FOSSology and SPDX

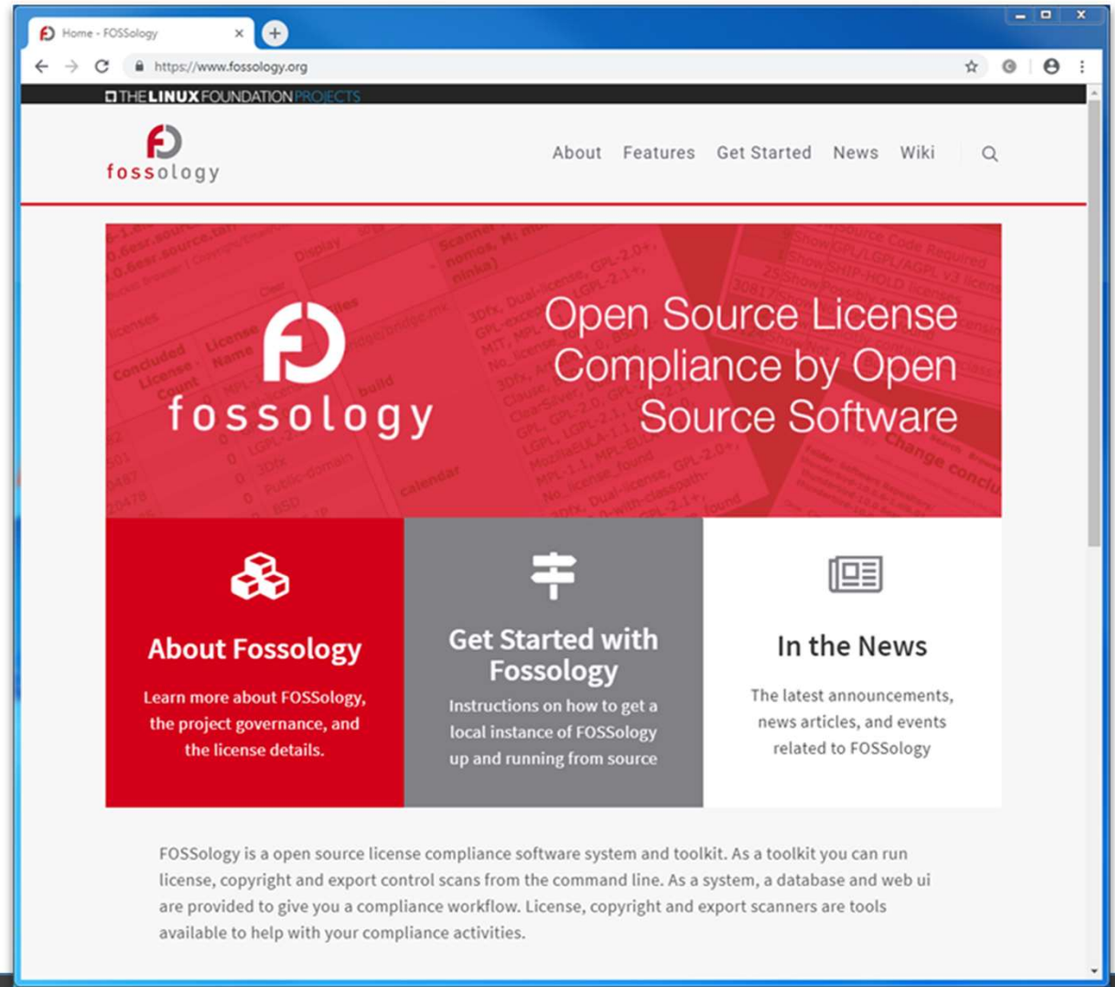
Gaurav Mishra & Shaheem Azmal M MD
@GMishx @shaheemazmal

