JBB

Curation of ORT output –

useful features from the perspective of FOSS license compliance

Dr. Till Jaeger | JBB Rechtsanwälte

ORT Community Days 2024, Berlin

JBB

- FOSS License Compliance
  - Common obligations
  - Particularities of binary distribution
  - Dealing with scan results
- SBOM
  - Legal Provisions (Cyber Resilience Act)
  - Content of an SBOM
- License Scanning and Curation
  - Main licenses and internal licenses
  - Dual licensing
  - (The issue of) Template Texts
  - Different types of copyrightable works
  - License compatibility
  - OSSelot integration

JBB

FOSS License Compliance

JBB

FOSS LICENSE COMPLIANCE: Common Obligations

Include / Retain copyright notices

Include / Retain license text

Provide source code / offer to provide (access to) source code

Mark modifications, including date of modification

Provide NOTICE file

Acknowledge origin

JBB

FOSS LICENSE COMPLIANCE
Particularities of Binary Distribution

- Source Code distribution vs Binary Distribution
  - Not human readable
  - License texts & copyright notices get lost / cannot be perceived
- Many licenses have special provisions for binary distribution
- Solution: prepare “Compulsory Statement Document”/”Disclaimer”/”FOSS Documentation”/”Disclosure Document” etc.
  - include all license texts
  - include all copyright notices and acknowledgments
  - include license election choices
  - include written offer for source code
  - include disclaimer

JBB

FOSS LICENSE COMPLIANCE: Common Obligations

E.g. Apache-2.0

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not

JBB

FOSS LICENSE COMPLIANCE: Common Obligations

E.g. Apache-2.0

- ☑ **USE CASE** Source code delivery
  - **YOU MUST** *Provide* **License text** Ref.
  - ☑ **IF** Software modification Ref.
    - **YOU MUST** *Provide* **Modification notice** Ref.
    - **YOU MUST** *Forward* **Copyright notices** Ref.
    - **YOU MUST** *Forward* **Patent notices** Ref.
    - **YOU MUST** *Forward* **Trademark notices** Ref.
    - **YOU MUST** *Forward* **Attribution notices** Ref.
    - ☑ **IF** Work *Includes* **File** "NOTICE" Ref.
      - **YOU MUST** *Delete* **Irrelevant parts** Ref.
      - ☑ **EITHER** Ref.
        - **YOU MUST** *Provide* **File** "NOTICE" Ref.
        - ☑ **OR**
        - **YOU MUST** *Provide* **File** "NOTICE" In **Source code** Ref.
        - ☑ **OR**
        - **YOU MUST** *Provide* **File** "NOTICE" In **Documentation** Ref.
        - ☑ **OR**
        - **YOU MUST** *Display* **File** "NOTICE" Ref.
  - ☑ **IF** Service offerings Ref.
    - **YOU MUST** *Indemnify* **Other contributors** Ref.

4. Redistribution. You may reproduce and distribu
   Work or Derivative Works thereof in any mediur
   modifications, and in Source or Object form, p
   meet the following conditions:

   (a) You must give any other recipients of the
       Derivative Works a copy of this License; a

   (b) You must cause any modified files to carry
       stating that You changed the files; and

   (c) You must retain, in the Source form of any
       that You distribute, all copyright, patent
       attribution notices from the Source form o
       excluding those notices that do not pertai
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file
       distribution, then any Derivative Works th
       include a readable copy of the attribution
       within such NOTICE file, excluding those n
       pertain to any part of the Derivative Work

JBB

FOSS LICENSE COMPLIANCE
Dealing with scan results

- All license texts to be extracted
  - Correct detection of licenses
  - Correction of false positives
- Extraction of NOTICE files on Apache-2.0 projects
- All Copyright notices to be extracted
  - Authors ≠ Copyright owners
  - Mapping copyright notices and licenses

JBB

FOSS LICENSE COMPLIANCE
Dealing with scan results

- Obligations in FOSS licenses are triggered by “distribution”
- Which code is distributed?
- Filtering files helps to reduce workload and applicable licenses

JBB

SBOM

JBB

Legal Provisions for SBOM: Cyber Resilience Act (CRA)

- EU regulation – addresses cyber security / vulnerabilities of software
- Measures include requirement of Software Bill of Materials (SBOM)
  - transparency
  - accountability
- CRA does not define contents of SBOM
  - Name and version of the software component
  - Link to download ressource
  - License in SPDX format
  - What else?

