



FOSSLight 실무에서 활용하는 법

LG전자 Open Source TP 김소임



LG Open Source

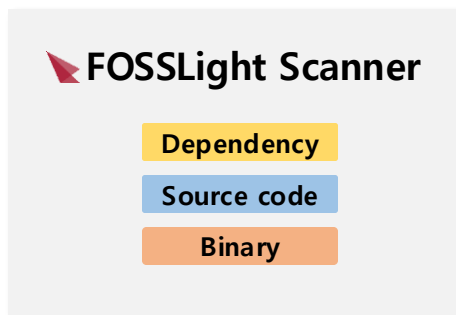
CONTENTS

- FOSSLight Hub와 Scanner 연동
- FOSSLight Prechecker with Jenkins
- FOSSLight Scanner with Jenkins
- FOSSLight MCP 서버

FOSSLight Hub와 Scanner 연동

FOSSLight Hub + FOSSLight Scanner

- FOSSLight Scanner 실행하여 오픈소스 분석 보고서 생성



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

FOSSLight Hub + FOSSLight Scanner

- 생성한 Report를 FOSSLight Hub에 업로드하여 OSC Process를 진행

The screenshot displays the FOSSLight Hub interface. On the left is a sidebar with navigation options: Dashboard, License, Open Source, Project (highlighted), 3rd Party, Binary DB, Vulnerability, Self-Check, and User Settings. The main area shows a 'Project' view with a table of projects. A red arrow points from a detailed report table (shown in an inset) to the 'Project' table.

Project Table:

ID	Project Name	Status	OSC Process	Download	Security	Division	Creator
881	Review Report Demo (1.0.1)	Progress	Identification > Packaging		Need to resolve(10.0)	LG Electro...	foss.lge
872	min_test	Progress	Identification > Packaging		Need to resolve(10.0)	LG Electro...	minksks
871	chs_test (1.10)	Request	Identification > Packaging		Discovered(N/A)	LG Electro...	balisa_fitst
869	lge-oss-example	Request	Identification > Packaging		Need to resolve(7.1)	LG Electro...	foss.lge
		Progress	Identification > Packaging		Need to resolve(7.5)	LG Electro...	foss.lge
		Progress	Identification > Packaging		Need to resolve(9.8)	LG Electro...	foss.lge
		Progress	Identification > Packaging		Need to resolve(9.8)	LG Electro...	foss.lge

Report Table (Inset):

Source Name or Path	OSS Name	OSS Version	License	Download Location	Homepage	Copyright	Exclude	Comments	Dependencies
1 package.json	npm:lge-example	1.0.0	Apache-2.0	https://github.com/LGE-OSS/example	https://www.npmjs.com/package/lge-example			root pack	npm:copy-
2 package.json	npm:copy-anything	2.0.6	MIT	https://github.com/mesqueeb/copy-anything	https://www.npmjs.com/package/copy-anything			direct	npm:is-wh
3 package.json	npm:is-what	3.14.1	MIT	https://github.com/mesqueeb/is-what	https://www.npmjs.com/package/is-what			transitive	
4 requirements.txt	pypi:CacheControl	0.12.11	Apache Software License	https://pypi.org/project/CacheControl/0.12.11	https://github.com/lonrock/cachecontrol			transitive	pypi:msgp
5 requirements.txt	pypi:Deprecated	1.2.14	MIT License	https://pypi.org/project/Deprecated/1.2.14	https://github.com/tantale/deprecated			transitive	pypi:wrapt
6 requirements.txt	pypi:linja2	3.1.2	BSD License	https://pypi.org/project/linja2/3.1.2	https://palletsprojects.com/p/linja/			transitive	pypi:Marku
7 requirements.txt	pypi:MarkupSafe	2.1.3	BSD License	https://pypi.org/project/MarkupSafe/2.1.3	https://palletsprojects.com/p/markupsafe/			transitive	
8 requirements.txt	pypi:PyGithub	2.1.1	GNU Library or Lesser Gen	https://pypi.org/project/PyGithub/2.1.1	https://github.com/pygithub/pygithub			transitive	pypi:Depre
9 requirements.txt	pypi:PyJWT	2.8.0	MIT License	https://pypi.org/project/PyJWT/2.8.0	https://github.com/padilla/pyjwt			transitive	
10 requirements.txt	pypi:PyNaCl	1.5.0	Apache License 2.0	https://pypi.org/project/PyNaCl/1.5.0	https://github.com/pyca/pynacl			transitive	pypi:cfli(1.
11 requirements.txt	pypi:PyYAML	6.0.1	MIT License	https://pypi.org/project/PyYAML/6.0.1	https://pyyaml.org/			transitive	
12 requirements.txt	pypi:XlsxWriter	3.1.8	BSD License	https://pypi.org/project/XlsxWriter/3.1.8	https://github.com/mcnamara/xlsxwriter			transitive	
13 requirements.txt	pypi:appdirs	1.4.4	MIT License	https://pypi.org/project/appdirs/1.4.4	http://github.com/ActiveState/appdirs			transitive	
14 requirements.txt	pypi:attrs	23.1.0	MIT License	https://pypi.org/project/attrs/23.1.0	https://www.attrs.org/en/stable/changelog.html			transitive	
15 requirements.txt	pypi:beautifulsoup4	4.12.2	MIT License	https://pypi.org/project/beautifulsoup4/4.12.2	https://www.crummy.com/software/BeautifulSoup/bs4/			transitive	pypi:soups
16 requirements.txt	pypi:binarnot	0.4.4	BSD License	https://pypi.org/project/binarnot/0.4.4	https://github.com/audreyr/binarnot			transitive	pypi:chard
17 requirements.txt	pypi:boolean.py	4.0	BSD-2-Clause	https://pypi.org/project/boolean.py/4.0	https://github.com/bastikr/boolean.py			transitive	
18 requirements.txt	pypi:certifi	2023.7.22	Mozilla Public License 2.0	https://pypi.org/project/certifi/2023.7.22	https://github.com/certifi/python-certifi			transitive	
19 requirements.txt	pypi:cffi	1.16.0	MIT License	https://pypi.org/project/cffi/1.16.0	http://cffi.readthedocs.org			transitive	pypi:pycpa
20 requirements.txt	pypi:chardet	5.2.0	GNU Lesser General Public	https://pypi.org/project/chardet/5.2.0	https://github.com/chardet/chardet			transitive	

