The Linux Foundation
License Scanning and Analysis Support Program for LF projects

Support plan summary for 2021: LF AI and Data

Support to be provided by: Steve Winslow <swinslow@linuxfoundation.org>

For the projects described below, the following actions will be performed:

1. Run recurring scans, on the schedule described below, of the project's codebases using Fossology
2. Analyze and clear licenses, notices and copyright statements contained in the project codebases
3. Publish SPDX documents with the license conclusions and copyright statements at https://github.com/lfscanning (or a similar public location), for broader community use in their own compliance processes
4. Produce summary reports for project leads / maintainers, with limited public visibility (or optionally public at the project's discretion) with the following:
    a. catalog and summary of licenses detected, categorized and identifying corresponding files
    b. description of key findings, particularly relating to incompatibility with project licenses and project IP policies
    c. recommendations for remediation where necessary
    d. guidance for best practices to improve project licensing notices and add statements to files without existing notices
5. Correspond with developers to address questions about findings, where possible without providing legal advice (see "Notes" section below)
6. **For Acumos**: On a recurring basis, review results of dependency scans using the instance of Sonatype Nexus IQ that is managed by LF IT; clear scanning results and research potentially concerning findings as appropriate; and flag key issues to the project leads / maintainers
7. Upon request from the project, up to approximately two times per year (such as prior to significant releases), assist with formal IP policy approvals under the project's charter:
    a. document the license scan findings as "license exceptions" for approval by the Governing Board or technical leadership committee, as applicable
    b. prepare summary slide deck describing the requested exceptions
    c. present to project Legal Committee or similar leadership body to describe the requested exceptions and facilitate approvals under the charter

Stretch goals: will perform where feasible, subject to available resources and time:

1. Run "red flag" pre-intake scans, for net new projects:
    a. Run Fossology scan of incoming codebase, prior to import into a project-controlled repository
    b. Identify any "red flag" or "high priority" issues that would be likely to present a significant problem for license compatibility
    c. Correspond with developers regarding these issues where remediation is recommended
2. Parallel to Fossology scans, also run dependency scans using WhiteSource:
    a. review and clear scanning results, researching potentially concerning findings as appropriate;
    b. flag key issues to the project leads / maintainers;
    c. work towards providing standardized reports of all dependencies; and
    d. work towards providing vulnerability findings as part of results.

    Note that WhiteSource has recently been incorporated into the license scanning workflow, so some of this functionality will be subject to continued development of the scanning workflow automation.

Notes:

- The Linux Foundation is not able to provide legal advice to project community members. The support program is focused on providing transparency about identified project licenses, and where possible describing general community understandings of license requirements. However, questions about e.g. whether a license is legally okay to use must be directed to the contributor's own legal counsel and/or a project's Legal Committee.
- The support program utilizes various automated tools supplemented by manual reviews. However, like any other scanning tool or process, the LF cannot guarantee the completeness or accuracy of the license scanning results, and does not guarantee that all possible license issues in a scanned codebase will be identified.

Dependencies on other LF and project teams:

- Will periodically need assistance from project manager or similar project staff support, to coordinate on preferred methods for communications with appropriate project community members.
- May periodically need LF IT assistance for configuring certain types of scans, for those that are dependent of CI/CD processes that are managed by LF IT
    - **Acumos**: LF IT manages configuration for Sonatype Nexus IQ tooling

Covered projects and schedule of scans:

<u>**Cycle 1**</u>: **January, April, July, October**:

- Acumos
- Adlik
- Delta
- FEAST
- ForestFlow
- ONNX
- Pyro
- SOAJS

<u>**Cycle 2**</u>: **February, May, August, November**:

- ART (Adversarial Robustness Toolbox)
- AI Explainability 360
- AI Fairness 360
- Angel
- Milvus
- OpenDS4All
- Sparklyr

<u>**Cycle 3**</u>: **March, June, September, December**:

