

사용자들이 많이 물어본

FOSSLight Scanner FAQ

20분 안에 Scanner 에 대한 궁금증을 풀어드립니다.

목차

01 어떤 Scanner를 사용해야 하나요?

02 분석이 정상적으로 완료됐는지 어떻게 확인하나요?

03 예상한 OSS가 검출되지 않은 이유는 무엇인가요?

04 Scanner마다 결과가 다른 이유는 무엇인가요?

05 Scanner 결과를 그대로 사용해도 되나요?

FOSSLight Scanner 의 종류 및 옵션

“무엇을 확인하려는가” 를 기준으로 선택합니다.



Source Scanner

소스 코드 안의
라이선스·저작권 문구, 코드 조각 등
OSS 흔적을 확인합니다.



Dependency Scanner

Manifest와 npm, Maven, pip 등
패키지 매니저가 제공하는
의존성 관계를 분석합니다.



Binary Scanner

jar, dll 등 빌드·배포 바이너리 안에서
OSS 흔적을 확인합니다.

통합 실행

여러 Scanner 를 함께 사용할 때는
fosslight 명령을 권장합니다.

다양한 옵션

복잡하거나 반복되는 옵션은
config 파일로 관리합니다.

플랫폼 특화

Android, Yocto는 플랫폼 별
특화 Scanner를 사용합니다.
ex) Android Scanner, Yocto Scanner

Private Git

-w로 저장소 URL을 지정하고,
--git_token으로 인증합니다.

목적에 맞는 Scanner를 선택하고, 통합 분석에는 fosslight 명령을 활용합니다.

FOSSLight Scanner Guide

<https://fosslight.org/fosslight-guide/scanner>

FOSSLight Scanner Guide

Search docs...

FOSSLIGHT SCANNER (ALL-IN-ONE)

FOSSLight Dependency Scanner

FOSSLight Source Scanner

FOSSLight Binary Scanner

Etc

FOSSLIGHT SCANNER SERVICE

FOSSLIGHT SCANNER GUI

FOSSLIGHT ANDROID SCANNER

FOSSLIGHT YOCTO SCANNER

FOSSLIGHT PRECHECKER

scanner / README.md

English /

FOSSLight Scanner

license Apache-2.0 | pypi v2.1.33 | python 3.10 | 3.11 | 3.12 | 3.13 | 3.14 | GitHub Repository

FOSSLight Scanner는 의존성(Dependency), 소스코드, 바이너리에 포함된 오픈소스 정보를 자동으로 분석하기 위한 통합 스캐닝 도구입니다. Git 또는 wget으로 다운로드 가능한 소스뿐 아니라 로컬 소스 경로를 입력하여 분석을 수행할 수 있으며, 그 결과는 SBOM 형식인 FOSSLight Report 형태로 생성됩니다.

FOSSLight Scanner는 다음 3가지 스캐너로 구성되어 있으며, 각각 다른 분석 영역을 담당합니다.

1. FOSSLight Dependency Scanner

Package manager 또는 빌드 시스템을 통해 사용되는 의존성(dependency)을 분석하여 오픈소스 정보를 추출하는 스캐너입니다. npm, pypi, maven, gradle 등 다양한 패키지 매니저를 지원하며, 직접 의존성뿐 아니라 그에 따라 포함되는 하위 의존성까지 함께 분석합니다.

2. FOSSLight Source Scanner

소스 코드를 분석하여 라이선스 문구, 저작권 문자열, 그리고 코드 스니펫 등의 오픈소스 관련 정보를 탐지합니다.

3. FOSSLight Binary Scanner

Binary 파일을 대상으로 오픈소스 분석을 수행합니다. 바이너리 자체를 리버스 엔지니어링하는 방식이 아니라, 바이너리 목록을 수집한 뒤 내부 DB에 존재하는 OSS 정보와 매칭하여 해당 바이너리에 포함된 오픈소스를 식별합니다.

Usage

fosslight [mode] [options] <arguments>

Description

FOSSLight Scanner performs comprehensive open source analysis by running multiple modes (Source, Dependency, Binary) together. It can download source code from URLs (git/wget) or analyze local paths, and generates results in OSS Report format.

