SBOM journey for an Open Source Project

- Apache NuttX RTOS -

Apache NuttX PMC Chair:

Alin Jerpelea

WHO AM I

- Open Source advocate
- Member of several communities
- Apache NuttX RTOS chair
- Open Source Software Architect in Sony OSPO

https://www.linkedin.com/in/ajerpelea/

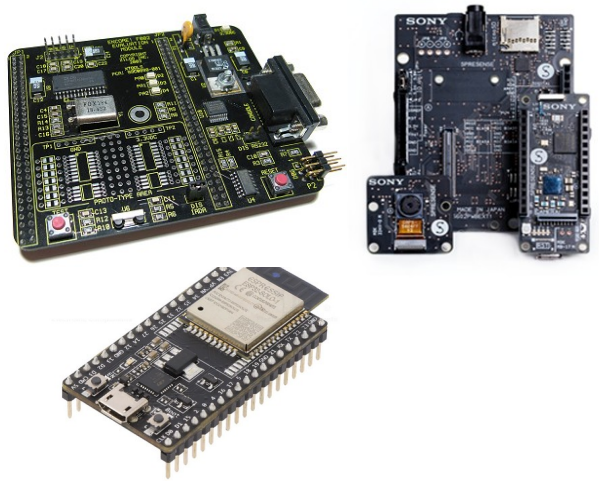
DISCLAIMER

The facts expressed in this presentation are my own and not necessarily represent my employer strategy or opinions

NuttX RTOS

Apache NuttX (RTOS)

- **small footprint** open-source real-time operating system (RTOS)
- technical standards **compliance**
- **scalable** from 8-bit to 64-bit micro-controller environments
- **available** for 400+ boards
- **documentation**
- **welcoming** community
- **wide use** in commercial products



History

2007 released under the permissive BSD license by Gregory Nutt.
2019 donated to Apache Software Foundation.
2022 graduated to a top-level project under Apache License
2024 Governance - Project Management Committee 24 members

Products using NuttX

- Digital audio recorders
- Bluetooth headphones
- Drones & Robots
- Protection Equipment
- RFID Readers
- IoT devices
- Fiscal printers
- Fitness trackers

Forks

- TizenRT,
- Google ARA





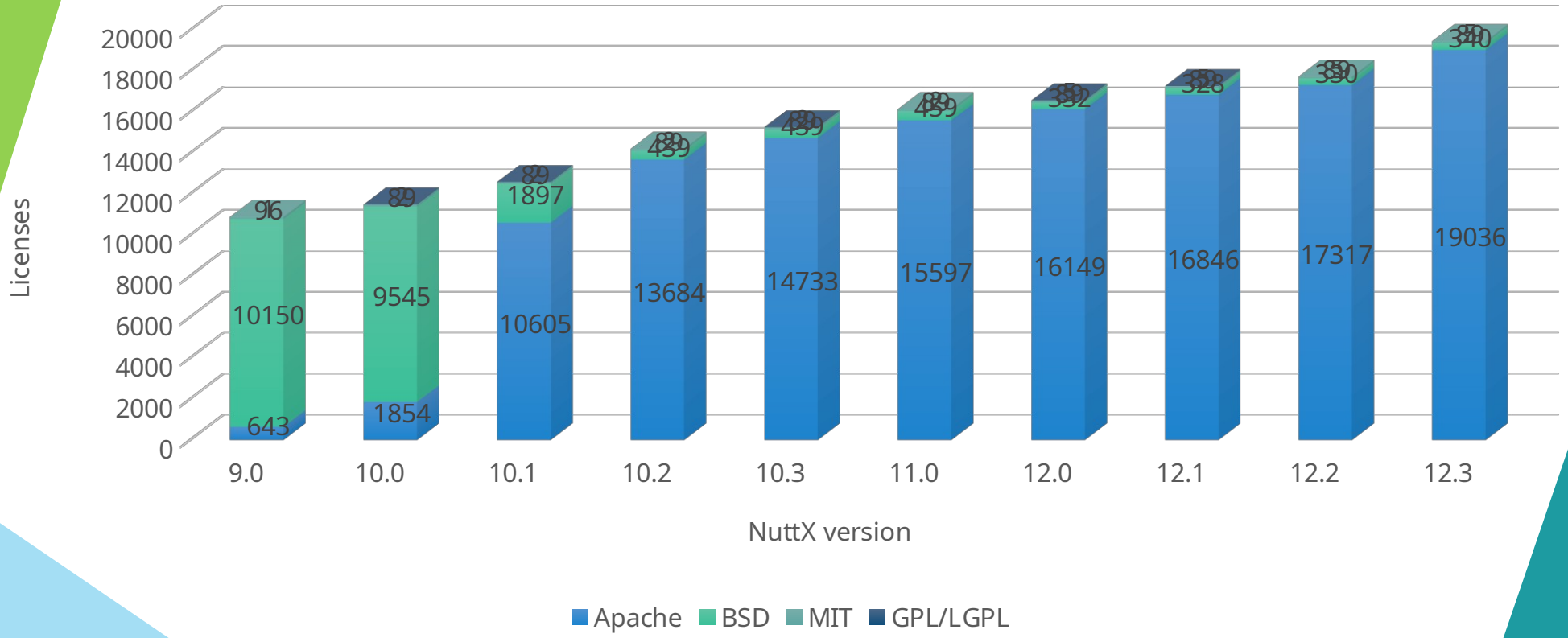

Companies using NuttX

- Sony
- Xiaomi
- Samsung
- Fitbit
- Motorola Mobility
- Haltian
- 3DRobotics
- Daruma
- VergeAero
- Many others