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

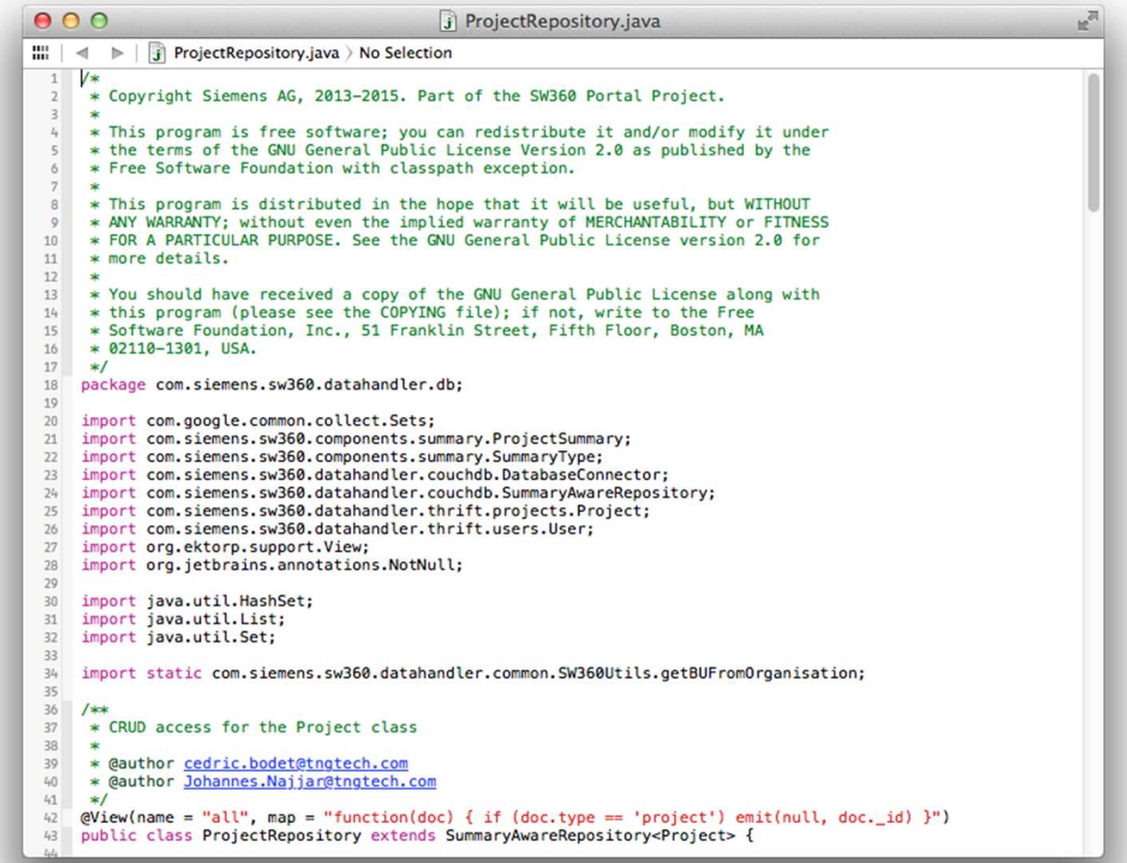
Finding Licenses

License texts

References to licenses

Written texts explaining licensing

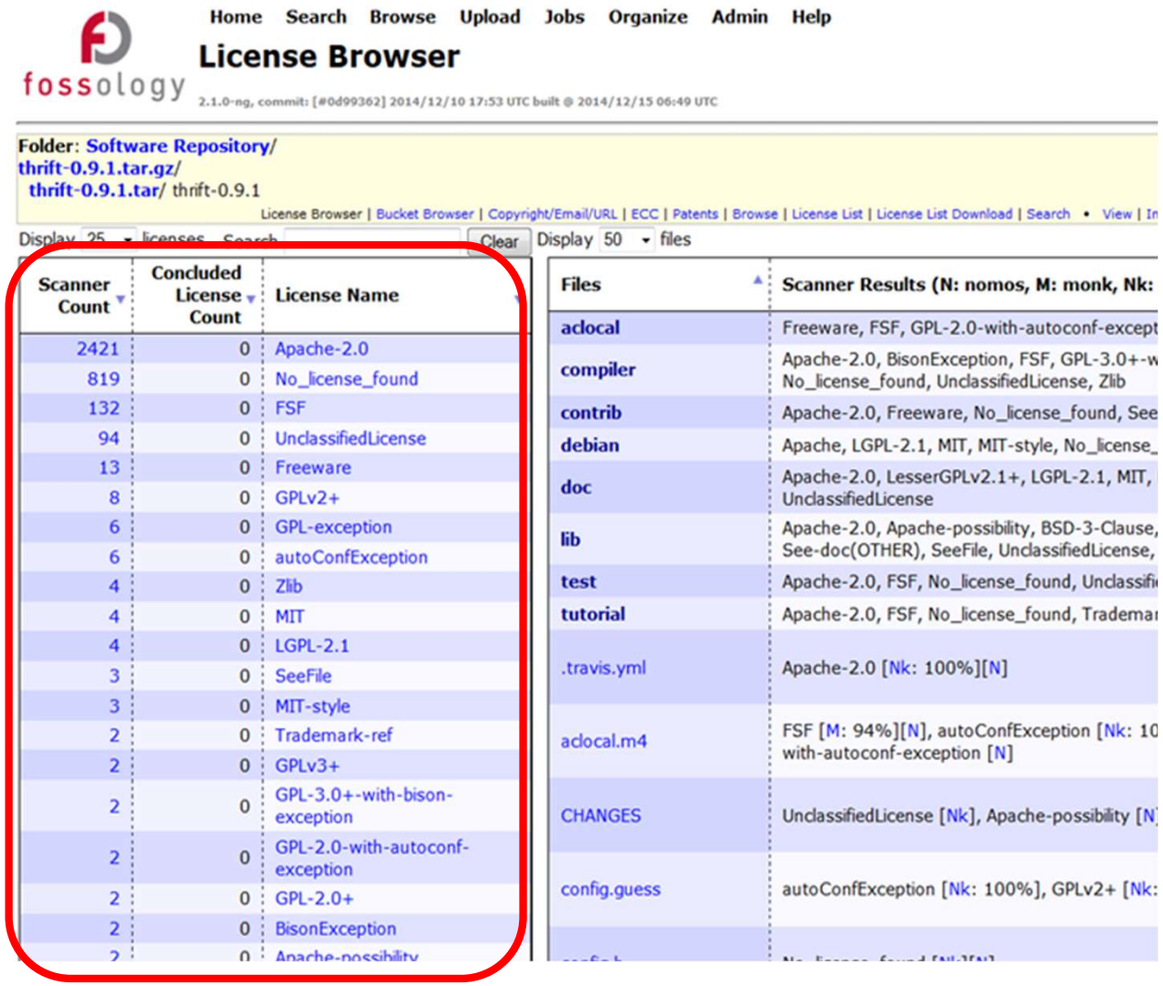
License relevant statements



An Example – What do we find?

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

```
SPDXVersion: SPDX-2.3
DataLicense: CC0-1.0
##-----------------------
## Document Information
##-----------------------
DocumentNamespace: http://debian/repo/SPDX2TV_fossology-
master-3.zip_1490661487.spdx
...
##File
FileName: fossology-master/utils/fo-installdeps
SPDXID: SPDXRef-item361
FileChecksum: SHA1: 3fc0aa4a4face8a0d317e0272c5e28e43f44c45a
FileChecksum: MD5: 1576b827a8b28ce1513a490fe2fecdcd
LicenseConcluded: GPL-2.0
LicenseInfoInFile: GPL-2.0
FileCopyrightText: <text> Copyright (C) 2008-2014 Hewlett-Packard
Development Company, L.P. </text>
…
```