Guide: <https://fosslight.org/fosslight-guide/scanner/>

Modes

all (default)	Run all modes (Source, Dependency, Binary)
source	Run FOSSLight Source analysis only
dependency	Run FOSSLight Dependency analysis only
binary	Run FOSSLight Binary analysis only
compare	Compare two FOSSLight reports

Note: Multiple modes can be specified separated by comma
Example: `fosslight source,binary -p /path/to/analyze`

General Options

-p <path>	Path to analyze <ul style="list-style-type: none">Compare mode: path to two FOSSLight reports (excel/yaml)
-w <url>	URL to download and analyze (git clone or wget)
--git_token <token>	Git HTTP personal access token for private URL (-w)
--id <user>	Git HTTP credential username (with --git_token) Default: oauth2 when only --git_token is given
-f <format>	Output format (excel, csv, opossum, yaml, spdx-yaml, spdx-json, spdx-xml, spdx-tag, cyclonedx-json, cyclonedx-xml) <ul style="list-style-type: none">Compare mode: excel, json, yaml, html
-e <pattern>	Multiple formats: ex) -f excel yaml json (separated by space) Exclude paths from analysis (files and directories) ⚠ IMPORTANT: Always wrap in quotes to avoid shell expansion Example: <code>fosslight -e "test/" "*.jar"</code>
-o <path>	Output directory or file name
-c <number>	Number of processes for source analysis
-r	Keep raw data from scanners
-t	Hide progress bar
-h	Show this help message
-v	Show version information
-s <path>	Apply settings from JSON file (check format with 'tests/fixtures/setting.json' in this repository) Note: CLI flags override settings file Example: <code>-f yaml -s tests/fixtures/setting.json -o output is .yaml</code>
--no_correction	Skip OSS information correction with sbom-info.yaml
--correct_fpath <path>	Path to sbom-info.yaml file for correction
--recursive_dep	Recursively analyze dependencies

공식 가이드에서 Scanner별 대상, 설치 방법 및 실행 옵션을 확인합니다.

Scanner Result Pass/Fail 확인

Scanner 를 실행하면 Report 파일과 로그 파일이 생성됩니다.
먼저 Report의 Info 시트에서 분석 상태와 오류 여부를 확인합니다

1 Report Info 시트 확인

프로젝트의 분석 상태 확인



2 Report Result 시트 확인

실행한 스캐너의 결과 확인



3 Scanner 실행 로그 확인

Scanner별 성공·실패 메시지



Pass/Fail 판단

Pass/Fail Case

Report 생성 + Info 오류

Source 성공 + Dependency 실패

분석 결과 0건

참고) SCANOSS, KB Skip

파일 Hash를 기반으로 유사한 OSS를 확인하는 DB 매칭 기능입니다.
SCANOSS는 호출 횟수 제한으로, KB는 유료 서비스 이용 조건에 따라 Skip될 수 있지만, 기본 소스 분석 결과는 정상적으로 생성됩니다.

Report 생성 여부가 아니라 Report 파일과 로그 파일을 통해 Scanner 별 분석 상태를 확인하세요.

Scanner Report 파일

Info 시트에서 실행 상태를 확인하고, Result 시트에서 Scanner별 분석 결과를 확인합니다.
 > fosslight_report_all_20261025_222747.xlsx

1. Info 시트

실행한 Scanner 및 버전 · 분석 대상 · 오류 메시지

ID	Package	LOSS Name	OSS Version	License	Download	Homepage	Copyright	Exclude	Comment	Depends On
1	pkg.npm/	npm:ag-grid-community	28.2.1	MIT	https://www.ag-grid.com/	https://github.com/ag-grid/ag-grid			transitive	
2	pkg.npm/	npm:ag-grid-react	28.2.1	MIT	https://www.ag-grid.com/	https://github.com/ag-grid/ag-grid			direct	pkg.npm/ag-grid-con
3	pkg.npm/	npm:copy anything	2.0.6	MIT	https://www.npmjs.com/package/copyanything	https://github.com/mesqueeb/copyanything			direct	pkg.npm/is-what@3.1
4	pkg.npm/	npm:is-what	3.14.1	MIT	https://www.npmjs.com/package/is-what	https://github.com/mesqueeb/is-what			transitive	
5	pkg.npm/	npm:js-tokens	4.0.0	MIT	https://www.npmjs.com/package/js-tokens	https://github.com/lydell/js-tokens			transitive	
6	pkg.npm/	npm:lg-examples	1.0.0	Apache-2.0	https://github.com/LG-SS/Exam	https://github.com/LG-SS/Exam			root package	
7	pkg.npm/	npm:loose-envify	1.4.0	MIT	https://www.npmjs.com/package/loose-envify	https://github.com/zertosh/loose-envify			transitive	pkg.npm/js-tokens@4
8	pkg.npm/	npm:object-assign	4.1.1	MIT	https://www.npmjs.com/package/object-assign	https://github.com/sindresorhus/object-assign			transitive	
9	pkg.npm/	npm:prop-types	15.8.1	MIT	https://www.npmjs.com/package/prop-types	https://github.com/facebook/prop-types			transitive	pkg.npm/loose-envify
10	pkg.npm/	npm:react-dom	18.3.1	MIT	https://www.npmjs.com/package/react-dom	https://github.com/facebook/react			transitive	pkg.npm/loose-envify
11	pkg.npm/	npm:react-is	16.13.1	MIT	https://www.npmjs.com/package/react-is	https://github.com/facebook/react			transitive	
12	pkg.npm/	npm:react	18.3.1	MIT	https://www.npmjs.com/package/react	https://github.com/facebook/react			transitive	pkg.npm/loose-envify
13	pkg.npm/	npm:scheduler	0.23.2	MIT	https://www.npmjs.com/package/scheduler	https://github.com/facebook/react			transitive	pkg.npm/loose-envify
14	pkg.py/	py:beautifulsoup4	4.15.0	MIT License	https://pypi.org/project/beautifulsoup4/	https://www.cummy.com/software/beautifulsoup			direct	pkg.py/soupsieve@
15	pkg.py/	py:certifi	2024.6.2	Mozilla Public Li	https://pypi.org/project/certifi/	https://github.com/certifi/python-c			direct	
16	pkg.py/	py:grpcio	1.84.0	Apache-2.0	https://pypi.org/project/grpcio/	https://github.com/grpc/grpc			direct	pkg.py/typing-exte
17	pkg.py/	py:html	5.3.0	BSD License	https://pypi.org/project/html/	https://github.com/hml/html			direct	
18	pkg.py/	py:numpy	2.5.4	BSD-3-Clause A	https://pypi.org/project/numpy/	https://github.com/numpy/numpy			direct	
19	pkg.py/	py:soupsieve	3.0.4	MIT	https://pypi.org/project/soupsieve/	https://github.com/facelessuser/so			transitive	
20	pkg.py/	py:typing-extensions	4.16.0	PSF-2.0	https://pypi.org/project/typing-extensions/	https://github.com/python/typing			transitive	
21	pkg.py/	py:xlrd	2.0.2	BSD License	https://pypi.org/project/xlrd/	http://www.python-excel.org/			direct	