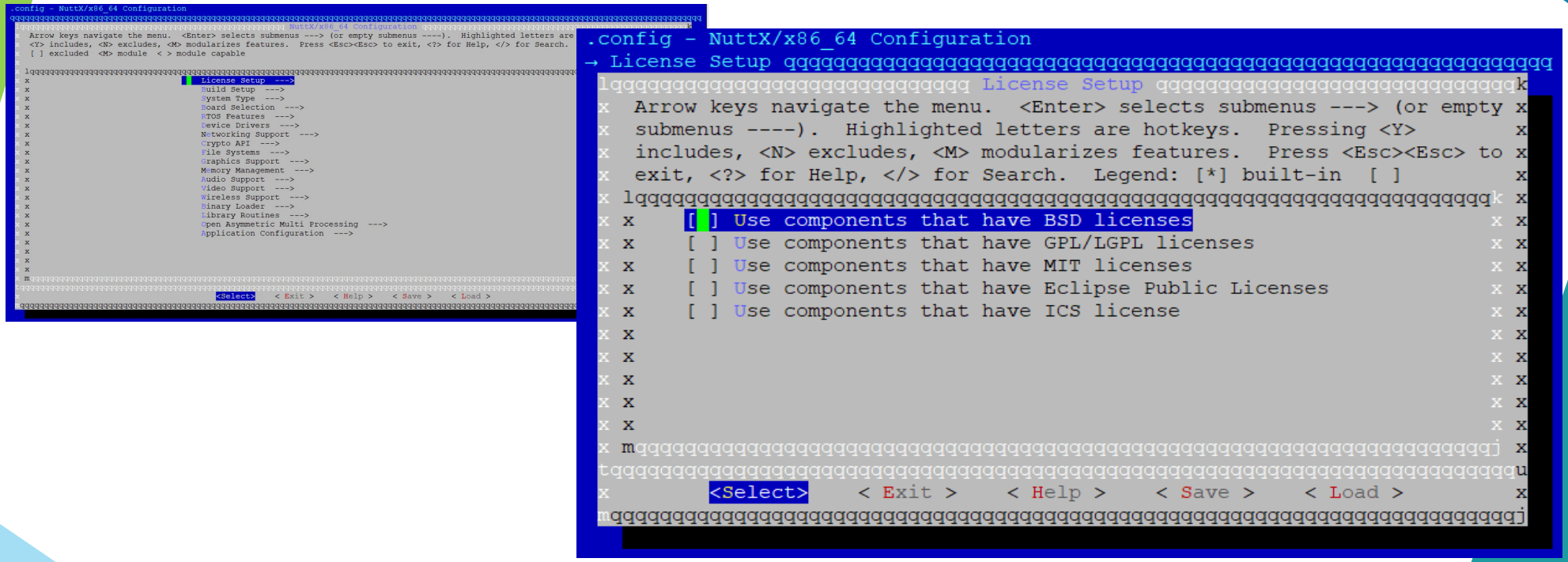
Apache NuttX Powers World's Smallest Lunar Robot in Japan's Historic Autonomous Lunar Exploration Mission

In an historic milestone in lunar exploration, Japan landed Lunar Excursion Vehicle 2 (LEV-2), t**he world's smallest lunar robot**, capturing historic images from the moon's surface with integrated **NuttX-powered technology in its Sony Spresense board.** The collaborative effort involved the **National Research and Development Agency Japan Aerospace Exploration Agency (JAXA), Takara Tomy Corporation, Doshisha University, and the incorporation of NuttX in the SPRESENSE TM board by Sony Group Corporation**, showcasing the robust real-time capabilities essential for the success of the mission.
As **Apache NuttX makes its mark on the moon**, this cosmic success not only marks a huge technological achievement but also shows the potential of open-source innovation in space. Ongoing data analysis, including driving logs, holds the promise of revealing further insights, with results anticipated for future publication.

License distribution



License selection



Exclude the unwanted licenses during setup

SBOM?

A software Bill of Materials (SBOM) is **a list** of all components present in a codebase, including **license**, **version**, and **metadata** which allows security teams to quickly identify license or security risks.

SBOM TYPES

Design - of intended design of included components (some of which may not exist) for a new software artifact.

Source - created directly from the development environment, source files, and included dependencies used to build a product artifact.

