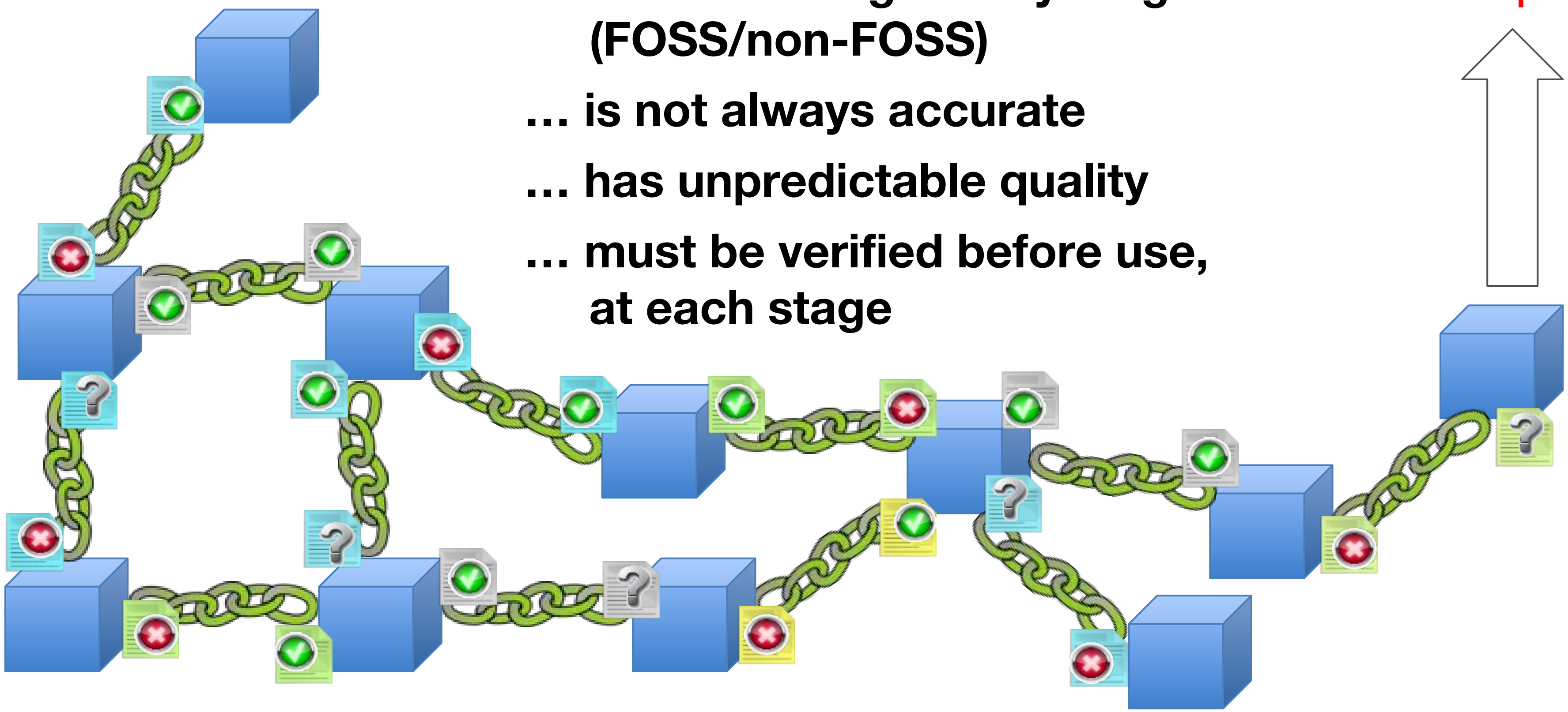
# Securing the FOSS Supply Chain

April 28, 11:30 | General Audience

Claus-Peter Wiedemann
LRT Team Lead
BearingPoint

# License Data in FOSS Supply Chains…



… travels through many stages
(FOSS/non-FOSS)

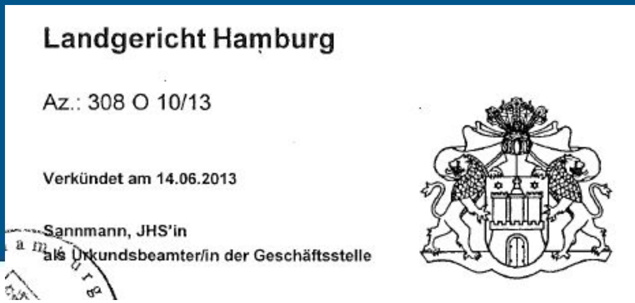
… is not always accurate

… has unpredictable quality

… must be verified before use,
at each stage

Compliant?

# The Fantec Case



Landgericht Hamburg

Az.: 308 O 10/13

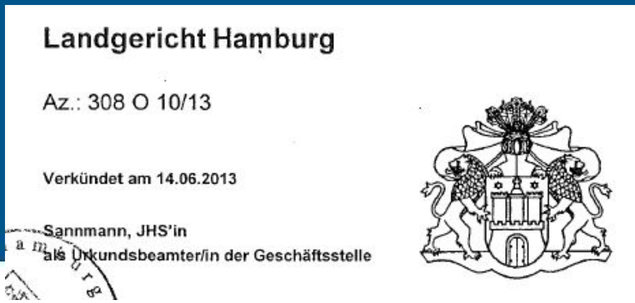
Verkündet am 14.06.2013

Sannmann, JHS'in
als Urkundsbeamter/in der Geschäftsstelle

- GPL violation discovered in a Fantec product during a hackers conference
  - The source code for the GPL components in the product was made available by Fantec, but it was an outdated version

- Fantec was sued, but argues that
  - their Chinese supplier asserted that the source code provided with the product was complete
  - only the copyright holder is able to effectively check if the source code is complete
  - a tool based source code inspection (audit) is very costly but without any warranty that the results are complete and correct.