2. Result 시트

시트 생성 여부 · OSS 갯수

ID	Source Path	OSS Name	OSS Version	License	Download Loc	Homepage	Copyright Text	Exclude	Comment
1	LICENSE			Apache-2.0					
2	LICENSES/Apache-2.0.txt			Apache-2.0					
3	LICENSES/BSD-3-Clause.txt			BSD-3-Clause			Copyright (c) <owner>		
4	LICENSES/MIT.txt			MIT					
5	README.md			Apache-2.0			Copyright (c) 2021 LG Electronics Inc.Cc		
6	package.json			Apache-2.0					
7	src/app.js			Apache-2.0			Copyright 2022 LG Electronics Inc.		
8	src/sample.js			CC0-1.0			Copyright 2022 LG Electronics Inc.		
9	test			Apache-2.0					
10	third_party/PySocks/LICENSE			BSD-3-Clause			Copyright 2006 Dan-Haim		
11	third_party/PySocks/README.md	sapling	0.2.20241203-120811-a2174689		https://github.com/facebook/		Copyright 2006 Dan-Haim		
12	third_party/PySocks/setup.py	hue	release-4.11.0	BSD	https://github.com/cloudera/hue				
13	third_party/PySocks/socks.py	bazarr	v1.4.3-beta.9		https://github.com/morpheus65535/bazarr				
14	third_party/PySocks/sockshandler.py	bazarr	v1.4.3-beta.9		https://github.com/morpheus65535/bazarr				
15	third_party/PySocks/tox.ini	info_scan	V1.1		https://github.com/huan-sdm/info_scan				
16	third_party/httpools (3)	abrechnung	v0.14.0	MIT	https://github.com/SFTech/a		Copyright (c) 2015 MagicStack Inc. http		

Scanner 실행 로그

실행 로그에서 Scanner별 성공·실패 여부와 오류 원인을 확인합니다.

> fosslight_log_all_20261025_222747.txt



SOURCE SCANNER

소스 코드 분석

```
[...INFO] [FOSSLIGHT_SCANNER] Tool Info: fosslight_scanner v2.1.33
[...DEBUG] [FOSSLIGHT_SCANNER] Skipped paths: ['.git', '.github', '.giti
[...INFO] ## Start to run Source Analysis
[...INFO] [---Path to analyze: .../example/
[...INFO] [FOSSLIGHT_SOURCE] Tool Info: fosslight_source v2.3.16
[...DEBUG] Scancode ignore patterns: 30
[...DEBUG] Scancode max_in_memory: 2722994
[...DEBUG] [---Running SCANOSS on /home/woocheol/Work/Example/example
[...DEBUG] [---Checking SCANOSS API connectivity to https://api.osskb.or
[...DEBUG] [SCANOSS] API Limit Exceeded: HTTP 503
[...DEBUG] [FOSSLIGHT_SOURCE] KB server is reachable. Response status: 2
[...INFO] KB scan job created: job_id=04251bf9298145569aa4a78d1b527bbe,
[...INFO] KB scan job completed: job_id=04251bf9298145569aa4a78d1b527bb
[...INFO] [FOSSLIGHT_SOURCE] No correction with yaml: Cannot find sbom
[...DEBUG] [FOSSLIGHT_SOURCE] [TIMING] merge_results_by_folder: 0.0002s
[...INFO] [FOSSLIGHT_SOURCE] Output file: /home/woocheol/Work/Example/.
[...INFO] [FOSSLIGHT_SOURCE] Scanned files: 43
[...INFO] [FOSSLIGHT_SOURCE] Detected source: 25
[...INFO] [FOSSLIGHT_SOURCE] SCANOSS replaced with KB
[...INFO] [FOSSLIGHT_SOURCE] Mode: kb, scancode, scanoss
[...INFO] [FOSSLIGHT_SOURCE] OS: Linux 5.15.0-139-generic
Path to analyze: /home/woocheol/Work/Example/example
Python version: 3
Running time: 20261022_10:42:12 ~ 20261022_10:42:18 (6s)
Scan Result: 'True'
Tool Info: fosslight_source v2.3.16
[...INFO] ## Complete Source Analysis
```