Build - generated through the analysis of artifacts during Build

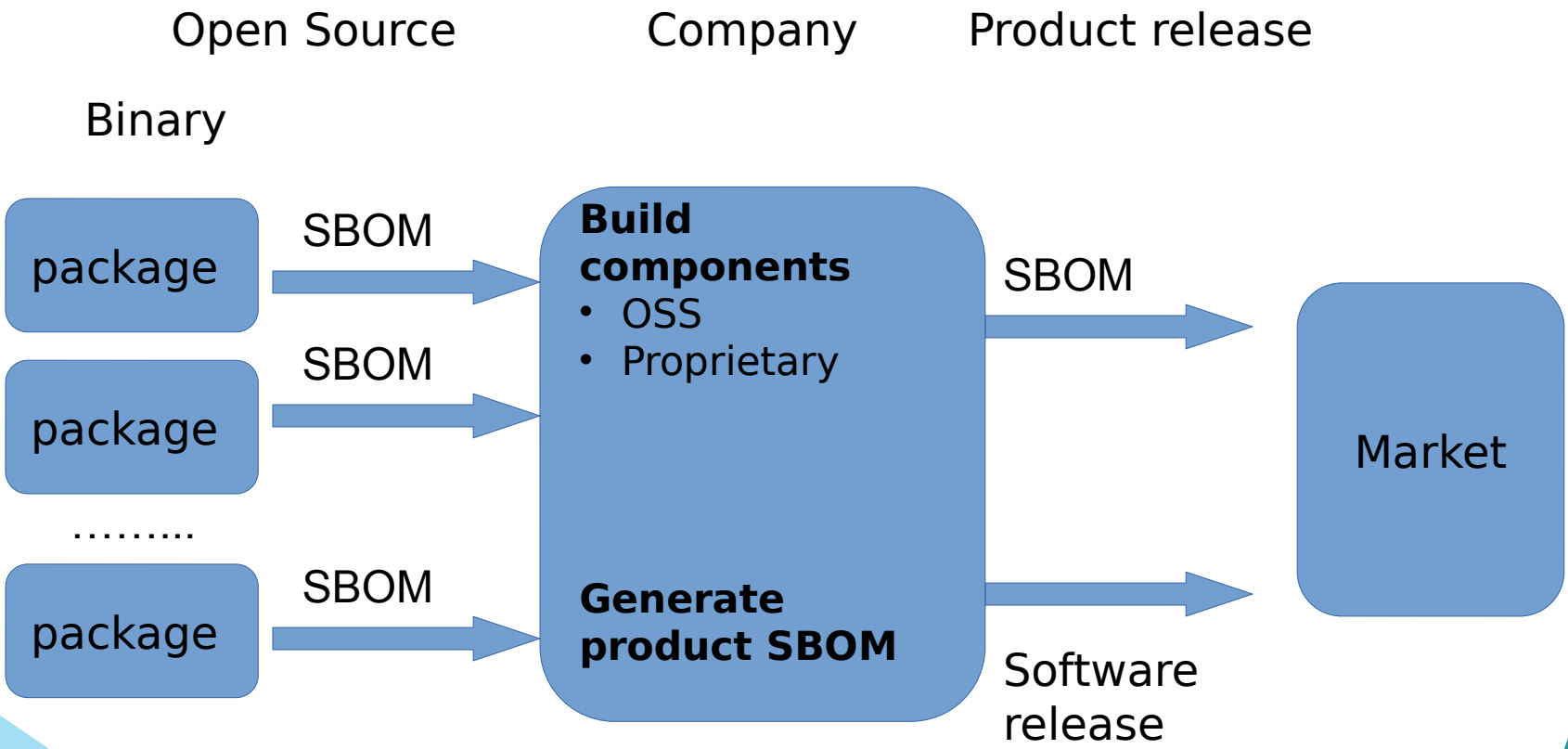
Analyzed - generated through analysis of artifacts after its build.

Deployed - provides an inventory of software that is present on a system.

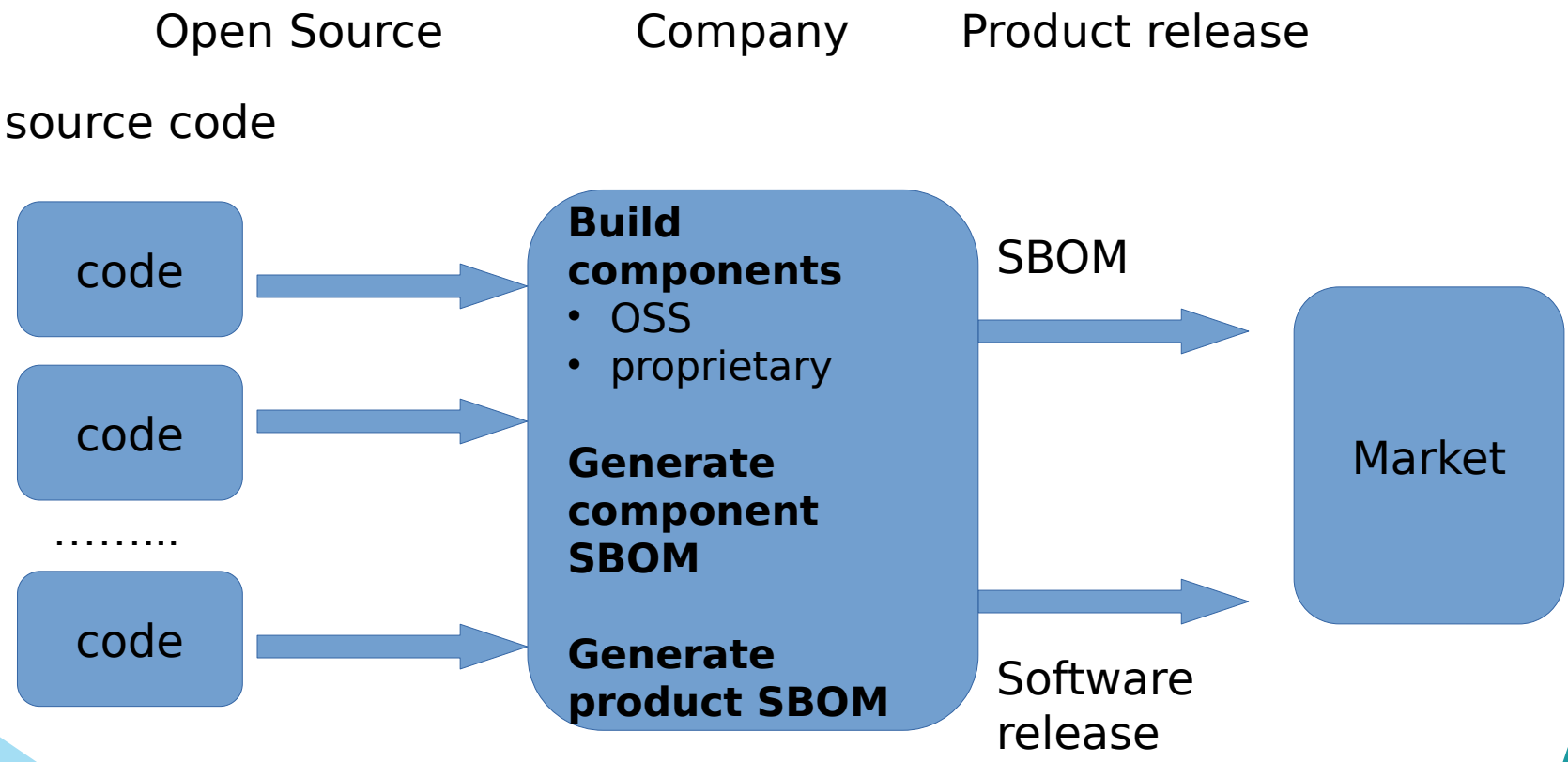
Runtime - generated through instrumenting the system running the software, to capture only components present in the system, as well as external call-outs or dynamically loaded components.

