FOSSology and SPDX

Gaurav Mishra & Shaheem Azmal M MD
@GMishx    @shaheemazmal

https://fossology.org
FOSsology – Linux Foundation Collaboration Project

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
It is about finding licenses

Finding Licenses

License texts

References to licenses

Written texts explaining licensing

License relevant statements
Open Source and Reuse

• It is natural that an OSS project reuses available likely OSS from another project

• For example, FOSSology will find 25 other licensing relevant text occurrences in Apache thrift
FOSSology – It is about Conclusions

**Licensing Challenges**

- Licensing can be simple …
  … or challenging:
- Unknown Licenses
- Written statements
- Unclear statements
- Ambiguous statements
- Incomplete statements
- Depends on domain

```plaintext
SPDXVersion: SPDX-2.3
DataLicense: CC0-1.0

## Document Information


---

## File

FileName: fossology-master/utils/fo-installdeps
SPDXID: SPDXRef-item361
FileChecksum: SHA1: 3fc0aa4a4face8a0d317e0272c5e28e43f44c45a
FileChecksum: MD5: 1576b827a8b28ce1513a490fe2fecdc
LicenseConcluded: GPL-2.0
LicenseInfoInFile: GPL-2.0
FileCopyrightText: <text> Copyright (C) 2008-2014 Hewlett-Packard Development Company, L.P. </text>
```

...
SBOM and FOSSology

**As Producer**

- FOSSology produces SBOM in SPDX v2.3 format
- Includes file level information
- License findings and conclusions
- Copyrights
- Custom license texts

**As Consumer**

- FOSSology can import SPDX SBOM
- Allow exchange of license clearings
- License findings and conclusions
- Copyrights
- Custom license texts
New Versions mean new Features

REST API++
GDPR updates
Bootstrap UI

ScanCode
Copyright Spacy
License sync

REUSE report
License sync
REUSE.software standard

... 4.0 2022-01-24 ... 4.1 2022-05-20 ... 4.2 2022-11-11 ...
SPDX Updates – License IDs

Phase 1 - Introduction of SPDX License ID

• Add SPDX ID to all licenses
• Will be used as license name in all reports
• IDs are checked against SPDX License List
• If empty/not in list, make it license ref LicenseRef-fossology-

Phase 2 - using of actual license expressions

• Allowing users to add **WITH, OR and AND** expressions
SPDX Updates – Reports

- Update report specification to version 2.3
- Several fixes were done at same time
  - Add the missing `spdx:ExtractedLicensingInfo`
- Fix algorithm used for `spdx:PackageVerificationCode`
- More fields were introduced
  - Add the `spdx:versionInfo` and `spdx:releaseDate` if they exist
- Use the `spdx:ExternalRef` for Package-URL, maven, nuget, npm and pypi links
SPDX Updates – Reports

- The license obligations are now `spdx:attributionText` for the `spdx:Package`
- Use the acknowledgements from file as `spdx:attributionText` for the `spdx:File`
- Update calculation of Conjunctive and Disjunctive license set (use special license “Dual-License” for disjunctive set)
- Add the missing license name and text for all licenses.
Thank you – Consider to “Start Us”!

Links

- https://www.fossology.org
- https://fossology.github.io/gsoc/
- https://github.com/fossology/fossology
- https://www.youtube.com/channel/UCZGPJnQZVnEPQWxOuNamLpw

License: CC-BY-SA-4.0