BINARY SCANNER

바이너리/JAR 분석

```
[...INFO] ## Start to run Binary Analysis
[...INFO] [---Path to analyze: .../example/
[...INFO] [FOSSLIGHT_BINARY] Tool Info: fosslight_binary v5.1.34
[...DEBUG] [FOSSLIGHT_BINARY] Skipped paths: ['.git', '.github', '.gitignore', 'third_party/httptools/tests',
[...INFO] [FOSSLIGHT_BINARY] Run to analyze: jar file
[...DEBUG] bin/tish-4.6.0.jar: not found in Maven Central -> falling back to JAR internals
[...DEBUG] Result: bin/tish-4.6.0.jar | TLSH -> Trend Micro Locality Sensitive Hash 4.5.0 | [] | dlt | sources
[...DEBUG] bin/jetty-util-ajax-9.4.40.v20210413.jar: Central and JAR pom.xml match (org.eclipse.jetty:jetty-u
[...DEBUG] bin/jetty-util-ajax-9.4.40.v20210413.jar: license from JAR pom.xml (matched Central) 'Apache Softw
[...DEBUG] Maven jar found: https://repo1.maven.org/maven2/org/eclipse/jetty/jetty-util-ajax/9.4.40.v20210413
[...DEBUG] Result: bin/jetty-util-ajax-9.4.40.v20210413.jar | org.eclipse.jetty:jetty-util-ajax-9.4.40.v2021
[...DEBUG] bin/logback-classic-1.2.3.jar: Central and JAR pom.xml match (ch.qos.logback:logback-classic-1.2.3
[...DEBUG] bin/logback-classic-1.2.3.jar: license from JAR pom.xml (matched Central) 'Eclipse Public License
[...DEBUG] Maven jar found: https://repo1.maven.org/maven2/ch/qos/logback/logback-classic/1.2.3/logback-class
[...DEBUG] Result: bin/logback-classic-1.2.3.jar | ch.qos.logback:logback-classic-1.2.3 | [Eclipse Public Lic
[...DEBUG] bin/error_prone_annotations-2.7.1.jar: Central and JAR pom.xml match (com.google.errorprone:error
[...DEBUG] bin/error_prone_annotations-2.7.1.jar: license from JAR pom.xml (matched Central) 'Apache 2.0'
[...DEBUG] Maven jar found: https://repo1.maven.org/maven2/com/google/errorprone/error_prone_annotations/2.7.
[...DEBUG] Result: bin/error_prone_annotations-2.7.1.jar | com.google.errorprone:error_prone_annotations:2.7.
[...DEBUG] third_party/bin/spring-security-web-6.3.0.jar: Central (org.springframework.security:spring-secu
[...DEBUG] POM downloaded to /tmp/tmp3k5x5d0-pom from https://repo1.maven.org/maven2/org/springframework/sec
[...DEBUG] third_party/bin/spring-security-web-6.3.0.jar: license from Central POM 'Apache License Version 2
[...DEBUG] Maven jar found: https://repo1.maven.org/maven2/org/springframework/security/spring-security-web/6
[...DEBUG] Result: third_party/bin/spring-security-web-6.3.0.jar | org.springframework.security:spring-secu
[...DEBUG] third_party/bin/commons-text-1.9.jar: Central and JAR pom.xml match (org.apache.commons:commons-te
[...DEBUG] third_party/bin/commons-text-1.9.jar: license from JAR pom.xml (matched Central) 'Apache License v
[...DEBUG] Maven jar found: https://repo1.maven.org/maven2/org/apache/commons/commons-text/1.9/commons-text-1
[...DEBUG] Result: third_party/bin/commons-text-1.9.jar | org.apache.commons:commons-text-1.9 | [Apache Licen
[...DEBUG] KB binary match endpoint responded with HTTP 422; treated as available
[...INFO] [FOSSLIGHT_BINARY] No correction with yaml: Cannot find sbom info yaml in: .../example.
[...INFO] [FOSSLIGHT_BINARY] Output file: /home/woocheol/Work/Example/.fosslight_temp_20261022_104211/fossli
[...INFO] [FOSSLIGHT_BINARY] Detected binaries: 8 (Scanned Files: 43)
[...INFO] [FOSSLIGHT_BINARY] Execution result: Success
Identified in Binary DB: Binaries: 1/8
Mode: Normal Mode
OS: Linux 5.15.0-139-generic
Path to analyze: /home/woocheol/Work/Example/example
Python version: 3
Running time: 20261022_10:42:19 ~ 20261022_10:42:26 (7s)
Tool Info: fosslight_binary v5.1.34
[...DEBUG] [FOSSLIGHT_BINARY] Moving binary analysis log file is skipped
[...INFO] ## Complete Binary Analysis
```