- Amundsen
- EDL
- Egeria
- Horovod
- Ludwig
- Marquez
- NNStreamer

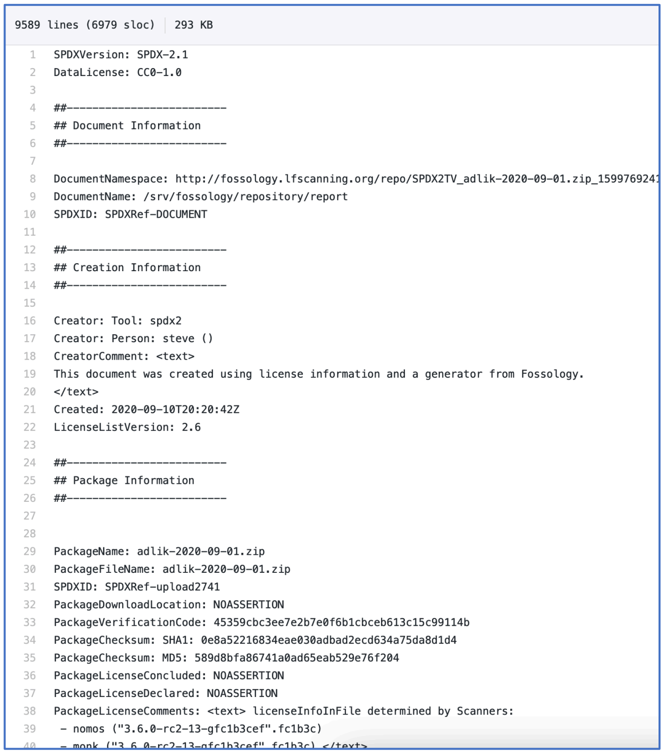
Anticipate up to approximately 10 new small-to-medium projects to come in during 2021. Will perform pre-intake scans and allocate to cycles based on project sizing.

Exhibits:

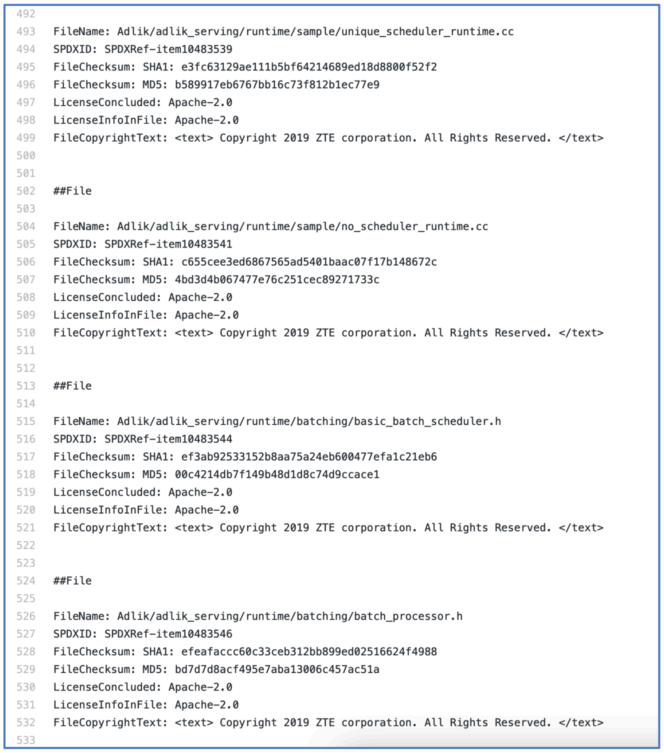
1. Screenshots from example SPDX document
2. Screenshots from example scan report for developers
3. Screenshots from example board deck

Exhibit 1

Screenshots from example SPDX document



```
9589 lines (6979 sloc) | 293 KB

SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0

##-------------------------
## Document Information
##-------------------------

DocumentNamespace: http://fossology.lfscanning.org/repo/SPDX2TV_adlik-2020-09-01.zip_1599769241
DocumentName: /srv/fossology/repository/report
SPDXID: SPDXRef-DOCUMENT

##-------------------------
## Creation Information
##-------------------------

Creator: Tool: spdx2
Creator: Person: steve ()
CreatorComment: <text>
This document was created using license information and a generator from Fossology.
</text>
Created: 2020-09-10T20:20:42Z
LicenseListVersion: 2.6

##-------------------------
## Package Information
##-------------------------


PackageName: adlik-2020-09-01.zip
PackageFileName: adlik-2020-09-01.zip
SPDXID: SPDXRef-upload2741
PackageDownloadLocation: NOASSERTION
PackageVerificationCode: 45359cbc3ee7e2b7e0f6b1cbceb613c15c99114b
PackageChecksum: SHA1: 0e8a52216834eae030adbad2ecd634a75da8d1d4
PackageChecksum: MD5: 589d8bfa86741a0ad65eab529e76f204
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageLicenseComments: <text> licenseInfoInFile determined by Scanners:
 - nomos ("3.6.0-rc2-13-gfc1b3cef".fc1b3c)
 - monk ("3.6.0-rc2-13-gfc1b3cef".fc1b3c) </text>
```

