

# FOSSLight Scanner for 뉴비

LG전자 Open Source Task 석지영



# CONTENTS

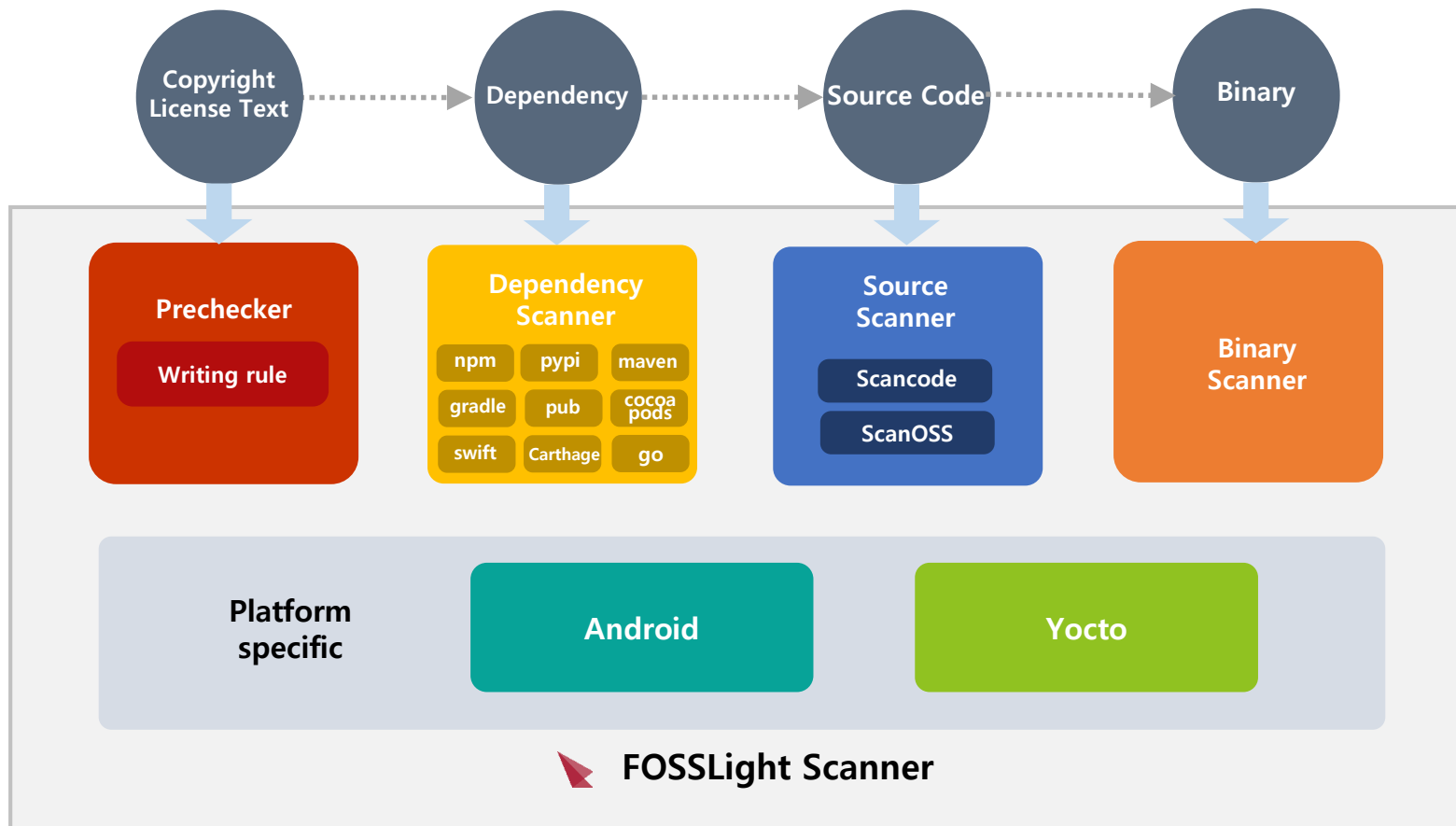
---

- FOSSLight Scanner 소개
- 설치 방법
- 각 Scanner별 상세 설명
- 시연

# FOSSLight Scanner

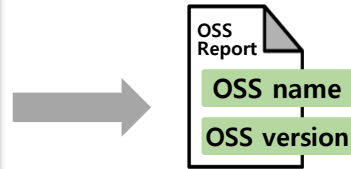
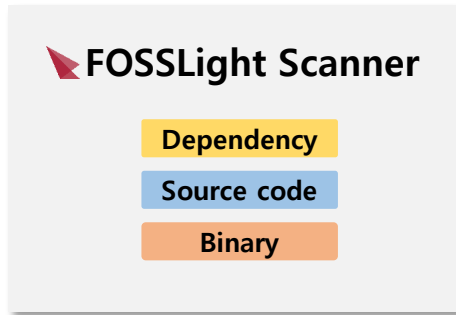
---