DEPENDENCY SCANNER

Manifest 기반 의존성 분석

```
[...INFO] ## Start to run Dependency Analysis
[...INFO] [---Path to analyze: .../example/
[...INFO] [FOSSLIGHT_DEPENDENCY] Tool Info: fosslight_dependency v4.1.59
[...INFO] [FOSSLIGHT_DEPENDENCY]
Detected Manifest Files automatically
Analyzed path: /home/woocheol/Work/Example/example
...pypi:
...requirements.txt
...npm:
...package.json
[...INFO] Created the temporary virtualenv (/tmp/fosslight_venv_2h0sj8ay).
[...INFO] Parse oss information with file: tmp_pip_license_output.json
[WARNING] ## Complete to analyze: pypi(/home/woocheol/Work/Example/example: requirements.txt)
[...INFO] node_modules directory is not existed. So it executes 'npm install --production --ig
[...INFO] Parse oss information with file: tmp_npm_license_output.json
[WARNING] ## Complete to analyze: npm(/home/woocheol/Work/Example/example: package.json)
[...INFO] [FOSSLIGHT_DEPENDENCY] Output file: /home/woocheol/Work/Example/.fosslight_temp_2026
[...INFO] [FOSSLIGHT_DEPENDENCY] Dependency Analysis Summary
--[Success]-- pypi:
--requirements.txt
--[Success]-- npm:
--package.json
[...INFO] [FOSSLIGHT_DEPENDENCY] OS: Linux 5.15.0-139-generic
Python version: 3
Running time: 20261022_10:42:26 ~ 20261022_10:42:53 (27s)
Tool Info: fosslight_dependency v4.1.59
[...INFO] ## Complete Dependency Analysis

[...INFO] Success to correct the src/bin-scanner/result
[...INFO] [FOSSLIGHT_SCANNER] OS: Linux 5.15.0-139-generic
Python version: 3
Running time: 20261022_10:42:11 ~ 20261022_10:42:53 (42s)
Tool Info: fosslight_scanner v2.1.33
[...DEBUG] Moved log file to final path
[...DEBUG] [FOSSLIGHT_SCANNER] Remove temporary files: /home/woocheol/Work/Example/.fosslight_t
[...INFO] [FOSSLIGHT_SCANNER] Output File: /home/woocheol/Work/Example/LOG/fosslight_report_01
```


Case 2. Source 성공 + Dependency 실패

Source 결과는 확인 가능하지만 Dependency 결과는 정상 결과로 볼 수 없음

1. Report 파일

About the scanner	
Tool information	fosslight_scanner v2.1.33 (fosslight_dependency v4.1.59, fosslight_source v2.3.16, fosslight_binary v5.1.34)
Running time	20261022_10:48:35 ~ 20261022_10:48:58 (23s)
Python version	3.12
Analyzed path	/home/woocheol/Work/Example/example
Excluded path	third_party/httpools/tests, third_party/PySocks/test
[fosslight_dependency v4.1.59] Dependency Analysis Summary	
- [Success] pypi: requirements.txt	
- [Fail] yarn: package.json	
If analysis fails, see fosslight_log*.txt and the prerequisite guide: https://fosslight.org/fosslight-guide-en/scanner/1_dependency.html#how-to-run-and-output	
[fosslight_source v2.3.16] Scanned files: 44 / Detected source: 25 / SCANOSS replaced with KB / Mode: kb, scancode, scanoss	
Comment	[fosslight_binary v5.1.34] Detected binaries: 8 (Scanned Files: 44)

