

Three Lessons Learned: How RSEs Succeed in License Management

Tim Drees, Dirk Feuchter, Tomas Stry, Achim Winandi

private, currently Legal
Counsel at Helmholtz
Association

KIT-IRM-IPM

Private, KIT-IBT until 12/24

KIT-BIB/HoC

de-RSE 25.02.2025



Lesson #1: Generate SBOM

→ Project to Market Example 01

Marvelous, Company contacted us, that our “GPL-led” Research-Software would brilliantly fit in its product and asks to get it proprietarily



pexels.com: @divinetchygirl

Lesson #1: Generate SBOM

→ Project to Market Example 02

external MIT-
+ GPL-code



Great, our partner wants to market a device together with our Research-Software, in which we included external components. How to deliver?

Lesson #1: Generate SBOM

→ Requirements from Industry

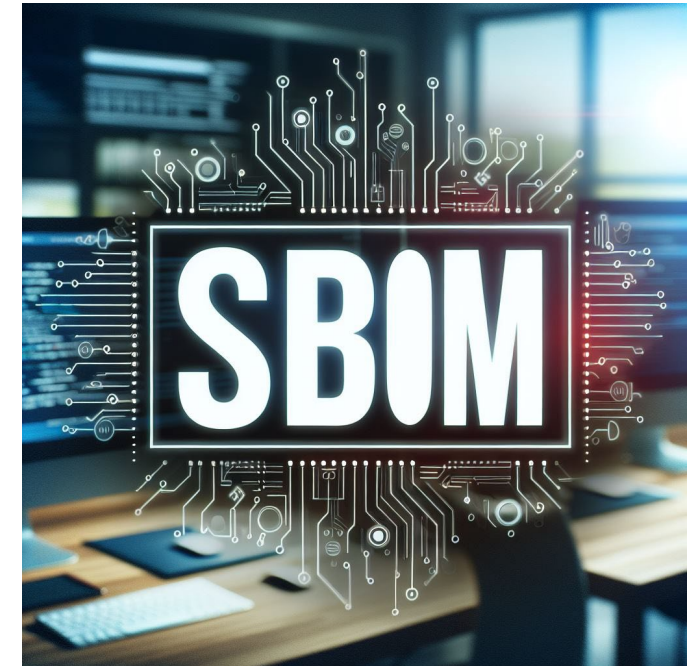
“ . . . The Contractor (→ Research Institution) warrants that the delivered code will meet the functional and performance requirements and contain neither vulnerabilities nor damagecode Contractor warrants that the delivered code will fulfill industrial standards according to ISO... and will not infringe copyrights of any third party, . . . “

■ **License Compliance Management → Open Chain → SBOM**

Lesson #1: Generate SBOM

→ A Recommendation

- Create and maintain a Software Bill of Materials
 - Make composition and origin of components transparent
 - All the way long and right from the start
 - Otherwise \$\$\$\$ at disclosure 😞



Lesson #1: Generate SBOM

→ What RSE might do...

- ... meet each other for exchange and help for self-help?
- ... manage their project with the Eclipse Foundation?
- ... hire an external „LCM“-expert?

How seriously
should we take
„LCM“ and SBOMs?