# FOSSLight Scanner



# FOSSLight Scanner를 통한 SBOM 생성

- FOSSLight Scanner 실행하여 오픈소스 분석 보고서 생성



	Source Name or Path	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Tex	Exclude	Comment	Dependencie
1	package.json	npm:lge-example	1.0.0	Apache-2.0	<a href="https://github.com/LGE-OSS/example">https://github.com/LGE-OSS/example</a>	<a href="https://www.npmjs.com/package/lge-example">https://www.npmjs.com/package/lge-example</a>			root packe	npm:copy-
2	package.json	npm:copy-anything	2.0.6	MIT	<a href="https://github.com/mesqueeb/copy-anything">https://github.com/mesqueeb/copy-anything</a>	<a href="https://www.npmjs.com/package/copy-anything">https://www.npmjs.com/package/copy-anything</a>			direct	npm:is-wha
3	package.json	npm:is-what	3.14.1	MIT	<a href="https://github.com/mesqueeb/is-what">https://github.com/mesqueeb/is-what</a>	<a href="https://www.npmjs.com/package/is-what">https://www.npmjs.com/package/is-what</a>			transitive	
4	requirements.txt	pypi:CacheControl	0.12.11	Apache Software License	<a href="https://pypi.org/project/CacheControl/0.12.11">https://pypi.org/project/CacheControl/0.12.11</a>	<a href="https://github.com/ionrock/cachecontrol">https://github.com/ionrock/cachecontrol</a>			transitive	pypi:msgpac
5	requirements.txt	pypi:Deprecated	1.2.14	MIT License	<a href="https://pypi.org/project/Deprecated/1.2.14">https://pypi.org/project/Deprecated/1.2.14</a>	<a href="https://github.com/tantale/deprecated">https://github.com/tantale/deprecated</a>			transitive	pypi:wrapt(
6	requirements.txt	pypi:Jinja2	3.1.2	BSD License	<a href="https://pypi.org/project/Jinja2/3.1.2">https://pypi.org/project/Jinja2/3.1.2</a>	<a href="https://palletsprojects.com/p/jinja/">https://palletsprojects.com/p/jinja/</a>			transitive	pypi:Marku
7	requirements.txt	pypi:MarkupSafe	2.1.3	BSD License	<a href="https://pypi.org/project/MarkupSafe/2.1.3">https://pypi.org/project/MarkupSafe/2.1.3</a>	<a href="https://palletsprojects.com/p/markupsafe/">https://palletsprojects.com/p/markupsafe/</a>			transitive	
8	requirements.txt	pypi:PyGithub	2.1.1	GNU Library or Lesser Gen	<a href="https://pypi.org/project/PyGithub/2.1.1">https://pypi.org/project/PyGithub/2.1.1</a>	<a href="https://github.com/pygithub/pygithub">https://github.com/pygithub/pygithub</a>			transitive	pypi:Depre
9	requirements.txt	pypi:PyJWT	2.8.0	MIT License	<a href="https://pypi.org/project/PyJWT/2.8.0">https://pypi.org/project/PyJWT/2.8.0</a>	<a href="https://github.com/jpadilla/pyjwt">https://github.com/jpadilla/pyjwt</a>			transitive	
10	requirements.txt	pypi:PyNaCl	1.5.0	Apache License 2.0	<a href="https://pypi.org/project/PyNaCl/1.5.0">https://pypi.org/project/PyNaCl/1.5.0</a>	<a href="https://github.com/pyca/pynacl">https://github.com/pyca/pynacl</a>			transitive	pypi:cffi(1.1
11	requirements.txt	pypi:PyYAML	6.0.1	MIT License	<a href="https://pypi.org/project/PyYAML/6.0.1">https://pypi.org/project/PyYAML/6.0.1</a>	<a href="https://pyyaml.org/">https://pyyaml.org/</a>			transitive	
12	requirements.txt	pypi:XlsxWriter	3.1.8	BSD License	<a href="https://pypi.org/project/XlsxWriter/3.1.8">https://pypi.org/project/XlsxWriter/3.1.8</a>	<a href="https://github.com/jmcnamara/XlsxWriter">https://github.com/jmcnamara/XlsxWriter</a>			transitive	
13	requirements.txt	pypi:appdirs	1.4.4	MIT License	<a href="https://pypi.org/project/appdirs/1.4.4">https://pypi.org/project/appdirs/1.4.4</a>	<a href="http://github.com/ActiveState/appdirs">http://github.com/ActiveState/appdirs</a>			transitive	
14	requirements.txt	pypi:attrs	23.1.0	MIT License	<a href="https://pypi.org/project/attrs/23.1.0">https://pypi.org/project/attrs/23.1.0</a>	<a href="https://www.attrs.org/en/stable/changelog.html">https://www.attrs.org/en/stable/changelog.html</a>			transitive	
15	requirements.txt	pypi:beautifulsoup4	4.12.2	MIT License	<a href="https://pypi.org/project/beautifulsoup4/4.12.2">https://pypi.org/project/beautifulsoup4/4.12.2</a>	<a href="https://www.crummy.com/software/BeautifulSoup/bs4/">https://www.crummy.com/software/BeautifulSoup/bs4/</a>			transitive	pypi:soups
16	requirements.txt	pypi:binaryornot	0.4.4	BSD License	<a href="https://pypi.org/project/binaryornot/0.4.4">https://pypi.org/project/binaryornot/0.4.4</a>	<a href="https://github.com/audreyr/binaryornot">https://github.com/audreyr/binaryornot</a>			transitive	pypi:charde
17	requirements.txt	pypi:boolean.py	4.0	BSD-2-Clause	<a href="https://pypi.org/project/boolean.py/4.0">https://pypi.org/project/boolean.py/4.0</a>	<a href="https://github.com/bastikr/boolean.py">https://github.com/bastikr/boolean.py</a>			transitive	
18	requirements.txt	pypi:certifi	2023.7.22	Mozilla Public License 2.0	<a href="https://pypi.org/project/certifi/2023.7.22">https://pypi.org/project/certifi/2023.7.22</a>	<a href="https://github.com/certifi/python-certifi">https://github.com/certifi/python-certifi</a>			transitive	
19	requirements.txt	pypi:cffi	1.16.0	MIT License	<a href="https://pypi.org/project/cffi/1.16.0">https://pypi.org/project/cffi/1.16.0</a>	<a href="http://cffi.readthedocs.org">http://cffi.readthedocs.org</a>			transitive	pypi:pycpai
20	requirements.txt	pypi:chardet	5.2.0	GNU Lesser General Public	<a href="https://pypi.org/project/chardet/5.2.0">https://pypi.org/project/chardet/5.2.0</a>	<a href="https://github.com/chardet/chardet">https://github.com/chardet/chardet</a>			transitive	