ID	Source Pa	OSS Name	OSS Versi	License	Download Homepag	Copyright	Exclude	Comment
1	build copy.gradle			JSON				
2	build/reports/license/ant-1.10.6	SAX-PD,Apache-2.0,W3C						
3	build/reports/license/ant-1.10.6	Apache-2.0				Copyright (c) 2002, Landmark Gra		
4	build/reports/license/ant-launc	SAX-PD,Apache-2.0,W3C						
5	build/reports/license/ant-launc	Apache-2.0				Copyright (c) 2002, Landmark Gra		
6	build/reports/license/checker-q	MIT				Copyright 2004-present by the Ch		
7	build/reports/license/commons	Apache-2.0						
8	build/reports/license/commons	AGPL-3.0-or-later,Apache-2.0				Copyright (c) 2002 K (AGPL-3.0-or		
9	build/reports/license/commons	Apache-2.0				Copyright 2001-2015 The Apache		

ID	Package LOSS Name	OSS Versi	License	Download Homepag	Copyright	Exclude	Comment	Depen

2. 실행 로그

```
[...INFO] [FOSSLIGHT_SOURCE] No correction with yamll: Cannot find sbom-info.yamll in /home/woocheol/Work/Example/example
[...DEBUG] [FOSSLIGHT_SOURCE] [TIMING] merge_results_by_folder: 0.0007s
[...INFO] [FOSSLIGHT_SOURCE] Output file: /home/woocheol/Work/Example/.fosslight_temp_20261022_104835
[...INFO] [FOSSLIGHT_SOURCE] Scanned files: 44
[...INFO] [FOSSLIGHT_SOURCE] Detected source: 25
[...INFO] [FOSSLIGHT_SOURCE] SCANOSS replaced with KB
[...INFO] [FOSSLIGHT_SOURCE] Mode: kb, scancode, scanoss
[...INFO] [FOSSLIGHT_SOURCE] OS: Linux 5.15.0-139-generic
Path to analyze: /home/woocheol/Work/Example/example
Python version: 3
Running time: 20261022_10:48:35 ~ 20261022_10:48:43 (8s)
Scan Result: 'True'
Tool Info: fosslight_source v2.3.16
[...INFO] ## Complete Source Analysis
```

```
Detected Manifest Files automatically
Analyzed path: /home/woocheol/Work/Example/example
-- pypi:
- requirements.txt
-- npm:
- package.json
[...INFO] Created the temporary virtualenv (/tmp/fosslight_venv_ksw2ytzg).
[...INFO] Parse oss information with file: tmp_pip_license_output.json
[...INFO] ### Complete to analyze: pypi(/home/woocheol/Work/Example/example: requirements.txt)
[WARNING] Node.js is not available on this system
[WARNING] Npm analysis failed. Attempting to use Yarn as fallback...
[WARNING] Node.js is not available on this system
[...ERROR] Yarn also failed
[...ERROR] ### Fail to analyze: yarn(/home/woocheol/Work/Example/example: package.json)
[...INFO] [FOSSLIGHT_DEPENDENCY] Output file: /home/woocheol/Work/Example/.fosslight_temp_20261022_104835
[WARNING] [FOSSLIGHT_DEPENDENCY] Dependency Analysis Summary
-- [Success] pypi:
- requirements.txt
-- [Fail] yarn:
- package.json
If analysis fails, see fosslight_log*.txt and the prerequisite guide: https://fosslight.org/fosslight-guide-en/scanner/1_dependency.html#how-to-run-and-output
[...INFO] [FOSSLIGHT_DEPENDENCY] OS: Linux 5.15.0-139-generic
Python version: 3
```


미검출 사례 및 확인 방법

1 실행 환경 확인

실행 환경 미충족

필수 도구가 없거나 실행 조건이 맞지 않음

예: Maven·Gradle·npm 미설치

저장소 접근 실패

권한·인증 또는 네트워크 연결에 실패함

예: Private Git 다운로드 실패

2 분석 대상 확인

분석 범위 불일치

실행 위치로 인해 일부 프로젝트가 제외됨

예: Monorepo 하위 폴더에서만 실행

Manifest 미검출·미지원

Manifest가 없거나 분석 경로에서 발견되지 않음

예: requirements.txt, pom.xml 없음

3 원본 정보 확인

License 정보 누락

OSS 이름·버전은 있으나 License가 공란

예: Manifest·Metadata 정보 불완전

OSS 정보 연결 실패

License는 있으나 OSS 이름·버전이 공란

예: LICENSE와 OSS 연결 근거 없음

미검출 시 확인 순서

Info 시트
실행 상태·오류



Manifest·분석 경로
분석 대상



Metadata·공식 저장소
원본 정보

미검출 시 실행 상태, 분석 범위, 원본 정보를 순서대로 확인하세요.

Q3 • 예상한 OSS가 검출되지 않은 이유는 무엇인가요?