https://www.cisa.gov/resources-tools/resources/types-software-bill-materials-sbom

Open Source in a product



Open Source in a product



Software Package Data Exchange - open standard for communicating SBOM, including:

- components
- licenses
- copyrights
- security references

https://spdx.dev

Version 2.x

(https://spdx.github.io/spdx-spec/v2.3/)

defines an SBOM document, which contains SPDX metadata about software. The document itself can be expressed in multiple formats, including JSON, YAML, RDF/XML, tag–value, and spreadsheet

Version 3.0

(https://spdx.github.io/spdx-spec/v3.0/)

SPDX 3.0 allows users to communicate information at a much more granular level without having to package it as “envelope” data.

https://en.wikipedia.org/wiki/Software_Package_Data_Exchange

This page lists Open Source tools that support SPDX.

- Augur
- bom
- Cavil
- CycloneDX CLI
- distro2sbom
- FOSSLight
- FOSSology
- GitHub Self-Service SBOMs
- GUAC (Graph for Understanding Artifact Composition)
- in-toto
- lib4sbom
- Nix / Nixpkgs
- ntia-conformance-checker
- Open Source Software Review Toolkit (ORT)
- Parlay
- Protobom
- REUSE
- sbom-manager
- sbomaudit
- sbomdiff
- sbommerge
- sbomqs
- sbomtrend
- sbom-tool
- ScanCode Toolkit
- SCANOSS
- SPDX Golang Libraries
- SPDX Java Libraries and Tools
- SPDX JavaScript Libraries
- SPDX Maven Plugin
- SPDX Online Tools
- SPDX Python Libraries
- spdx-sbom-generator
- SW360
- Syft
- Tern
- Yocto Project / OpenEmbedded

?

https://spdx.dev/tools/open-source-tools/

RTOS landscape

RTOS	License	Format	Governance	Activity(30 days)	SBOM
Azure-RTOS	Microsoft Software License	Plain text	Microsoft	Archived	NO
Contiki-NG	BSD-3-Clause license	Plain text	Community	Low	NO
FreeRTOS	MIT	SPDX	Community	Low	**BUILD**
mbed OS	Apache 2.0	SPDX	ARM	Low	NO
myNewt	Apache 2.0	Plain text	ASF	Low	NO
NuttX	Apache 2.0	SPDX	ASF	High	**BUILD**(WIP)
RIOT	LGPL-2.1	Plain text	Community	Moderate	NO
RT-Thread	Apache 2.0	SPDX	Community	Moderate	NO
CMSIS-5	Apache 2.0	SPDX	ARM	None	NO
Tyzen RT	Apache 2.0	Plain text	Samsung	Moderate	NO
Zephyr	Apache 2.0	SPDX	Linux Foundation	High	**BUILD**

Inspired by Kate Stewart

SPDX Identifiers

SPDX migration

Perfect case

```
* drivers/input/uinput.c
*
* SPDX-License-Identifier: Apache-2.0
*
* Licensed to the Apache Software Foundation (ASF) under one or more
* contributor license agreements.  See the NOTICE file distributed with
* this work for additional information regarding copyright ownership.  The
* ASF licenses this file to you under the Apache License, Version 2.0 (the
* "License"); you may not use this file except in compliance with the
* License.  You may obtain a copy of the License at
*
*   http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS, WITHOUT
* WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.  See the
* License for the specific language governing permissions and limitations
* under the License.
*
```

SPDX migration

old code

```
* crypto/xform.c
*
* SPDX-License-Identifier: 0BSD
* SPDX-FileCopyrightText: 1995, 1996, 1997, 1998, 1999 John Ioannidis
* SPDX-FileCopyrightText: 1995, 1996, 1997, 1998, 1999 Angelos D. Keromytis
* SPDX-FileCopyrightText: 1995, 1996, 1997, 1998, 1999 Niels Provos.
* SPDX-FileCopyrightText: 2001 Angelos D. Keromytis.
* SPDX-FileCopyrightText: 2008 Damien Miller
* SPDX-FileCopyrightText: 2010, 2015 Mike Belopuhov
* SPDX-FileContributor: John Ioannidis (ji@tla.org)
* SPDX-FileContributor: Angelos D. Keromytis (kermit@csd.uch.gr)
* SPDX-FileContributor: Niels Provos (provos@physnet.uni-hamburg.de)
* SPDX-FileContributor: Damien Miller (djm@mindrot.org)
* SPDX-FileContributor: Mike Belopuhov (mikeb@openbsd.org)
*
* The authors of this code are John Ioannidis (ji@tla.org),
* Angelos D. Keromytis (kermit@csd.uch.gr),
* Niels Provos (provos@physnet.uni-hamburg.de),
* Damien Miller (djm@mindrot.org) and
* Mike Belopuhov (mikeb@openbsd.org).
*
* This code was written by John Ioannidis for BSD/OS in Athens, Greece,
* in November 1995.
*
* Ported to OpenBSD and NetBSD, with additional transforms,
* in December 1996,
* by Angelos D. Keromytis.
*
* Additional transforms and features in 1997 and 1998 by
* Angelos D. Keromytis and Niels Provos.
*
* Additional features in 1999 by Angelos D. Keromytis.
*
* AES XTS implementation in 2008 by Damien Miller
*
* AES-GCM-16 and Chacha20-Poly1305 AEAD modes by Mike Belopuhov.
*
```