# FOSSLight Scanner 설치 방법

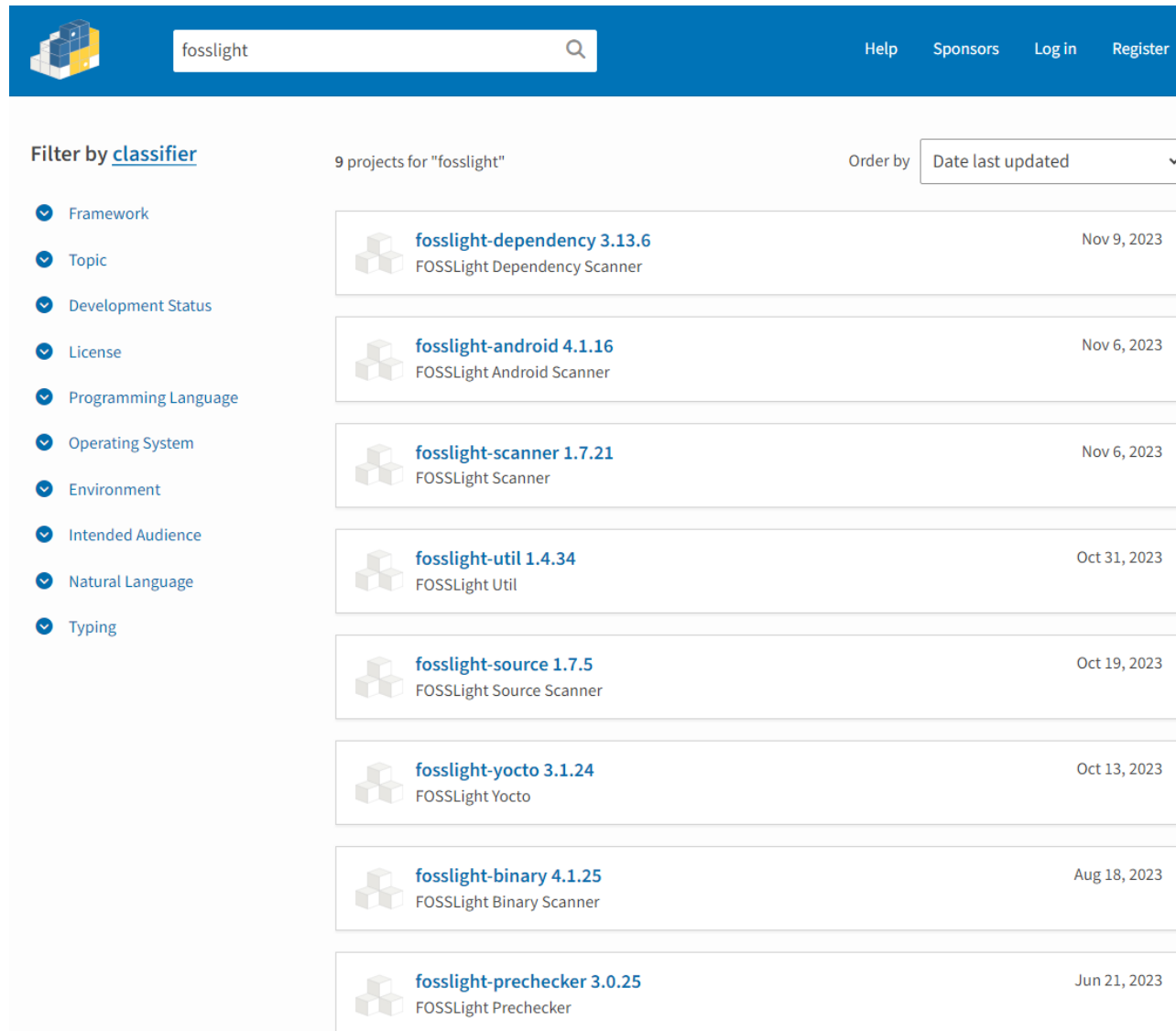
---

# FOSSLight Scanner 설치

	Ubuntu	Windows	MacOS
실행 파일 (.exe)	FOSSLight Binary Scanner	FOSSLight Binary Scanner, FOSSLight Dependency Scanner	FOSSLight Binary Scanner
PyPI 패키지	전체 Scanner 지원		

- 실행 파일
  - FOSSLight Dependency Scanner (Windows만 가능)
    - [https://github.com/fosslight/fosslight\\_dependency\\_scanner/releases](https://github.com/fosslight/fosslight_dependency_scanner/releases)
  - FOSSLight Binary Scanner (Ubuntu, MacOS, Windows 가능)
    - [https://github.com/fosslight/fosslight\\_binary\\_scanner/releases](https://github.com/fosslight/fosslight_binary_scanner/releases)

# FOSSLight Scanner PyPI 패키지



The screenshot shows the FOSSLight PyPI package search results for the query 'fosslight'. The page features a blue header with the FOSSLight logo, a search bar containing 'fosslight', and navigation links for Help, Sponsors, Log in, and Register. Below the header, there is a filter section on the left with a 'Filter by classifier' dropdown menu. The main content area displays 9 projects for 'fosslight', ordered by 'Date last updated'. Each project entry includes a small cube icon, the project name and version, a brief description, and the last update date.

Project Name	Description	Last Updated
fosslight-dependency 3.13.6	FOSSLight Dependency Scanner	Nov 9, 2023
fosslight-android 4.1.16	FOSSLight Android Scanner	Nov 6, 2023
fosslight-scanner 1.7.21	FOSSLight Scanner	Nov 6, 2023
fosslight-util 1.4.34	FOSSLight Util	Oct 31, 2023
fosslight-source 1.7.5	FOSSLight Source Scanner	Oct 19, 2023
fosslight-yocto 3.1.24	FOSSLight Yocto	Oct 13, 2023
fosslight-binary 4.1.25	FOSSLight Binary Scanner	Aug 18, 2023
fosslight-prechecker 3.0.25	FOSSLight Prechecker	Jun 21, 2023



# FOSSLight Scanner 패키지 설치 전 요구사항

## 1. Python 설치

- 지원 Python 버전 : 3.8 ~ 3.11
- 권장 버전 : 3.10

## 2. Virtualenv 환경 설치(권장)

- 시스템에 설치된 python에 영향을 주지 않고 새로운 python 가상 환경 세팅 가능
- 추가로 패키지를 설치해도 기존 시스템에 영향을 주지 않음

### ❖ FOSSLight Binary Scanner의 경우

- jar 파일에 대한 분석을 위해, Java 설치 권장 (Open Source JDK 설치)  
<https://learn.microsoft.com/ko-kr/java/openjdk/download> (권장 버전 : 11)

### ❖ FOSSLight Dependency Scanner의 경우

- 각 package manager를 이용한 개발 환경과 동일한 빌드 환경 설정이 필요함  
(ex. npm dependency 분석 수행을 위해 npm 빌드 도구 서버 내 설치 필요)

# FOSSLight Scanner 패키지 설치 방법 (Ubuntu)

- Python 3.10 필수 패키지 설치

```
$ sudo apt-get update  
$ sudo apt-get install python3.10 python3.10-dev python3.10-distutils  
python3-pip
```

- Virtualenv 설치 및 활성화

```
$ pip install virtualenv  
$ virtualenv -p /usr/bin/python3.10 venv  
$ source venv/bin/activate
```

# FOSSLight Scanner 패키지 설치 방법 (MacOS)

- 사전 필수 패키지 설치

```
% brew install openssl  
% brew install libmagic  
% brew install postgresql
```

# FOSSLight Scanner 패키지 설치 방법 (Windows)

- Python 설치

- <https://www.python.org/downloads/windows/>
- 지원 Python 버전 : 3.8 ~ 3.11
- 권장 버전 : 3.10

- Microsoft Visual C++ 14.0 이상 버전 다운로드

- <https://visualstudio.microsoft.com/visual-cpp-build-tools/> 에서 build tools > C++를 사용한 데스크톱 개발  
체크 후 설치