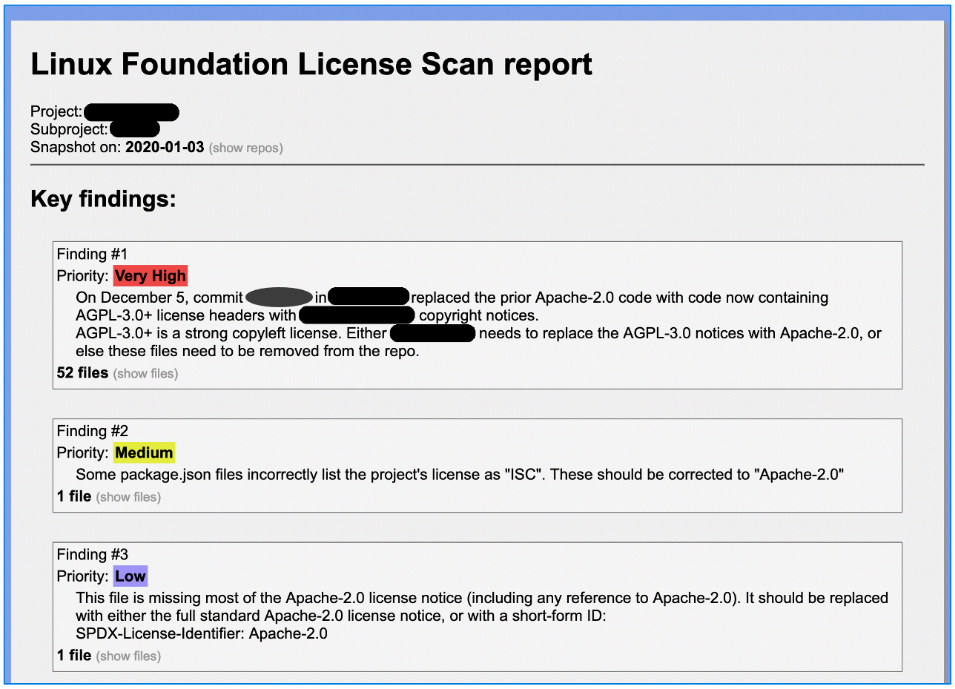


```

FileName: Adlik/adlik_serving/runtime/sample/unique_scheduler_runtime.cc
SPDXID: SPDXRef-item10483539
FileChecksum: SHA1: e3fc63129ae111b5bf64214689ed18d8800f52f2
FileChecksum: MD5: b589917eb6767bb16c73f812b1ec77e9
LicenseConcluded: Apache-2.0
LicenseInfoInFile: Apache-2.0
FileCopyrightText: <text> Copyright 2019 ZTE corporation. All Rights Reserved. </text>


##File

FileName: Adlik/adlik_serving/runtime/sample/no_scheduler_runtime.cc
SPDXID: SPDXRef-item10483541
FileChecksum: SHA1: c655cee3ed6867565ad5401baac07f17b148672c
FileChecksum: MD5: 4bd3d4b067477e76c251cec89271733c
LicenseConcluded: Apache-2.0
LicenseInfoInFile: Apache-2.0
FileCopyrightText: <text> Copyright 2019 ZTE corporation. All Rights Reserved. </text>


##File

FileName: Adlik/adlik_serving/runtime/batching/basic_batch_scheduler.h
SPDXID: SPDXRef-item10483544
FileChecksum: SHA1: ef3ab92533152b8aa75a24eb600477efa1c21eb6
FileChecksum: MD5: 00c4214db7f149b48d1d8c74d9ccace1
LicenseConcluded: Apache-2.0
LicenseInfoInFile: Apache-2.0
FileCopyrightText: <text> Copyright 2019 ZTE corporation. All Rights Reserved. </text>


##File

FileName: Adlik/adlik_serving/runtime/batching/batch_processor.h
SPDXID: SPDXRef-item10483546
FileChecksum: SHA1: efeafaccc60c33ceb312bb899ed02516624f4988
FileChecksum: MD5: bd7d7d8acf495e7aba13006c457ac51a
LicenseConcluded: Apache-2.0
LicenseInfoInFile: Apache-2.0
FileCopyrightText: <text> Copyright 2019 ZTE corporation. All Rights Reserved. </text>

```

Exhibit 2

Screenshots from example scan report for developers

Key findings and recommended actions:



Linux Foundation License Scan report

Project: [redacted]
Subproject: [redacted]
Snapshot on: **2020-01-03** (show repos)