JBB

Legal Provisions for SBOM: Cyber Resilience Act (CRA)

- Federal Office for Information Security (BSI) – technical directive published

- Technische Richtlinie TR-03183
  - Dependencies
  - Hash
  - Information about producer of the SBOM (URI, i.e. email, time stamp)
  - Name of producer -> name and URI of FOSS project?

JBB

License scanning and curation

JBB

License scanning and curation

- Main license and “internal” licenses
  - The main license is usually in a "COPYING" or "LICENSE" file at the top level of a source tree
  - Individual folders or even single files may have code from other projects under the others project's license
  - Such internal licenses are not void but apply next to the main license
  - SPDX: Apache-2.0 AND MIT AND BSD-3-Clause
  - Curation: deleting false positives and licenses which do not apply
  - Curation: helpful to have easy access to the relevant source code for control

JBB

License scanning and curation

- Dual Licensing
  - Some files or even components provide for two or more licenses among which licensee can elect one
  - SPDX: Apache-2.0 OR UPL-1.0
  - Choice may be important for license compatibility
  - Curation needed to elect one license
  - Control of concrete text

Code | Blame | 85 lines (64 loc) · 12.9 KB

```
1  Copyright (c) 2016, 2020, Oracle and/or its affiliates.  All rights reserved.
2
3  This software is dual-licensed to you under the Universal Permissive License (UPL) 1.0 as shown at https://oss.oracle.com/licenses/upl
4  or Apache License 2.0 as shown at http://www.apache.org/licenses/LICENSE-2.0. You may choose either license.
5
6
```

JBB

License scanning and curation

- Template licenses and individual licenses
  - The Apache-2.0 looks always the same (but be aware of "Frankenstein licenses“)
  - BSD-3-Clause licenses look mostly different
  - Curation: individual text to be added

Copyright (c) <year> <owner>.

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 copyright holder nor the names of its contributors may* be used to endorse or promote products derived from this *software* without specific prior written permission. e.g. "Google, Inc.

THIS *SOFTWARE* IS PROVIDED *BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS* "AS IS" AND ANY *EXPRESS* OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL *THE COPYRIGHT HOLDER OR CONTRIBUTORS* BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS *SOFTWARE*, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JBB

License scanning and curation

- Source code packages may contain different copyrightable works
  - Computer programs ("functional code")
  - Fonts (may be protected by design law and/or as computer programs)
  - Icons (e.g. .png, .jpg files)
  - Logos (may be protected as trademarks)
  - Documentation (e.g. text files)
  - Specifications (may have specific licenses which are related to the implementation of the standard and/or sample code)
  - Curation: what is really distributed? Knowing file type and corresponding license
  - Curation: filter out works that are not distributed