# FOSSLight Scanner 설치

- Pip 설치 명령어를 통해 바로 설치 가능

```
$ pip install fosslight_scanner
```

- 여러 FOSSLight Scanner 한 번에 설치 가능

- FOSSLight Dependency Scanner
- FOSSLight Source Scanner
- FOSSLight Binary Scanner
- FOSSLight Prechecker

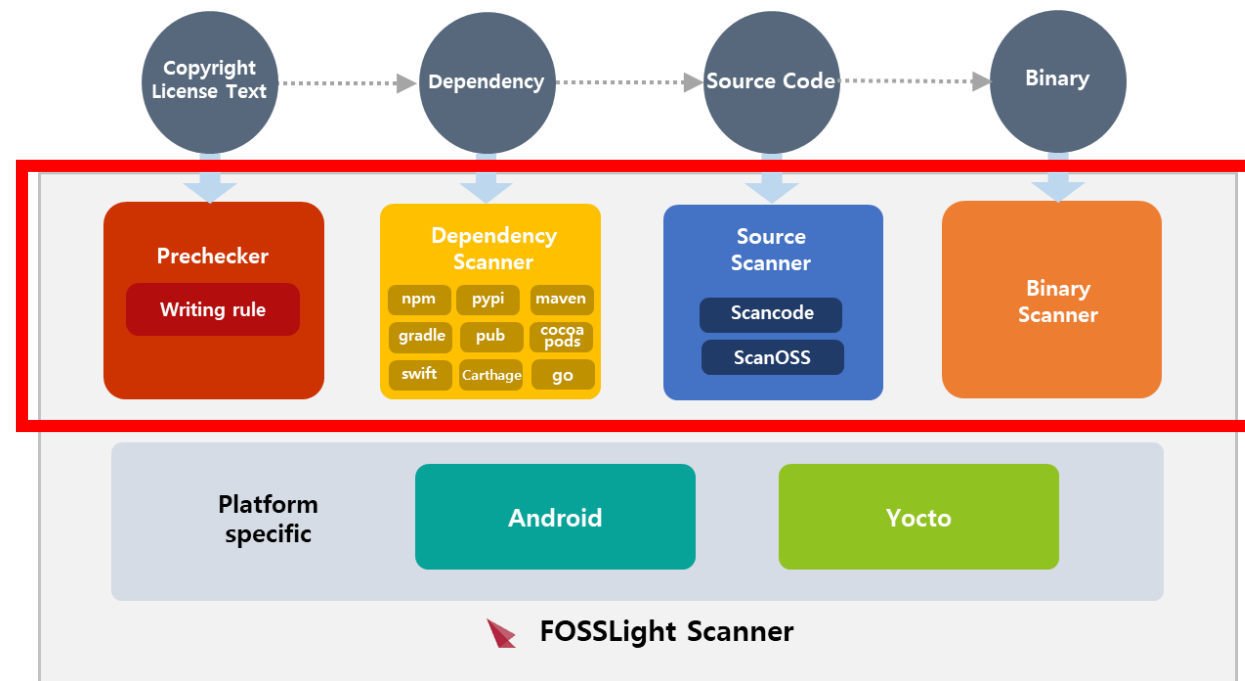
- ❖ FOSSLight Android Scanner, FOSSLight Yocto Scanner의 경우

- 별도로 설치해야 함 (\$ pip install fosslight\_android / \$ pip install fosslight\_yocto)

# FOSSLight Scanner 사용 방법

# FOSSLight Scanner

- FOSSLight Scanner를 하나로 합친 Scanner
  - FOSSLight Prechecker
  - FOSSLight Dependency Scanner
  - FOSSLight Source Scanner
  - FOSSLight Binary Scanner



- 특정 Path 또는 다운로드 받을 수 있는 링크에 대해 Open Source 분석을 수행하고, FOSSLight Report를 출력하는 도구

# FOSSLight Scanner

- 실행 방법

```
$ fosslight [Mode] [option1] <arg1> [option2] <arg2>
```

```
Parameters:
  Mode
    all           Run all scanners(Default)
    source        Run FOSSLight Source Scanner
    dependency    Run FOSSLight Dependency Scanner
    binary        Run FOSSLight Binary Scanner
    prechecker    Run FOSSLight Prechecker
    compare       Compare two FOSSLight reports

  Options:
    -h           Print help message
    -p <path>   Path to analyze (ex, -p {input_path})
                * Compare mode input file: Two FOSSLight reports (supports excel, yaml)
                (ex, -p {before_name}.xlsx {after_name}.xlsx)
    -w <link>   Link to be analyzed can be downloaded by wget or git clone
    -f <format> FOSSLight Report file format (excel, yaml)
                * Compare mode result file: supports excel, json, yaml, html
    -o <output> Output directory or file
    -c <number> Number of processes to analyze source
    -r           Keep raw data
    -t           Hide the progress bar
    -v           Print FOSSLight Scanner version

  Options for only 'all' or 'bin' mode
    -u <db_url> DB Connection(format : 'postgresql://username:password@host:port/database_name')

  Options for only 'all' or 'dependency' mode
    -d <dependency_argument> Additional arguments for running dependency analysis
```



# FOSSLight Scanner – 실행 모드 선택

```
Parameters:
Mode
all          Run all scanners(Default)
source      Run FOSSLight Source Scanner
dependency  Run FOSSLight Dependency Scanner
binary      Run FOSSLight Binary Scanner
prechecker  Run FOSSLight Prechecker
compare     Compare two FOSSLight reports
```

