

FOSSology and SW360: Updates

Presenter: michael.c.jaeger@siemens.com

FOSSology and SW360



**Component
Analysis Tool**

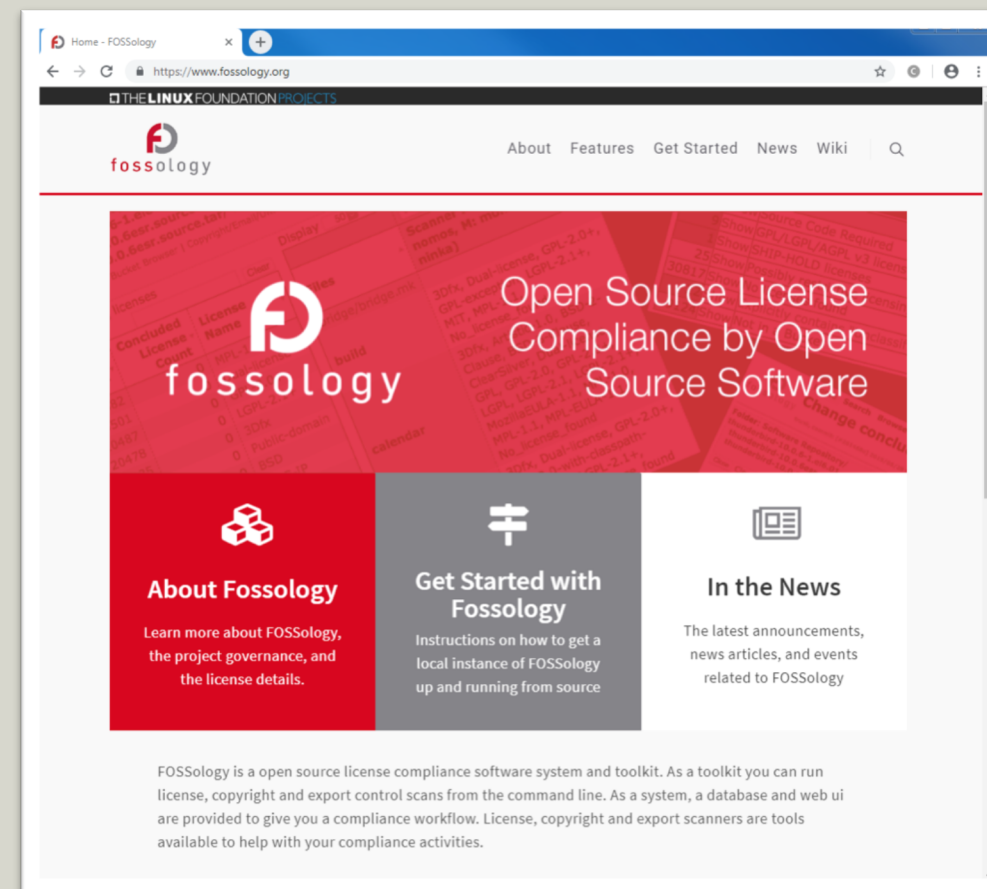


**Software
Catalogue**

FOSSology – Linux Foundation Collaboration

www.fossology.org

- 2008 initial publication by HP
- 2015 Linux Foundation Collaboration Project
- It is a Linux Application
- Different tasks for OSS license compliance
 - Scanning for licenses
 - Copyright, authorship, e-mails
 - ECC statements
 - Generation of documentation
 - Export and import SPDX files



FOSSology – It is about Overview

High Level and Drill Down

- Aggregation
 - Folder hierarchy of license findings
 - License-statement oriented view on files
 - Copyright aggregation
- Drill down
 - Navigate into folders
 - Filtering
 - Identify “the single” file

| Scanner Count | Concluded License Count | License Name |
|---------------|-------------------------|--------------------------------|
| 7702 | 8018 | EPL-1.0 |
| 2339 | 52 | Apache-2.0 |
| 275 | 0 | MPL-2.0 |
| 112 | 0 | MPL-1.1 |
| 110 | 0 | LGPL-2.0+ |
| 110 | 0 | Dual-license |
| 64 | 0 | Apache-possibility |
| 57 | 23 | W3C |
| 51 | 50 | MIT |
| 49 | 0 | GPL |
| 34 | 0 | W3C-IP |
| 24 | 0 | W3C-possibility |
| 18 | 0 | Public-domain |
| 13 | 11 | BSD-3-Clause |
| 12 | 0 | WebM |
| 8 | 8 | Apache-1.1 |
| 7 | 8 | Apache-1.1-variant-jakarta-oro |
| 6 | 0 | CPL-1.0 |
| 5 | 0 | W3C-style |
| 4 | 0 | UnclassifiedLicense |
| 4 | 0 | CPL-0.5 |
| 4 | 0 | BSD-style |
| 3 | 0 | Microsoft-possibility |
| 2 | 0 | libtiff |
| 2 | 0 | Unicode |