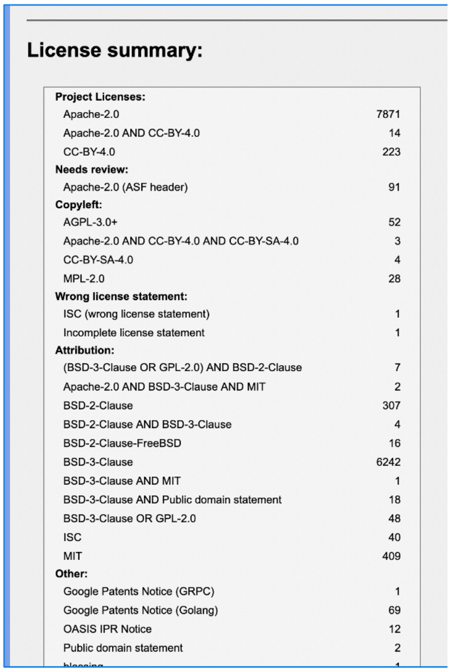
Key findings:

Finding #1
Priority: **Very High**
On December 5, commit [redacted] in [redacted] replaced the prior Apache-2.0 code with code now containing AGPL-3.0+ license headers with [redacted] copyright notices.
AGPL-3.0+ is a strong copyleft license. Either [redacted] needs to replace the AGPL-3.0 notices with Apache-2.0, or else these files need to be removed from the repo.
52 files (show files)

Finding #2
Priority: **Medium**
Some package.json files incorrectly list the project's license as "ISC". These should be corrected to "Apache-2.0"
1 file (show files)

Finding #3
Priority: **Low**
This file is missing most of the Apache-2.0 license notice (including any reference to Apache-2.0). It should be replaced with either the full standard Apache-2.0 license notice, or with a short-form ID:
SPDX-License-Identifier: Apache-2.0
1 file (show files)

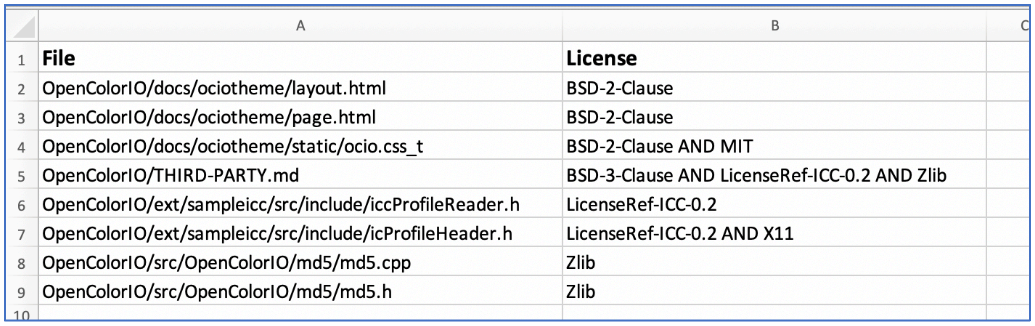
Summary of findings:



License summary:

Project Licenses:	
Apache-2.0	7871
Apache-2.0 AND CC-BY-4.0	14
CC-BY-4.0	223
Needs review:	
Apache-2.0 (ASF header)	91
Copyleft:	
AGPL-3.0+	52
Apache-2.0 AND CC-BY-4.0 AND CC-BY-SA-4.0	3
CC-BY-SA-4.0	4
MPL-2.0	28
Wrong license statement:	
ISC (wrong license statement)	1
Incomplete license statement	1
Attribution:	
(BSD-3-Clause OR GPL-2.0) AND BSD-2-Clause	7
Apache-2.0 AND BSD-3-Clause AND MIT	2
BSD-2-Clause	307
BSD-2-Clause AND BSD-3-Clause	4
BSD-2-Clause-FreeBSD	16
BSD-3-Clause	6242
BSD-3-Clause AND MIT	1
BSD-3-Clause AND Public domain statement	18
BSD-3-Clause OR GPL-2.0	48
ISC	40
MIT	409
Other:	
Google Patents Notice (GRPC)	1
Google Patents Notice (Golang)	69
OASIS IPR Notice	12
Public domain statement	2
blessing	1