## 분석

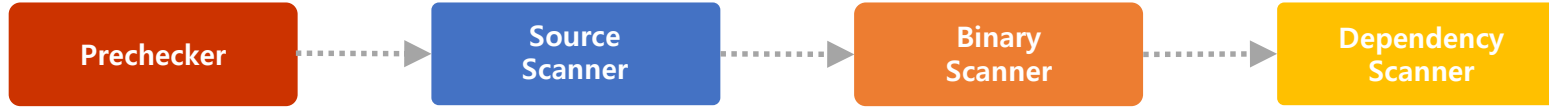
오픈 소스 분석

툴을 선택하여  
실행 가능

## Compare

BOM (FOSSLight  
Report) 비교 가능

# FOSSLight Scanner – 분석 all 모드 (default)



## • 실행 방법

```
$ fosslight all -p test_oss/
```

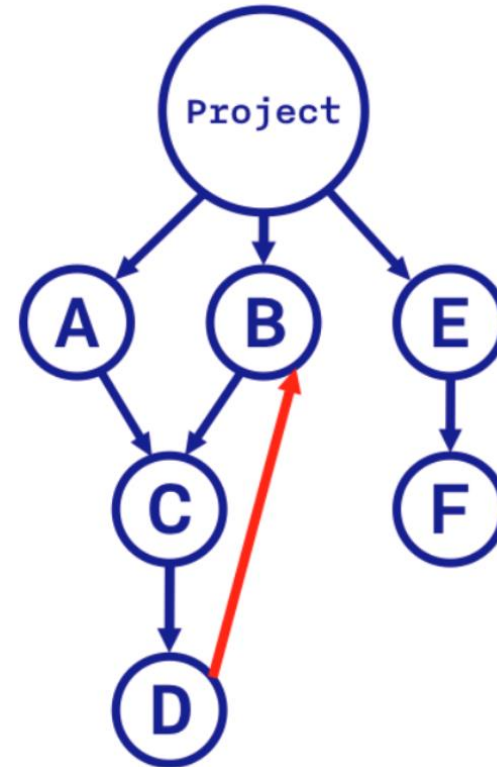
## • 실행 결과

### • FOSSLight Report : Dependency, Source, Binary 분석 결과

22	requireme	pypi:impor	5.12.0	Apache-2.	<a href="https://pypi.org/project/python-importlib-metadata/">https://pypi.org/project/python-importlib-metadata/</a>	<a href="https://github.com/python/importlib-metadata">https://github.com/python/importlib-metadata</a>	transitive
23	requireme	pypi:jsonm	1.9.0	MIT	<a href="https://pypi.org/project/jsonmerge/1.9.0">https://pypi.org/project/jsonmerge/1.9.0</a>		transitive
24	requireme	pypi:jsons	4.17.3	MIT	<a href="https://pypi.org/project/jsonschema/4.17.3">https://pypi.org/project/jsonschema/4.17.3</a>		transitive
25	requireme	pypi:las	2.4.11	BSD-2-Cl	<a href="https://pypi.org/project/las">https://pypi.org/project/las</a>	<a href="https://github.com/dvershinin/las">https://github.com/dvershinin/las</a>	transitive
		SRC_FL_Dependency	SRC_FL_Source	BIN_FL_Binary	scancode_reference	scanoss_reference	

# FOSSLight Dependency Scanner

- Package Manager에 대한 Dependency 분석을 지원하는 도구
- Package Manager의 Manifest 파일 자동 감지하여 오픈 소스 정보 분석
- Direct / Transitive Dependency 오픈 소스 정보 분석



# FOSSLight Dependency Scanner

- 지원 Package Manager

Language/ Project	Package Manager	Manifest file	Direct dependencies	Transitive dependencies	Relationship of dependencies (Dependencies of each dependency)
Javascript	Npm	package.json	O	O	O
Java	Gradle	build.gradle	O	O	O
	Maven	pom.xml	O	O	O
Java (Android)	Gradle	build.gradle	O	O	O
ObjC, Swift (iOS)	Cocoapods	Podfile.lock	O	O	O
	Carthage	Cartfile.resolved	O	O	X
Swift (iOS)	Swift	Package.resolved	O	O	O
Dart, Flutter	Pub	pubspec.yaml	O	O	O
Go	Go	go.mod	O	O	O
Python	Pypi	requirements.txt, setup.py	O	O	O
.NET	Nuget	packages.config, obj/project.assets.json	O	O	O
Kubernetes	Helm	Chart.yaml	O	X	X

