

# Issues of Open Source Compliance Check of Modern Programming Languages and Container Images

Open Source Leadership Summit

Gergely Csatari

14-03-2019

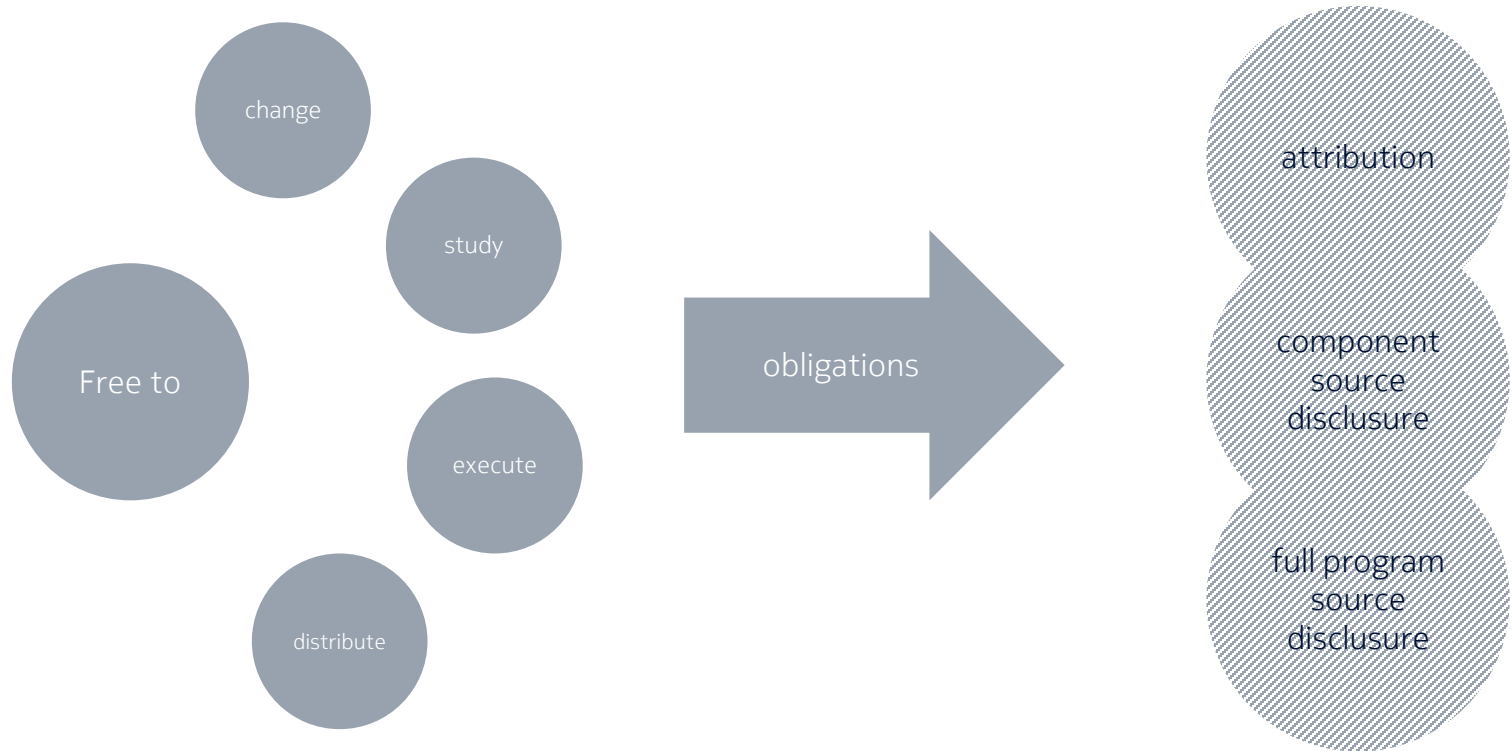
whoami