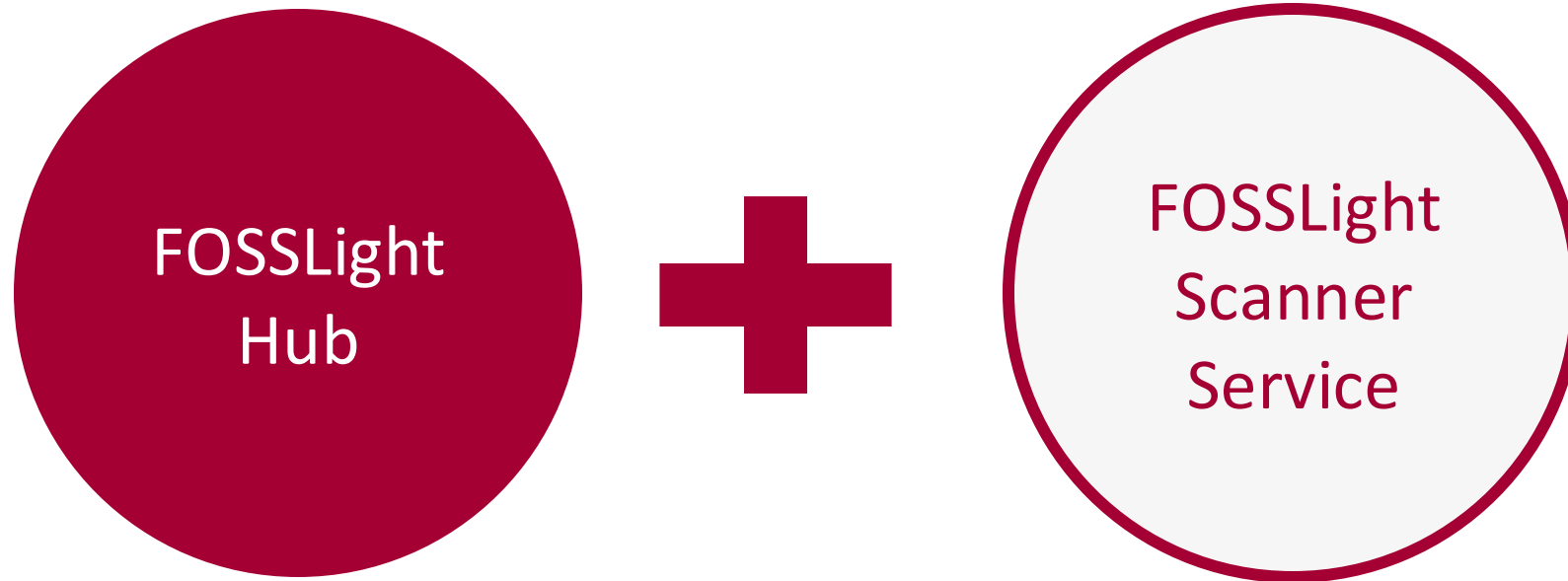
FOSSLight Hub + FOSSLight Scanner

- FOSSLight Hub에서 한번에 처리할 수 없을까?



FOSSLight Hub + FOSSLight Scanner

- FOSSLight Hub에서 한번에 처리할 수 있을까?



FOSSLight Hub에서 한번에 호출

- Self-Check > URL 분석

The screenshot shows the FOSSLight-LGE web interface. The top navigation bar includes tabs for Dashboard, License, Open Source, Project, 3rd Party, Self-Check, and 1576_selfCheck. The left sidebar lists various system components like Dashboard, License, Open Source, Project, 3rd Party, BAT, Binary DB, Vulnerability, Self-Check, Compliance Status, External Link, User Settings, and System.

In the Self-Check section, the 'URL' radio button is selected. A red box highlights the input field labeled 'Enter the link of the source to be analyzed' and the 'send' button. A red arrow points to the 'URL' radio button.

Below the input field, there is a 'Pre-Review' dropdown and a table of analysis results.

