Opossum 툴 소개

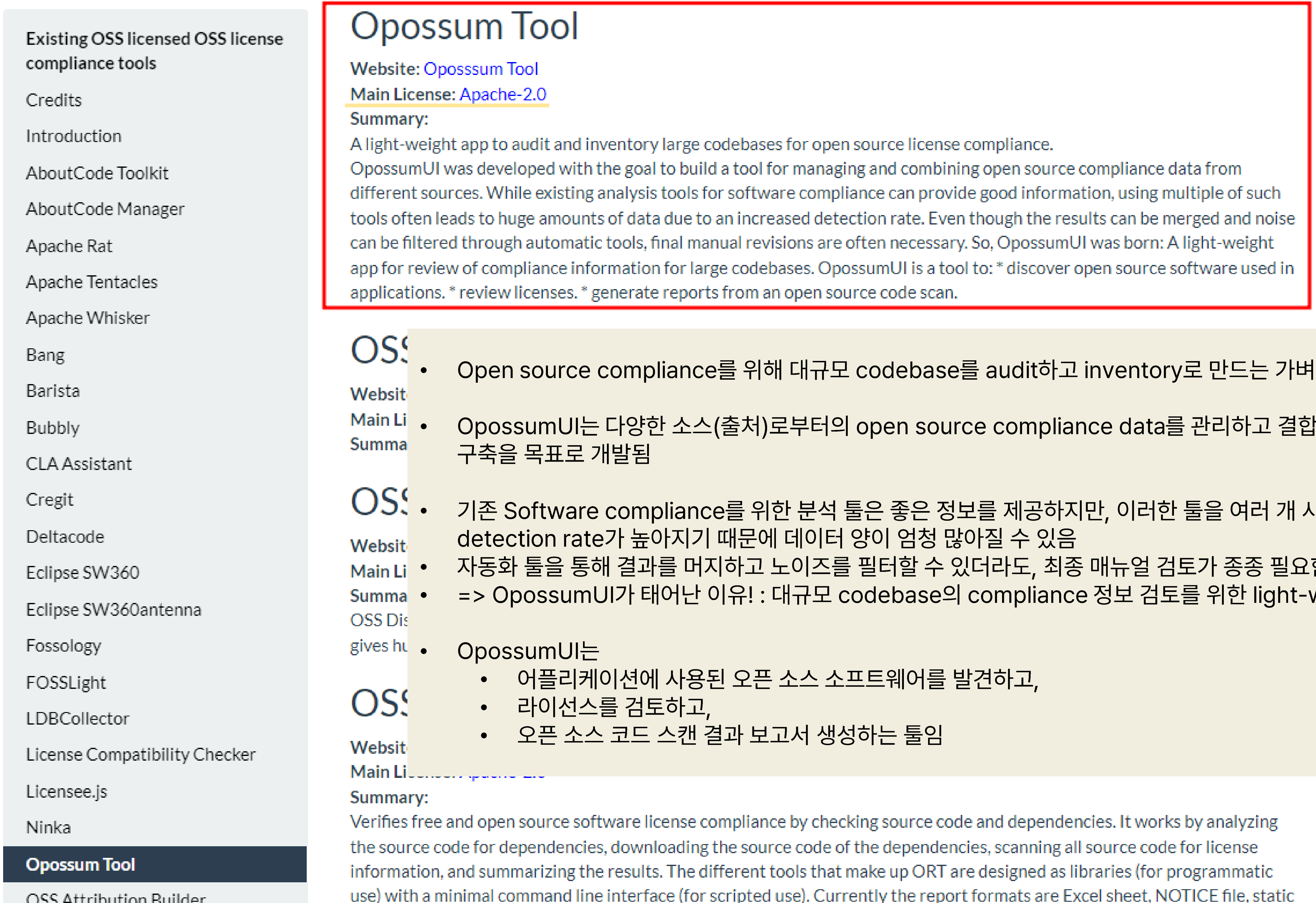
2022. 07. 20

LG전자 석지영

Opossum 툴이란?