# The Fantec Case



Landgericht Hamburg

Az.: 308 O 10/13

Verkündet am 14.06.2013

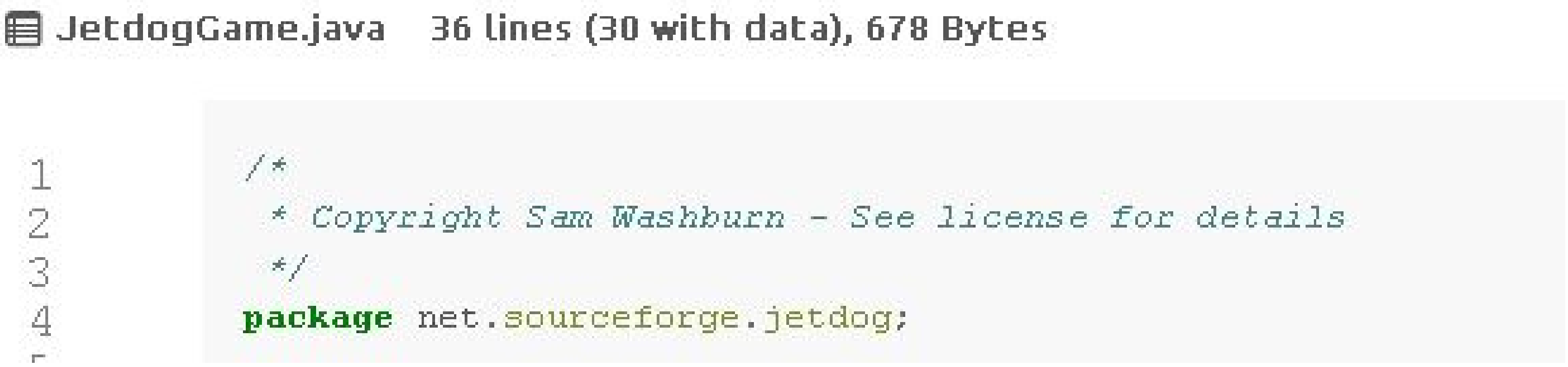
Sannmann, JHS'in
als Urkundsbeamter/in der Geschäftsstelle

- The Court says
  - *Fantec* was required to ensure the GPL obligations are fulfilled for their delivery
  - *Fantec* acted negligently by relying on the statements of its Chinese supplier
  - *Fantec* was required to inspect the software delivery, either by themselves or by contracting a competent 3rd party, even if this meant to incur additional cost

# License and copyright information must be maintained on file level

- Files are the unit of storage. They
  - can (and eventually will) be used and distributed individually
  - can be (and eventually are) used in many different projects
  - can be (and eventually are) combined  in many ways
- License info in each file must be complete and unambiguous
  - Copyright notice(s)
  - Full license text or unique, permanent  ID (e.g. SPDX license identifier) or URI
- References to LICENSE/Readme/… etc. are not sufficient because
  - project licenses may change with new versions, so would LICENSE/Readme
  - the project/site may not be around anymore when the file is caught in the wild after many years

# Example 1: No way to determine the license

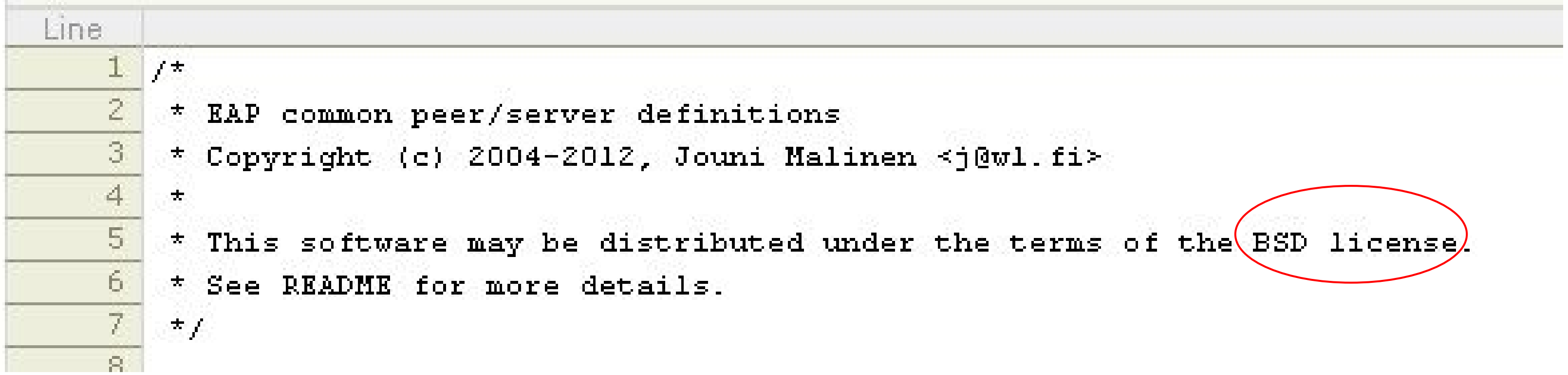


JetdogGame.java 36 lines (30 with data), 678 Bytes

```
/*
 * Copyright Sam Washburn - See license for details
 */
package net.sourceforge.jetdog;
```

