Training: Open Source Licenses and Copyright Notices

Steve Winslow
ONAP VF2F - February 8, 2018
Antitrust Policy Notice

› Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

› Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.
Agenda

1. Licensing and Copyright Basics
2. LF License Scans
3. ONAP Processes and Best Practices
4. Q&A
Preliminary: Talk to your legal counsel!

- This training is intended to focus on community norms and best practices in license and copyright management. It is not intended as legal advice.
- The LF is not able to provide you with legal advice. For questions on interpretation of licenses contained in the code repository, ONAP members should consult with their own legal counsel.
An Ongoing Process

› License compliance is a matter of ongoing improvement
  › ...like all aspects of collaborative software development

› Areas of focus will change over time as we improve together

› Focusing on key priorities first

› Reach out with any questions!
  › Steve Winslow: swinslow@linuxfoundation.org
  › your in-house legal counsel (for any legal interpretation questions)
Licensing and Copyright Basics
Open Source Licensing: Basics

› Copyright – certain rights owned in software code (among other things)
› License – permission to do something
  ‣ ”Proprietary” – typically very limited rights to use but not modify or redistribute; restrictive conditions and obligations
  ‣ “Open Source” – typically broad rights to use, modify and redistribute, with varying conditions
› Standardized language for various (100+) open source licenses
Open Source Licensing: Types

Fewer obligations

More obligations
Open Source Licensing: Types

Fewer obligations

Permissive

More obligations
Open Source Licensing: Types

Permissive

Examples

MIT

BSD-2-Clause

BSD-3-Clause

Apache-2.0
Open Source Licensing: Types

- Fewer obligations
  - Permissive
    - Examples
      - MIT
      - BSD-2-Clause
      - BSD-3-Clause
      - Apache-2.0
  - Strong Copyleft

- More obligations
Open Source Licensing: Types

- Fewer obligations
  - Permissive
    - Examples
      - MIT
      - BSD-2-Clause
      - BSD-3-Clause
      - Apache-2.0
    - MIT

- More obligations
  - Strong Copyleft
    - Examples
      - GPL-2.0, GPL-3.0
      - Affero GPL (AGPL-3.0)
Open Source Licensing: Types

- **Permissive**
  - Examples:
    - MIT
    - BSD-2-Clause
    - BSD-3-Clause
    - Apache-2.0

- **Weak Copyleft**
  - Examples:
    - GPL-2.0, GPL-3.0

- **Strong Copyleft**
  - Examples:
    - Affero GPL (AGPL-3.0)
Open Source Licensing: Types

- **Permissive**
  - Examples
    - MIT
    - BSD-2-Clause
    - BSD-3-Clause
    - Apache-2.0

- **Weak Copyleft**
  - Examples
    - Mozilla (MPL-2.0)
    - Eclipse (EPL-2.0)
    - Lesser GPL (LGPL-2.0, LGPL-3.0)

- **Strong Copyleft**
  - Examples
    - GPL-2.0, GPL-3.0
    - Affero GPL (AGPL-3.0)
Open Source Licensing: Types

- Fewer obligations
  - Public Domain
    - MIT
    - BSD-2-Clause
    - BSD-3-Clause
    - Apache-2.0

- Weak Copyleft
  - Mozilla (MPL-2.0)
  - Eclipse (EPL-2.0)
  - Lesser GPL (LGPL-2.0, LGPL-3.0)

- Strong Copyleft
  - GPL-2.0, GPL-3.0
  - Affero GPL (AGPL-3.0)
Open Source Licensing: Types

Fewer obligations

Permissive
- Examples
  - MIT
  - BSD-2-Clause
  - BSD-3-Clause
  - Apache-2.0

Public Domain
- Examples
  - CC0-1.0
  - "Public domain" statement

Weak Copyleft
- Examples
  - Mozilla (MPL-2.0)
  - Eclipse (EPL-2.0)
  - Lesser GPL (LGPL-2.0, LGPL-3.0)

Strong Copyleft
- Examples
  - GPL-2.0, GPL-3.0
  - Affero GPL (AGPL-3.0)

More obligations
Open Source Licensing: Types

- **Permissive**
  - Examples: MIT, BSD-2-Clause, BSD-3-Clause, Apache-2.0

- **Weak Copyleft**
  - Examples: Mozilla (MPL-2.0), Eclipse (EPL-2.0), Lesser GPL (LGPL-2.0, LGPL-3.0)

- **Strong Copyleft**
  - Examples: GPL-2.0, GPL-3.0, Affero GPL (AGPL-3.0)

- Public Domain
  - Examples: CC0-1.0, “Public domain” statement

---

**Not OSS**
Open Source Licensing: Types

- **Permissive**
  - Fewer obligations
  - Examples: MIT, BSD-2-Clause, BSD-3-Clause, Apache-2.0