# FOSSLight Dependency Scanner

- 실행 결과 예시

ID	Source Name or P	OSS Name	OSS Versi	License	Download Location	Homepage	Copyri	Exclui	Commen	Dependencies
1	package.json	npm:verror	1.10.0	MIT	<a href="https://github.com/davepacheco/node-verror">https://github.com/davepacheco/node-verror</a>	<a href="https://www.npmjs.com/package/verror">https://www.npmjs.com/package/verror</a>			transitive	npm:assert-plus(1.0.0),npm:core-util-is(1.0.2),npm:xtsprintf(1.3.0)
2	package.json	npm:@trysound/sax	0.2.0	ISC	<a href="https://github.com/svg/sax">https://github.com/svg/sax</a>	<a href="https://www.npmjs.com/package/@trysound/sax">https://www.npmjs.com/package/@trysound/sax</a>			transitive	
3	package.json	npm:ajv	6.12.6	MIT	<a href="https://github.com/ajv-validator/ajv">https://github.com/ajv-validator/ajv</a>	<a href="https://www.npmjs.com/package/ajv">https://www.npmjs.com/package/ajv</a>			transitive	npm:fast-deep-equal(3.1.3),npm:fast-json-stable-stringify(2.1.0),npm:json-schema-tr
4	package.json	npm:ansi-escapes	3.2.0	MIT	<a href="https://github.com/sindresorhus/ansi-escapes">https://github.com/sindresorhus/ansi-escapes</a>	<a href="https://www.npmjs.com/package/ansi-escapes">https://www.npmjs.com/package/ansi-escapes</a>			transitive	
5	package.json	npm:ansi-regex	3.0.1	MIT	<a href="https://github.com/chalk/ansi-regex">https://github.com/chalk/ansi-regex</a>	<a href="https://www.npmjs.com/package/ansi-regex">https://www.npmjs.com/package/ansi-regex</a>			transitive	
6	package.json	npm:ansi-styles	3.2.1	MIT	<a href="https://github.com/chalk/ansi-styles">https://github.com/chalk/ansi-styles</a>	<a href="https://www.npmjs.com/package/ansi-styles">https://www.npmjs.com/package/ansi-styles</a>			transitive	npm:color-convert(1.9.3)
7	package.json	npm:asn1	0.2.6	MIT	<a href="https://github.com/joyent/node-asn1">https://github.com/joyent/node-asn1</a>	<a href="https://www.npmjs.com/package/asn1">https://www.npmjs.com/package/asn1</a>			transitive	npm:safer-buffer(2.1.2)
15	package.json	npm:browserslist	4.21.8	MIT	<a href="https://github.com/browserslist/browserslist">https://github.com/browserslist/browserslist</a>	<a href="https://www.npmjs.com/package/browserslist">https://www.npmjs.com/package/browserslist</a>			transitive	npm:caniuse-lite(1.0.30001502),npm:electron-to-chromium(1.4.428),npm:node-relea
16	package.json	npm:caniuse-api	3.0.0	MIT	<a href="https://github.com/nyalab/caniuse-api">https://github.com/nyalab/caniuse-api</a>	<a href="https://www.npmjs.com/package/caniuse-api">https://www.npmjs.com/package/caniuse-api</a>			transitive	npm:browserslist(4.21.8),npm:caniuse-lite(1.0.30001502),npm:lodash.memoize(4.1.2),n
17	package.json	npm:caniuse-lite	1.0.300015	CC-BY-4.0	<a href="https://github.com/browserslist/caniuse-lite">https://github.com/browserslist/caniuse-lite</a>	<a href="https://www.npmjs.com/package/caniuse-lite">https://www.npmjs.com/package/caniuse-lite</a>			transitive	
18	package.json	npm:caseless	0.12.0	Apache-2.	<a href="https://github.com/mikeal/caseless">https://github.com/mikeal/caseless</a>	<a href="https://www.npmjs.com/package/caseless">https://www.npmjs.com/package/caseless</a>			transitive	
19	package.json	npm:chalk	2.4.2	MIT	<a href="https://github.com/chalk/chalk">https://github.com/chalk/chalk</a>	<a href="https://www.npmjs.com/package/chalk">https://www.npmjs.com/package/chalk</a>			transitive	npm:ansi-styles(3.2.1),npm:escape-string-regexp(1.0.5),npm:supports-color(5.5.0)
26	package.json	npm:combined-stream	1.0.8	MIT	<a href="https://github.com/felixge/node-combined-strea">https://github.com/felixge/node-combined-strea</a>	<a href="https://www.npmjs.com/package/combined-stream">https://www.npmjs.com/package/combined-stream</a>			transitive	npm:delayed-stream(1.0.0)
27	package.json	npm:commander	7.2.0	MIT	<a href="https://github.com/tj/commander.js">https://github.com/tj/commander.js</a>	<a href="https://www.npmjs.com/package/commander">https://www.npmjs.com/package/commander</a>			transitive	
28	package.json	npm:copy-anything	2.0.6	MIT	<a href="https://github.com/mesqueeb/copy-anything">https://github.com/mesqueeb/copy-anything</a>	<a href="https://www.npmjs.com/package/copy-anything">https://www.npmjs.com/package/copy-anything</a>			direct	npm:is-what(3.14.1)
37	package.json	npm:cssnano-utils	4.0.0	MIT	<a href="https://github.com/cssnano/cssnano">https://github.com/cssnano/cssnano</a>	<a href="https://www.npmjs.com/package/cssnano-utils">https://www.npmjs.com/package/cssnano-utils</a>			transitive	npm:postcss(8.4.24)
38	package.json	npm:cssnano	6.0.1	MIT	<a href="https://github.com/cssnano/cssnano">https://github.com/cssnano/cssnano</a>	<a href="https://www.npmjs.com/package/cssnano">https://www.npmjs.com/package/cssnano</a>			direct	npm:cssnano-preset-default(6.0.1),npm:lilconfig(2.1.0),npm:postcss(8.4.24)
39	package.json	npm:csso	5.0.5	MIT	<a href="https://github.com/css/csso">https://github.com/css/csso</a>	<a href="https://www.npmjs.com/package/csso">https://www.npmjs.com/package/csso</a>			transitive	npm:css-tree(2.2.1)
49	package.json	npm:entities	4.5.0	BSD-2-Cla	<a href="https://github.com/fb55/entities">https://github.com/fb55/entities</a>	<a href="https://www.npmjs.com/package/entities">https://www.npmjs.com/package/entities</a>			transitive	
76	package.json	npm:lge-example	1.0.0	Apache-2.	<a href="https://github.com/LGE-OSS/example">https://github.com/LGE-OSS/example</a>	<a href="https://www.npmjs.com/package/lge-example">https://www.npmjs.com/package/lge-example</a>			root pack	npm:copy-anything(2.0.6),npm:cssnano(6.0.1),npm:postcss-plugins(1.10.1)
77	package.json	npm:lilconfig	2.1.0	MIT	<a href="https://github.com/antonk52/lilconfig">https://github.com/antonk52/lilconfig</a>	<a href="https://www.npmjs.com/package/lilconfig">https://www.npmjs.com/package/lilconfig</a>			transitive	

# FOSSLight Dependency Scanner

- SBOM 양식 지원 (SPDX)

```
$ fosslight_dependency -f spdx-yaml
```

```
Document:
SPDXID: SPDXRef-DOCUMENT
creationInfo:
  created: '2023-06-12T09:20:44Z'
  creators:
    - 'Tool: FOSSLIGHT_DEPENDENCY 3.13.4'
  licenseListVersion: '3.20'
dataLicense: CC0-1.0
documentDescribes:
- Package:
  SPDXID: SPDXRef-1
  copyrightText: NONE
  downloadLocation: https://github.com/LGE-OSS/example
  files: []
  homepage: https://www.npmjs.com/package/lge-example
  licenseConcluded: None
  licenseDeclared: Apache-2.0
  licenseInfoFromFiles: []
  name: npm:lge-example
  packageVerificationCode:
    packageVerificationCodeValue: null
  versionInfo: 1.0.0
- Package:
  SPDXID: SPDXRef-2
  copyrightText: NONE
  downloadLocation: https://github.com/mesqueeb/copy-anything
  files: []
  homepage: https://www.npmjs.com/package/copy-anything
  licenseConcluded: None
  licenseDeclared: MIT
  licenseInfoFromFiles: []
  name: npm:copy-anything
  packageVerificationCode:
    packageVerificationCodeValue: null
  versionInfo: 2.0.6
- Package:
  SPDXID: SPDXRef-3
  copyrightText: NONE
  downloadLocation: https://github.com/mesqueeb/is-what
  files: []
  homepage: https://www.npmjs.com/package/is-what
  licenseConcluded: None
  licenseDeclared: MIT
  licenseInfoFromFiles: []
  name: npm:is-what
  packageVerificationCode:
    packageVerificationCodeValue: null
  versionInfo: 3.14.1
documentNamespace: http://spdx.org/spdxdocs/fosslight_dependency-953f9e51-a202-4777-9c59-ae4ddc3f5590
name: SPDX Document by FOSSLIGHT_DEPENDENCY
relationships:
- relatedSpdxElement: SPDXRef-1
  relationshipType: DESCRIBES
  spdxElementId: SPDXRef-DOCUMENT
- relatedSpdxElement: SPDXRef-2
```

# FOSSLight Source Scanner

- 소스 코드를 분석하여 오픈소스 및 버전, 라이선스를 검출
- 여러 스캐너 지원을 통해 String Search뿐만 아니라 Snippet 매칭 지원

