도구별 의존성 분석 방식

카카오 오픈소스기술파트
임현지
rain.im

목차

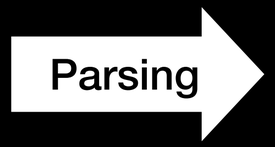
용어 정리

Static 분석 / Dynamic 분석

```
lxml
pandas>=0.19.2
pytest>=3
requests>=2.3.0
# Documentation Only
sphinx_rtd_theme

# The order of packages is significant, because pip processes
them in the order
# of appearance. Changing the order has an impact on the
overall integration
# process, which may cause wedges in the gate later.
sphinx!=1.6.6,!=1.6.7,>=1.6.2 # BSD
sphinx-feature-classification>=0.2.0 # Apache-2.0
os-api-ref>=1.4.0 # Apache-2.0
```

Manifest file




```
{artifact = lxml}
{artifact = pandas, version = 0.19.2}
{artifact = pytest, version = 3}
{artifact = requests, version = 2.3.0}
{artifact = sphinx_rtd_theme}
{artifact = sphinx, version = [1.6.6, 1.6.7, 1.6.2]}
{artifact = sphinx-feature-classification, version = 0.2.0}
{artifact = os-api-ref, version = 1.4.0}
```

Dependency list

용어 정리

Static 분석 / Dynamic 분석

```
module example.com/mymodule

go 1.16

require (
    github.com/some/dependency v1.2.3
    github.com/another/dependency v0.4.0
)
```

Manifest file

go mod graph

```
example.com/mymodule github.com/some/dependency@v1.2.3
example.com/mymodule github.com/another/dependency@v0.4.0
```

Output by command

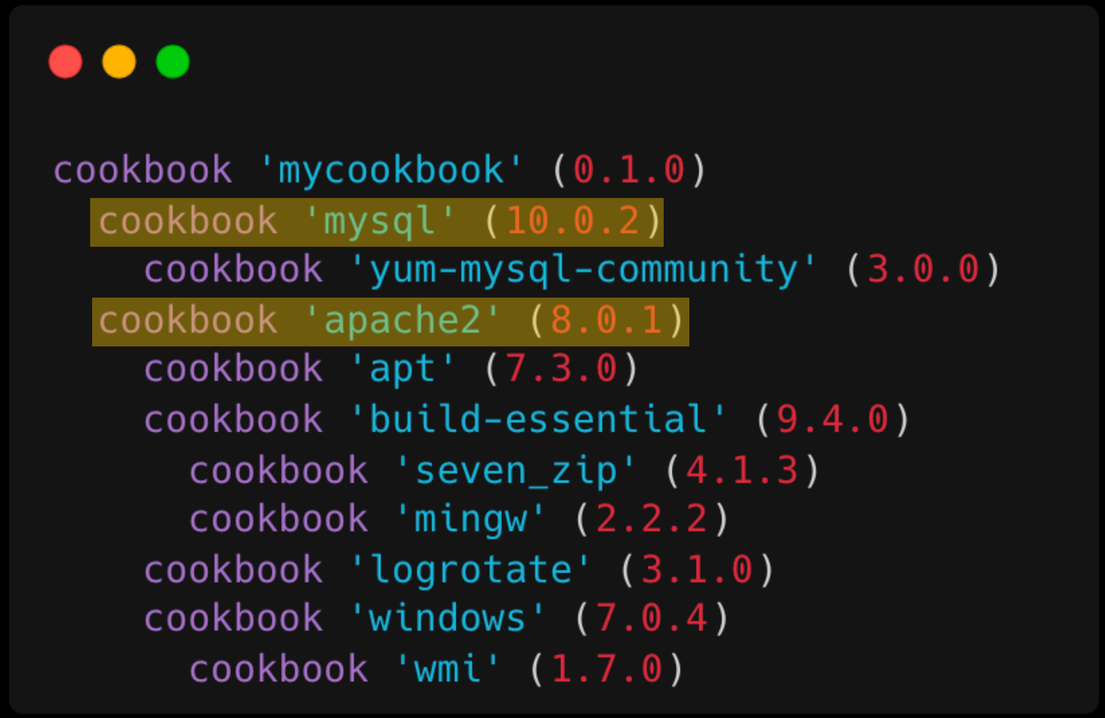
Parsing

```
{artifact = github.com/some/dependency, version = v1.2.3}
{artifact = github.com/another/dependency, version = v0.4.0}
```

