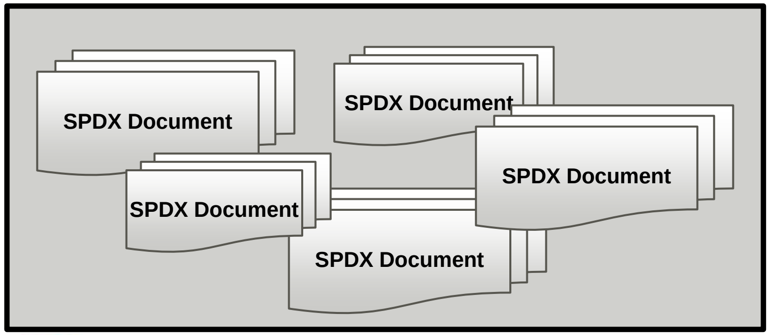
OPTION: Value
OPTION: Value
OPTION: Value
OPTION: Value

Specify SPDX Version and setup environment

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

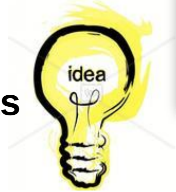
Plan of Next-step(3/3)

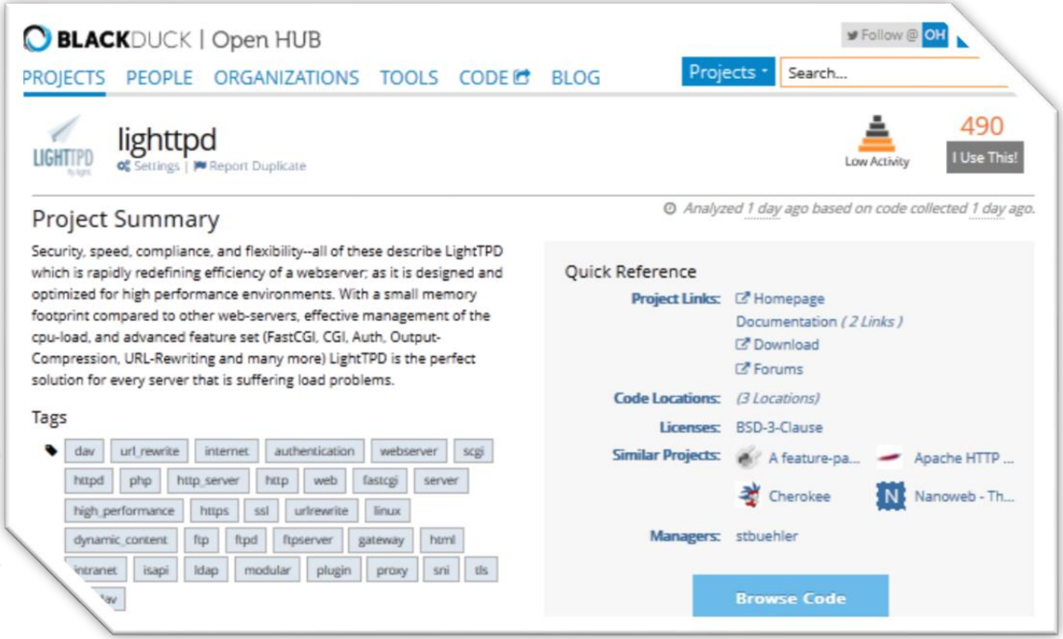
- Web-style SPDX File Management



We hava so many SPDX documents
How to maintain them?

A Web-style management such as OpenHUB looks like good.





lighttpd

Analyzed 1 day ago based on code collected 1 day ago.

Project Summary

Security, speed, compliance, and flexibility--all of these describe LightTPD which is rapidly redefining efficiency of a webserver; as it is designed and optimized for high performance environments. With a small memory footprint compared to other web-servers, effective management of the cpu-load, and advanced feature set (FastCGI, CGI, Auth, Output-Compression, URL-Rewriting and many more) LightTPD is the perfect solution for every server that is suffering load problems.

Tags

dav url_rewrite internet authentication webserver scgi httpd php http_server http web fastcgi server high_performance https ssl urlrewrite linux dynamic_content ftp ftpd ftpserver gateway html intranet isapi ldap modular plugin proxy sni tls dav

Quick Reference

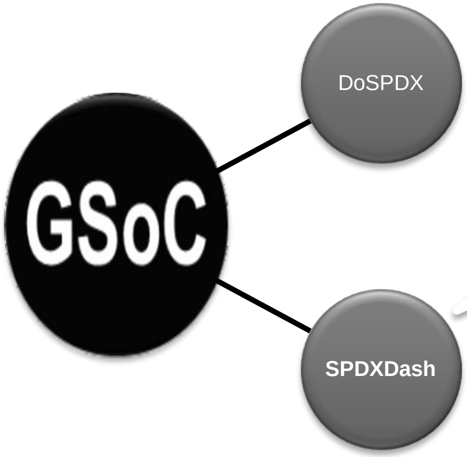
Project Links: Homepage
Documentation (2 Links)
Download
Forums

Code Locations: (3 Locations)

Licenses: BSD-3-Clause

Similar Projects: A feature-pa... Apache HTTP ... Cherokee Nanoweb - Th...

Managers: stbuehler



Nice!!!

There is a OSS project named GSoC including component DoSPDX and SPDXDash.

SPDXDash is a Web-style SPDX File management!

Obtain detail from

- https://www.openhub.net
- https://github.com/spdx-tools/SPDXDash

Q&A

Any Questions?

Copyright 2015 FUJITSU COMPUTER TECHNOLOGIES LIMITED

FUJITSU

shaping tomorrow with you