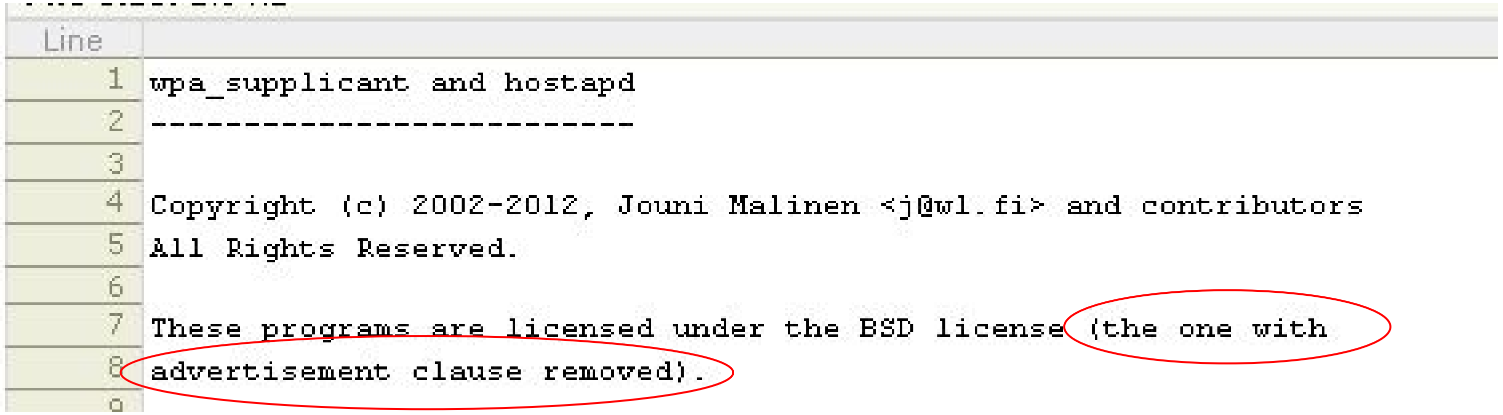
# Example 2: Contradicting licenses

## Source File



```
/*
 * EAP common peer/server definitions
 * Copyright (c) 2004-2012, Jouni Malinen <j@w1.fi>
 *
 * This software may be distributed under the terms of the BSD license.
 * See README for more details.
 */
```

## Readme File

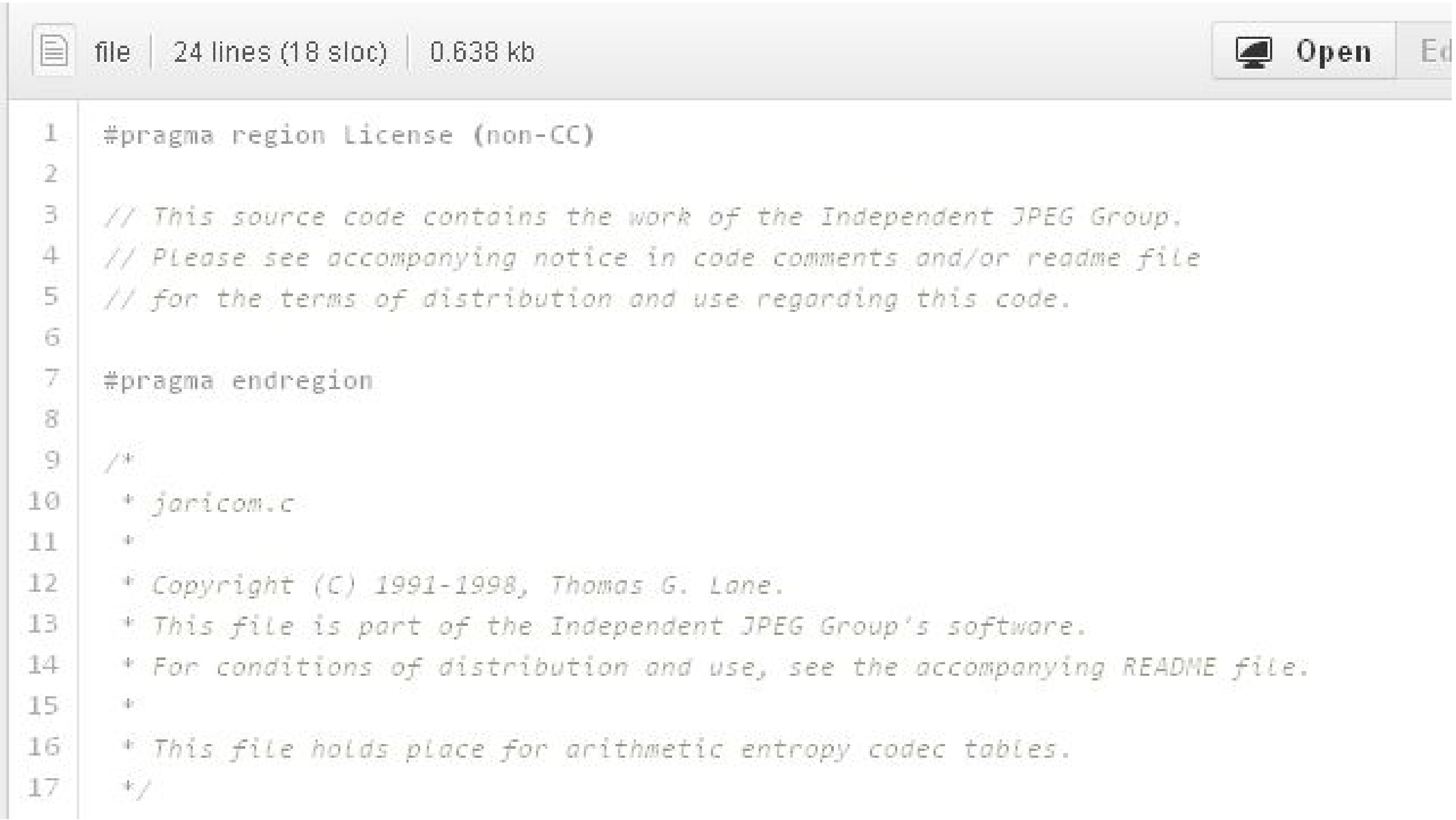


```
wpa_supplicant and hostapd
--------------------------

Copyright (c) 2002-2012, Jouni Malinen <j@w1.fi> and contributors
All Rights Reserved.

These programs are licensed under the BSD license (the one with
advertisement clause removed).
```