A	B	C	D	E	F	G	H	I	J	K	L	M	N	
1	ID	Source	NaOSS Name	OSS Versi	License	Download	Homepage	Copyright	Exclude	Comment	license_reference	scanoss_matched_line	scanoss_fileURL	scanoss_vendor
2	1	reuse/resources/licenses.json	bleasing	agpl-1.0	crystalstacker	pl-1.0	bsd-2-clause	lgpl-2.0-plus	with wxwindows-exception-3.1	gpl-2.0 with classpath-exception-2.0	cc-by-4.0 or cc-by-3.0	gpl-2.0 with gcc-linking-exception-2.0	freetype or gpl-2.0	gpl-2.0-plus or lgpl-2.1-plus or mpl-1.1
3	2	reuse/resources/exceptions.json	cc0-1.0							Copyright Linux Foundation and its Contributors				
4	3	reuse/resources/licenses.json	lic	cc0-1.0						Copyright Linux Foundation and its Contributors				
5	4	reuse/templates/default_template	cc0-1.0							Copyright 2019 Free Software Foundation Europe e.V. <https://fsfe.org>				
6	5	reuse/resources/exceptions.json	gnu-javamail-exception	389-exception	gpl-2.0	ecos-e	gpl-2.0	with universal-foss-exception-1.0	gpl-3.0	with gcc-exception-3.1	gpl-2.0-plus	with freertos-exception-2.0	gpl-2.0-plus	with ecos-exception-2.0
7	6	reuse/_main.py								Copyright 2019 Free Software Foundation Europe e.V. <https://fsfe.org>				
8	7	reuse/_ini	reuse-tool	0.14.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2017 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-only, gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/5d16db923c75cc14f90a3">https://osskb.org/api/file_contents/5d16db923c75cc14f90a3</a>	fsfe	
9	8	reuse/sup	reuse-tool	0.14.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2021 Free (mit or apache-2.0) and other	(Scancode) mit, gpl-3.0, apache-2.0, other-permissive / (Scanoss) gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/bcbd8df45e7d21baa0e5">https://osskb.org/api/file_contents/bcbd8df45e7d21baa0e5</a>	fsfe	
10	9	reuse/rep	reuse-tool	0.10.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2017 Free Software Foundation Europe	(Scancode) cc0-1.0, gpl-3.0 / (Scanoss) gpl-3.0-or-later, cc0-1.0			94%(1-266,270-382)	<a href="https://osskb.org/api/file_contents/04ccd19ee27ba863f37ccf">https://osskb.org/api/file_contents/04ccd19ee27ba863f37ccf</a>	fsfe	
11	10	reuse/_cor	reuse-tool	0.14.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2019 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later			99%(1-705)	<a href="https://osskb.org/api/file_contents/7edb106b63c7948ea23bd">https://osskb.org/api/file_contents/7edb106b63c7948ea23bd</a>	fsfe	
12	11	reuse/_for	reuse-tool	0.10.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2018 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/7ae7b65dd442bbb3b31a">https://osskb.org/api/file_contents/7ae7b65dd442bbb3b31a</a>	fsfe	
13	12	reuse/_ma	reuse-tool	0.14.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2017 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/2299f5e58eed70969aad5">https://osskb.org/api/file_contents/2299f5e58eed70969aad5</a>	fsfe	
14	13	reuse/hea	code-com	0.0.3	gpl-3.0-or	<a href="https://github.com/mi">https://github.com/mi</a>	Copyright 2019 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later			93%(14-46,46-226,236)	<a href="https://osskb.org/api/file_contents/2b07bec3a9689d762946">https://osskb.org/api/file_contents/2b07bec3a9689d762946</a>	miguelvictor	
15	14	reuse/init	reuse-tool	0.10.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2019 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/ad3709b8ac32a35a011ce">https://osskb.org/api/file_contents/ad3709b8ac32a35a011ce</a>	fsfe	
16	15	reuse/_lint	reuse-tool	0.14.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2017 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/1244fc293c79045186e403">https://osskb.org/api/file_contents/1244fc293c79045186e403</a>	fsfe	
17	16	reuse/proj	reuse	0.13.0	gpl-3.0-or	<a href="https://pypl.org/proje">https://pypl.org/proje</a>	Copyright 2017 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/069dca08882a15c19922ce">https://osskb.org/api/file_contents/069dca08882a15c19922ce</a>	Carmen Bianca Bakker	
18	17	reuse/spd	reuse-tool	0.10.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2017 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/6dced70e072b66af6844d">https://osskb.org/api/file_contents/6dced70e072b66af6844d</a>	fsfe	
19	18	reuse/vcs	reuse-tool	0.10.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2017 Free Software Foundation Europe	(Scancode) gpl-3.0 / (Scanoss) gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/151098752336cfe62ce431">https://osskb.org/api/file_contents/151098752336cfe62ce431</a>	fsfe	
20	19	reuse/_lic	reuse	0.11.0	gpl-3.0-or	<a href="https://pypl.org/proje">https://pypl.org/proje</a>	Copyright 2019 Free Software Foundation Europe	(Scancode) gpl-3.0, apache-2.0 / (Scanoss) gpl-3.0-or-later, apache			100%(all)	<a href="https://osskb.org/api/file_contents/2dd68264374297f09a3a">https://osskb.org/api/file_contents/2dd68264374297f09a3a</a>	Carmen Bianca Bakker	
21	20	reuse/_util	reuse	0.13.0	gpl-3.0-or	<a href="https://pypl.org/proje">https://pypl.org/proje</a>	Copyright 2017 Free Software Foundation Europe	(Scancode) gpl-3.0, unknown-spdx / (Scanoss) gpl-3.0-or-later			99%(1-360)	<a href="https://osskb.org/api/file_contents/8552f8658f368126860ae">https://osskb.org/api/file_contents/8552f8658f368126860ae</a>	Carmen Bianca Bakker	
22	21	reuse/dow	reuse-tool	0.14.0	gpl-3.0-or	<a href="https://github.com/fsf">https://github.com/fsf</a>	Copyright 2019 Free unknown-spdx or unknown-	(Scancode) gpl-3.0, unknown-spdx / (Scanoss) gpl-3.0-or-later			100%(all)	<a href="https://osskb.org/api/file_contents/f965edd9602d6e183e3e">https://osskb.org/api/file_contents/f965edd9602d6e183e3e</a>	fsfe	
23	22	reuse/templates/default_template	unknown-only											

- FOSSLight Source Scanner가 채우지 못한 정보 및 오탐 정보 보완
  - Code Match 과정에서 OSS Name / OSS Version이 잘못된 정보로 기술될 수 있음
  - > 사용자 판단에 따라 실제 사용된 OSS Name, Version으로 보완 필요