- **Weak Copyleft**
  - More obligations
  - Examples: Mozilla (MPL-2.0), Eclipse (EPL-2.0), Lesser GPL (LGPL-2.0, LGPL-3.0)

- **Strong Copyleft**
  - More obligations
  - Examples: GPL-2.0, GPL-3.0, Affero GPL (AGPL-3.0)

**Public Domain**
- Examples: CC0-1.0, "Public domain" statement

**Not OSS**
- Examples: Proprietary, EULA, Non-comm’l use only
Open Source Licensing: Types

- Fewer obligations
  - Permissive
    - Examples
      - MIT
      - BSD-2-Clause
      - BSD-3-Clause
      - Apache-2.0
  - Weak Copyleft
    - Examples
      - Mozilla (MPL-2.0)
      - Eclipse (EPL-2.0)
      - Lesser GPL (LGPL-2.0, LGPL-3.0)
  - Strong Copyleft
    - Examples
      - GPL-2.0, GPL-3.0
      - Affero GPL (AGPL-3.0)

- More obligations
  - Public Domain
    - Examples
      - CC0-1.0
      - "Public domain" statement
  - Not OSS
    - Examples
      - Proprietary
      - Non-comm’l use only

---

THE LINUX FOUNDATION
Open Source Licensing: Basics

› But – more considerations than just permissive vs. copyleft:
  › Patent licenses?
  › Compatibility?
  › Other obligations? (e.g. advertising clauses; reverse-engineering)
Open Source Licensing: Basics

› Who cares about license compliance?
  › Contributors to the project
  › The project itself
  › Downstream users (expectations and compliance burdens)
Open Source Licensing: In ONAP

› ONAP’s IP policy specifies the project’s licenses for contributions:
  › Code: Apache License 2.0 (Apache-2.0)
  › Documentation: Creative Commons Attribution 4.0 (CC-BY-4.0)

› Exceptions for use of other licenses:
  › Subject to TSC approval...
  › ...with TSC informed by LF Networking Governing Board’s Legal Committee
Open Source Licensing: Contexts

› Within ONAP code base:
  › snippets
  › entire files

› And beyond that – can be relevant for:
  › build-time dependencies (e.g., Java JARs)
  › install-time dependencies (e.g., Python packages)
  › run-time dependencies (e.g., system libraries)
Open Source Licensing: Which license?

› Knowing what license applies isn’t easy
  › “declared” licenses: LICENSE.txt; package manager metadata
  › “observed” licenses: what we find in source files
  › These are often different or incomplete

› Notices in individual files are important
LF License Scans
LF License Scans: Tools

FOSSology

Used to scan a codebase for licenses
Performs textual analysis and regular expression scanning to identify likely license notices and references
Supplemented with manual review to remove false positives and investigate unusual findings
**Sonatype Nexus IQ**

Used to scan Java dependencies imported at build time

Based on Sonatype (Maven) Java artifacts, with declared and observed licenses

Supplemented with manual review and, where appropriate, FOSSology scans of artifacts
LF License Scans: Tools

SPDX

Used to communicate license information in a standardized, machine-readable format

SPDX documents are produced from each FOSSology source code scan

SPDX short-form identifiers used to enable quickly adding license info to source code with minimal burden

https://spdx.org

SPDX License List: https://spdx.org/licenses
LF License Scans: Reports

Reports for Developers

- Summary and listing of license combinations identified per-file
- Calls to discuss situations where remediation may be appropriate
- Information gathering to facilitate license exception approvals
LF License Scans: Reports

<table>
<thead>
<tr>
<th>License</th>
<th># of files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache-2.0</td>
<td>19479</td>
</tr>
<tr>
<td>Apache-2.0 AND CC-BY-4.0</td>
<td>2285</td>
</tr>
<tr>
<td>Apache-2.0 OR EPL-1.0</td>
<td>129</td>
</tr>
<tr>
<td>CC-BY-4.0</td>
<td>431</td>
</tr>
</tbody>
</table>

**Use restrictions:**

<table>
<thead>
<tr>
<th>License</th>
<th># of files</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATT-Proprietary</td>
<td>14</td>
</tr>
<tr>
<td>ATT-Proprietary AND Apache-2.0</td>
<td>8</td>
</tr>
<tr>
<td>Apache-2.0 AND CC-BY-4.0 AND Olympic-logo-reference</td>
<td>2</td>
</tr>
<tr>
<td>Dynamic-Drive-2015</td>
<td>2</td>
</tr>
<tr>
<td>bpmn.io License AND Apache-2.0 AND BSD-3-Clause AND MIT</td>
<td>1</td>
</tr>
</tbody>
</table>