SPDX migration

multiple licenses

```
* include/crypto/cryptodev.h
*
* SPDX-License-Identifier: OAR AND BSD-2 Clause
* SPDX-FileCopyrightText: 2000 Angelos D. Keromytis
* SPDX-FileCopyrightText: 2001 Theo de Raadt
* SPDX-FileContributor: Angelos D. Keromytis (angelos@cis.upenn.edu)
*
* The author of this code is Angelos D. Keromytis (angelos@cis.upenn.edu)
*
* This code was written by Angelos D. Keromytis in Athens, Greece, in
* February 2000. Network Security Technologies Inc. (NSTI) kindly
* supported the development of this code.
*
* Copyright (c) 2000 Angelos D. Keromytis
*
* Permission to use, copy, and modify this software with or without fee
* is hereby granted, provided that this entire notice is included in
* all source code copies of any software which is or includes a copy or
* modification of this software.
*
* THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR
* IMPLIED WARRANTY. IN PARTICULAR, NONE OF THE AUTHORS MAKES ANY
* REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE
* MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR
* PURPOSE.
*
* Copyright (c) 2001 Theo de Raadt
*
* 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.
*
```

SPDX migration

Less known licenses

```
/*
 * include/crypto/cryptosoft.h
 *
 * SPDX-License-Identifier: OAR
 * SPDX-FileCopyrightText: 2000 Angelos D. Keromytis
 * SPDX-FileContributor: Angelos D. Keromytis (angelos@cis.upenn.edu)
 *
 * The author of this code is Angelos D. Keromytis (angelos@cis.upenn.edu)
 *
 * This code was written by Angelos D. Keromytis in Athens, Greece, in
 * February 2000. Network Security Technologies Inc. (NSTI) kindly
 * supported the development of this code.
 *
 * Copyright (c) 2000 Angelos D. Keromytis
 *
 * Permission to use, copy, and modify this software with or without fee
 * is hereby granted, provided that this entire notice is included in
 * all source code copies of any software which is or includes a copy or
 * modification of this software.
 *
 * THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR
 * IMPLIED WARRANTY. IN PARTICULAR, NONE OF THE AUTHORS MAKES ANY
 * REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE
 * MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR
 * PURPOSE.
 *
```

SPDX migration

Tools can give false positives
Community can help!

```
    crypto/xform.c: migrate to SPDX identifier

    Most tools used for compliance and SBOM generation use SPDX identifiers
    This change brings us a step closer to an easy SBOM generation.

    NOTE
    The code was reported as GPL by FOSS ID
    and Xiaomi scanned the file xform.c with Black Duck Security and it showed
    that the license was BSD-3-Clause and no risk was reported.

    Since there is no clause on the license it was concluded as 0BSD

    Refference
    https://github.com/apache/nuttx/pull/15252

    Signed-off-by: Alin Jerpelea <alin.jerpelea@sony.com>

diff --git a/crypto/xform.c b/crypto/xform.c
index 3802112b2f..5e4c28445e 100644
--- a/crypto/xform.c
+++ b/crypto/xform.c
@@ -1,6 +1,18 @@
 /*****************************************************************************
  * crypto/xform.c
- * $OpenBSD: xform.c,v 1.61 2021/10/22 12:30:53 bluhm Exp $
+ *
+ * SPDX-License-Identifier: 0BSD
+ * SPDX-FileCopyrightText: 1995, 1996, 1997, 1998, 1999 John Ioannidis
+ * SPDX-FileCopyrightText: 1995, 1996, 1997, 1998, 1999 Angelos D. Keromytis
+ * SPDX-FileCopyrightText: 1995, 1996, 1997, 1998, 1999 Niels Provos.
+ * SPDX-FileCopyrightText: 2001 Angelos D. Keromytis.
+ * SPDX-FileCopyrightText: 2008 Damien Miller
+ * SPDX-FileCopyrightText: 2010, 2015 Mike Belopuhov
+ * SPDX-FileContributor: John Ioannidis (ji@tla.org)
+ * SPDX-FileContributor: Angelos D. Keromytis (kermit@csd.uch.gr)
+ * SPDX-FileContributor: Niels Provos (provos@physnet.uni-hamburg.de)
+ * SPDX-FileContributor: Damien Miller (djm@mindrot.org)
+ * SPDX-FileContributor: Mike Belopuhov (mikeb@openbsd.org)
  *
  * The authors of this code are John Ioannidis (ji@tla.org),
  * Angelos D. Keromytis (kermit@csd.uch.gr),
```

SPDX migration

Defined
local SPDX identifier

To do
contribute to
SPDX identifier
database

```
include/crypto/sha1: migrate to SPDX identifier

Most tools used for compliance and SBOM generation use SPDX identifiers
This change brings us a step closer to an easy SBOM generation.

define NuttX local NuttX-PublicDomain identifier

 “Public Domain” is a concept distinct from copyright licensing;
it generally means that the work no longer has any copyright protection
or ownership, and therefore requires no license permission in order to
use, copy, modify, distribute, perform, display, etc.
In the United States - and many jurisdictions - copyright protections
attach automatically to creative works upon creation if they satisfy
certain minimum criteria.
“Public Domain” would thus represent a significant change to the legal
status of the work.
The rules around “Public Domain” often vary or are unspecified
jurisdiction to jurisdiction. Adding to the confusion, some
jurisdictions may not even recognize the concept of “Public Domain”
(or similar). As such, a license may nevertheless be required or implied
in these cases. Even in the U.S., there is no clear,
officially-sanctioned procedure for affirmatively placing
copyright-eligible works into the “Public Domain” aside from natural
statutory expiration of copyright. The bottom-line is, there are few if
any objective, brightline rules for proactively placing
copyright-eligible works into the Public Domain that we can broadly
rely on.
```