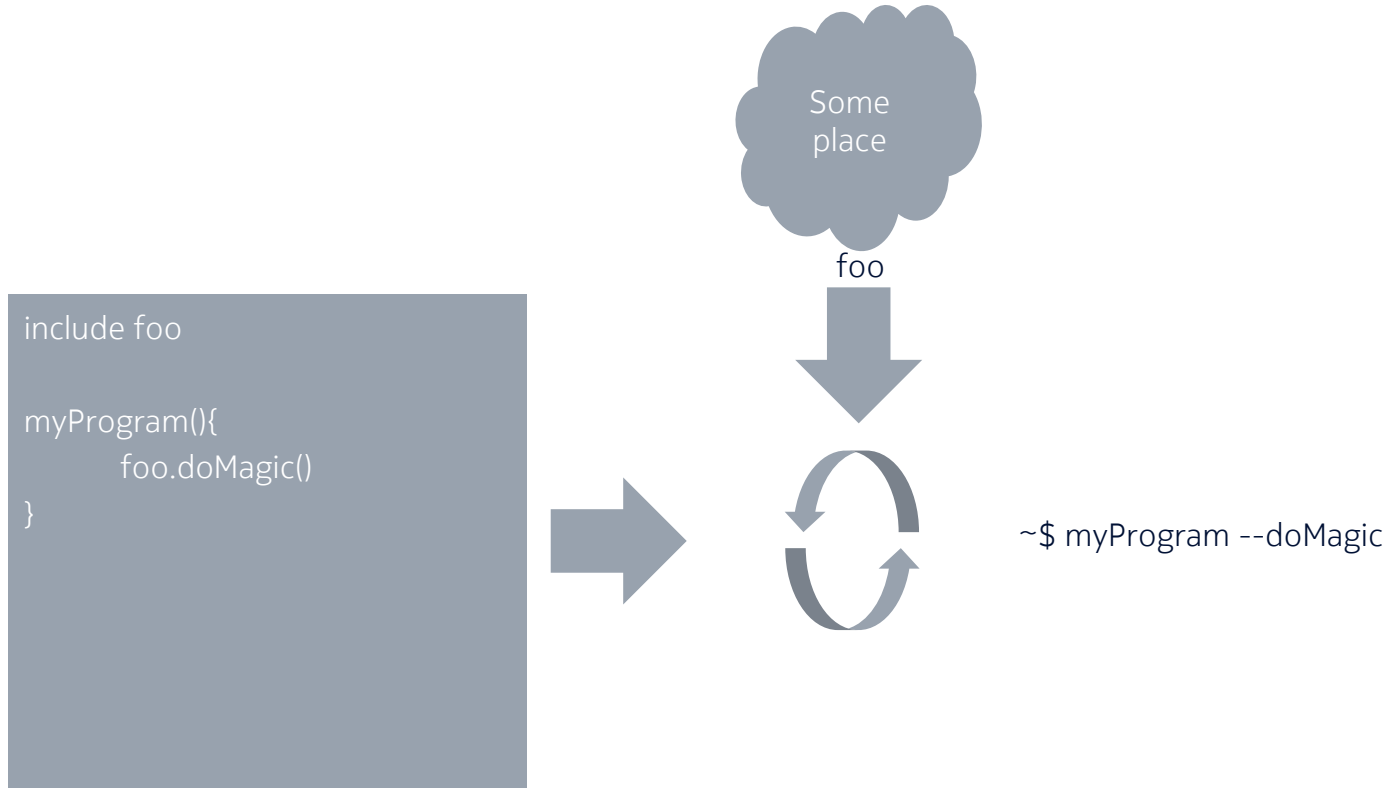
Photo: Gaspard Albert

NOKIA

# What is what – open source

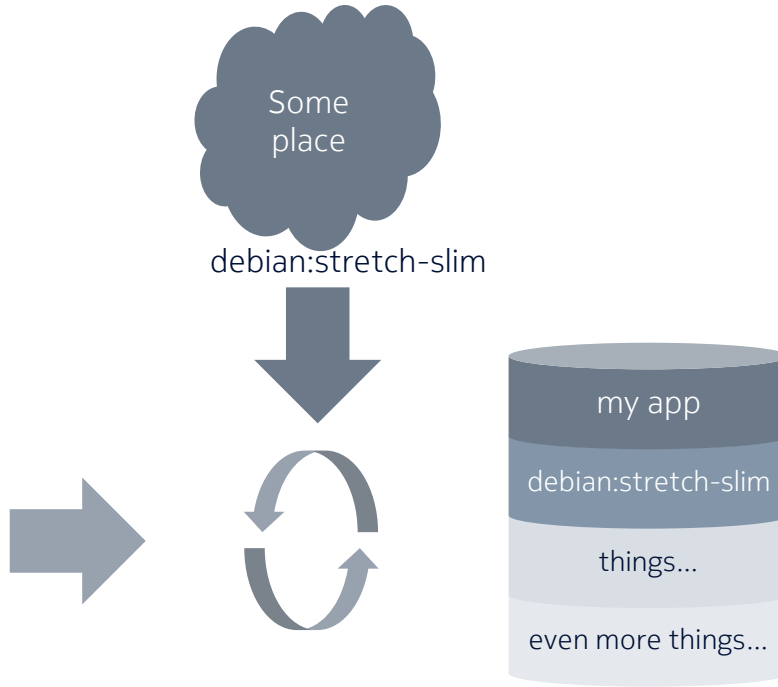


# What is what – modern programming language

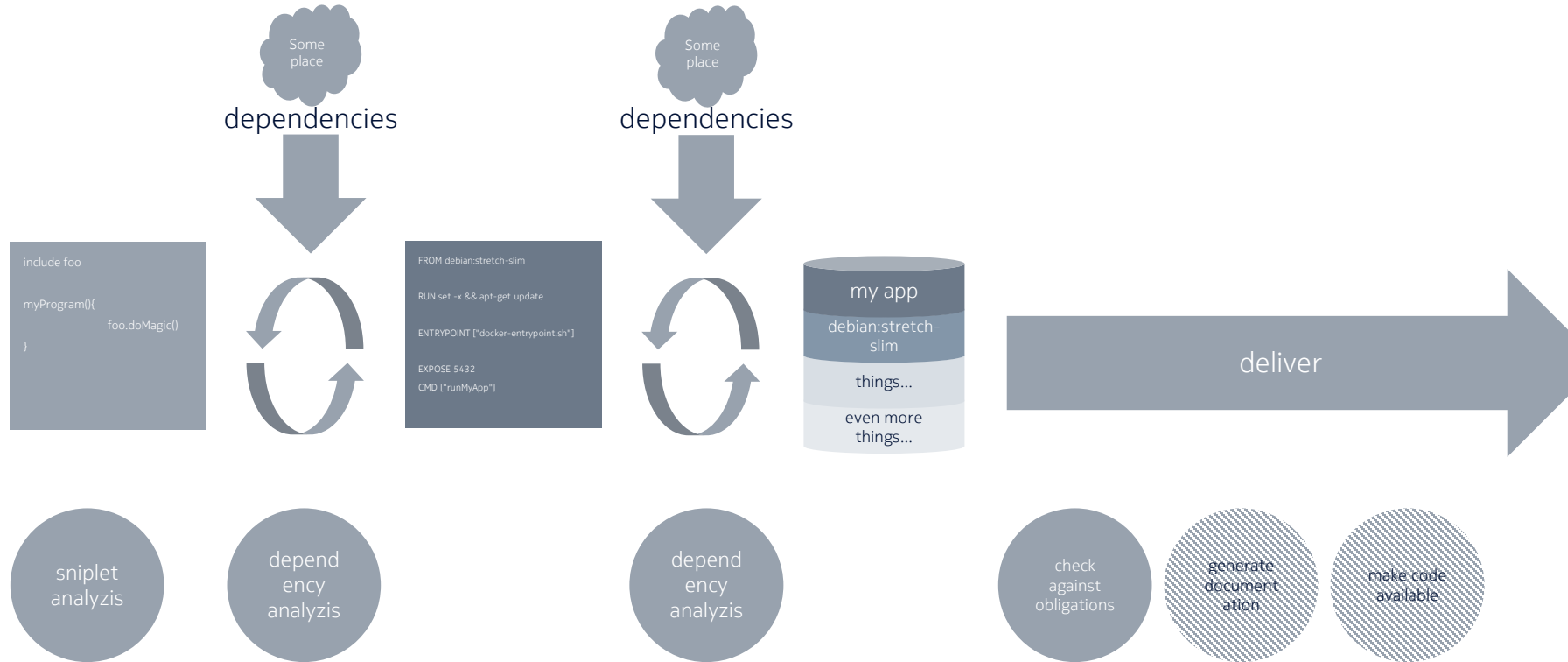


# What is what – container image

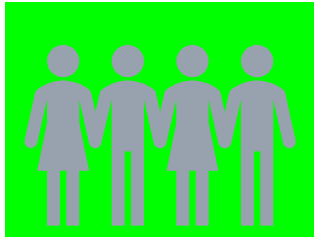
```
FROM debian:stretch-slim  
  
RUN set -x && apt-get update  
  
ENTRYPOINT ["docker-  
entrypoint.sh"]  
  
EXPOSE 5432  
CMD ["runMyApp"]
```