- **Open Chain Automation Case Study에서 소개**
  - Part #1 explores a **new graphical tool from Facebook/TNG** to make open source tooling easier to use.
    - https://www.openchainproject.org/featured/2021/09/22/automation-case-study
  - Part #2 explores the engineering behind the new graphical tool from Facebook/TNG that makes open source tooling easier to use.
    - https://www.openchainproject.org/featured/2021/09/29/automation-case-study-2

- **Oss-compliance-tooling 그룹의 OSS-Based-License-Compliance-Tools에 추가**
  - https://oss-compliance-tooling.org/Tooling-Landscape/OSS-Based-License-Compliance-Tools/#opossum-tool



Opossum Tool

Website: Oposssum Tool
Main License: Apache-2.0
Summary:
A light-weight app to audit and inventory large codebases for open source license compliance.
OpossumUI was developed with the goal to build a tool for managing and combining open source compliance data from different sources. While existing analysis tools for software compliance can provide good information, using multiple of such tools often leads to huge amounts of data due to an increased detection rate. Even though the results can be merged and noise can be filtered through automatic tools, final manual revisions are often necessary. So, OpossumUI was born: A light-weight app for review of compliance information for large codebases. OpossumUI is a tool to: * discover open source software used in applications. * review licenses. * generate reports from an open source code scan.