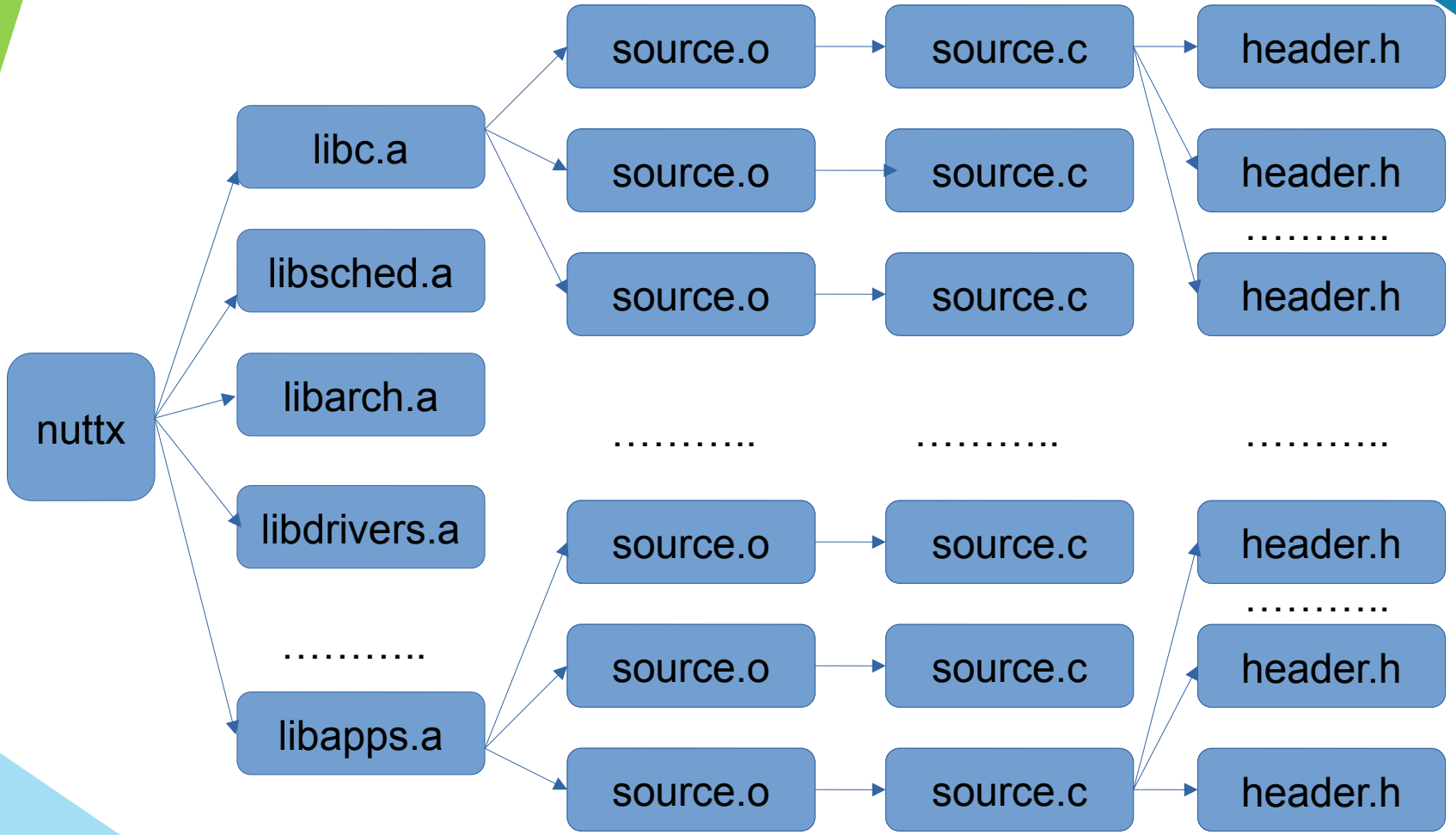
Implementation

OBJECTIVES

- make it fully automated
- existing build system

Collected information:

- ?


nuttx
libc.a
libsched.a
libarch.a
libdrivers.a
libapps.a
source.o
source.c
header.h
source.o
source.c
header.h
source.o
source.c
header.h
source.o
source.c
header.h
source.o
source.c
header.h
source.o
source.c
header.h

NuttX Build system

Makefile based
Generates Make.dep filles

```
./libs/libc/bin/Make.dep
./libs/libxx/Make.dep
./mm/bin/Make.dep
./arch/arm/src/Make.dep
./fs/Make.dep
./binfmt/Make.dep
./boards/Make.dep
./boards/arm/cxd56xx/common/Make.dep
./drivers/Make.dep
./sched/Make.dep
```