# Example 3: Code comments are not useful



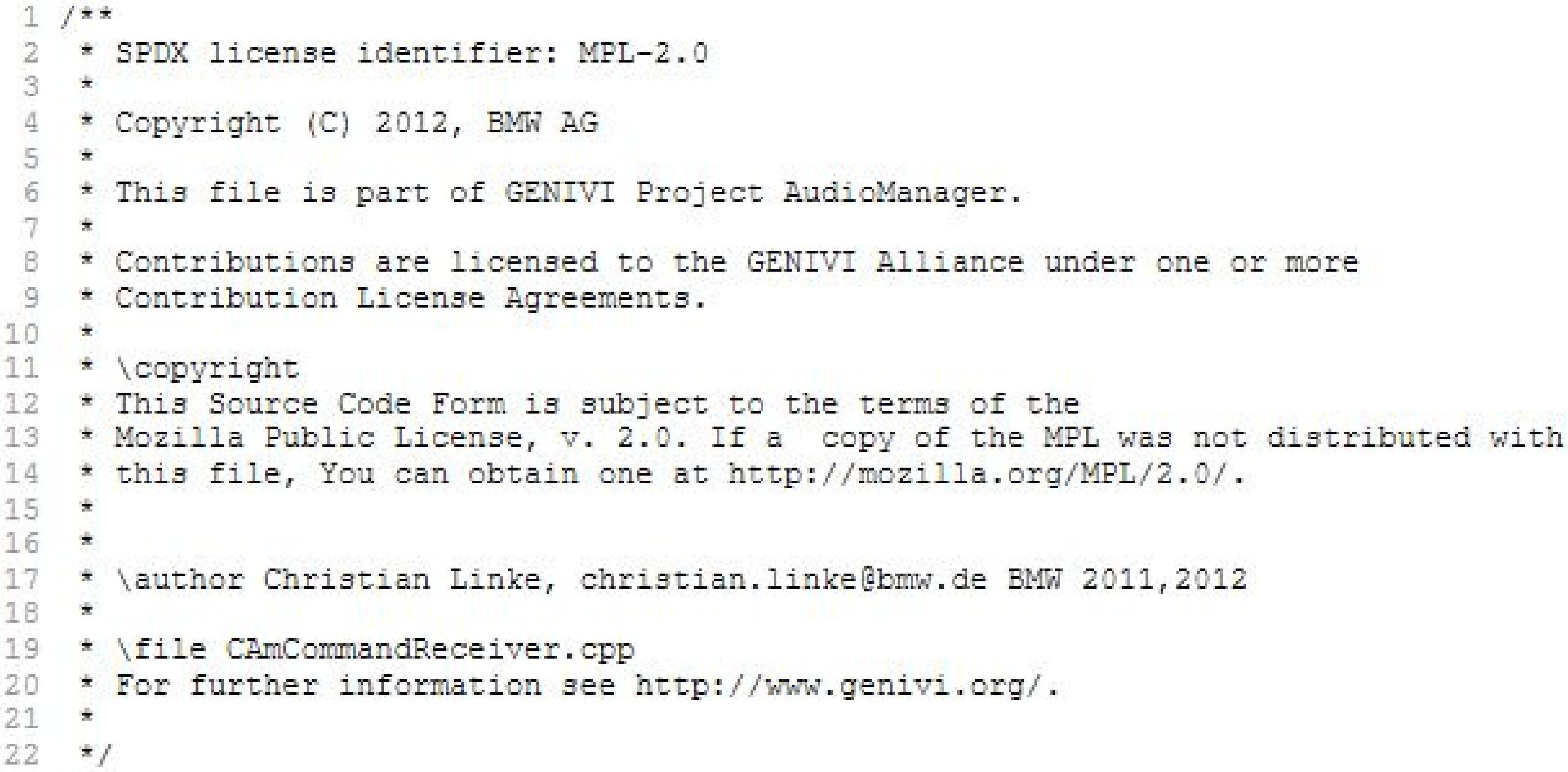
```
#pragma region License (non-CC)

// This source code contains the work of the Independent JPEG Group.
// Please see accompanying notice in code comments and/or readme file
// for the terms of distribution and use regarding this code.

#pragma endregion

/*
 * jaricom.c
 *
 * Copyright (C) 1991-1998, Thomas G. Lane.
 * This file is part of the Independent JPEG Group's software.
 * For conditions of distribution and use, see the accompanying README file.
 *
 * This file holds place for arithmetic entropy codec tables.
 */
```