ID	Binary Name or Source Pa	OSS Name	OSS Versior	License	Download Loca	Homepage	Copyright Text	OSS De	License	Vulnerability	Notic	Sourc	Restric	Ex
1		pypi:cyclonedx-pyt...	8.5.1	Apache-2.0	https://pypi.org	https://github.com					✓			
4	src/fossilight_util/reso...	Required		Required							?	?		
25	src/fossilight_util/help...	Required		Apache-2.0			Copyright (c) 2021 ...				✓			

FOSSLight Hub에서 한번에 호출

• Self-Check > URL 분석

1. FOSSLight Scanner Service에 project 생성 & 분석
2. 분석 결과를 호출한 FOSSLight Hub 의 self-check project로 업로드

FOSSLIGHT-LGE

soim.kim

Dashboard License Open Source Project 3rd Party Self-Check 1576_selfCheck

Project Name | testtttt Created | 김소임/책임연구원/SW공학(연)Open Source TP CTO SW센터 (2025-02-13) Edit

Comment | https://github.com/LGE-OSS/example loaded from https://fs.lge.com/project/pypi-test-f4c861bf/

Edit Permission

Self-Check Notice

☐ Upload Analysis Result ☒ URL ☐ Project Search (fs.lge.com)

Enter the link of the source to be analyzed

URL send

Pre-Review

ID	Binary Name or Source Pa	OSS Name	OSS Versior	License	Download Loc	Homepage	Copyright Text	OSS De	License	Vulnera	Notic	Sourc	Restric	Ex
1		pypiclonepx-pyt... New open source	8.5.1	Apache-2.0	https://pypi.or	https://github.				!	✓			
4	src/fossilight_util/reso...	Required		Required							?	?		
25	src/fossilight_util/help...	Required		Apache-2.0			Copyright (c) 2021 ...			!	✓			

FOSSLight Hub에서 한번에 호출

- Self-Check > FOSSLight Scanner Service Project Search

FOSSLIGHT-LGE

soim.kim

Close << Dashboard License Open Source Project 3rd Party Self-Check 1576_selfCheck

Project Name | testtttt Created | 김소임/책임연구원/SW공학(연)Open Source
 Comment | https://github.com/LGE-OSS/example
 loaded from https://fs.lge.com/project/pypi-test-f4c861bf/

Edit Permission +

Self-Check Notice

☐ Upload Analysis Result ☐ URL ☒ Project Search (fs.lge.com)

Project UUID 52fae401-4ecf-4d5a-8b89-2b6090e6f730 send

PYPI_test.xlsx 2025-11-10 14:51:13

Pre-Review

ID	Binary Name or Source Pa	OSS Name	OSS Versior	License	Download Loc	Homepage	Copyright Text	OSS De	License	Vulner	Notic	Sourc	Restric	Ex
1		pypi:cyclonedx-pyt... New open source	8.5.1	Apache-2.0	https://pypi.or	https://github.					✓			
4	src/fosslight_util/reso...	Required		Required							?	?		
25	src/fosslight_util/help...	Required		Apache-2.0			Copyright (c) 2021 ...				✓			

FOSSLight Scanner Service에 별도로 생성해둔 Project가 있는 경우 load

FOSSLight Hub에서 한번에 호출

- 각각 서비스 구동 후 간단하게 연동!

FOSSLIGHT-LGE

soim.kim

Close << Dashboard License Open Source Project 3rd Party Self-Check 1576_selfCheck Code management >> [Full Screen]

706 Code Name [Search]

Code No	Code Name	Code Description
706	External Analysis Setting	System Detail Setting Code

Page 1 of 1 15 Count: 1

Save

Detail No	Detail Name	Detail Description	Sub Code	Order	Use YN	Delete
101	FL Scanner Url	https://fs.lge.com		1	Y	Delete
102	Admin Token	ac024cdef4391e5dceaa70a1a5a6f947e1a56496		2	Y	Delete