© Emil Meckel

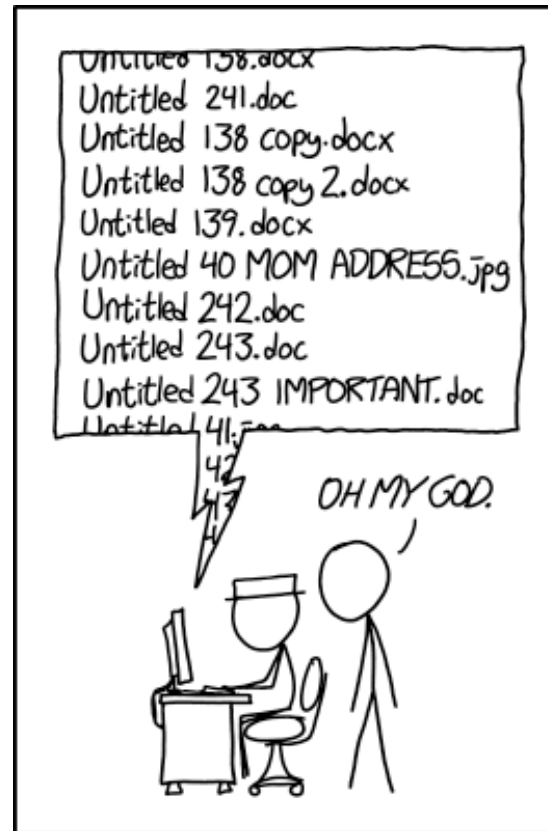
Lesson #1: Generate SBOM

→ Conclusion

- Balance effort und benefit.
- Should help you for
 - risk mitigation,
 - sustainability
 - value of your Research Software
- Make sure you have license texts and copyrights together
→ pass them on during delivery
- An “acap”*-SBOM is better than no SBOM (*acap = as complete as possible)
- makes you more interesting for industry
- Keep an eye on the legal perspective...



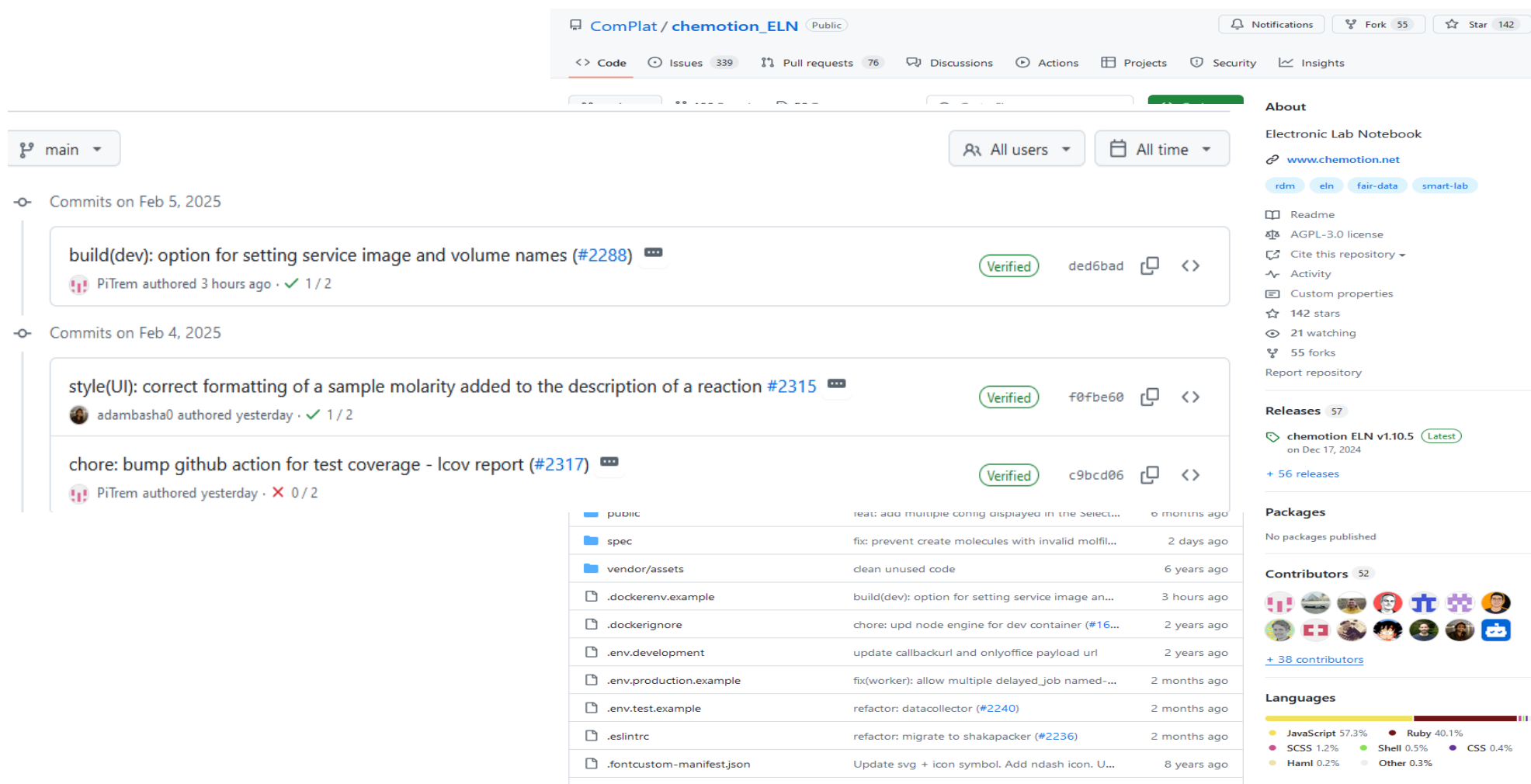
Lesson #2: Carefully Manage Contributions