**Copyleft:**

<table>
<thead>
<tr>
<th>License</th>
<th># of files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache-2.0 AND CDDL-1.1 OR GPL-2.0-WITH-classpath-excep</td>
<td>1</td>
</tr>
<tr>
<td>Apache-2.0 AND CC-BY-4.0 AND CC-BY-SA-4.0</td>
<td>1</td>
</tr>
<tr>
<td>BSD-3-Clause AND EPL-1.0 AND EDL-1.0 AND MIT</td>
<td>2</td>
</tr>
<tr>
<td>CC-BY-SA-4.0</td>
<td>1</td>
</tr>
<tr>
<td>GPL-2.0 AND Link-exception</td>
<td>3</td>
</tr>
<tr>
<td>GPL-3.0-WITH-OpenSSL-linking-exception</td>
<td>32</td>
</tr>
<tr>
<td>LGPL</td>
<td>6</td>
</tr>
<tr>
<td>LGPL-3.0 AND Link-exception</td>
<td>3</td>
</tr>
<tr>
<td>MIT AND MPL-1.1</td>
<td>7</td>
</tr>
</tbody>
</table>

**Attribution:**

<table>
<thead>
<tr>
<th>License</th>
<th># of files</th>
</tr>
</thead>
<tbody>
<tr>
<td>(MIT OR GPL-2.0) AND (MIT OR BSD OR GPL)</td>
<td>4</td>
</tr>
<tr>
<td>Apache (version unspecified)</td>
<td>2</td>
</tr>
<tr>
<td>S</td>
<td>W</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Jenkins view: [https://jenkins.onap.org/view/CLM/](https://jenkins.onap.org/view/CLM/)
Project aai-aai-service-maven-clm-release-1.0.0

Recent Changes

Application Composition Report

Permalinks
- Last build (#24), 5 days 13 hr ago
- Last stable build (#16), 2 mo 8 days ago
- Last successful build (#24), 5 days 13 hr ago
- Last unstable build (#24), 5 days 13 hr ago
- Last unsuccessful build (#24), 5 days 13 hr ago
- Last completed build (#24), 5 days 13 hr ago

Click here (login required)
Sonatype Nexus IQ

This report provides security and license assessments for identified components found within an application.

SCAPE OF ANALYSIS

374 COMPONENTS IDENTIFIED
96% OF ALL COMPONENTS ARE IDENTIFIED

1 POLICY ALERTS
AFFECTING 81 COMPONENTS

12 SECURITY ALERTS
AFFECTING 44 COMPONENTS

68 LICENSE ALERTS
AFFECTING 44 COMPONENTS

SECURITY ISSUES

How bad are the vulnerabilities and how many are there?

<table>
<thead>
<tr>
<th>Critical (7-10)</th>
<th>Severity (6-8)</th>
<th>Moderate (1-3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>59</td>
<td>7</td>
</tr>
</tbody>
</table>

The summary of security issues demonstrates the breakdown of vulnerabilities based on severity and the threat level it poses to your application.

The dependency depth highlights quantity and severity and distribution within the application's dependencies.

LICENSE ANALYSIS

What type of licenses and how many of each?

<table>
<thead>
<tr>
<th>Critical (8-10)</th>
<th>Severe (4-7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>18%</td>
</tr>
<tr>
<td>1</td>
<td>3%</td>
</tr>
</tbody>
</table>

The summary of license analysis demonstrates the number of licenses detected in each category.

The dependency depth compares quantity by...
Sonatype Nexus IQ
### License Threats

<table>
<thead>
<tr>
<th>License Threat</th>
<th>Component</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache-2.0, BSD-3-Clause, GPL-2.0-with-classpath+</td>
<td>org.powermock:powermock-module-javassistent:1.6.2</td>
<td>Selected</td>
</tr>
</tbody>
</table>

**powermock-javassistent.jar located at ajs-caa/target/agents**

<table>
<thead>
<tr>
<th>License</th>
<th>Component</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>LGPL-2.1</td>
<td>org.xtrim:renderer:core:renderer:R8</td>
<td>Selected</td>
</tr>
<tr>
<td>Not Declared, No Source License</td>
<td>org.codehaus.plexus:plexus-hfbc:1.0-beta-7</td>
<td>Confirmed</td>
</tr>
<tr>
<td>LGPL-2.1</td>
<td>bsh: bsh: 1.3.0</td>
<td>Overridden</td>
</tr>
</tbody>
</table>
ONAP Processes and Best Practices
ONAP: Review monthly reports

› LF will continue to send monthly to PTLs:
  › FOSSology reports (licenses detected within ONAP repos)
  › Nexus IQ reports (licenses detected in build-time JAR dependencies)

› Please review these reports for findings in your repos
› Discuss questions with me (and/or your legal counsel)
ONAP: License findings

› Remediate (e.g., remove and replace) where possible for high-priority findings:
  › Non-OSS / use restrictions
  › Copyleft (especially strong copyleft)

› Where any non-Apache.2.0, non-CC-BY-4.0 licenses will remain in the project, a license exception approval from the TSC will be required
  › This process is being defined, following transition to LF Networking
ONAP: License notices within individual files

- Different types of notices:
  - Full license text in top-level LICENSE.txt file
  - Copyright notice
  - Standard license headers in each file
  - SPDX short-form IDs in each file

(sample; not from ONAP)
ONAP: License notices within individual files

For files without license notices, we recommend developers add SPDX short-form IDs.