OS

Websit
Main Li
Summa

OS

Websit
Main Li
Summa
OSS Dis
gives hu

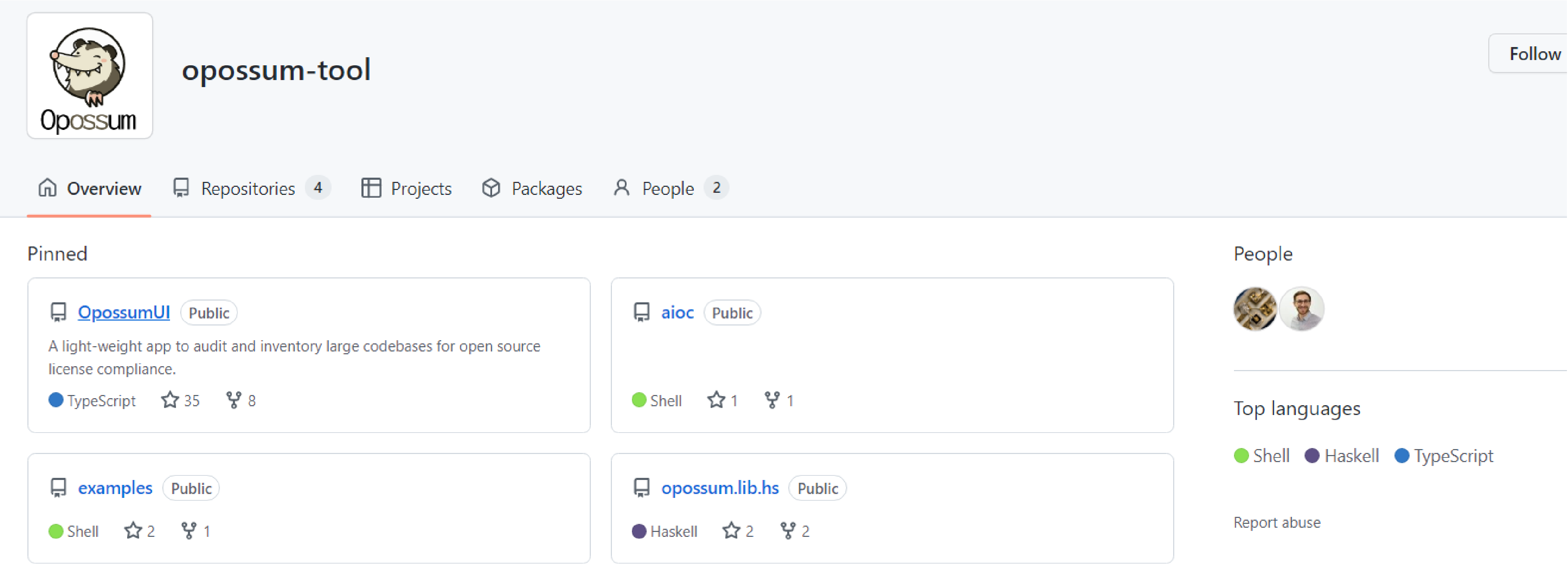
OS

Websit
Main Li
Summary:
Verifies free and open source software license compliance by checking source code and dependencies. It works by analyzing the source code for dependencies, downloading the source code of the dependencies, scanning all source code for license information, and summarizing the results. The different tools that make up ORT are designed as libraries (for programmatic use) with a minimal command line interface (for scripted use). Currently the report formats are Excel sheet, NOTICE file, static

- Open source compliance를 위해 대규모 codebase를 audit하고 inventory로 만드는 가벼운 앱
- OpossumUI는 다양한 소스(출처)로부터의 open source compliance data를 관리하고 결합하기 위한 툴 구축을 목표로 개발됨
- 기존 Software compliance를 위한 분석 툴은 좋은 정보를 제공하지만, 이러한 툴을 여러 개 사용하면 detection rate가 높아지기 때문에 데이터 양이 엄청 많아질 수 있음
- 자동화 툴을 통해 결과를 머지하고 노이즈를 필터할 수 있더라도, 최종 매뉴얼 검토가 종종 필요함
- => OpossumUI가 태어난 이유! : 대규모 codebase의 compliance 정보 검토를 위한 light-weight app
- OpossumUI는
  - 어플리케이션에 사용된 오픈 소스 소프트웨어를 발견하고,
  - 라이선스를 검토하고,
  - 오픈 소스 코드 스캔 결과 보고서 생성하는 툴임

Github Repository

- https://github.com/opossum-tool



opossum-tool

Pinned

OpossumUI Public

A light-weight app to audit and inventory large codebases for open source license compliance.