PROTIP: NEVER LOOK IN SOMEONE
ELSE'S DOCUMENTS FOLDER.

„Documents“ (<https://xkcd.com/1459/>) by Randall Munroe,
licensed under CC BY-NC 2.5

Lesson #2: Carefully Manage Contributions -use GIT



ComPlat / chemotion_ELN (Public)

Notifications Fork 55 Star 142

<> Code Issues 339 Pull requests 76 Discussions Actions Projects Security Insights

main

Commits on Feb 5, 2025

- build(dev): option for setting service image and volume names (#2288) Verified ded6bad <>
PiTrem authored 3 hours ago · ✓ 1 / 2

Commits on Feb 4, 2025

- style(UI): correct formatting of a sample molarity added to the description of a reaction #2315 Verified f0fbe60 <>
adambasha0 authored yesterday · ✓ 1 / 2
- chore: bump github action for test coverage - lcov report (#2317) Verified c9bcd06 <>
PiTrem authored yesterday · ✗ 0 / 2

public

test: add multiple config displayed in the select...	6 months ago
spec	fix: prevent create molecules with invalid molfil... 2 days ago
vendor/assets	clean unused code 6 years ago
.dockerenv.example	build(dev): option for setting service image an... 3 hours ago
.dockerignore	chore: upd node engine for dev container (#16... 2 years ago
.env.development	update callbackurl and onlyoffice payload url 2 years ago
.env.production.example	fix(worker): allow multiple delayed_job named-... 2 months ago
.env.test.example	refactor: datacollector (#2240) 2 months ago
.eslintrc	refactor: migrate to shakapacker (#2236) 2 months ago
.fontcustom-manifest.json	Update svg + icon symbol. Add ndash icon. U... 8 years ago

About

Electronic Lab Notebook

www.chemotion.net

rdm eln fair-data smart-lab

Readme
AGPL-3.0 license
Cite this repository
Activity
Custom properties
142 stars
21 watching
55 forks
Report repository

Releases 57

chemotion ELN v1.10.5 (Latest)
on Dec 17, 2024

+ 56 releases

Packages

No packages published

Contributors 52

+ 38 contributors

Languages

JavaScript 57.3%	Ruby 40.1%
SCSS 1.2%	Shell 0.5%
Hamli 0.2%	CSS 0.4%
Other 0.3%	

■ Example Chemotion ELN

Lesson #2: Carefully Manage Contributions



Lesson #2: Carefully Manage Contributions – Insert copyright notice in file header

Copyright 2020-2025,
Copyright Owner: Research Center ABC,
Author: Dr. Martina Musterfrau, Max Mustermann,
Contact: email@institute.center.edu, Institute of Software
Development

licensed under [full license text]
reference SPDX-Format such as „MIT“, „BSD-2-Clause“ or other

Lesson #2: Carefully Manage Contributions – Use REUSE for licence management

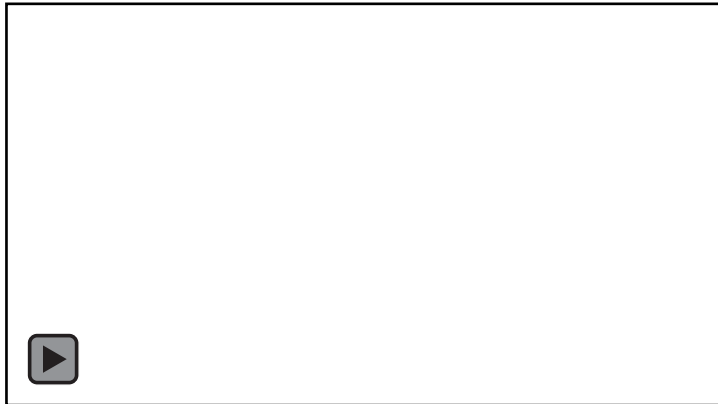
“We make licensing easy for humans and machines alike. We solve a fundamental issue that Free Software licensing has at the very source: what license is a file licensed under, and who owns the copyright?