# Example 4: Best practice



```
/**
 * SPDX license identifier: MPL-2.0
 *
 * Copyright (C) 2012, BMW AG
 *
 * This file is part of GENIVI Project AudioManager.
 *
 * Contributions are licensed to the GENIVI Alliance under one or more
 * Contribution License Agreements.
 *
 * \copyright
 * This Source Code Form is subject to the terms of the
 * Mozilla Public License, v. 2.0. If a  copy of the MPL was not distributed with
 * this file, You can obtain one at http://mozilla.org/MPL/2.0/.
 *
 *
 * \author Christian Linke, christian.linke@bmw.de BMW 2011,2012
 *
 * \file CAmCommandReceiver.cpp
 * For further information see http://www.genivi.org/.
 *
 */
```

# Upstream License Data

- License files more and more common in repos
- Machine readable license data provided with many Linux distros (e.g. Debian)

Looks good, but what about completeness?

Why not use Fossology and have a closer look at some Yocto components used in the GDP

# Example: mesa-2_10.6.3-r0

License information provided by Yocto

- MIT license (license.html file)
- Generic MIT

# Example: mesa-2_10.6.3-r0

File level license information determined with Fossology

- MIT license
- BSD 3-clause license
- BSD 2-clause license
- XFree86 license
- SGI Free Software License B 2.0
- GNU GPL v3+ with Bison exception
- GNU GPL v3+ with Autoconf Macro exception
- Holger Weiss Permission Notice (Freeware)
- Boost Software License 1.0
- BSD style-license with acknowledgement
- AMD readme

# Example: mesa-2_10.6.3-r0

## AMD Readme (mesa-2_10.6.3-r0/mesa-10.6.3/docs/README.UVD)

The software may implement third party technologies (e.g. third party libraries) that are not licensed to you by AMD and for which you may need to obtain licenses from other parties.  Unless explicitly stated otherwise, these third party technologies are not licensed hereunder.  Such third party technologies include, but are not limited, to H.264, MPEG-2, MPEG-4, AVC, and VC-1.

For MPEG-2 Encoding Products ANY USE OF THIS PRODUCT IN ANY MANNER OTHER THAN PERSONAL USE THAT COMPLIES WITH THE MPEG-2 STANDARD FOR ENCODING VIDEO INFORMATION FOR PACKAGED MEDIA **IS EXPRESSLY PROHIBITED** WITHOUT A LICENSE UNDER APPLICABLE PATENTS IN THE MPEG-2 PATENT PORTFOLIO, WHICH LICENSES IS AVAILABLE FROM MPEG LA, LLC, 6312 S. Fiddlers Green Circle, Suite 400E, Greenwood Village, Colorado 80111 U.S.A.

# Example: libinput-1.1.1-r0

License information provided by Yocto

- MIT license (license.html file)
- Generic MIT

# Example: libinput-1.1.1-r0

File level license information determined with Fossology

- MIT license
- FSF permission notice (.m4 files)
- GNU GPL v2+ with Libtool exception (ltmain.sh)
- GNU GPL v2

# Example: libinput-1.1.1-r0

## libinput-1.1.1-r0/ libinput-1.1.1/ src/ libinput-util.c (line 1)

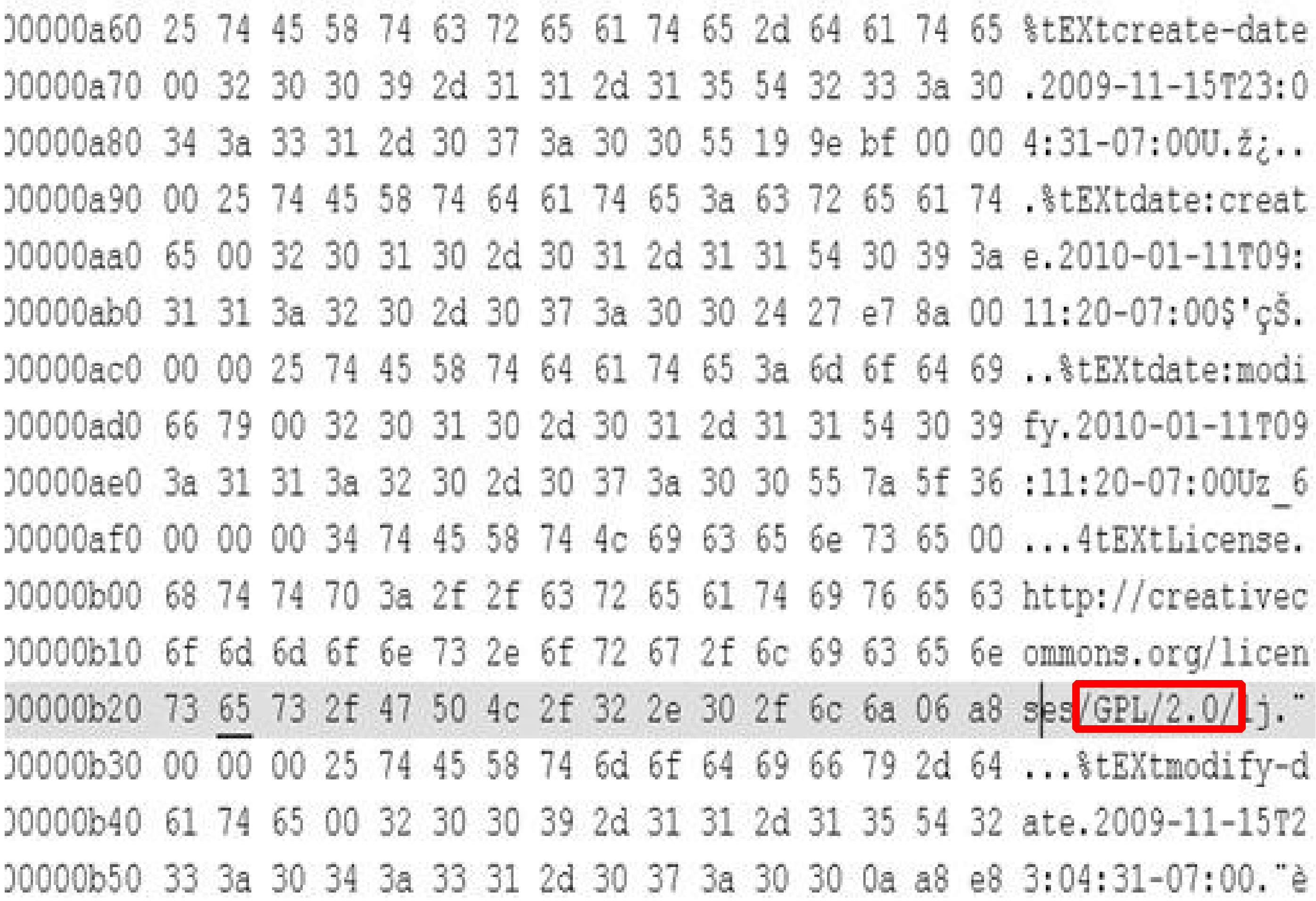
```
/*
 * Copyright © 2008-2011 Kristian Høgsberg
 * Copyright © 2011 Intel Corporation
 * Copyright © 2013-2015 Red Hat, Inc.
 *
 * Permission is hereby granted, free of charge, to any person obtaining a
 * copy of this software and associated documentation files (the "Software"),
 * to deal in the Software without restriction, including without limitation
 * the rights to use, copy, modify, merge, publish, distribute, sublicense,
 * and/or sell copies of the Software, and to permit persons to whom the
 * Software is furnished to do so, subject to the following conditions:
 *
*/
```