| Files | Scanner Results (N: nomos, M: monk, Nk: ninka, I: reportImport) | Edited Results |
|--|---|----------------------------|
| com.lowagie.text_2.1.7.v201004222200.jar | Adobe, Apache-2.0, APAFML, BSD-3-Clause, CUA-OPL-1.0, EPL-1.0, LGPL-2.0, libtiff, MIT-style, MPL-1.1, No_license_found, Permission Notice, Unicode | EPL-1.0, Apache-2.0 |
| com.lowagie.text.source_2.1.7.v201004222200.jar | Apache-2.0, BSD-3-Clause, CUA-OPL-1.0, Dual-license, EPL-1.0, LGPL, LGPL-2.0+, libtiff, MIT, MIT-style, MPL, MPL-1.1, No_license_found, Permission Notice, Public-domain, Unicode, WebM | MIT, BSD-3-Clause, EPL-1.0 |
| javax.wsdl_1.5.1.v201012040544.jar | CPL-0.5, GPL-1.0, EPL-1.0 | |
| javax.xml.rpc_1.1.0.v201209140446.jar | | Apache-2.0 |
| javax.xml.soap_1.2.0.v201005080501.jar | | Apache-2.0 |
| javax.xml.stream_1.0.1.v201004272200.jar | | Apache-2.0 |
| org.apache.axis_1.4.0.v201411182030.jar | Apache-2.0, Apache-possibility, EPL-1.0, No_license_found, W3C-possibility | Apache-2.0 |
| org.apache.batik.bridge_1.6.0.v201011041432.jar | Apache-2.0, Apache-possibility, EPL-1.0, No_license_found, Public-domain, W3C, W3C-IP | W3C, EPL-1.0, Apache-2.0 |
| org.apache.batik.bridge.source_1.6.0.v201011041432.jar | Apache-2.0, Apache-possibility, EPL-1.0, No_license_found, Public-domain, W3C, W3C-IP | W3C, EPL-1.0, Apache-2.0 |

Recursive unpacking of files too!

FOSSology – Review Findings

Specialized in Review

- Single file review
 - Highlighting of license relevant content
 - Reference text comparison
 - License statement decisions on statement level (“bulk scan”)

Close Cleared: 8030/11520

Hide Legend

```

/*
 * $Id: ImgJBIG2.java,v 1.1.2.1 2010/03/05 21:12:09 rbrooks Exp $
 *
 * Copyright 2009 by Nigel Kerr.
 *
 * The contents of this file are subject to the Mozilla Public License Version 1.1
 * (the "License"); you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at http://www.mozilla.org/MPL/
 *
 * Software distributed under the License is distributed on an "AS IS" basis,
 * WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License
 * for the specific language governing rights and limitations under the License.
 *
 * The Original Code is 'iText, a free JAVA-PDF library'.
 *
 * The Initial Developer of the Original Code is Bruno Lowagie. Portions created by
 * the Initial Developer are Copyright (C) 1999-2009 by Bruno Lowagie.
 * All Rights Reserved.
 * Co-Developer of the code is Paulo Soares. Portions created by the Co-Developer
 * are Copyright (C) 2000-2009 by Paulo Soares. All Rights Reserved.
 *
 * Contributor(s): all the names of the contributors are added in the source code
 * where applicable.
 *
 * Alternatively, the contents of this file may be used under the terms of the
 * LGPL license (the "GNU LIBRARY GENERAL PUBLIC LICENSE"), in which case the
 * provisions of LGPL are applicable instead of those above. If you wish to
 * allow use of your version of this file only under the terms of the LGPL
 * License and not to allow others to use your version of this file under
 * the MPL, indicate your decision by deleting the provisions above and
 * replace them with the notice and other provisions required by the LGPL.
 * If you do not delete the provisions above, a recipient may use your version
 * of this file under either the MPL or the GNU LIBRARY GENERAL PUBLIC LICENSE.
 *
 * This library is free software; you can redistribute it and/or modify it
 * under the terms of the MPL as stated above or under the terms of the GNU
 * Library General Public License as published by the Free Software Foundation;
 * either version 2 of the License, or any later version.
 *
 * This library 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 Library general Public License for more
 * details.
 *
 * If you didn't download this code from the following link, you should
 * you aren't using an obsolete version:
 * http://www.lowagie.com/iText/
 */
    
```