Adopting our recommendations is as easy as one-two-three!”

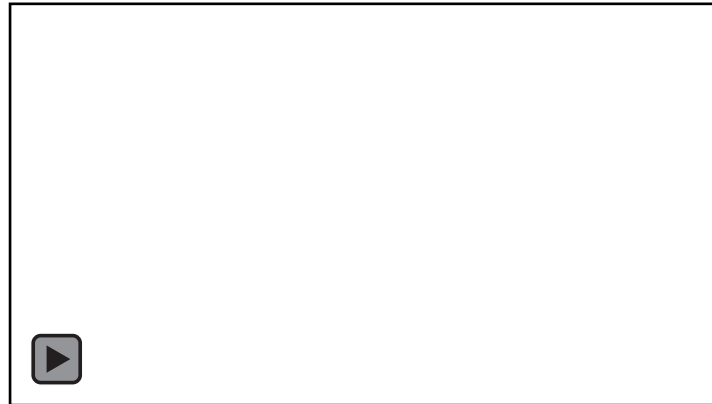
<https://reuse.software/>

Lesson #2: Carefully Manage Contributions – REUSE: Add copyright and licensing to each file

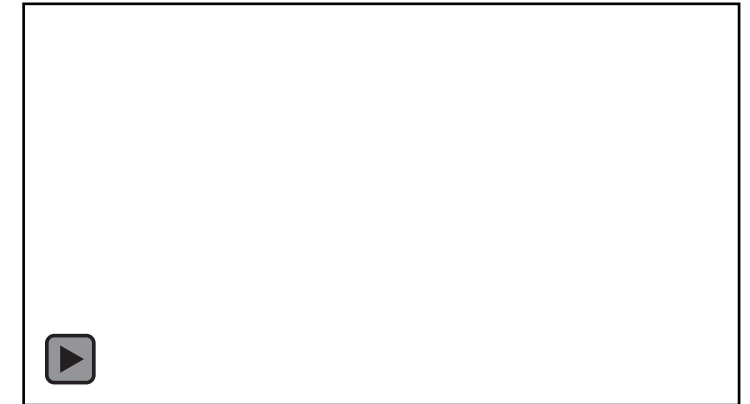
- Select licenses from [SPDX license list](#)
- Specify the license...



... as a comment in the header



... as a separate .license file



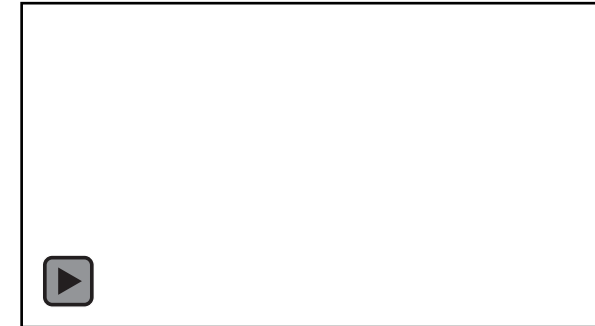
... in REUSE.toml

```
reuse annotate
```

Lesson #2: Carefully Manage Contributions – REUSE: Download licenses

- Select licenses from SPDX license list
- Custom licenses can also be provided (Prefix LicenseRef-)
- Save licenses to LICENSES folder