Count: 2

System

Statistics

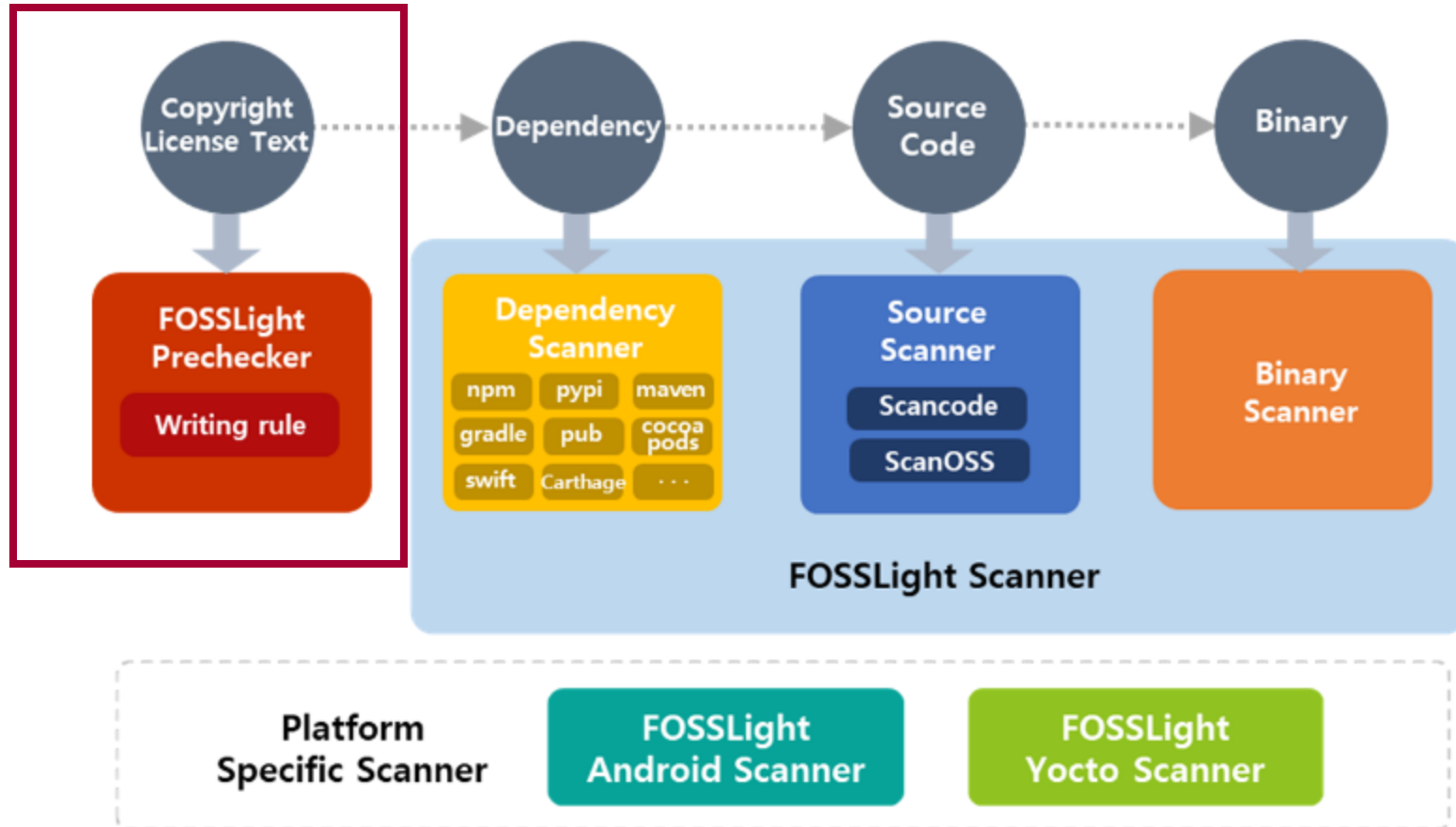
Code management

Restriction management

FOSSLight Prechecker with Jenkins

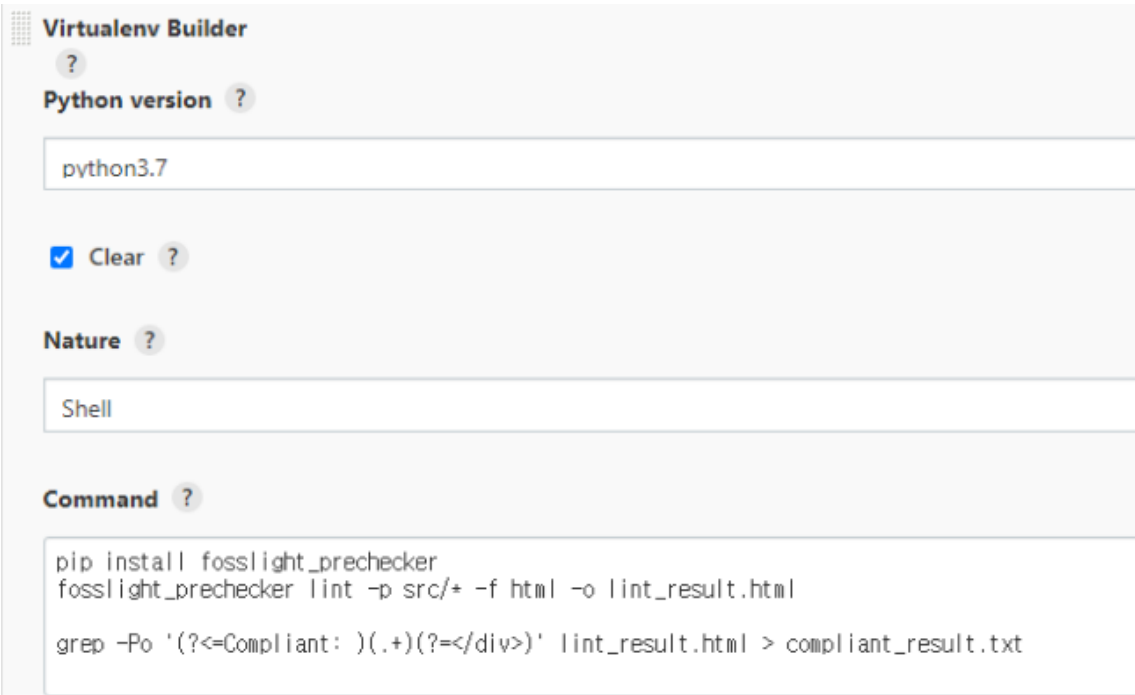
FOSSLight Prechecker

- 소스 코드 내 저작권 및 라이선스 규칙 준수 여부 체크



Jenkins 프로젝트에서 FOSSLight Prechecker 연동하기

1. Project 생성
2. 실행 주기 설정 -> 빌드 유발
3. FOSSLight Prechecker 실행 환경 설정 (lint 모드 실행)



Virtualenv Builder

Python version ?

python3.7

☒ Clear ?