● TypeScript ☆ 35 ⑂ 8

aioc Public

● Shell ☆ 1 ⑂ 1

examples Public

● Shell ☆ 2 ⑂ 1

opossum.lib.hs Public

● Haskell ☆ 2 ⑂ 2

People

Top languages

● Shell ● Haskell ● TypeScript

Report abuse

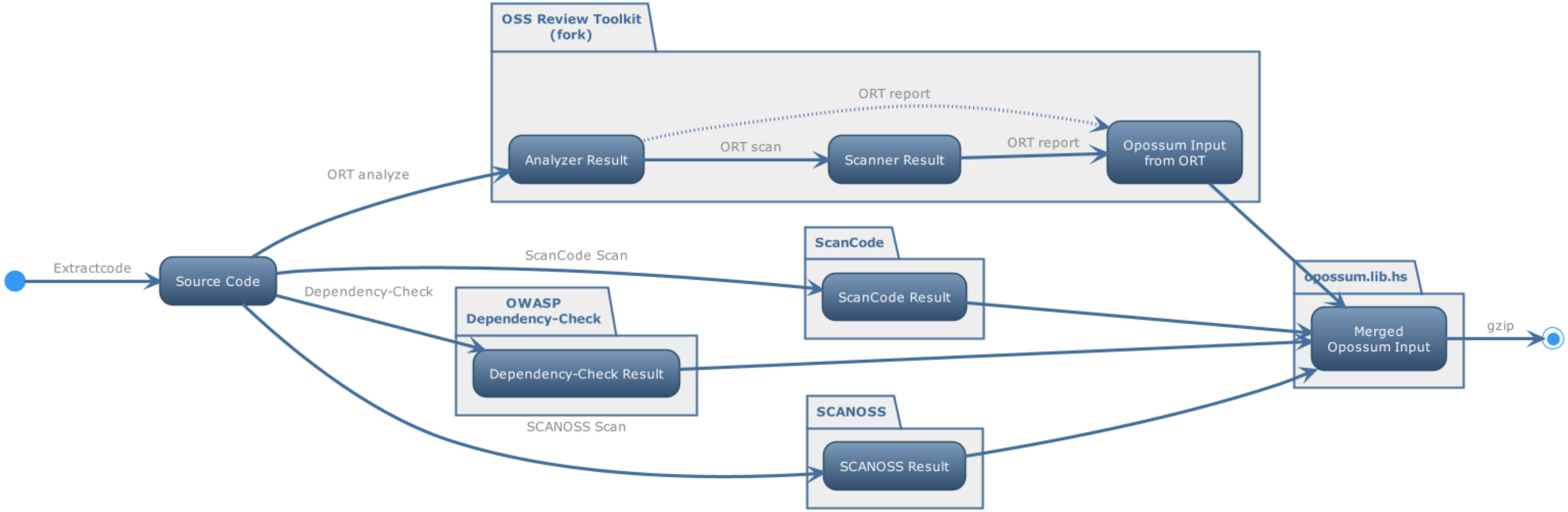
aioc

- all in one container

aioc란?

- …
- OpossumUI는 다양한 소스(출처)로부터의 open source compliance data를 관리하고 결합하기 위한 툴 구축을 목표로 개발됨
- …

- **Docker pipeline에서 다양한 open source compliance 툴** (OSS Review Toolkit, ScanCode, OWASP Dependency-check, SCANOSS)**를 사용해 소스 디렉토리를 스캔함**
- **스캔 결과들은 opossum.lib.hs 툴을 통해 단일 OpossumUI input 파일로 병합됨**



aioc scanners

- **OSS Review Toolkit** (https://github.com/oss-review-toolkit/ort)
    - Analzyer(각 dependency의 소스코드에 대해 scancode를 통해 소스 분석), scanner(Scancode 이용) 수행

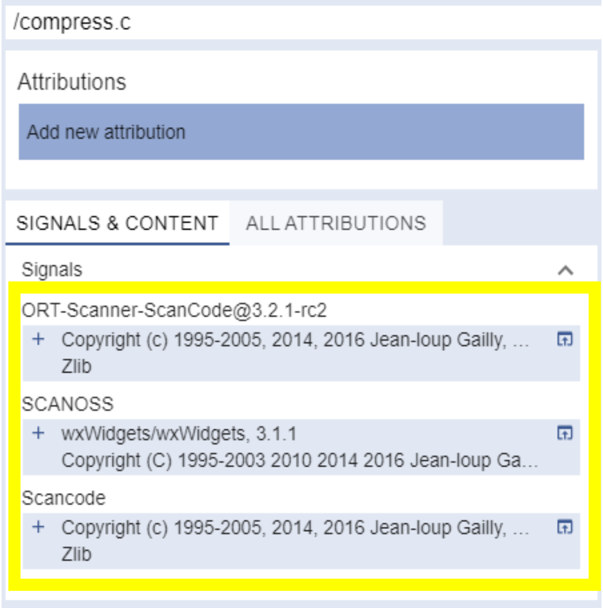
- **ScanCode** (https://github.com/nexB/scancode-toolkit/)
    - String match를 통해 license명, copyright 검출

- **OWASP Dependency-Check** (https://owasp.org/www-project-dependency-check/)
    - Dependency에 대해 vulnerability 검출
    - aioc에서는 dependency 결과 evidence로만 사용

- **SCANOSS** (https://github.com/scanoss/scanner.c)
    - 파일 fingerprint 생성하여 OSSKB API를 통해 OSSKB와 매칭된 결과 보여줌
        - *OSSKB : Open source database, Component(OSS) / Source Code(file) / Snipper에 대한 정보 포함하고 있음
    - OSS name, version 정보 얻을 수 있음

aioc 특징

- **Docker 이미지 빌드 후 실행 가능**
- **장점**
  - 소스 디렉토리에 대해 도커 이미지 한번 실행으로 쉽게 다양한 스캐너 실행 가능함
  - aioc를 통해 OpossumUI에서 하나의 파일당 다양한 evidence 추출 가능함