reuse download

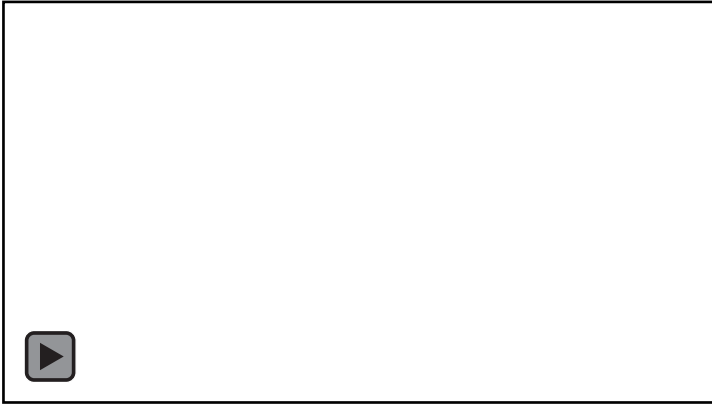


Download single license

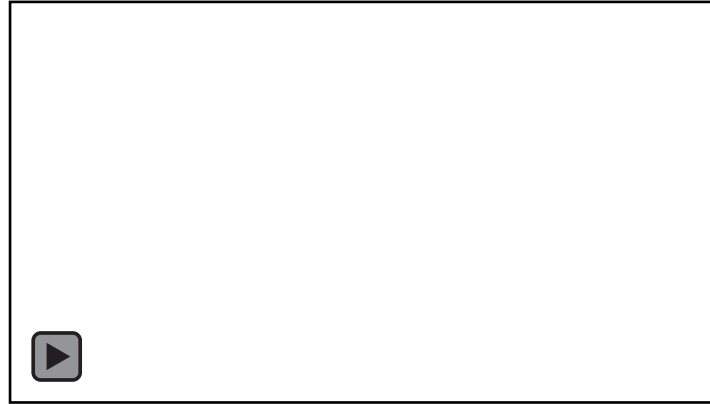


Download all missing licenses

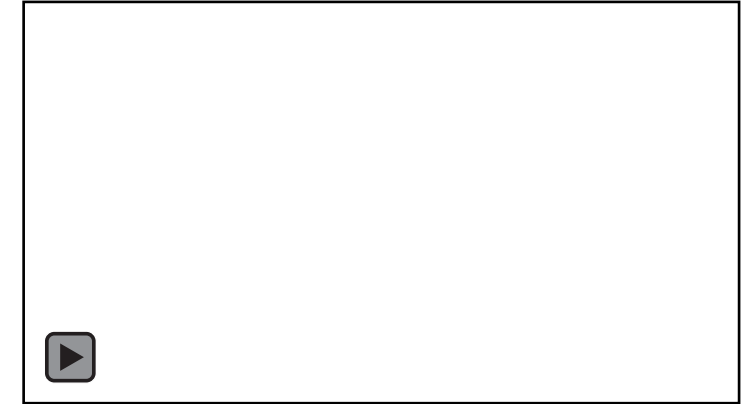
Lesson #2: Carefully Manage Contributions – REUSE: Confirm REUSE compliance



CLI: with REUSE tool



CI/CD: docker image
for GitLab, GitHub, etc.

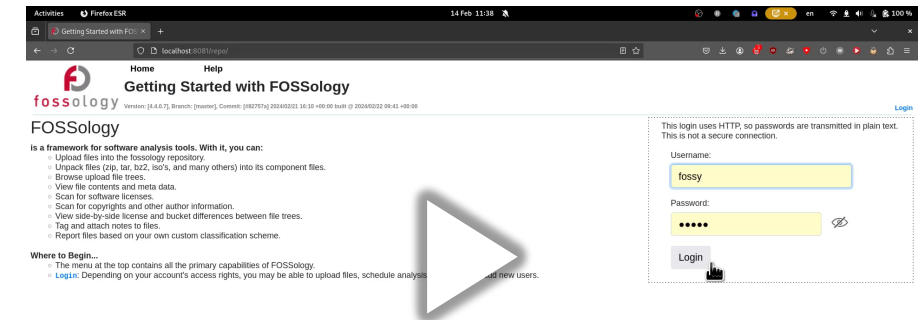


API: for public
repositories (with status
badge for your repo!)

```
reuse lint
```

Lesson #2: Carefully Manage Contributions – Use FOSSOLOGY for license scanning

- Scan for copyrights and licensing information
- Review and curate manually
- Export SPDX information
- Web based tool (GPL-v2 license)



Lesson #3: Maintain Flexibility to Adapt License Model



Your contributions and suggestions how RSEs succeed in License Management ?



- Pictures on slides 1, 5, 10 and 17: KI-generated with DALL-E.
- Pictures on slides 2, 3 and 18: downloaded from pexels.com