# Example: libinput-1.1.1-r0

## libinput-1.1.1-r0/ libinput-1.1.1/ src/ libinput-util.c (line 83)

```
/*
 * Perform rate-limit test. Returns RATELIMIT_PASS if the rate-limited action
 * is still allowed, RATELIMIT_THRESHOLD if the limit has been reached with
 * this call, and RATELIMIT_EXCEEDED if you're beyond the threshold.
 * It's safe to treat the return-value as boolean, if you're not interested in
 * the exact state. It evaluates to "true" if the threshold hasn't been
 * exceeded, yet.
 *
 * The ratelimit object must be initialized via ratelimit_init().
 *
 * Modelled after Linux' lib/ratelimit.c by Dave Young
 * <hidave.darkstar@gmail.com>, which is licensed GPLv2.
 */
```

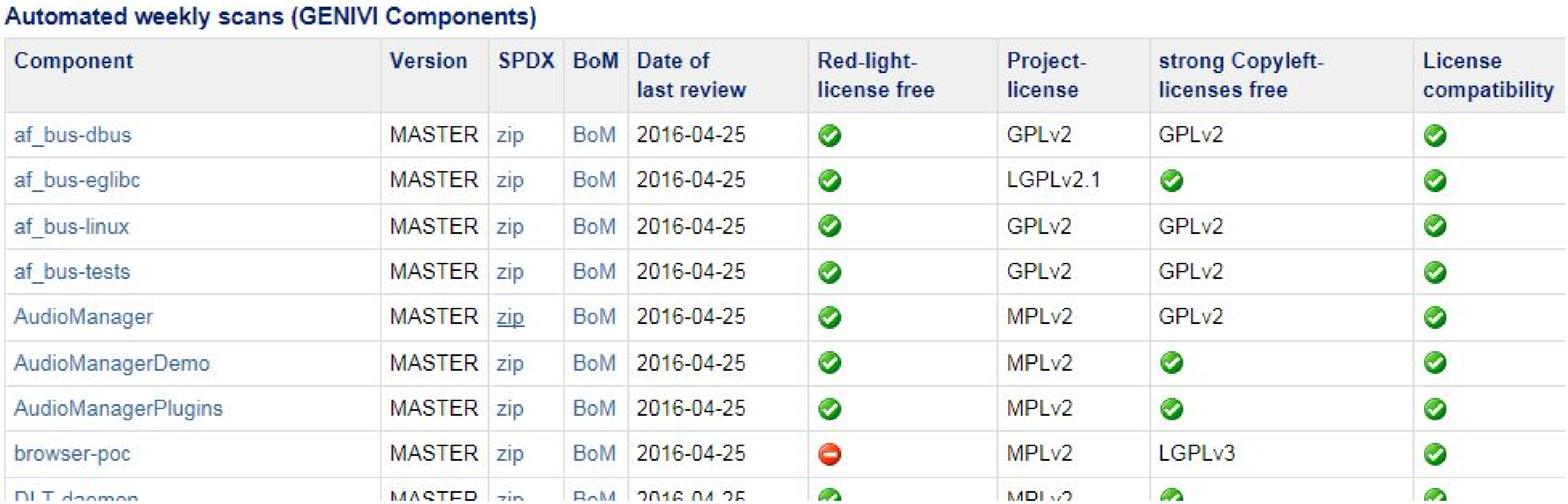
# Example: License information in image files



```
00000a60 25 74 45 58 74 63 72 65 61 74 65 2d 64 61 74 65 %tEXtcreate-date
00000a70 00 32 30 30 39 2d 31 31 2d 31 35 54 32 33 3a 30 .2009-11-15T23:0
00000a80 34 3a 33 31 2d 30 37 3a 30 30 55 19 9e bf 00 00 4:31-07:00U.ž¿..
00000a90 00 25 74 45 58 74 64 61 74 65 3a 63 72 65 61 74 .%tEXtdate:creat
00000aa0 65 00 32 30 31 30 2d 30 31 2d 31 31 54 30 39 3a e.2010-01-11T09:
00000ab0 31 31 3a 32 30 2d 30 37 3a 30 30 24 27 e7 8a 00 11:20-07:00$'çŠ.
00000ac0 00 00 25 74 45 58 74 64 61 74 65 3a 6d 6f 64 69 ..%tEXtdate:modi
00000ad0 66 79 00 32 30 31 30 2d 30 31 2d 31 31 54 30 39 fy.2010-01-11T09
00000ae0 3a 31 31 3a 32 30 2d 30 37 3a 30 30 55 7a 5f 36 :11:20-07:00Uz_6
00000af0 00 00 00 34 74 45 58 74 4c 69 63 65 6e 73 65 00 ...4tEXtLicense.
00000b00 68 74 74 70 3a 2f 2f 63 72 65 61 74 69 76 65 63 http://creativec
00000b10 6f 6d 6d 6f 6e 73 2e 6f 72 67 2f 6c 69 63 65 6e ommons.org/licen
00000b20 73 65 73 2f 47 50 4c 2f 32 2e 30 2f 6c 6a 06 a8 ses/GPL/2.0/lj.¨
00000b30 00 00 00 25 74 45 58 74 6d 6f 64 69 66 79 2d 64 ...%tEXtmodify-d
00000b40 61 74 65 00 32 30 30 39 2d 31 31 2d 31 35 54 32 ate.2009-11-15T2
00000b50 33 3a 30 34 3a 33 31 2d 30 37 3a 30 30 0a a8 e8 3:04:31-07:00.¨è
```