Apply decision to all future occurrences of this file

Clearing decision type

- No license known
- To be discussed
- Irrelevant
- Identified

| Action | License | Source | License Text | Acknowledgement | Comment |
|--------|--------------|-----------|--------------|-----------------|----------|
| X | LGPL-2.0+ | nomos: #1 | Click to add | Click to add | Click to |
| X | Dual-license | nomos: #1 | Click to add | Click to add | Click to |
| X | MPL-1.1 | nomos: #1 | Click to add | Click to add | Click to |

Showing 1 to 3 of 3 entries

User Decision Bulk Recognition Clearing History

Bulk recognition

Notice: Since punctuation is included in the matching process, periods needs to be included in the phrases if the word just before is included.
Hint: New license candidates can be added via [menu Organize»Licenses](#)

Dual-license Show license

| Action | License | License Text | Acknowledgement | Comment | |
|--------|--------------|--------------|-----------------|--------------|---|
| Add | MPL-1.1 | Click to add | Click to add | Click to add | - |
| Add | LGPL-2.0+ | Click to add | Click to add | Click to add | - |
| Remove | Dual-license | Click to add | Click to add | Click to add | - |

Reference text:

Legend:
license relevant text

FOSSology SPDX Import and Export

Import = Consuming SPDX

- Consistency!
 - Handling SPDX conclusions
 - Handling copyright statements
 - Handling new licenses
- Goal was to consistently import the data given existing records

Multiple Use Cases:

- *Checking SPDX from supplier*
- *Correcting existing SPDX and regenerate*
- *Using SPDX of one software package version to generate SPDX for updated version*
- *Transfer conclusions between different FOSSology instances*

FOSSology – Of course you can automate!

REST API

- Manage folders, uploads
- Trigger scans and options
- Download reporting
- More info at:
<https://www.fossology.org/get-started/basic-rest-api-calls/>
- (complete flow explained)

FOSSdriver

- Python based library
- Write your own Python workflow
- Not only what REST API can do
 - ... but also manage bulk scans
- More info at:
<https://github.com/fossology/fossdriver>

Command line tools

- Many functions and agents have command line interfaces
 - Nomos license scanner
 - Copyright scanner
 - License listings
 - ...
- Upload and download tools

FOSSology – License Obligations

Obligation Mngmt

- Attach obligation entries to licenses
- Admin management UI
- Report documentation for components

Obligation Source

- Different sources available
 - OSADL License Checklist
 - FINOS OSS Handbook
 - Github: Choose-a-license
- Machine readable formats

| License name | SPDX abbreviation | Link to checklist raw data |
|---|-------------------|---|
| Academic Free License v2.0 | AFL-2.0 | https://www.osadl.org/fileadmin/... |
| GNU Affero General Public License v3.0 only | AGPL-3.0-only | https://www.osadl.org/fileadmin/... |
| GNU Affero General Public License v3.0 or later | AGPL-3.0-or-later | https://www.osadl.org/fileadmin/... |
| Apache License 1.0 | Apache-1.0 | https://www.osadl.org/fileadmin/... |
| Apache License 1.1 | Apache-1.1 | https://www.osadl.org/fileadmin/... |
| Apache License 2.0 | Apache-2.0 | https://www.osadl.org/fileadmin/... |
| Artistic License 1.0 (Perl) | Artistic-1.0-Perl | https://www.osadl.org/fileadmin/... |

Obligation Import

- FOSSology can import records
- Currently: Convert your own data
- Potentially hosted conversion of obligations