Nature ?

Shell

Command ?

```
pip install fosslight_prechecker
fosslight_prechecker lint -p src/+ -f html -o lint_result.html

grep -Po '(?<=Compliant: )(.)?(?</div>)' lint_result.html > compliant_result.txt
```

4. FOSSLight Prechecker 결과 파일 메일링

FOSSLight Prechecker lint 모드 결과 메일링 예시

File (Total 1) ▾  lint_result.html (2.9KB)

Internet Header ▾

FOSSLight Reuse Lint

Compliant: OK

- Open Source Package file: N/A
- Detected licenses:
 - LicenseRef-LGE-Proprietary
- Files without copyright / total: 0 / 2
- Files without license / total: 0 / 2

« Files without License or Copyright »

File	License	Copyright
------	---------	-----------

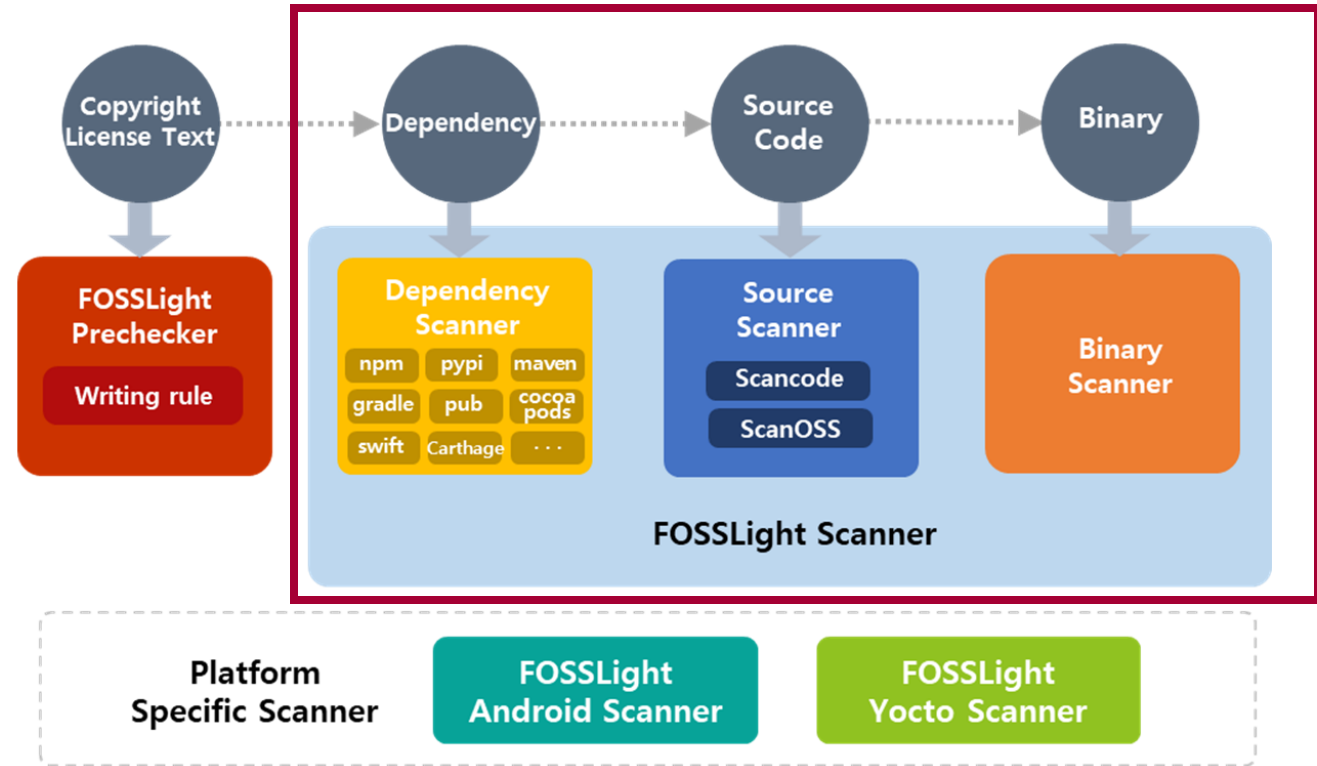
신규 수정 사항을 반영하면서
저작권이나 License 표기가 없는
파일 알림하여 보완 요청

Compliant가 NOT-OK인 경우, [Source Code 내 저작권 및 License 표기 규칙](#)을 참조하시기 바랍니다.