# GENIVI License Data

- File based, SPDX2 format (rdf and html)
- Available in the Wiki for Specific Components and Reference Implementations referenced by the GENIVI Compliance Specification
- Updated weekly



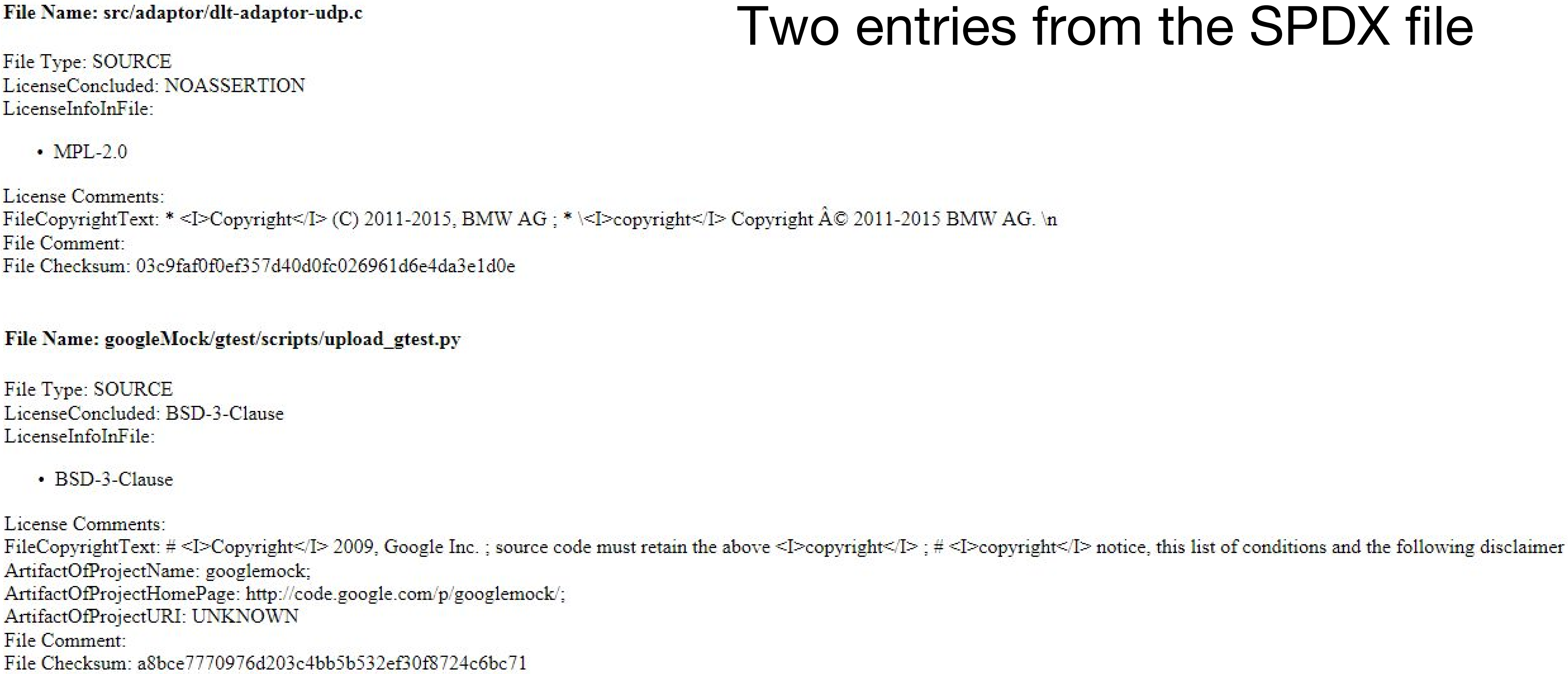
Automated weekly scans (GENIVI Components)

