Why switch to ScanCode.io as OSS License compliance tools for ONAP’s Dockers.

Alexander Mazuruk (Samsung Electronics)
Mateusz Perc (Samsung Electronics)

Why switch from Tern

Tern seemed like a good option to handle analysis of whole Docker containers at the time (late 2020/ early 2021) when scancode.io was in *very* early stage, yet it last few months it grew to a usable server for automation of software composition analysis with ability to be extended to be a lot more.

Key differences between Tern & Scancode.io

- CLI app designed to gather info on packages in a Docker image & generate SBoM in many formats
- Lack of database- all scan info is kept in single JSON file, breaking Tern when it has scanned too many images.

- Server application with Celery included for worker management making it possible to run it as cloud solution with as many workers as we would have (ability for companies to contribute resources)
- PostgreSQL & SQLite support

ScanCode.io demo

DEMO

Accuracy

TERN

- Unpacks and mounts each layer over previous ones, and queries found package managers
- As accurate as what package maintainers filled in the package

ScanCode

- Scans each layer by parsing files (e.g. package manager data: for alpine info about installed packages can be found in: /lib/apk/db/installed
- Easy to make scans more in-depth

Missing Features - Policies

- - Support policies for Packages
- - Allow policies by license expression
- - Policy overrides on project level (for handling waivers)

Missing Features – Alpine specific (WIP)

- Download package build recipes & sources
- Scan package sources to retrieve License files, Copyright notices, etc. as those are not part of packages
-

Missing features - General

- Resolved license (human input) + resolved license db
- Generate compliance document
- Push artifacts (source code, copyright notices, licenses) as backup
- Publish compliance doc somewhere

How would it integrate in ONAP processes?