오픈소스 라이선스가 요구하는 고지 의무와 SBOM 표준(SPDX)에 기반한 오픈소스 고지문 자동 생성 방안

한국저작권위원회 오픈소스라이선스 전문가 커뮤니티 2022년 연구과제
(장학성, 황은경)

SK텔레콤 장학성

2022-12-02

오픈소스 라이선스 고지 요구 사항

Binary form 재배포 시

MIT

- https://opensource.org/licenses/MIT

```
Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

...
```

- 저작권 고지
- 라이선스 포함

BSD

- https://opensource.org/licenses/BSD-2-Clause

```
Copyright (c) <YEAR>, <OWNER>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this
list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer in the documentation
and/or other materials provided with the distribution.
```

- 저작권 고지
- 라이선스 포함

Apache

- https://www.apache.org/licenses/LICENSE-2.0

```
4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
```

- 저작권 고지
- 라이선스 포함
- (수정사항에 대한 고지)

GPL-2.0 / LGPL-2.1

- https://www.gnu.org/licenses/old-licenses/gpl-2.0.html

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

- 저작권 고지
- 라이선스 포함
- 수정사항에 대한 고지

GPL-2.0 / LGPL-2.1 – Written Offer

- https://www.gnu.org/licenses/old-licenses/gpl-2.0.html

> 3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
>
> a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- 저작권 고지
- 라이선스 포함
- 수정사항에 대한 고지
- (소스 코드를 직접 제공하지 않는다면) Written Offer

Written Offer

- 다운로드 링크 만으로는 부족하다는 법원 판결

> Skype Technologies SA was selling a Linux-based phone on its website, allegedly without providing the source code and the mandatory references to the GPL text. Skype argued that both of them were available through a URL mentioned in the documentation. The Court, however, found this kind of reference insufficient under paragraphs 1 and 3 of the GPL v2 licence: «The license states that offering source code for downloading, is only applicable if and when the binaries are downloadable from the same place» [1]. The licence text and the source code should be included in the packaging itself. To

- 포함해야 할 내용
  - valid for at least three years
  - to give any third party
  - for a charge no more than your cost of physically performing source distribution

주요 라이선스 고지 요구 사항 요약

- 바이너리 형태로 오픈소스 재배포 시 고지 요구 사항

	MIT	BSD	Apache	GPL
저작권	O	O	O	O (소스 코드 내 고지 가능)
라이선스 사본	O	O		O
수정 사항			△	O (소스 코드 내 고지 가능)
Written Offer				O

Written Offer

SBOM과 SPDX 표준

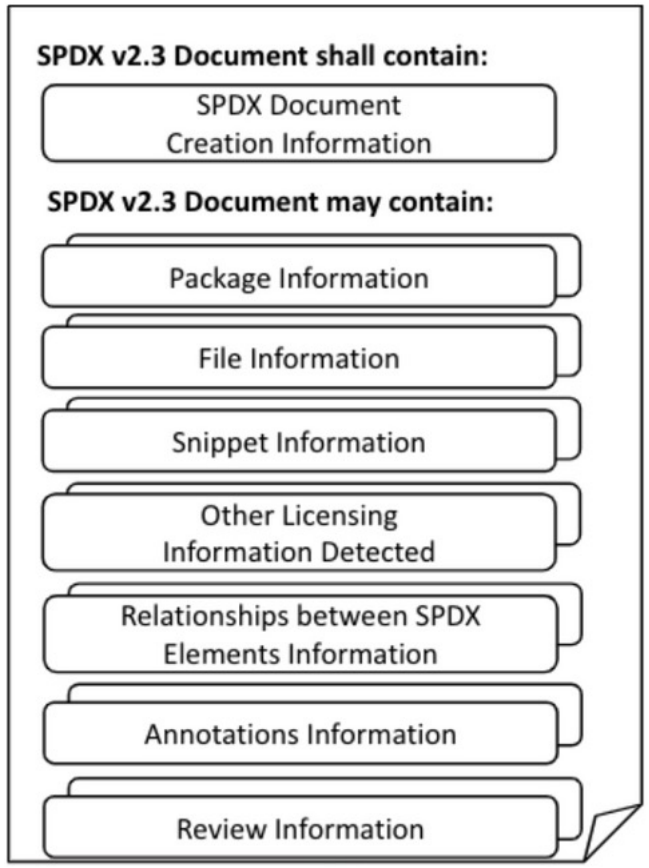
Software Bill of Materials

미 연방 행정명령 (14208)