Dependency list

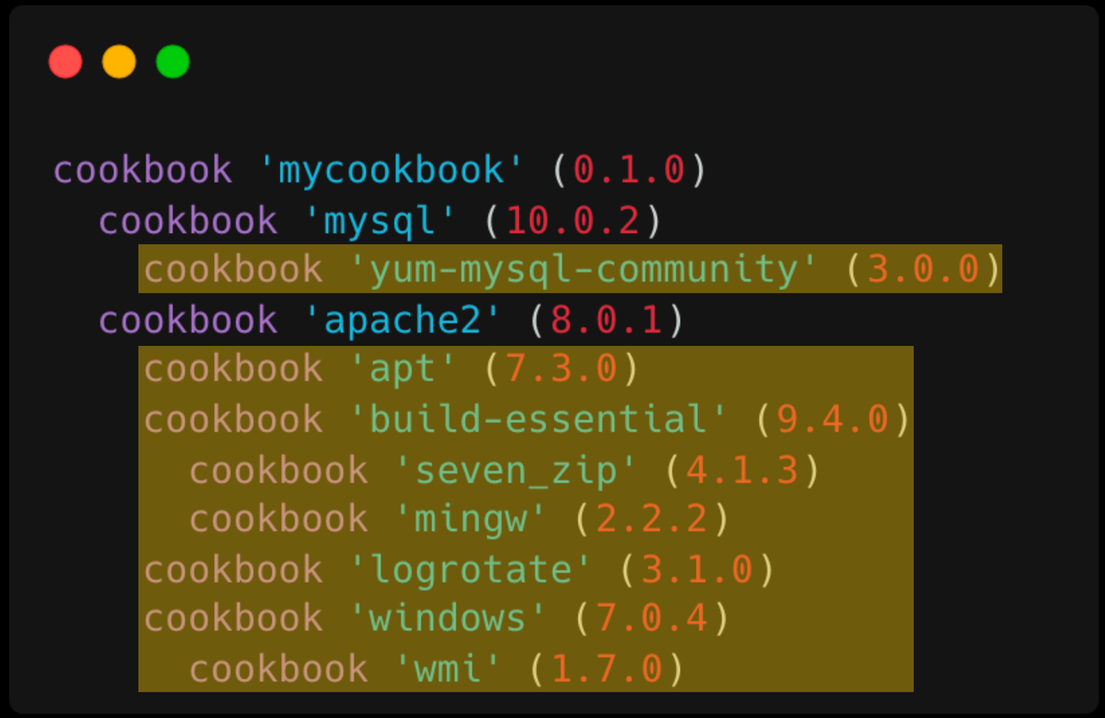
용어 정리

Direct Dependency / Transitive Dependency



용어 정리

Direct Dependency / Transitive Dependency



FOSSA

- https://fossa.com/
- 분석 가능한 의존성 리스트
  - https://github.com/fossas/fossa-cli/tree/master/docs/references/strategies
  - 총 30개의 Package Manager에 대해 의존성 분석을 지원
- 한 패키지 매니저에 대해 우선순위를 두고 다양한 방법의 분석 방식 시도

FOSSA

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
.NET	NuGet	Static	.nuspec .csproj .xproj .vbproj .dbproj .fsproj packages.config project.json	O	X	
			project.assets.json	O	O	
	Paket	Static	paket.lock	O	O	
Clojure	Leiningen	Dynamic	-	O	O	lein deps :tree-data
Elixer	mix	Dynamic	-	O	O	mix deps -all
Erlang	Rebar	Dynamic	-	O	O	rebar3 tree -v

FOSSA

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
Dart	Pub	Dynamic	pubspec.yaml pub spec.lock	O	O	pub deps -s compact
		Static	pubspec.yaml	O	X	
fortran	fpm	Static	fpm.toml	O	X	
golang	Dep	Static	Gopkg.lock Gopkg.toml	O	X	
	Glide	Static	glide.lock	O	X	
	golang modules	Dynamic	-	O	O	go mod graph
Haskell	Cabal	Dynamic	../plan.json	O	O	
	Stack	Dynamic	-	O	O	stack ls dependencies json
PHP	Composer	Static	composer.lock	O	O	

FOSSA

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
Java	Gradle	Dynamic	-	O	O	공식문서 참조
	Maven	Dynamic	-	O	O	1. Maven plugin
						2. maven dependency:tree
		Static	pom.xml	O	X	3. parsing pom.xml
iOS / Objective-C	Carthage	Static	Cartfile.resolved	O	O	
	CocoaPods	Static	Podfile.lock	O	O	
			Podfile	O	X	
	SPM	Static	Package.swift	O	Δ	package.resolved 포함시 transitive 분석 가능
			project.pbxproj	O	Δ	

FOSSA

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
Node.js	yarn	Static	yarn.lock	O	O	
	npm	Static	package-lock.json	O	O	
	pnpm	Static	pnpm-lock.yaml	O	O	
	-	Static	package.json	O	X	
Perl		Static	MYMETA.json MYMETA.yml META.json META.yml	O	O	
Ruby	bundler	Static	Gemfile.lock	O	O	
		Dynamic	-	O	O	bundle show
Rust	Cargo	Dynamic	Cargo.lock	O	O	cargo metadata — format-version 1

FOSSA

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
Python	Conda	Dynamic	-	O	O	conda env create —json -file environemnt.yml —dry-run —force
	Pipenv	Dynamic	-	O	O	pipenv graph —json-tree
	Poetry	Static	pyproject.toml	O	Δ	poetry.lock 포함시 transitive 분석 가능
	Setup tools	Static	requirements.txt setup.py	O	X	
R	renv	Static	DESCRIPTION	O	X	1. DESCRIPTION 파싱 2. renv.lock 파싱
			renv.lock	Δ	O	
Scala	sbt	Dynamic	-	O	O	sbt dependencyTree sbt dependencyBrowseTreeHtml
		Static	pom.xml	O	X	sbt makePom