# FOSSLight Binary Scanner

- 바이너리 목록 추출하여 Database에서 오픈소스 정보 확인
- Jar 파일에 대하여 보안 취약점 확인도 가능



	A	B	C	D	E	F	G	H	I	J	K
1	ID	Source Na	OSS Name	OSS Versi	License	Download Location	Homepage	Copyright Text	Exclude	Comment	Vulnerability Link
2	22	lib/aho-cc	hankcsah	1.2.3	Apache License Version 2.0	hankcs/AhoCorasickDoubleArrayTrie				OWASP Result.	
3	23	lib/android	vaadin.ext	0.0.201311	Apache License 2.0	<a href="http://developer.android.com/sdk">http://developer.android.com/sdk</a>				OWASP Result.	
4	24	lib/annota	jetbrains:a	22.0.0	The Apache Software License	JetBrains/java-annotations				OWASP Result.	
5	25	lib/ant-1.1	apache.an	1.10.12		<a href="https://ant.apache.org/">https://ant.apache.org/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
6	26	lib/checke	checkerfra	3.12.0	The MIT License	<a href="https://checkerframework.org">https://checkerframework.org</a>				OWASP Result.	
7	27	lib/comm	commons:	1.9.4		<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a> , <a href="https://commons.apache.org/proper/commons-beanutils/">https://commons.apache.org/proper/commons-beanutils/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
8	28	lib/comm	commons:	1.5.0		<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a> , <a href="https://commons.apache.org/proper/commons-cli/">https://commons.apache.org/proper/commons-cli/</a>				OWASP Result.	
9	29	lib/comm	commons:	1.15		<a href="https://www.apache.org/licenses">https://www.apache.org/licenses</a> , <a href="https://commons.apache.org/proper/commons-codec/">https://commons.apache.org/proper/commons-codec/</a>				OWASP Result.	
10	30	lib/comm	commons:	3.2.2		<a href="http://www.apache.org/licenses/">http://www.apache.org/licenses/</a> , <a href="http://commons.apache.org/collections/">http://commons.apache.org/collections/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
11	31	lib/comm	apache.co	1.21		<a href="https://www.apache.org/licenses/">https://www.apache.org/licenses/</a> , <a href="https://commons.apache.org/proper/commons-compress/">https://commons.apache.org/proper/commons-compress/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
12	32	lib/comm	apache.co	2.9.0		<a href="https://www.apache.org/licenses/">https://www.apache.org/licenses/</a> , <a href="https://commons.apache.org/dbcp/">https://commons.apache.org/dbcp/</a>				OWASP Result.	
13	33	lib/comm	commons:	2.1		<a href="http://www.apache.org/licenses/">http://www.apache.org/licenses/</a> , <a href="http://commons.apache.org/digester/">http://commons.apache.org/digester/</a>				OWASP Result.	
14	34	lib/comm	commons:	2.11.0		<a href="https://www.apache.org/licenses/">https://www.apache.org/licenses/</a> , <a href="https://commons.apache.org/proper/commons-io/">https://commons.apache.org/proper/commons-io/</a>				OWASP Result.	<a href="https://nvd.nist.gov/vuln/search/results?form_type=Ad">https://nvd.nist.gov/vuln/search/results?form_type=Ad</a>
15	35	lib/comm	apache.co	2.2.1		<a href="https://www.apache.org/licenses/LICENSE-2.0.txt">https://www.apache.org/licenses/LICENSE-2.0.txt</a>				OWASP Result.	
16	36	lib/comm	apache.co	3.12.0		<a href="https://www.apache.org/licenses/">https://www.apache.org/licenses/</a> , <a href="https://commons.apache.org/proper/commons-lang/">https://commons.apache.org/proper/commons-lang/</a>				OWASP Result.	
17	37	lib/comm	commons:	1.2		<a href="http://www.apache.org/licenses/">http://www.apache.org/licenses/</a> , <a href="http://commons.apache.org/proper/commons-logging/">http://commons.apache.org/proper/commons-logging/</a>			Exclude	OWASP Result. Exclud	ed due to Binary DB.
18	38	lib/comm	commons:	1.2	Apache-2.0					Binary DB Result	

- Comment : OSS 정보 추출 방법



# FOSSLight Scanner – Compare 모드

- 두개의 BOM(FOSSLight Report)를 비교

```
$ fosslight compare -p fosslight_report1.xlsx fosslight_report2.xlsx
```

- 비교 가능 input 지원 포맷 : xlsx, yaml
- Compare 모드 실행 결과 (지원 포맷 : xlsx, json, yaml, html)

## FOSSLight Scanner Compare Result

### BOM Compare Result

- Before FOSSLight Report file: /home/soim/git/scanner/fosslight\_scanner/tests/fosslight\_raw\_data/fosslight\_report\_230308\_prj-5204.yaml
- After FOSSLight Report file: /home/soim/git/scanner/fosslight\_scanner/tests/fosslight\_raw\_data/fosslight\_report\_230308\_prj-5203.yaml

Status	OSS_Before	License_Before	OSS_After	License_After
add			FFT	FFT License
delete	JsonCPP(1.8.4)	MIT		
change	gson(2.8.2)	Apache-2.0	gson(3.1)	Apache-2.0

# 네트워크 연결 없이 동작 가능 여부

- **FOSSLight Dependency Scanner**

Package manager	필요 사항
Gradle	<a href="https://github.com/hierynomus/license">com.github.hierynomus.license '0.16.1'</a> 플러그인 미리 설치 필요 (프로젝트 패키지 미리 설치 필요)
Maven	<a href="https://org.codehaus.mojo/license-maven-plugin">org.codehaus.mojo:license-maven-plugin</a> 플러그인 미리 설치 필요 (프로젝트 패키지 미리 설치 필요)
NPM	<a href="https://license-checker">license-checker</a> 플러그인 미리 설치 필요 (프로젝트 패키지 미리 설치 필요 (node_modules 디렉토리 생성된 상태))
Android	<a href="https://android-dependency-scanning">android-dependency-scanning</a> 플러그인 미리 설치 필요 (프로젝트 패키지 미리 설치 필요)
Pub	<a href="https://flutter_oss_licenses">flutter_oss_licenses</a> 플러그인 미리 설치 필요 (프로젝트 패키지 미리 설치 필요)
Cocoapods	'pod spec which --regex {package name}' 명령어 동작 가능한 상태 (프로젝트 패키지 미리 설치 필요)
Carthage	프로젝트 패키지 미리 설치 필요 ('Carthage/Checkouts' 디렉토리 생성된 상태).
PYPI, Go, Swift	불가

- **FOSSLight Source Scanner**

- Snippet 매칭은 네트워크 연결된 환경에서만 동작함

- **FOSSLight Binary Scanner**

- 보안취약점 정보는 네트워크 연결된 환경에서만 얻을 수 있음

# 설치 및 동작 시연

---