- https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
- 국가 사이버 보안 강화의 일환으로 SBOM(Software Bill of Materials) 제출 의무화
- NITA에 의해 SBOM 최소 요구 사항 정의
  - 다음 세가지 표준화된 형식 중 하나로 작성되어야 함
  - SPDX : https://spdx.org/
  - CycloneDX : https://cyclonedx.org/
  - SWID Tags : https://nvd.nist.gov/products/swid

SPDX

- Linux Foundation 프로젝트
- 2021년 9월 ISO 표준 등록 : https://www.iso.org/standard/81870.html

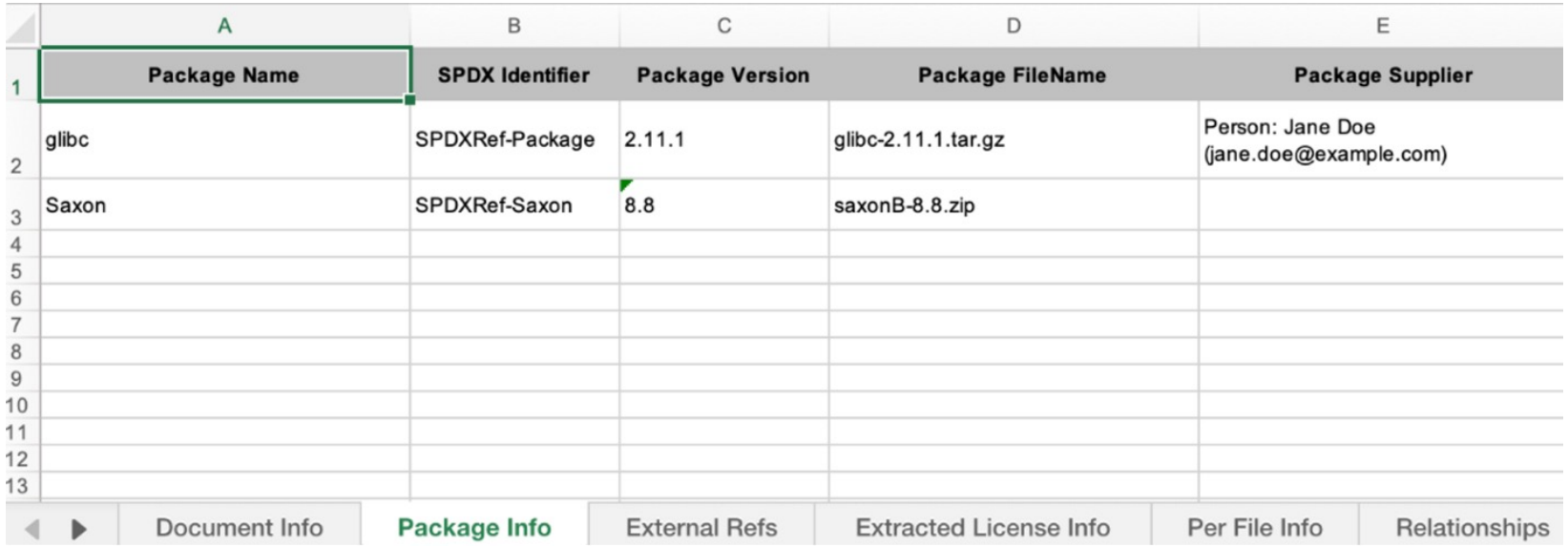


SPDX 데이터 포맷

- JSON
  - https://github.com/spdx/spdx-spec/blob/development/v2.2.2/examples/SPDXJSONExample-v2.2.spdx.json
- YAML
  - https://github.com/spdx/spdx-spec/blob/development/v2.2.2/examples/SPDXYAMLExample-2.2.spdx.yaml
- Tag/Value
  - https://github.com/spdx/spdx-spec/blob/development/v2.2.2/examples/SPDXTagExample-v2.2.spdx
- RDF/xml
  - https://github.com/spdx/spdx-spec/blob/development/v2.2.2/examples/SPDXRdfExample-v2.2.spdx.rdf.xml

SPDX Excel Template

- https://github.com/spdx/tools/blob/master/Examples/SPDXRdfExample-v2.1.xls
- SPDX 제공 Excel Template