Dependency Scanner 패키지 지원 현황

지원 여부	Language / Project	Package Manager	Manifest file	Direct	Transitive	Relation
지원	Javascript	Npm	package.json	O	O	O
지원	Javascript	Pnpm	pnpm-lock.yaml	O	O	O
지원	Java	Gradle	build.gradle	O	O	O
지원	Java	Maven	pom.xml	O	O	O
지원	Java (Android)	Gradle	build.gradle	O	O	O
지원	ObjC, Swift (iOS)	Cocoapods	Podfile.lock	O	O	O
일부 지원	ObjC, Swift (iOS)	Carthage	Cartfile.resolved	O	O	X
지원	Swift (iOS)	Swift	Package.resolved	O	O	O
지원	Dart, Flutter	Pub	pubspec.yaml	O	O	O
지원	Go	Go	go.mod	O	O	O
지원	Python	Pypi	requirements.txt, setup.py, pyproject.toml, uv.lock	O	O	O
지원	.NET	Nuget	packages.config, obj/project.assets.json	O	O	O
일부 지원	Kubernetes	Helm	Chart.yaml	O	X	X
일부 지원	Unity	Unity	Library/PackageManager/ProjectCache	O	O	X
지원	Rust	Cargo	Cargo.toml	O	O	O

미검출 시 Package Manager별 지원 범위와 Manifest, 실행 조건을 함께 확인하세요.

Scanner별 분석 방식

Scanner마다 분석 대상과 방식이 다르며, 실행 조건과 분석 범위에 따라서도 결과가 달라질 수 있습니다.



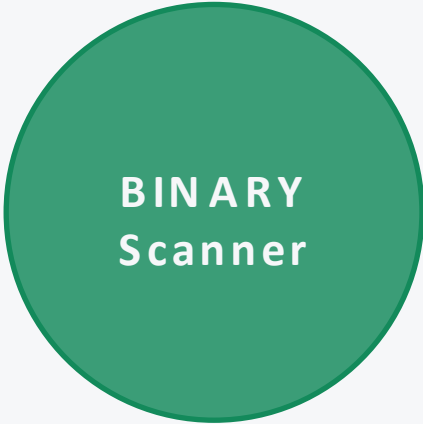
SOURCE Scanner

- 분석 경로와 제외 경로
- 파일 유형 및 크기
- 코드 유사도·DB 매칭 조건



DEPENDENCY Scanner

- Manifest·Lock 파일 상태
- Package Manager 실행 결과
- 직접·전이 및 개발·테스트 범위



BINARY Scanner

- 빌드 옵션과 대상 플랫폼
- 정적·동적 링크 여부
- 실제 산출물 포함 여부

Scanner 별 분석 대상·방식·실행 범위에 따라 결과가 달라질 수 있습니다.

Scanner 결과 검토

Scanner 결과의 정확성과 근거를 확인한 후 필요한 정보만 보완합니다.

SCANNER RESULT

빠르고 폭넓게 검출하지만
최종 확정 정보는 아닙니다.

결과 검증



실제 사용·배포 대상인가?



이름·버전·License가 정확한가?



중복·오탐·누락이 있는가?



여러 Version이 각각 구분되어 있는가?



작성한 Version이 정확한가?



Download Location을 확인했는가?

검출됨 ≠ 실제 배포됨 · 미검출됨 ≠ 미사용 · 검출 결과 ≠ 최종 확정 정보

Scanner 결과를 실제 사용·배포 기준으로 검토하고, 근거가 있는 정보만 보완합니다.

Report는 어떤 순서로 보완하나요?

Scanner 결과의 정확성과 근거를 확인한 후 필요한 정보만 보완합니다.

1

사용 대상 확인

실제 사용·배포 대상인지 확인

2

검출 결과 확인

이름·버전·License와
중복·오탐·누락 확인

3

공식 근거 확인

Manifest·Metadata·공식 저장소
·Download Location 확인

4

Report 보완

근거가 있는 항목만 수정·추가

근거가 없는 정보는 추정하여 입력하지 않고 공란으로 유지합니다.

검출 결과는 어떻게 보완하나요?

Source Path와 공식 정보를 근거로 결과를 확인하고, 필요한 항목을 수정, 삭제, 제외합니다.



판단 기준

OSS가 맞는가?

아니요 → Delete



실제 OSS 정보와 일치하는가?

아니요 → Modify



배포 대상인가?

아니요 → Exclude

Source Path와 OSS 저장소를 확인하여 OSS명, 버전, 라이선스 등 수정 근거를 검토합니다.