SBOM and FOSSology

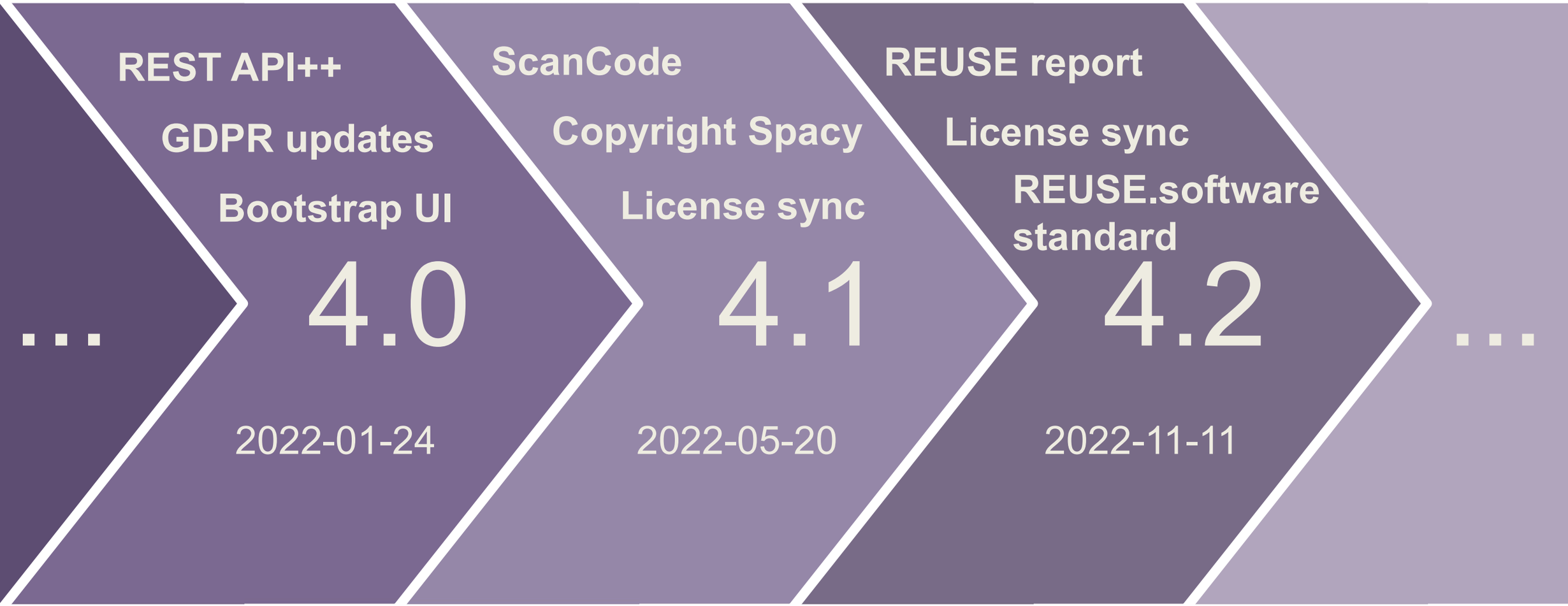
As Producer

- 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



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

Search: | Search SPDX | Search Shortn | Search Fullname | Search Text

Edit	Checked	SPDX ID	Shortname	Fullname	Text
	No	CC-BY-SA-2.0-UK	CC-BY-SA-2.0-UK	Creative Commons Attribution Share Alike 2.0 England and Wales	Creative Commons Attribution - Share-Alike 2.0 England and Wales
	No	CC-BY-SA-2.1-JP	CC-BY-SA-2.1-JP	Creative Commons Attribution Share Alike 2.1 Japan	アトリビューション—シェアアライク 2.1
	No	CC-BY-SA-2.5	CC-BY-SA-2.5	Creative Commons Attribution Share Alike 2.5 Generic	Creative Commons Attribution-ShareAlike 2.5
	No	CC-BY-SA-3.0	CC-BY-SA-3.0	Creative Commons Attribution Share Alike 3.0 Unported	Creative Commons Attribution-ShareAlike 3.0 Unported
	No	CC-BY-SA-3.0-AT	CC-BY-SA-3.0-AT	Creative Commons Attribution Share Alike 3.0 Austria	CREATIVE COMMONS IST KEINE RECHTSANWALTSKANZL
	No	CC-BY-SA-3.0-DE	CC-BY-SA-3.0-DE	Creative Commons Attribution Share Alike 3.0 Germany	Creative Commons Namensnennung - Weitergabe unter gleichen
	No	CC-BY-SA-4.0	CC-BY-SA-4.0	Creative Commons Attribution Share Alike 4.0 International	Creative Commons Attribution-ShareAlike 4.0 International
	No	CC-PDDC	CC-PDDC	Creative Commons Public Domain Dedication and Certification	The person or persons who have associated work with this document (the
	No	CC0-1.0	CC0-1.0	Creative Commons Zero v1.0 Universal	Creative Commons Legal Code
	No		CCLRC	CCLRC License	CCLRC License for CCLRC Software forming part of the Climate Data