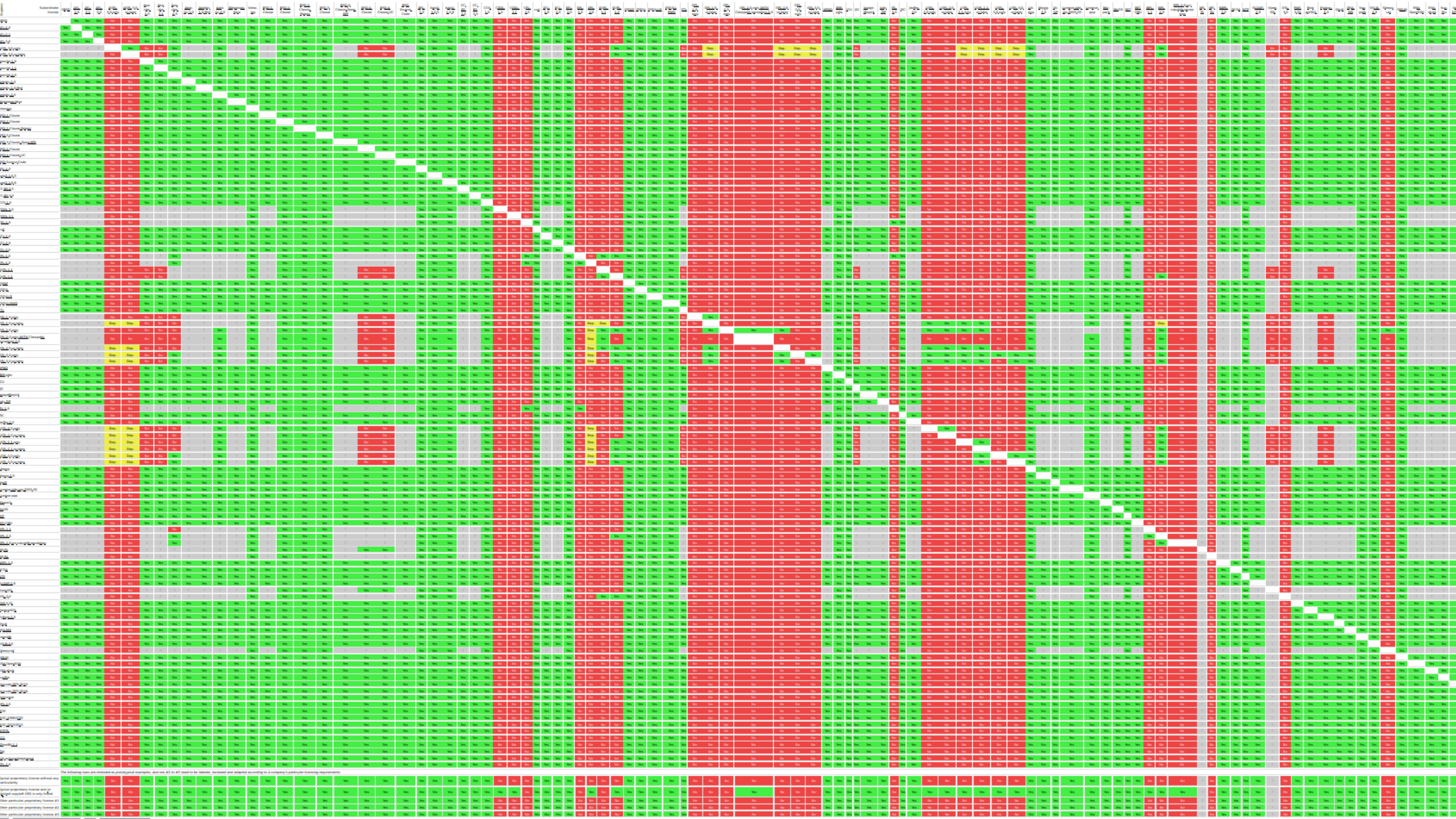
JBB

License scanning and curation

- Sourcecode files may refer to URLs
  - URL still available?
  - Does the URL contain the license text or is further research necessary?
  - Typical example: Unicode Terms of Use

```
# EmojiSources-12.0.0.txt
# Date: 2018-08-03, 00:00:00 GMT [MS, KW]
# © 2018 Unicode®, Inc.
# For terms of use, see http://www.unicode.org/terms_of_use.html
#
# Unicode Character Database
# For documentation, see http://www.unicode.org/reports/tr44/
#
```

Source: https://www.unicode.org/Public/12.0.0/ucd/EmojiSources.txt



JBB

License scanning and curation

- License compatibility
  - Licenses within one component
  - Which component is linked to which other components -> dependency tree helpful
  - Dual licensing or "any later version" licensing – e.g. MPL-1.1 is not compatible with GPL-2.0 but MPL-2.0 is -> documentation of relicense or dual license options
  - Automated compatibility check? -> OSADL compatibility matrix (https://www.osadl.org/html/CompatMatrix-noexpl.html) but: still work to do

JBB

License scanning and curation

- Integrating curation data
  - OSSelot – the open source curation database
  - Contains SPDX-files with curated data of components (currently 337 packages)
  - https://github.com/Open-Source-Compliance/package-analysis/
  - License: CC0-1.0
  - Integration in scan tools would be helpful (either trusting or control)

Any Questions?

Dr. Till Jaeger – jaeger@jbb.de

JBB

JBB Rechtsanwälte
Jaschinski Biere Brexl Partnerschaft mbB

Christinenstraße 18/19
10119 Berlin

Tel. +49 30 443 765 0

Web www.jbb.de

jbb.de