FOSSology and SW360



Component
Analysis Tool

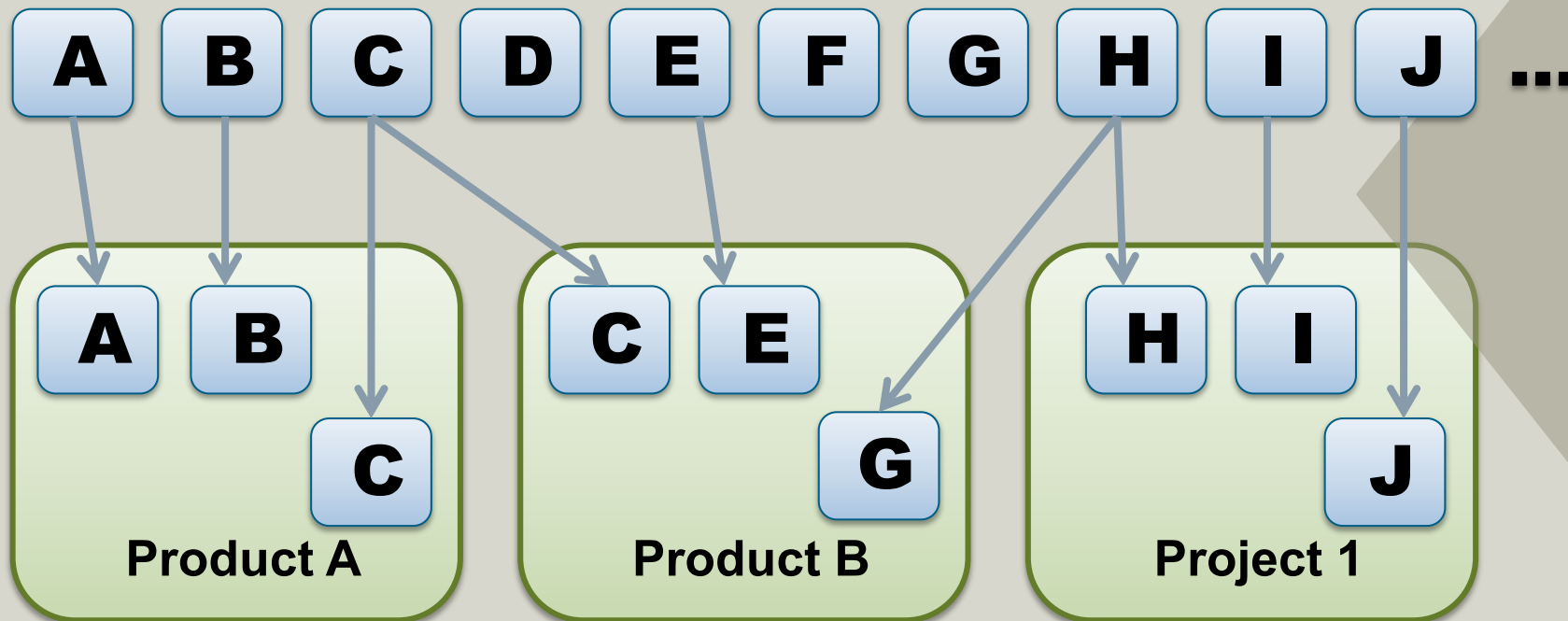


**Software
Catalogue**

SW360 Quick Recap

SW360 is a 3rd party software component catalogue

Assigns 3rd party components to products or projects



**Inventory
(in use)**

vs.

**Component Library
(generally
available)**

S-BOM-Driven View

S-BOM: Bill of Material

- Once the software contents are in a number of new use cases:
 - License compliance documentation
 - Collection of source code
 - ECC
 - Vulnerabilities
 - Statistics

SW360 cannot determine the S-BOM, but other OSS tools can:

- *SW360antenna*
- *OSS Review Toolkit*
- *Qmstr*
- *Tern*
- *...*

Compliance Documentation

Different Use Cases per Product / Project

- Component approval
 - Listing approval status of components
- Compliance documentation
 - Generating license texts, copyrights from SPDX as HTML or Text
- Source code bundle generation
 - Covering the work of source code collections
- Product approval documentation
 - WIP: Major updates to data model: project obligations

SW360 – Next Feature: Product Approval

The next use case: Product Approval Document

- Work on product approval document
- Product approval:
 - Do all components fit together?
 - What is the big picture?
 - What is the BOM?
 - What are the total obligations?