# Ideal open source compliance checking process



# Issues and solution alternatives



# Snippet analysis

Issues	Solution alternatives
Code is from diverse sources.	Self declaration. Scanning tool.
Code is with different licenses.	Self declaration. Scanning tool.

snippet  
analysis

depend  
ency  
analysis

depend  
ency  
analysis

check  
against  
obligations

generate  
document  
ation

make code  
available



# Include dependency analysis

Issues	Solution alternatives
Transitive dependencies are not visible in the requirements file	Package manager must know the dependencies.
Different languages use different package managers	A tool can abstract the package managers.
Licenses are not always available from the package manager tools	Package creators should add the license
Source code link is not available from the package manager tools	Tool support is needed. Package creators should add link to the package

snippet  
analysis

depend  
ency  
analysis

depend  
ency  
analysis

check  
against  
obligations

generate  
document  
ation

make code  
available

# Container image dependency analysis

Issues	Solution alternatives
Content of the container image is not visible	Docker file analyzis, container scanning tools, add list of content as metadata, add spdx document to a well known place to the container, possibility to add license list to Docker hub
Different container images use different base images	Distroless base images, common base images

snippet  
analyzis

depend  
ency  
analyzis

depend  
ency  
analyzis

check  
against  
obligations

generate  
document  
ation

make code  
available

# Check against obligations

Issues	Solution alternatives
Communication method is important for some licenses	Developers can set it, there are defaults, a tool can figure out from the build files
Communicate the decision to the developers	Tool support is needed

snippet  
analysis

depend  
ency  
analysis

depend  
ency  
analysis

check  
against  
obligations

generate  
document  
ation

make code  
available

# Generate documentation

Issues	Solution alternatives
Licenses should be added to the documentation	Tool support is needed

snippet  
analysis

depend  
ency  
analysis

depend  
ency  
analysis

check  
against  
obligations

generate  
document  
ation

make code  
available

# Generate documentation

Issues	Solution alternatives
Link to the code should be provided	Tool support is needed

snippet  
analysis

depend  
ency  
analysis

depend  
ency  
analysis

check  
against  
obligations








generate  
document  
ation

make code  
available




# Solutions and tools

	 FOSSA	 <b>BLACKDUCK</b> by synopsys	 <b>FOSSID</b>	 <b>flexera</b> FlexNet Code Insight	 <b>OSS Review Toolkit</b>	licensed
Code snippet analysis	€	€	€	€	-	-
Abstract package managers	-	€	-	€	+	+
Determine communication method	-	€	-	-	-	-
Integrate to DevOps	CLI	API/CLI	CLI	CLI	CLI	CLI
Generate documentation	€	€	€	€	+	-

# Solutions and tools – package managers domain

	 Python: pip	 Node.js: npm	 Java: Maven	 Java: Gradle	 Rust: Cargo	 Go: go modules	 Ruby: gems
Show dependency tree	pipdeptree	+	+	+	+	+	+
Show licenses	1	license-checker	license-maven-plugin	-	-	?	1
Show code source links	-	license-checker	maven-source-plugin	-	+	?	+

# Solutions and tools – container image domain

	conan	BLACKDUCK BY SYNOPSYS	 docker Trusted Registry	FLEXERA FlexNet Code Insight	 Xray	 docker Hub	distroless
Docker file analysis	+	-	-	€	-	-	n/a
Container image analysis	-	€	+	€	€	+ / 2	n/a
Add license list to docker hub	n/a	n/a	n/a	n/a	n/a	-	n/a
Distroless base images	n/a	n/a	n/a	n/a	n/a	n/a	+





Different technologies

Different tools

Integration

Increasing volume

Automation



Comments, questions?

# References

- [BlackDuck](#)
- [conan](#)
- [Crate](#)
- [distroless](#)
- [Docker Hub](#)
- [Docker Trusted Registry](#)
- [FlexNet Code Insight](#)
- [Fossa](#)
- [Fossid](#)
- [Go modules](#)
- [Gradle](#)
- [Jeff McAffer: Open source license compliance distilled](#)
- [Jfrog Xray](#)
- [licensed](#)
- [license-maven-plugin](#)
- [Maven](#)
- [npm](#)
- [oss-review-toolkit](#)
- [Pypi](#)
- [Ruby Gems](#)

**NOKIA**