Showing 141 to 150 of 662 entries

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:hasExtractedLicensingInfo>
  <spdx:ExtractedLicensingInfo rdf:about="#LicenseRef-fossology-CDDL">
    <spdx:licenseId>LicenseRef-fossology-CDDL</spdx:licenseId>
    <spdx:name>Common Development and Distribution License</spdx:name>
    <spdx:extractedText><![CDATA[
CDDL is referenced without a version number. Please look up CDDL in the License Admin to view the d
    ]]></spdx:extractedText>
  </spdx:ExtractedLicensingInfo>
</spdx:hasExtractedLicensingInfo>
<spdx:relationship>
  <spdx:Relationship>
    <spdx:relationshipType rdf:resource="http://spdx.org/rdf/terms#relationshipType_describes" />
    <spdx:relatedSpdxElement>
      <spdx:Package rdf:about="#SPDXRef-upload2">
        <spdx:name>30-seconds-of-code-master.tar.gz</spdx:name>
        <spdx:packageFileName>30-seconds-of-code-master.tar.gz</spdx:packageFileName>
        <spdx:downloadLocation rdf:resource="http://spdx.org/rdf/terms#noassertion" />
        <spdx:versionInfo>1.2.3</spdx:versionInfo>
        <spdx:releaseDate>2018-12-05T00:00:00Z</spdx:releaseDate>
        <spdx:filesAnalyzed>true</spdx:filesAnalyzed>
        <spdx:externalRef>
          <spdx:ExternalRef>
            <spdx:referenceCategory rdf:resource
              ="http://spdx.org/rdf/terms#referenceCategory_packageManager" />
            <spdx:referenceType rdf:resource
              ="http://spdx.org/rdf/references/purl" />
            <spdx:referenceLocator>pkg:npm/30-seconds-of-code@1.2.3</spdx:referenceLocator>
          </spdx:ExternalRef>
        </spdx:externalRef>
        <spdx:packageVerificationCode>
          <spdx:PackageVerificationCode>
          <spdx:packageVerificationCodeValue>5f4bdb07a80392c25ab8671a7c4c090ba5f64820</spdx:packa
          </spdx:PackageVerificationCode>
        </spdx:packageVerificationCode>
```

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.