/compress.c

ORT-Scanner-ScanCode@3.2.1-rc2
+ Copyright (c) 1995-2005, 2014, 2016 Jean-loup Gailly, ...
Zlib

SCANOSS
+ wxWidgets/wxWidgets, 3.1.1
Copyright (C) 1995-2003 2010 2014 2016 Jean-loup Ga...

Scancode
+ Copyright (c) 1995-2005, 2014, 2016 Jean-loup Gailly, ...
Zlib

- **단점**
  - 실행 속도 느림
  - 다양한 스캐너 실행 결과 중 ORT 소스 Scanner(Scancode), Scancode 소스코드 분석 중복되어 표시됨

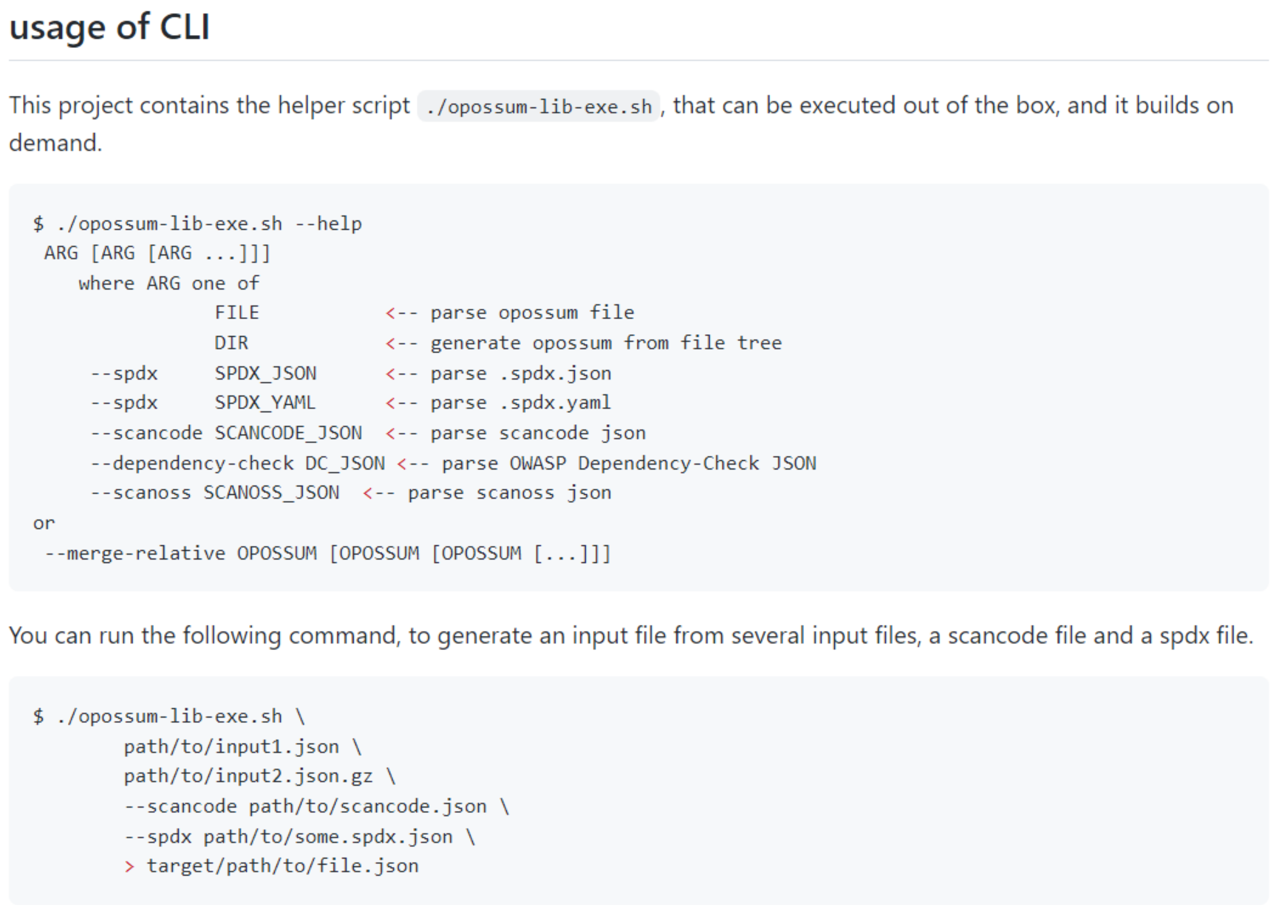
opossum.lib.hs

opOSSum-lib

- OpossumUI input 생성을 위한 helper library
- License : BSD-3-Clause

- Input 파일 양식
  - Opossum input json
  - SPDX-2.2 json / yaml
  - ScanCode json
  - OWASP Dependency-Check json

* ORT는 툴에서 자체적으로 Opossum input 양식에 맞춰
json / yaml 결과 파일 생성함 (-f option : opossum)



usage of CLI

This project contains the helper script `./opossum-lib-exe.sh`, that can be executed out of the box, and it builds on demand.

```
$ ./opossum-lib-exe.sh --help
 ARG [ARG [ARG ...]]]
    where ARG one of
                FILE           <-- parse opossum file
                DIR            <-- generate opossum from file tree
     --spdx      SPDX_JSON      <-- parse .spdx.json