FOSSLight

- https://fosslight.org/ko/
- 분석 가능한 의존성 리스트
  - https://fosslight.org/fosslight-guide/scanner/3_dependency.html
  - 총 11개의 Package Manager에 대해 의존성 분석을 지원
- 의존성 분석과 OSS 정보 생성을 위해 다양한 오픈소스 활용

FOSSLight

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
Java	Maven	Dynamic	-	O	O	license-maven-plugin
	Gradle	Dynamic	-	O	O	License Gradle Plugin
Android	Gradle	Dynamic	-	O	O	android-dependency-scanning
Node.js	NPM	Dynamic	-	O	O	NPM license checker
Python	Pipenv	Dynamic	-	O	O	pip-licenses
Dart	Pub	Dynamic	-	O	O	flutter_oss_licenses
iOS / Objective-C	CocoaPods	Static	Podfile.lock	O	O	
	SPM	Static	Package.resolved	O	O	v1, v2 분석 가능
	Carthage	Static	Cartfile.resolved	O	O	

FOSSLight

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
Golang	golang modules	Dynamic	-	O	O	go list -m mod=mod -json all
.NET	Nuget	Static	packages.config project.assets.json	O	O	nuget api를 활용하여 license, repository 정보 수집
Kubernetes	Helm	Dynamic	-	O	X	helm dependency build

ORT

- oss-review-toolkit.org/
- 분석 가능한 의존성 리스트
  - https://github.com/oss-review-toolkit/ort#details-on-the-tools
  - 총 22개의 Package Manager에 대해 의존성 분석을 지원
- Transitive dependency 분석을 위해 재귀 함수를 활용한 파싱 로직 사용

ORT

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
C / C++	Conan	Dynamic	conan.lock	O	O	conanfile.txt conanfile.py -> lock 생성
SPDX documents		Static	SPDX documents	O	O	
Dart	Pub	Dynamic	-	O	O	
Golang	Dep	Dynamic	Gopkg.lock	O	O	go get -d $dependency
	golang modules	Dynamic	-	O	O	go mod graph …
Haskell	Stack	Dynamic	-	O	O	stack ls dependencies json
Java	Gradle	Dynamic	-	O	O	
	Maven	Dynamic	-	O	O	

ORT

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
Node.js	Bower	Dynamic	-	O	O	-allow-root list —json
	NPM	Dynamic	node_modules	O	O	install 명령어로 의존성 설치후 node_modules 파싱
	PNPM					
	Yarn					
.NET	NuGet	Static	.nuspec packages.config	O	O	
iOS / Objective-C	Carthage	Static	Cartfile.resolved	O	O	
	CocoaPods	Dynamic	-	O	O	podspec 생성 후 파싱
PHP	Composer	Dynamic	composer.lock	O	O	install 명령어로 lock 파일 생성
Ruby	Bundler	Dynamic	Gemfile.lock	O	O	Ruby script 사용

ORT

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
Python	Pip	Dynamic	-	O	O	python-inspector
	Pipenv	Dynamic	requirements.txt	O	O	install 명령어로 requirements.txt 생성
	Poetry					
Rust	Cargo	Dynamic	Cargo.lock	O	O	cargo metadata -format-version1
Scala	sbt	Dynamic	-	O	O	Maven과 같은 분석 방식 공유

OLIVE Platform

- https://olive.kakao.com/intro
- 분석 가능한 의존성 리스트
  - https://olive.kakao.com/docs/project/analyzable
  - 총 15개의 Package Manager에 대해 의존성 분석을 지원
- 올해 Transitive dependency 분석 지원 예정

OLIVE Platform

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
JAVA	Gradle	Dynamic	-	O	X	
		Static	*.gradle *.gralde.kts	O	X	
	Maven	Static	pom.xml	O	X	
iOS / Objective-C	Carthage	Static	Cartfile	O	X	
	CocoaPods	Static	Podfile .podspec	O	X	
	SPM	Static	Package.swift project.pbxproj	O	X	
	Tuist	Static	graph.json	O	X	지원 예정
Node.js	NPM	Static	package.json	O	X	
Python	Setup tools	Static	requirements.txt setup.py	O	X	

OLIVE Platform

Language / Package Manager		분석 방식	분석 대상 파일	Direct Dependency	Transitive Dependency	비고
Golang	Dep	Static	Godeps.json Gopkg.toml Gopkg.lock	O	X	
	go modules	Static	go.mod	O	X	
Ruby	Bundler	Static	Gemfile	O	X	
Chef		Static	Berksfile	O	X	
CMake		Static	CMakeLists.txt	O	X	
Android NDK		Static	Android.mk	O	X	
Git Module		Static	.gitmodules	O	X	
File Search		-	*.framework *.lib, *.jar, *.dll *.ttf, *.otf	O	X	확장자 파일 검색