| Component | Version | SPDX | BoM | Date of last review | Red-light-license free | Project-license | strong Copyleft-licenses free | License compatibility |
|---|---|---|---|---|---|---|---|---|
| af_bus-dbus | MASTER | zip | BoM | 2016-04-25 | ✓ | GPLv2 | GPLv2 | ✓ |
| af_bus-eglibc | MASTER | zip | BoM | 2016-04-25 | ✓ | LGPLv2.1 | ✓ | ✓ |
| af_bus-linux | MASTER | zip | BoM | 2016-04-25 | ✓ | GPLv2 | GPLv2 | ✓ |
| af_bus-tests | MASTER | zip | BoM | 2016-04-25 | ✓ | GPLv2 | GPLv2 | ✓ |
| AudioManager | MASTER | zip | BoM | 2016-04-25 | ✓ | MPLv2 | GPLv2 | ✓ |
| AudioManagerDemo | MASTER | zip | BoM | 2016-04-25 | ✓ | MPLv2 | ✓ | ✓ |
| AudioManagerPlugins | MASTER | zip | BoM | 2016-04-25 | ✓ | MPLv2 | ✓ | ✓ |
| browser-poc | MASTER | zip | BoM | 2016-04-25 | ⛔ | MPLv2 | LGPLv3 | ✓ |
| DLT-daemon | MASTER | zip | BoM | 2016-04-25 | ✓ | MPLv2 | ✓ | ✓ |

https://collab.genivi.org/wiki/display/genivi/Results+of+Code+License+Scan

# Example: dlt_daemon

## Two entries from the SPDX file



**File Name: src/adaptor/dlt-adaptor-udp.c**

File Type: SOURCE
LicenseConcluded: NOASSERTION
LicenseInfoInFile:

- MPL-2.0

License Comments:
FileCopyrightText: * <I>Copyright</I> (C) 2011-2015, BMW AG ; * \<I>copyright</I> Copyright Â© 2011-2015 BMW AG. \n
File Comment:
File Checksum: 03c9faf0f0ef357d40d0fc026961d6e4da3e1d0e

**File Name: googleMock/gtest/scripts/upload_gtest.py**

File Type: SOURCE
LicenseConcluded: BSD-3-Clause
LicenseInfoInFile:

- BSD-3-Clause

License Comments:
FileCopyrightText: # <I>Copyright</I> 2009, Google Inc. ; source code must retain the above <I>copyright</I> ; # <I>copyright</I> notice, this list of conditions and the following disclaimer
ArtifactOfProjectName: googlemock;
ArtifactOfProjectHomePage: http://code.google.com/p/googlemock/;
ArtifactOfProjectURI: UNKNOWN
File Comment:
File Checksum: a8bce7770976d203c4bb5b532ef30f8724c6bc71

# Summary

- FOSS supply chain management is key for downstream compliance
- Relying on supplier‘s license data is high risk
- The license data must be determined on file level
- Upstream license data is not always accurate/reliable
- GENIVI components come with file based license information in SPDX2-format, available on the Wiki

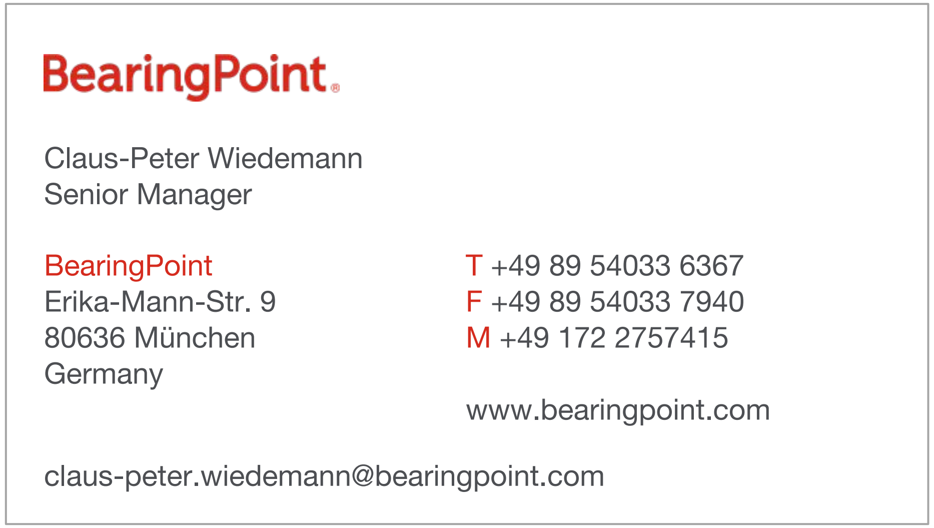
- **The FOSS supply chain must be actively managed.**

No headcount? Outsurcing options are available.

# Questions?

Q&A

# THANK YOU!



BearingPoint.

Claus-Peter Wiedemann
Senior Manager

BearingPoint
Erika-Mann-Str. 9
80636 München
Germany

T +49 89 54033 6367
F +49 89 54033 7940
M +49 172 2757415

www.bearingpoint.com

claus-peter.wiedemann@bearingpoint.com