     --spdx      SPDX_YAML      <-- parse .spdx.yaml
     --scancode SCANCODE_JSON  <-- parse scancode json
     --dependency-check DC_JSON <-- parse OWASP Dependency-Check JSON
     --scanoss SCANOSS_JSON  <-- parse scanoss json
or
 --merge-relative OPOSSUM [OPOSSUM [OPOSSUM [...]]]
```

You can run the following command, to generate an input file from several input files, a scancode file and a spdx file.

```
$ ./opossum-lib-exe.sh \
        path/to/input1.json \
        path/to/input2.json.gz \
        --scancode path/to/scancode.json \
        --spdx path/to/some.spdx.json \
        > target/path/to/file.json
```

OpossumUI

OpossumUI

- …
- OpossumUI는
  - 어플리케이션에 사용된 오픈 소스 소프트웨어를 발견하고,
  - 라이선스를 검토하고,
  - 오픈 소스 코드 스캔 결과 보고서 생성하는 툴임

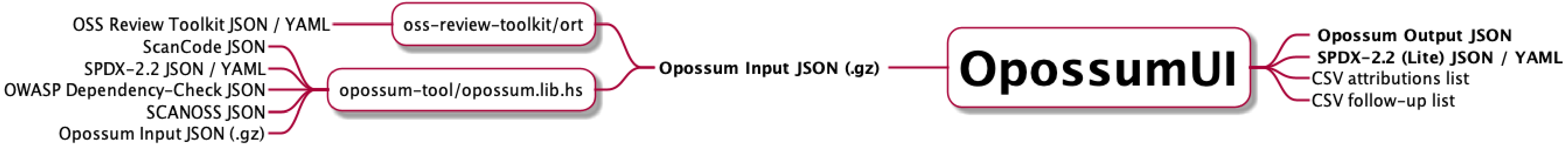
- **Features**
  - 다양한 scanner 사용
    - 현재 ORT, FOSSLight, Scancode와 integrate되어 있음
  - Scanner evidence 브라우징을 위한 통합 인터페이스
  - 코드베이스의 파일 트리를 통한 간단한 내비게이션 기능
  - 각 파일 또는 그룹별 attribution 생성 가능

- **Linux, macOS, Windows 앱 이미지 제공**
  - Github Repository Release에서 다운로드 가능 (https://github.com/opossum-tool/OpossumUI/releases/latest)
  - Chromium 기반 application