Readme OSS - \$project-name \$project-version

| | | |
|---|-------------------|---|
| Product Clearing report for 3rd party SW components | | \$owner-group |
| Product | \$project-name | |
| Version | \$project-version | |
| Clearing date | 2019-01-23 | |
| Attendees: | | |
| Name | Department | Role |
| The requirements of all 3 rd party components have been fulfilled. | | <input checked="" type="checkbox"/> yes* <input type="checkbox"/> no* |
| <small>(*) in case of Siemens components, delivery of <u>Readme_OSS</u> and source code delivery must be done by <u>superordinate</u> product</small> | | There are remaining risks. For further detail see [1] |

Table of Contents

- 1 Conclusions3
- 1.1 Summary 3
- 1.2 Issues not Considered 3
- 1.3 Obligations to be Fulfilled 3
- 1.4 Remaining Risks 3
 - 1.4.1 General Risks relating to OSS 3
 - 1.4.2 Specific Risks relating to OSS 4
 - 1.4.3 General risks relating to commercial 3rd party software 4
 - 1.4.4 Specific risks relating to commercial 3rd party software 4
- 2 Product Overview4
- 2.1 Product description 4

SW360 –Product Approval Documents

Proposed Document Structure

1 Conclusions

1.1 Summary

1.2 Issues not Considered

1.3 Obligations to be Fulfilled

1.4 Remaining Risks

1.4.1 General Risks relating to OSS

1.4.2 Specific Risks relating to OSS

1.4.3 General risks relating to commercial 3rd party software

1.4.4 Specific risks relating to commercial 3rd party software

2 Product Overview

2.1 Product Description

2.2 Delivery Channels

2.3 Development Details

2.4 Overview 3rd party components/services

3 Obligations

3.1 Common Rules

3.2 Additional Requirements

3.3 Disclosure Document

3.4 Build Instructions

3.5 Source Code Bundle

SW360: REST API

Integration with other tools

- Check of approved components
- Create S-BOM
- Automated upload of SPDX files to components
- Synchronize component catalogue with other tools

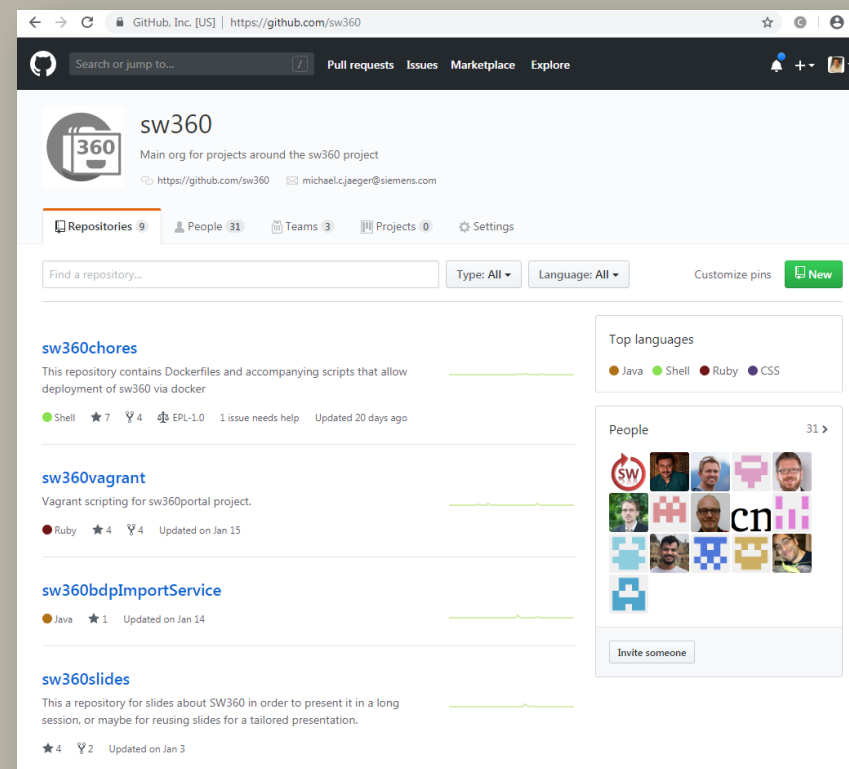
On a normal SW360 instance, full documentation is available:

`https://[hostname]:[port]/resource/docs/index.html`

SW360: More Projects

SW360 has a number of smaller projects

- **sw360antenna**
Analyses the build and pulls data from other sources
- **sw360vagrant**
Full instance deployment, including AWS
- **sw360chores**
Docker deployment scripts
- **sw360slides**
Documentation (also in Japanese)



<https://github.com/sw360>

Thank you for your attention ... questions?



Michael C. Jaeger

Siemens AG
Corporate Technology
Otto-Hahn-Ring 6
81379 München

michael.c.jaeger@siemens.com

FOSSology links

<https://www.fossology.org/>

<https://github.com/fossology/fossology>

SW360 links

<https://sw360.github.io/>

<https://github.com/sw360/sw360portal>