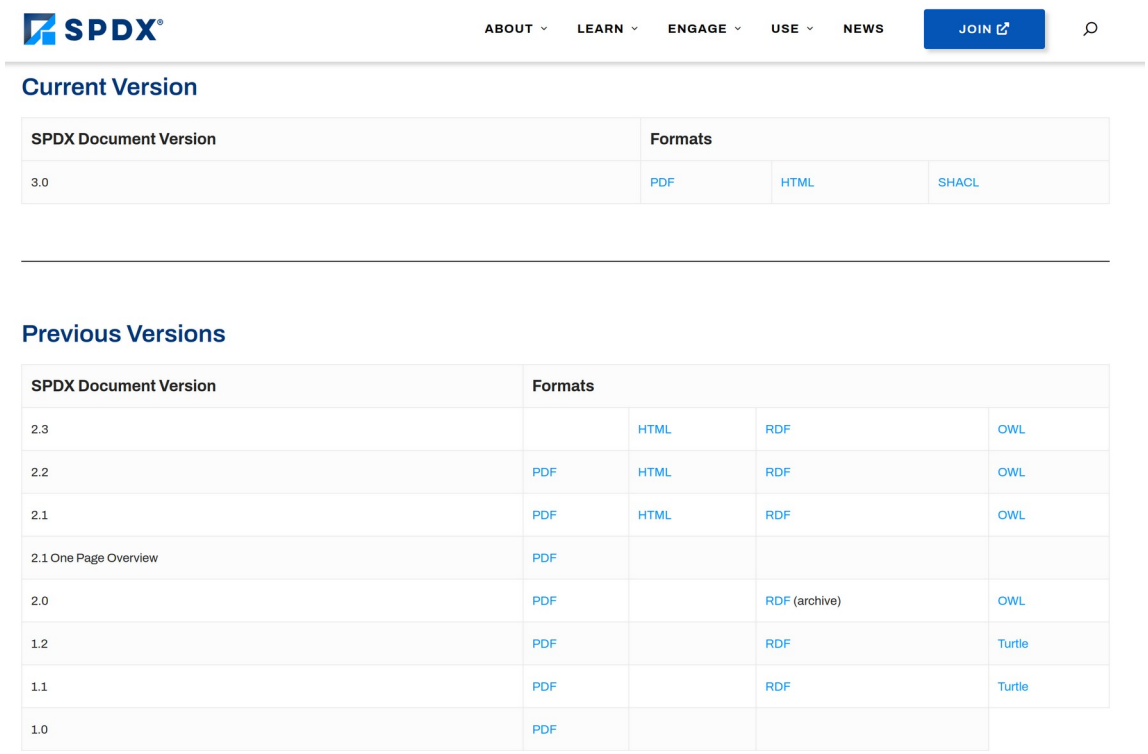
build_sbom_dep.map

```
fs_initialize.o: ../fs/fs_initialize.c \
 /home/me/nuttx/nuttx/include/nuttx/config.h \
 /home/me/nuttx/nuttx/include/nuttx/reboot_notifier.h \
 /home/me/nuttx/nuttx/include/nuttx/notifier.h \
 /home/me/nuttx/nuttx/include/nuttx/irq.h \
 /home/me/nuttx/nuttx/include/stdint.h \
 /home/me/nuttx/nuttx/include/nuttx/compiler.h \
 /home/me/nuttx/nuttx/include/arch/types.h \
 /home/me/nuttx/nuttx/include/arch/inttypes.h \
 /home/me/nuttx/nuttx/include/limits.h \
 /home/me/nuttx/nuttx/include/arch/limits.h \
```

```
fs/fs_initialize.c
include/nuttx/config.h
include/nuttx/reboot_notifier.h
include/nuttx/notifier.h
include/nuttx/irq.h
include/stdint.h
include/nuttx/compiler.h
include/arch/types.h
include/arch/inttypes.h
include/limits.h
include/arch/limits.h
```

WE HAVE A PROBLEM!

What version ?



SPDX®

ABOUT LEARN ENGAGE USE NEWS JOIN

Current Version

SPDX Document Version	Formats		
3.0	PDF	HTML	SHACL

Previous Versions

SPDX Document Version	Formats			
2.3		HTML	RDF	OWL
2.2	PDF	HTML	RDF	OWL
2.1	PDF	HTML	RDF	OWL
2.1 One Page Overview	PDF			
2.0	PDF		RDF (archive)	OWL
1.2	PDF		RDF	Turtle
1.1	PDF		RDF	Turtle
1.0	PDF			

https://spdx.dev/use/specifications/

Detailed specifications

SPDX
specification v2.3.0
v2.3
Search docs

Copyright
Introduction
Clause 1: Scope
Clause 2: Normative references
Clause 3: Terms and definitions
Clause 4: Conformance
Clause 5: Composition of an SPDX document
Clause 6: Document Creation Information
Clause 7: Package Information
Clause 8: File Information
8.1 File name field
8.2 File SPDX identifier field
8.3 File type field
8.4 File checksum field
8.5 Concluded license field
8.6 License information in file field
8.7 Comments on license field
8.8 Copyright text field
8.9 Artifact of project name field (deprecated)
8.10 Artifact of project homepage field (deprecated)
8.11 Artifact of project uniform resource identifier field (deprecated)
8.12 File comment field
8.13 File notice field
8.14 File contributor field
« Previous Next »

SPDX
»Clause 8: File Information

8 File information section

8.1 File name field

8.1.1 Description

Identify the full path and filename that corresponds to the file information in this section. The metadata for the file name field is shown in Table 36.

Table 36 — Metadata for the file name field

Attribute	Value
Required	Yes
Cardinality	1..1
Format	A relative filename with the root of the package archive or directory. In general, every filename is preceded with a `./`, see http://www.ietf.org/rfc/rfc3986.txt fo

8.1.2 Intent

To aid finding the correct file which corresponds to the file information.