- **다양한 오픈 소스 스캐너 결과를 빠르고 쉬운 방법으로 사용할 수 있도록 하는 UI 툴**

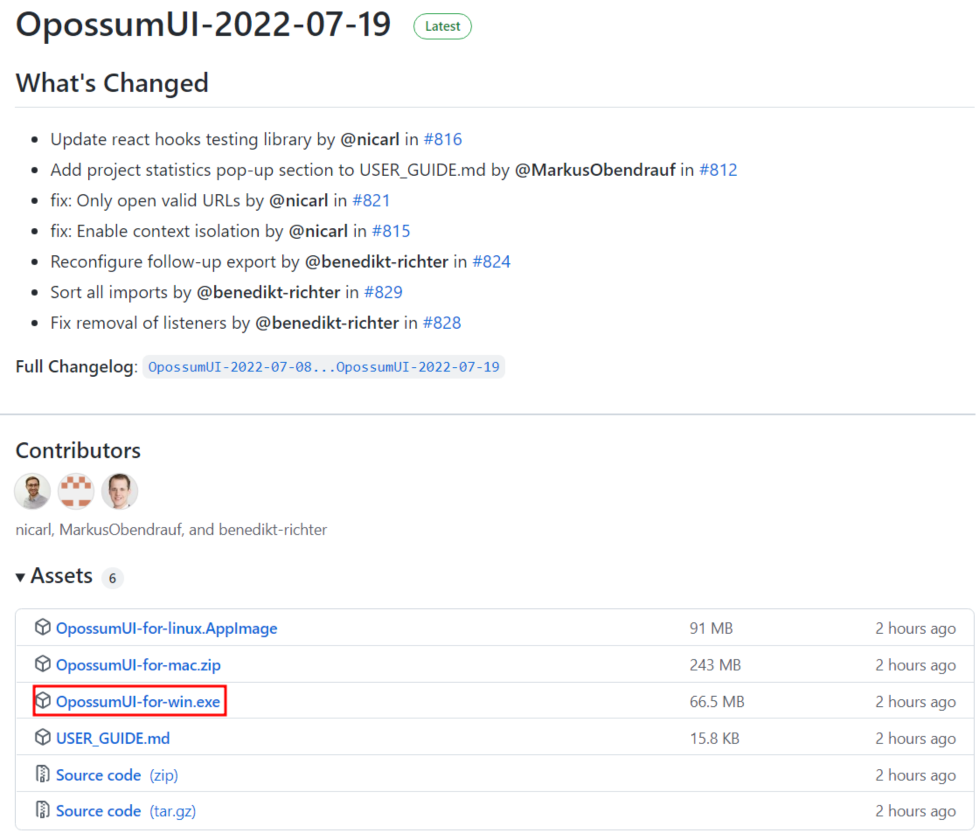
OpossumUI Export options

- **Default output file** : raw data json 파일
- **SPDX documents**
  - SpdxVersion : 2.2, json / yaml 양식
- **BOM-like CSV files**
  - Compact component list
    - package name, version, license name, copyright, url
  - Detailed component list
    - package name, version, license name, copyright, url, package namespace(ex: @babel), package type(ex: npm), purl(ex: pkg:npm/heap@0.2.6), license text
- **follow-up document**
  - follow-up 체크박스 선택한 component list



OpossumUI demo

- https://github.com/opossum-tool/OpossumUI/releases
    - OpossumUI-for-win.exe 다운로드



OpossumUI-2022-07-19 Latest

What's Changed

- Update react hooks testing library by **@nicarl** in #816
- Add project statistics pop-up section to USER_GUIDE.md by **@MarkusObendrauf** in #812
- fix: Only open valid URLs by **@nicarl** in #821
- fix: Enable context isolation by **@nicarl** in #815
- Reconfigure follow-up export by **@benedikt-richter** in #824
- Sort all imports by **@benedikt-richter** in #829
- Fix removal of listeners by **@benedikt-richter** in #828