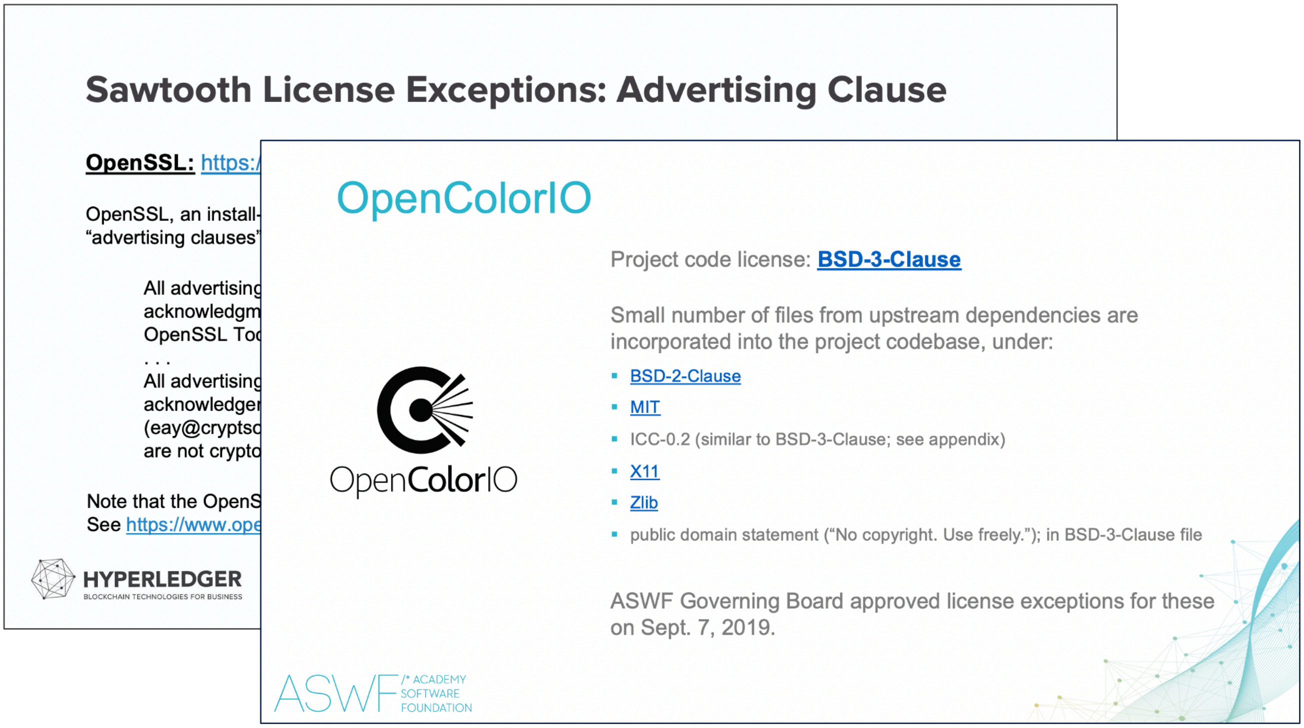
Spreadsheet with detailed findings:



File	License
OpenColorIO/docs/ociotheme/layout.html	BSD-2-Clause
OpenColorIO/docs/ociotheme/page.html	BSD-2-Clause
OpenColorIO/docs/ociotheme/static/ocio.css_t	BSD-2-Clause AND MIT
OpenColorIO/THIRD-PARTY.md	BSD-3-Clause AND LicenseRef-ICC-0.2 AND Zlib
OpenColorIO/ext/sampleicc/src/include/iccProfileReader.h	LicenseRef-ICC-0.2
OpenColorIO/ext/sampleicc/src/include/icProfileHeader.h	LicenseRef-ICC-0.2 AND X11
OpenColorIO/src/OpenColorIO/md5/md5.cpp	Zlib
OpenColorIO/src/OpenColorIO/md5/md5.h	Zlib

Exhibit 3

Screenshots from example board deck



Sawtooth License Exceptions: Advertising Clause

OpenSSL: https:/

OpenSSL, an install-
"advertising clauses"

All advertising
acknowledgm
OpenSSL Too
. . .
All advertising
acknowledger
(eay@cryptso
are not crypto

Note that the OpenS
See https://www.ope

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

OpenColorIO

Project code license: **BSD-3-Clause**

Small number of files from upstream dependencies are incorporated into the project codebase, under:

- BSD-2-Clause
- MIT
- ICC-0.2 (similar to BSD-3-Clause; see appendix)
- X11
- Zlib
- public domain statement ("No copyright. Use freely."); in BSD-3-Clause file

ASWF Governing Board approved license exceptions for these on Sept. 7, 2019.