FOSSLight Scanner with Jenkins

FOSSLight Scanner

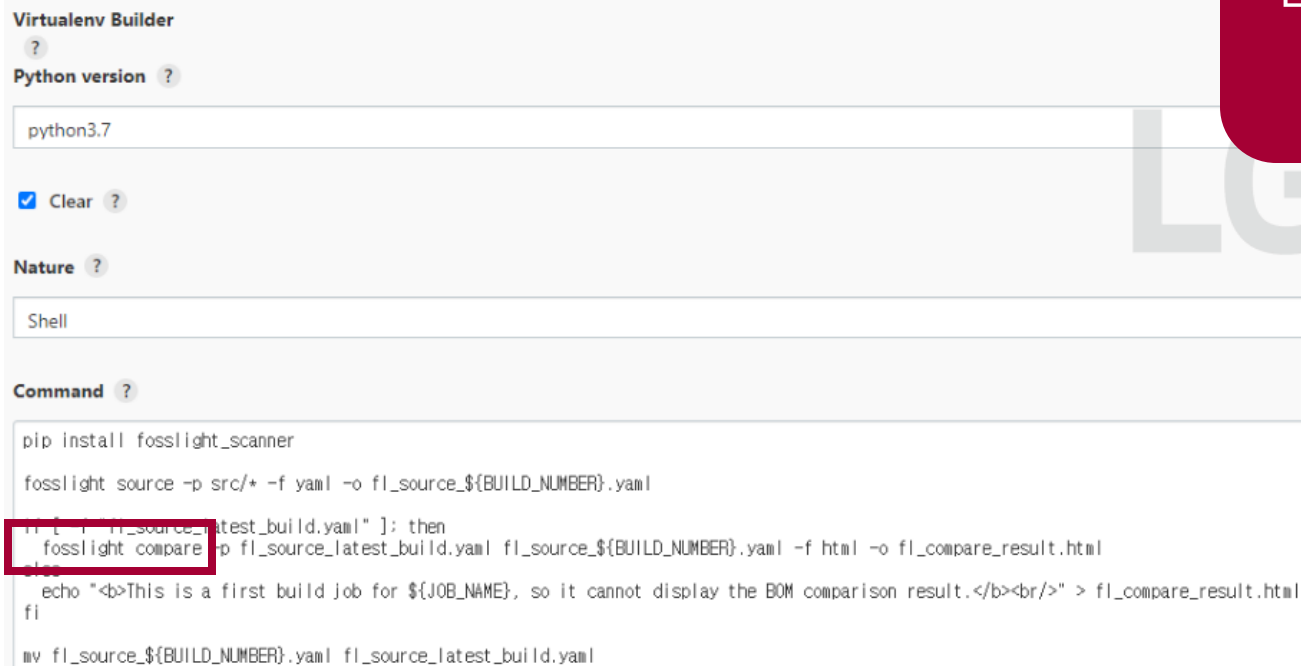
- 하기 분석을 수행하는 Scanner
 - FOSSLight Dependency Scanner
 - FOSSLight Source Scanner
 - FOSSLight Binary Scanner



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

Jenkins 프로젝트에서 FOSSLight Scanner 연동하기

1. Project 생성
2. 실행 주기 설정 -> 빌드 유발
3. FOSSLight Scanner 실행 환경 설정



```
Virtualenv Builder
Python version ?
python3.7

[ ] Clear ?

Nature ?
Shell

Command ?
pip install fosslight_scanner

fosslight source -p src/* -f yaml -o fl_source_${BUILD_NUMBER}.yaml

if [ -f "fl_source_latest_build.yaml" ]; then
  fosslight compare -p fl_source_latest_build.yaml fl_source_${BUILD_NUMBER}.yaml -f html -o fl_compare_result.html
else
  echo "<b>This is a first build job for ${JOB_NAME}, so it cannot display the BOM comparison result.</b><br/>" > fl_compare_result.html
fi

mv fl_source_${BUILD_NUMBER}.yaml fl_source_latest_build.yaml
```

분석 후 추출된 SBOM을 이전
버전에서 분석된 SBOM파일과
Compare

4. 결과 파일 메일링

FOSSLight Scanner Compare 결과 예시

File (Total 3) ▾ ☐ X fl_compare_result.xlsx (5.2KB)

Internet Header ▾

FOSSLight Scanner Compare Result

BOM Compare Result

- Before FOSSLight Report file: /var/lib/jenkins/workspace/FL Scanner Example project/fl_source_latest_build.yaml
- After FOSSLight Report file: /var/lib/jenkins/workspace/FL Scanner Example project/fl_source_2.yaml