Full Changelog: `OpossumUI-2022-07-08...OpossumUI-2022-07-19`

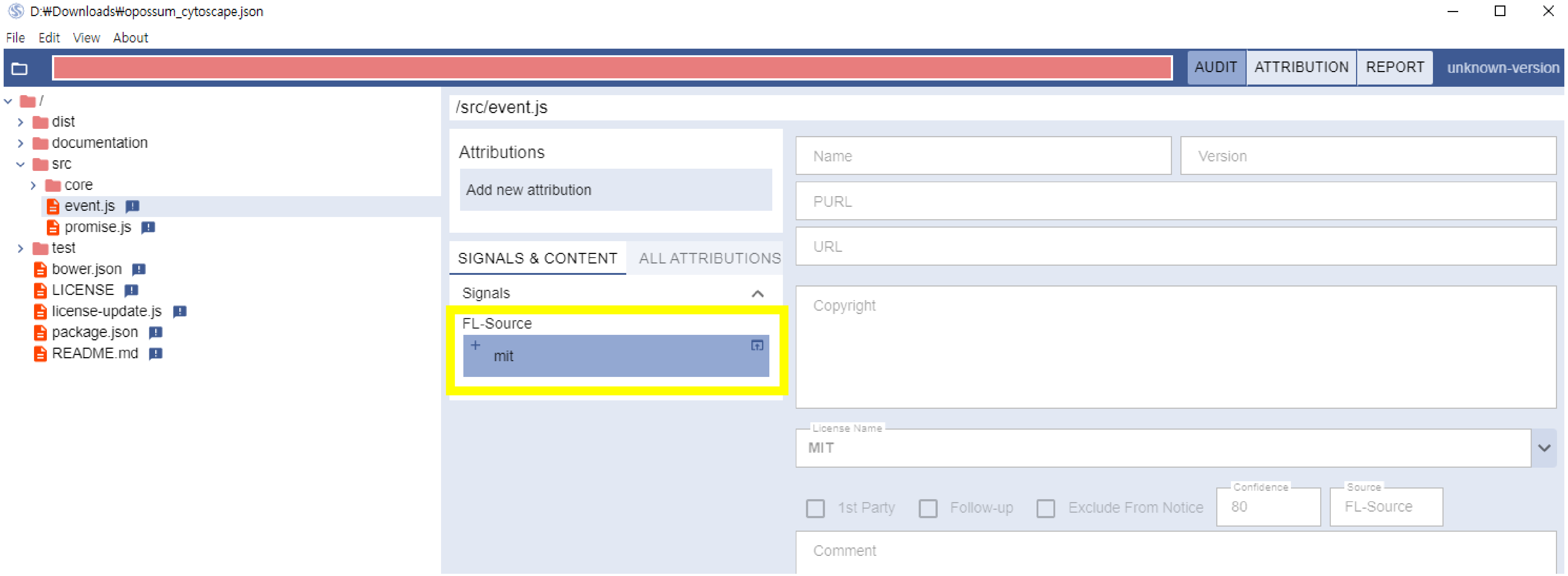
Contributors

nicarl, MarkusObendrauf, and benedikt-richter

▾ Assets 6

OpossumUI-for-linux.AppImage	91 MB	2 hours ago
OpossumUI-for-mac.zip	243 MB	2 hours ago
OpossumUI-for-win.exe	66.5 MB	2 hours ago
USER_GUIDE.md	15.8 KB	2 hours ago
Source code (zip)		2 hours ago
Source code (tar.gz)		2 hours ago

OpossumUI with FOSSLight Scanner



D:₩Downloads₩opossum_cytoscape.json

/src/event.js

Name:

Version:

PURL:

URL:

Copyright:

License Name: MIT

□ 1st Party □ Follow-up □ Exclude From Notice

Confidence: 80

Source: FL-Source

Comment:

Q&A