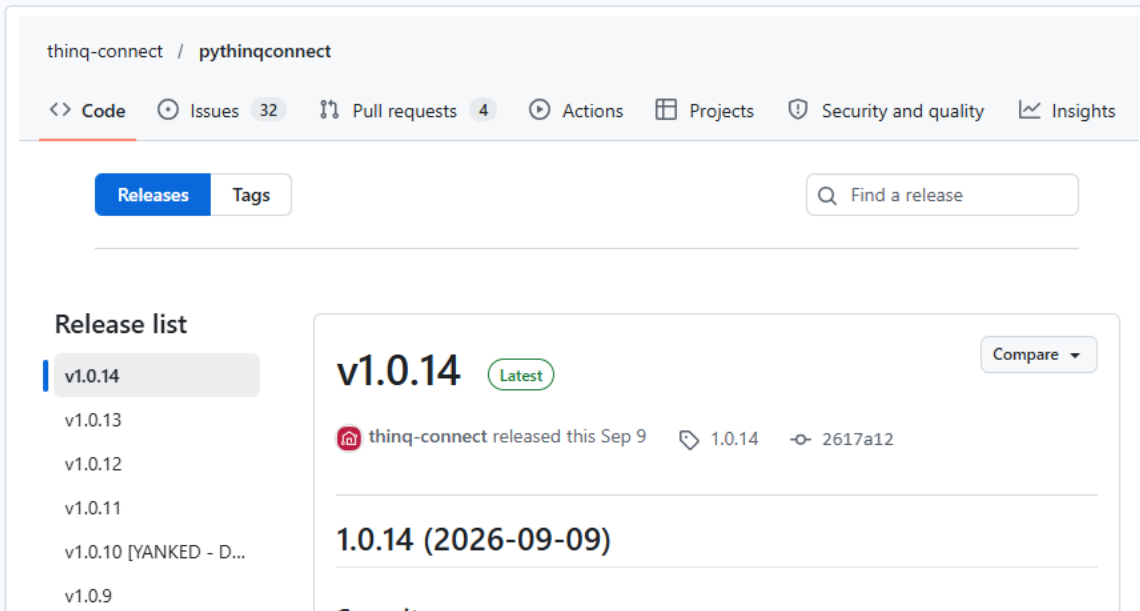
OSS Version은 어떤 기준으로 작성하나요?

공식 배포 버전과 확인 가능한 근거를 Report에 반영합니다.

정확한 보안 취약점 매핑을 위해 Semantic Versioning(SemVer) 형식의 버전 표기를 권장합니다.

1 사용한 소스의 Release list 확인

저장소 또는 Source Path를 통해 실제 사용한 OSS Version을 확인합니다.



The screenshot shows the GitHub Releases page for the repository 'thing-connect / pythingconnect'. The 'Releases' tab is selected. A search bar contains the text 'Find a release'. On the left, a 'Release list' sidebar shows a list of versions: v1.0.14 (selected), v1.0.13, v1.0.12, v1.0.11, v1.0.10 [YANKED - D...], and v1.0.9. The main content area displays details for 'v1.0.14', which is marked as 'Latest'. It includes a release date of 'this Sep 9', a commit hash '2617a12', and a date '1.0.14 (2026-09-09)'.



2 Report의 Version에 기재

확인한 버전을 입력합니다.

Version

1.0.14

공식 Release 또는 Tag에서 확인한
SemVer 형식의 버전을 기재합니다.

Version은 공식 근거로 확인하고, 확인할 수 없는 값은 임의로 표준화해서 수정하지 않습니다.

OSS · License Name은 어떤 기준으로 표준화하나요?

공식 출처와 확인 가능한 근거를 기준으로 동일한 명칭을 적용합니다.
FOSSLight Hub 등록 시 Download Location 기준으로 등록된 이름으로 변경됩니다.

OSS NAME

프로젝트 명칭 표준화

1

공식 OSS Name 우선

임의 약어 사용 금지

공식 저장소·홈페이지·패키지 저장소에서 확인되는 프로젝트 명을 사용

2

OSS Nickname 매칭 활용

중복 등록 방지

다양한 OSS Name 표기는 FOSSLight Hub의 Nickname 매칭을 통해 통합

LICENSE NAME

라이선스 명칭 표준화

3

SPDX License ID 적용

Apache License 2.0 → Apache-2.0

SPDX License ID 또는 정식 License Name으로 작성

4

License 원문 확인

근거가 없으면 공란 유지

LICENSE·COPYING·NOTICE와 공식 저장소를 확인하고 임의로 추정하지 않음

OSS Name은 공식 프로젝트 명칭을, License Name은 SPDX ID 또는 원문에서 확인된 명칭을 사용합니다.

이것만 기억하세요

Scanner FAQ 핵심 정리

01

목적에 맞는 Scanner 선택

02

Report가 아닌 Scanner별 실행 상태 확인

03

0건·미검출을 미사용으로 단정하지 않기

04

Scanner 별 결과 차이는 분석 관점과 범위로 해석

05

결과를 검토하고 필요한 내용 보완

분석 결과가 예상과 다를 때는?

- 사용한 Scanner와 버전
- 실행 명령어
- OS 및 실행 환경
- 전체 실행 로그
- Report의 Info 시트
- Manifest 종류와 프로젝트 구조

FOSSLight 많이 사용해 주세요.
감사합니다.