Status	OSS_Before	License_Before	OSS_After	License_After
Same				

BUILD SUCCESS

URL: <http://10.178.94.16:8088/job/FL%20Scanner%20Example%20project/2/>

Project: FL Scanner Example project

Date: Tue, 16 Aug 2022 19:37:54 +0900

Duration: 1 min 43 sec

Cause: Started by user admin

이전 버전 대비
추가/수정/삭제된 OSS 정보를
리포팅

-> 신규 추가된 OSS에 대한
보안취약점 확인하고,
License를 확인하여 Compliance
준수하도록 가이드

FOSSLight MCP 서버

FOSSLight MCP 서버

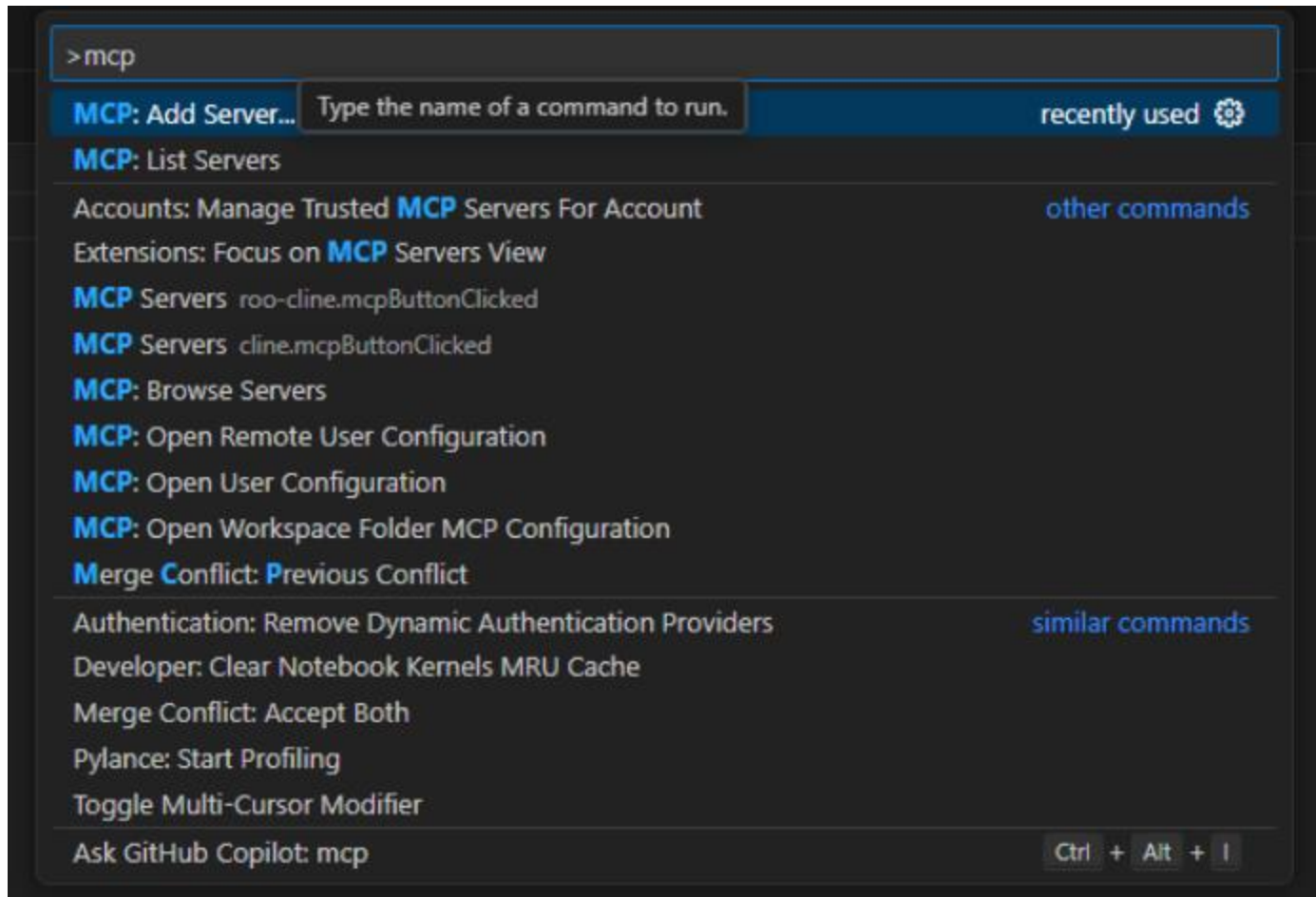
- FOSSLight Scanner Service에 프로젝트 생성 / 조회 / 분석 / 요약 등의 기능 제공

The screenshot displays the FOSSLight Scanner Service interface. At the top, there's a navigation bar with the FOSSLight logo, 'scanner' text, and links for Projects, Guide, Support, and Notice. A user profile 'soim.kim' is visible in the top right. Below the navigation bar, the 'Projects' section shows '43 Active' and '1 Archived' projects. A search bar and filters for ViewPermission, Pipeline, Status, and Sort are present. The main table lists projects with columns: Name, Dependencies, Detected Open Source, Pipelines, Status, and ViewPermission. Four large red circles are overlaid on the table, highlighting specific features: '생성' (Create) over the first project row, '분석' (Analyze) over the second project row, '조회' (Search) over the third project row, and '요약' (Summary) over the fourth project row. The table data includes project names like 'testtttttt', 'test', and 'scan_all', with various status indicators like 'Success' and 'PRIVATE'.

Name	Dependencies	Detected Open Source	Pipelines	Status	ViewPermission
testtttttt Created 3 days ago	8	17	scan_all		PRIVATE
test	8	17			PRIVATE
			scan_all		PRIVATE
			scan_all	Success	PRIVATE
			scan_all	Success	PRIVATE