Examples:

› For ONAP original code:

   `SPDX-License-Identifier: Apache-2.0`

› For a file that contains ONAP-original code, together with third-party code under MIT:

   `SPDX-License-Identifier: (Apache-2.0 AND MIT)`

› For ONAP-original documentation:

   `SPDX-License-Identifier: CC-BY-4.0`
ONAP: License notices within individual files

Some files can’t easily have license notices added.

Examples:

› Image files (.jpeg, .png, …)
› Structured metadata without comment fields (.json, binary formats)
› Other binary files (e.g. test files)

For these types of files, the best that can easily be done is to rely on the top-level LICENSE.txt notices.
ONAP: Copyright notices within individual files

Many different formats possible; your company / legal counsel may have a preference.

Our recommendation:

Copyright (c) [your company name]

› It is not typically necessary to include the year

› If the year is present, you can choose to update your own copyright notices when you update the file, but it is not mandatory to do so
ONAP: Things Not to Do

Do NOT:

› Remove or modify a third party’s license or copyright notice
› Add a license notice that is incompatible with one already present
   › E.g., don’t add an Apache-2.0 notice to a GPL-2.0 file
› Add a reference to Apache-2.0 just to bypass the license checker
› Add third-party code from another source without including its license information

DO:

› If you aren’t sure about what’s compatible, please ask (and include your legal counsel).
  There are differences of opinions and no single definition of “compatible.”
ONAP: Miscellaneous

› Brand new ONAP repos from existing seed code:
  › We'll run a quick initial scan before upload, looking for major red flags
  › After upload to ONAP repo, will become part of ongoing monthly scans

› Record-keeping for Open Source within repos:
  › Recommend using outputs from scanning process, rather than “Project FOSS” pages (manual updates not occurring)
  › To be discussed with the TSC
An Ongoing Process

- License compliance is a matter of ongoing improvement
  - ...like all aspects of collaborative software development
- Areas of focus will change over time as we improve together
- Focusing on key priorities first

- Reach out with any questions!
  - Steve Winslow: swinslow@linuxfoundation.org
  - your in-house legal counsel (for any legal interpretation questions)
Contact Us

The Linux Foundation
1 Letterman Drive
Building D, Suite D4700
San Francisco CA 94129
Phone/Fax: +1 415 7239709
www.linuxfoundation.org

General Inquiries
info@linuxfoundation.org
Membership
membership@linuxfoundation.org
Corporate Training
training@linuxfoundation.org
Event Sponsorship
sponsorships@linuxfoundation.org
Legal Notices

- The Linux Foundation, The Linux Foundation logos, and other marks that may be used herein are owned by The Linux Foundation or its affiliated entities, and are subject to The Linux Foundation’s Trademark Usage Policy at https://www.linuxfoundation.org/trademark-usage, as may be modified from time to time.

- Linux is a registered trademark of Linus Torvalds. Please see the Linux Mark Institute’s trademark usage page at https://lmi.linuxfoundation.org for details regarding use of this trademark.

- Some marks that may be used herein are owned by projects operating as separately incorporated entities managed by The Linux Foundation, and have their own trademarks, policies and usage guidelines.

- TWITTER, TWEET, RETWEET and the Twitter logo are trademarks of Twitter, Inc. or its affiliates.

- Facebook and the “f” logo are trademarks of Facebook or its affiliates.

- LinkedIn, the LinkedIn logo, the IN logo and InMail are registered trademarks or trademarks of LinkedIn Corporation and its affiliates in the United States and/or other countries.

- YouTube and the YouTube icon are trademarks of YouTube or its affiliates.

- All other trademarks are the property of their respective owners. Use of such marks herein does not represent affiliation with or authorization, sponsorship or approval by such owners unless otherwise expressly specified.

- The Linux Foundation is subject to other policies, including without limitation its Privacy Policy at https://www.linuxfoundation.org/privacy and its Antitrust Policy at https://www.linuxfoundation.org/antitrust-policy, each as may be modified from time to time. More information about The Linux Foundation’s policies is available at https://www.linuxfoundation.org.

- Please email legal@linuxfoundation.org with any questions about The Linux Foundation’s policies or the notices set forth on this slide.