8.1.3 Examples

EXAMPLE 1 Tag: `FileName:`

```
FileName: ./package/foo.c
```

EXAMPLE 2 RDF: Property `spdx:fileName` in class `spdx:File`

```
<File rdf:about="...">
    <fileName>./package/foo.c</fileName>
    ...
```

https://spdx.github.io/spdx-spec/v2.3/file-information/

Detailed examples

spdx-examples / software / example10 / spdx2.3 / **hello-source.spdx.json**

goneall and nishakm Move the software examples into the software profile

Code | Blame | 128 lines (128 loc) · 3.25 KB


```
{
  "SPDXID": "SPDXRef-DOCUMENT",
  "spdxVersion": "SPDX-2.3",
  "creationInfo": {
    "created": "2022-10-28T17:24:21Z",
    "creators": [
      "Person: Nisha Kumar"
    ],
    "licenseListVersion": "3.18"
  },
  "name": "hello",
  "dataLicense": "CC0-1.0",
  "documentDescribes": [
    "SPDXRef-hello-source"
  ],
  "documentNamespace": "https://github.com/spdx/spdx-examples/example10/spdx",
  "packages": [
    {
      "SPDXID": "SPDXRef-hello-source",
      "name": "hello",
      "downloadLocation": "NOASSERTION",
      "originator": "Person: Nisha Kumar",
      "licenseDeclared": "MIT",
      "licenseConcluded": "NOASSERTION",
      "copyrightText": "Copyright (c) 2022 Authors of Hello",
      "homepage": "https://github.com/spdx/spdx-examples",
      "filesAnalyzed": true,
      "primaryPackagePurpose": "LIBRARY",
      "hasFiles": [
        "SPDXRef-hello-py",
        "SPDXRef-hello-init",
        "SPDXRef-hello-pyproject",
        "SPDXRef-hello-license",
        "SPDXRef-hello-readme"
      ],
```


https://github.com/spdx/spdx-examples/

OBJECTIVES

- make it fully automated
- existing build system
- **SPDX 2.3**
- **JSON SBOM format**

Collected information:
- file hashes
- licenses
- relationships

for sources and build artifacts

SBOM – SPDX 2.3 - Header


```
{
    "SPDXVersion": "SPDX-2.3",
    "DataLicense": "CC0-1.0",
    "SPDXID": "SPDXRef-DOCUMENT",
    "DocumentName": "NuttX-12.8.0",
    "documentNamespace": "https://github.com/apache/nuttx/spdx",
    "creationInfo": {
        "Comment": "Generated by NuttX build",
        "Creator": "Person:user",
        "Tool": "nuttx_build_sbom.py",
        "created": "24/01/2025 10:41:41"
    }
},
```

SBOM – SPDX 2.3 - source


```
{
    "FileName": "fs/fs_initialize.c",
    "FileType": "SOURCE",
    "SPDXID": "SPDXID-File-fs/fs_initialize.c",
    "checksum": "SHA1: 968c701f562262dd07b8421cd10c14abc66f8596",
    "LicenseConcluded": [
        "Apache-2.0"
    ],
    "LicenseInfoInFile": [
        "Apache-2.0"
    ],
    "FileCopyrightText": [
        "NOASSERTION"
    ],
    "FileContributor": [
        "NOASSERTION"
    ]
},
```

SBOM – SPDX 2.3 - headers


```
{
    "FileName": "include/nuttx/config.h",
    "FileType": "SOURCE",
    "SPDXID": "SPDXID-File-include/nuttx/config.h",
    "checksum": "SHA1: 86b4672a2d57a2121a51ca0c53b86df00da86006",
    "LicenseConcluded": [
        "NOASSERTION"
    ],
    "LicenseInfoInFile": [
        "NOASSERTION"
    ],
    "FileCopyrightText": [
        "NOASSERTION"
    ],
    "FileContributor": [
        "NOASSERTION"
    ]
},
```

```
{
    "FileName": "/usr/lib/gcc/arm-none-eabi/13.2.1/include/stdarg.h",
    "FileType": "SOURCE",
    "SPDXID": "SPDXID-File-/usr/lib/gcc/arm-none-eabi/13.2.1/include/stdarg.h",
    "checksum": "SHA1: 5d5992d7ea977abf4ae526880f995c19d4865aaa",
    "LicenseConcluded": [
        "NOASSERTION"
    ],
    "LicenseInfoInFile": [
        "NOASSERTION"
    ],
    "FileCopyrightText": [
        "NOASSERTION"
    ],
    "FileContributor": [
        "NOASSERTION"
    ]
},
```

Challenges – external projects

nuttx/apps/math/libtommath$ ls
CMakeLists.txt Kconfig Make.defs Makefile

Possible fix
- license check
- SPDX identifiers
- Upstream contribution

Alternate fix
Patch licenses after integration

```
CONFIG_LIBTOMMATH_URL ?= "https://github.com/libtom/libtommath/archive"

LIBTOMMATH_VERSION = $(patsubst "%",%,$(strip $(CONFIG_LIBTOMMATH_VERSION)))
LIBTOMMATH_ZIP = v$(LIBTOMMATH_VERSION).zip

LIBTOMMATH_UNPACKNAME = libtommath
UNPACK ?= unzip -o

$(LIBTOMMATH_ZIP):
	@echo "Downloading: $(LIBTOMMATH_ZIP)"
	$(Q) curl -O -L $(CONFIG_LIBTOMMATH_URL)/$(LIBTOMMATH_ZIP)

$(LIBTOMMATH_UNPACKNAME): $(LIBTOMMATH_ZIP)
	@echo "Unpacking: $(LIBTOMMATH_ZIP) -> $(LIBTOMMATH_UNPACKNAME)"
	$(Q) $(UNPACK) $(LIBTOMMATH_ZIP)
	$(Q) mv libtommath-$(LIBTOMMATH_VERSION) $(LIBTOMMATH_UNPACKNAME)
	$(Q) touch $(LIBTOMMATH_UNPACKNAME)
```

Some thoughts

- **Available SBOM information** may be overwhelming
- **Open Chan and SPDX** are welcoming communities
- **SPDX identifier** may be missing for your dependencies
- Join the **open source community** !

THANK YOU!