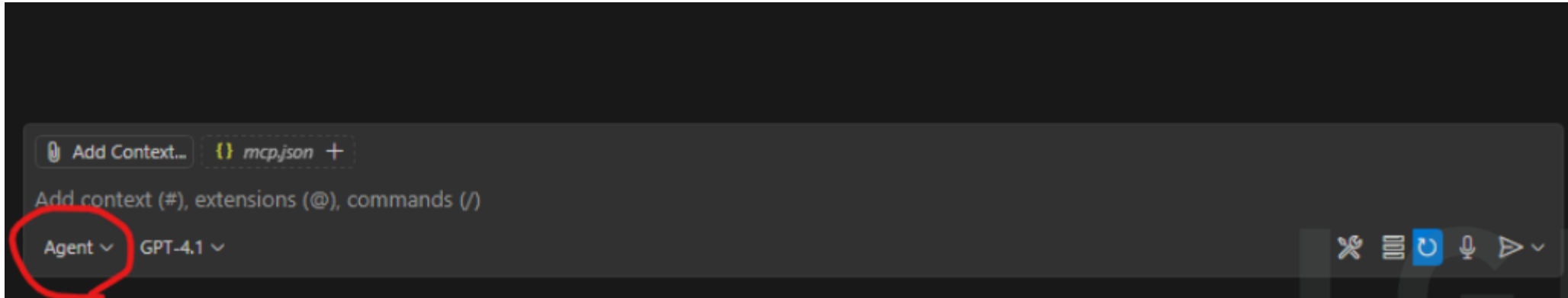
VSCode내 Github Copilot 연동 예시

- MCP : Add Server 로 FOSSLight MCP 서버 연동



VSCode내 Github Copilot 연동 예시

- Copilot Chat 에서 Agent 모드로 설정



VSCode내 Github Copilot 연동 예시

- FOSSLight Scanner Service Project 생성 및 분석

```

fosslight에 minss_test 프로젝트를 만들고 분석해줘. repository는 https://github.com/fosslight/fosslight_source_scanner.git 아

Ran create_and_analyze_project - fosslight (MCP Server) ✓

Input
{
  "name": "minss_test",
  "url": "https://github.com/fosslight/fosslight_source_scanner.git"
}

Output
{"success":true,"reply":"✅ **프로젝트 생성 및 분석 시작 완료!**\n\n📌 **프로젝트 URL**: https://fs.lge.com/project/minss_test-202509092357-e384876b\n📄 **분석 데이터**: {'project_uuid': 'e384876b-d8b5-4b54-b098-bad5d5e60f50'}\n\n⌚ 분석이 진행 중입니다. 완료되면 결과를 다운로드할 수 있습니다."}

{
  "success": true,
  "reply": "✅ **프로젝트 생성 및 분석 시작 완료!**\n\n📌 **프로젝트 URL**: https://fs.lge.com/project/minss_test-202509092357-e384876b\n📄 **분석 데이터**: {'project_uuid': 'e384876b-d8b5-4b54-b098-bad5d5e60f50'}\n\n⌚ 분석이 진행 중입니다. 완료되면 결과를 다운로드할 수 있습니다."
}

minss_test 프로젝트가 FOSSLight에 생성되었고 분석이 시작되었습니다.

• 프로젝트 URL: https://fs.lge.com/project/minss_test-202509092357-e384876b
• 분석 진행 중이며, 완료 후 결과를 다운로드할 수 있습니다.

분석이 완료되면 결과를 바로 안내해드릴 수 있습니다.
  
```


VSCode내 Github Copilot 연동 예시

- FOSSLight Scanner Service Project 조회

```
> Ran list_projects - fosslight (MCP Server) ✓
```

FOSSLight에서 조회된 나의 프로젝트 리스트(총 164개)입니다. 최근 생성된 주요 프로젝트 일부는 아래와 같습니다:

1. fosslight_source_scanner_analysis_retry-202509090701 (분석결과 있음)
2. ethan_mcp_test-202509090658 (분석결과 없음)
3. fosslight_mcp_test-202509031359 (분석결과 있음)
4. file_upload_mcp-202509011532 (분석결과 없음)
5. AISE_SAMPLE_project-202509010520 (분석결과 없음)

더 많은 프로젝트가 있으며, 특정 프로젝트의 분석결과가 궁금하면 [번호]번 프로젝트 결과 분석해줘 라고 요청하시면 됩니다.

VSCode내 Github Copilot 연동 예시

• FOSSLight Scanner Service Project 결과 요약

1번 프로젝트 결과 분석해줘

> Ran `download_and_analyze_results` - fosslight (MCP Server)

✓

1번 프로젝트(fosslight_source_scanner_analysis_retry-202509090701) 결과 분석입니다.

🔥 주요 위험 요소

- **GPL** 라이선스(매우 높음): pypi:rfc3987, pypi:gemfileparser2, pypi:text-unidecode (총 6개 파일)
- **LGPL** 라이선스(높음): pypi:charset, pypi:crc32c, pypi:intbitset, pypi:psycpg2-binary (총 8개 파일)
- **MPL** 라이선스(중간): pypi:certifi, pypi:pathspec, pypi:fqdn (총 6개 파일)

📊 시트별 현황

구분	파일/패키지 수	주요 위험 라이선스	위험도
소스코드	36개	없음	낮음
의존성 패키지	297개	GPL, LGPL, MPL	높음/중간
바이너리 파일	데이터 없음	없음	낮음

💡 대응 방안

1. **GPL/AGPL** 패키지 제거 또는 대체: 위험 패키지(GPL 등)는 MIT, Apache 2.0, BSD 등으로 대체 권장
2. **LGPL/MPL** 패키지 검토: 수정/링크 여부 및 공개 요구사항 확인
3. 라이선스 클리어링 문서화 및 컴플라이언스 프로세스 구축

참고자료

- FOSSLight Hub 가이드
- 라이선스 가이드
- 대체 OSS 검색

추가로 상세 시트별 위험도, 패키지별 라이선스 정보도 제공 가능합니다. 필요한 정보가 있으면 말씀해 주세요!



Q&A