```
<spdx:attributionText>Do not change or delete Copyright, patent, trademark, attribution notices or any further legal
<spdx:hasFile>
  <spdx:File rdf:about="#SPDXRef-item1373">
    <spdx:fileName>30-seconds-of-code-master.tar.gz/30-seconds-of-code-master.tar/30-seconds-of-code-master.zip/30-se
    <spdx:checksum>
    </spdx:checksum>
    <spdx:checksum>
    </spdx:checksum>
    <spdx:checksum>
    </spdx:checksum>
    <spdx:licenseConcluded>
      <spdx:ConjunctiveLicenseSet>
        <spdx:member>
          <spdx:ListedLicense rdf:about="http://spdx.org/licenses/GPL-3.0-only">
            <spdx:name>GNU General Public License v3.0 only</spdx:name>
            <spdx:licenseId>GPL-3.0-only</spdx:licenseId>
            <spdx:licenseText><![CDATA[
            ]]></spdx:licenseText>
            <rdfs:seeAlso>https://www.gnu.org/licenses/gpl-3.0-standalone.html</rdfs:seeAlso>
          </spdx:ListedLicense>
        </spdx:member>
        <spdx:member rdf:resource="#LicenseRef-fossology-CDDL" />
      </spdx:ConjunctiveLicenseSet>
    </spdx:licenseConcluded>
    <spdx:licenseComments><![CDATA[This Travis conf is licensed by the tool under GPL version 3.0
Just added for testing comments.]]></spdx:licenseComments>
    <spdx:licenseInfoInFile>
      <spdx:ListedLicense rdf:about="http://spdx.org/licenses/GPL-3.0-only" />
    </spdx:licenseInfoInFile>
    <spdx:copyrightText><![CDATA[
      Copyright (c) Martin Brehm (2009-2015) Martin Thomas (2012-2015) Barbara Kirchner (2009-2015) University of Lei
    ]]></spdx:copyrightText>
    <spdx:attributionText><![CDATA[This project is like collection of popular JS projects.]]></spdx:attributionText>
  </spdx:File>
</spdx:hasFile>
```

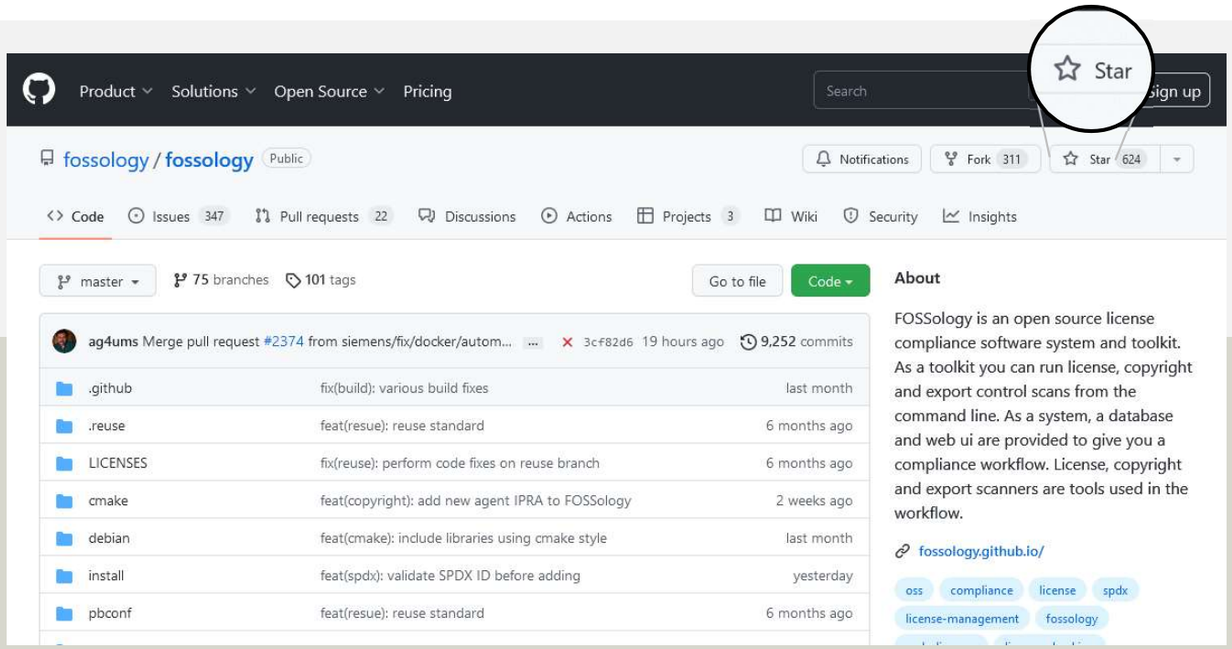
Thank you – Consider to “Start Us”!

Shaheem Azmal M MD
@shaheemazmal
Siemens AG
Mentor and maintainer

E-mail shaheem.azmal@gmail.com

Gaurav Mishra
@GMishx
Siemens AG
Mentor and maintainer

https://gmishx.in
E-mail gmishx@gmishx.in



Links

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