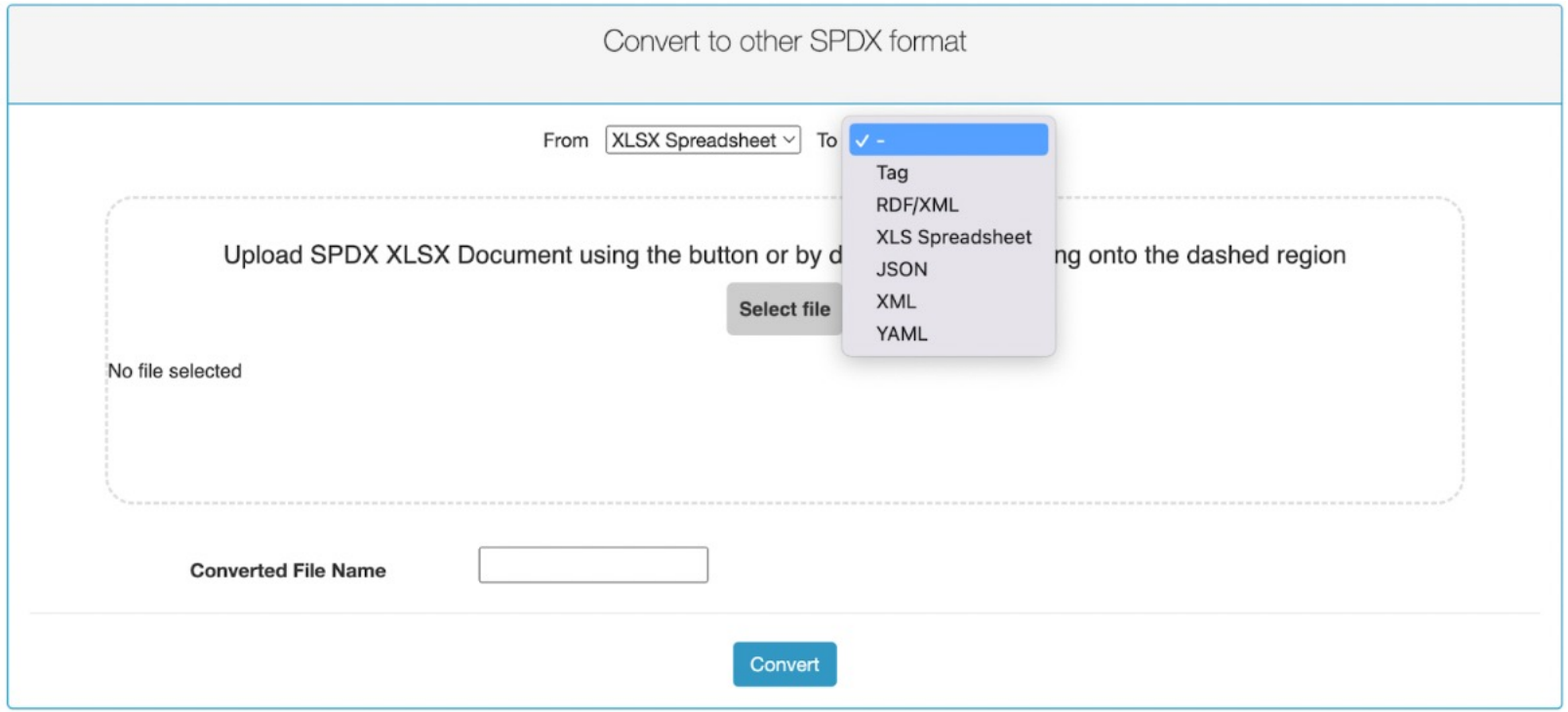


	A	B	C	D	E
1	**Package Name**	**SPDX Identifier**	**Package Version**	**Package FileName**	**Package Supplier**
2	glibc	SPDXRef-Package	2.11.1	glibc-2.11.1.tar.gz	Person: Jane Doe (jane.doe@example.com)
3	Saxon	SPDXRef-Saxon	8.8	saxonB-8.8.zip	
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					

Document Info | **Package Info** | External Refs | Extracted License Info | Per File Info | Relationships

SPDX Online Tool

- Convert to other SPDX format



SPDX 기반
오픈소스 고지문 자동 생성 도구

onot

onot

- https://github.com/sktelecom/onot

onot

onot is a tool that automatically creates open source software notices based on SPDX documents.

Installation

Use the package manager pip to install foobar.

```
pip install onot
```

or you can install latest verson from source code.

```
git clone https://github.com/sktelecom/onot.git ~/onot
cd ~/onot; python setup.py install
```

onot 사용법 (1)

- SPDX 문서 작성 : Package Info
  - Package Name, Version, License, Copyright, …

	A	B	C	D	E
1	**Package Name**	**SPDX Identifier**	**Package Version**	**Package FileName**	**Package Supplier**
2	glibc	SPDXRef-Package	2.11.1	glibc-2.11.1.tar.gz	Person: Jane Doe (jane.doe@example.com)
3	Saxon	SPDXRef-Saxon	8.8	saxonB-8.8.zip	
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					

Document Info | **Package Info** | External Refs | Extracted License Info | Per File Info | Relationships

onot 사용법 (2)

- onot 실행

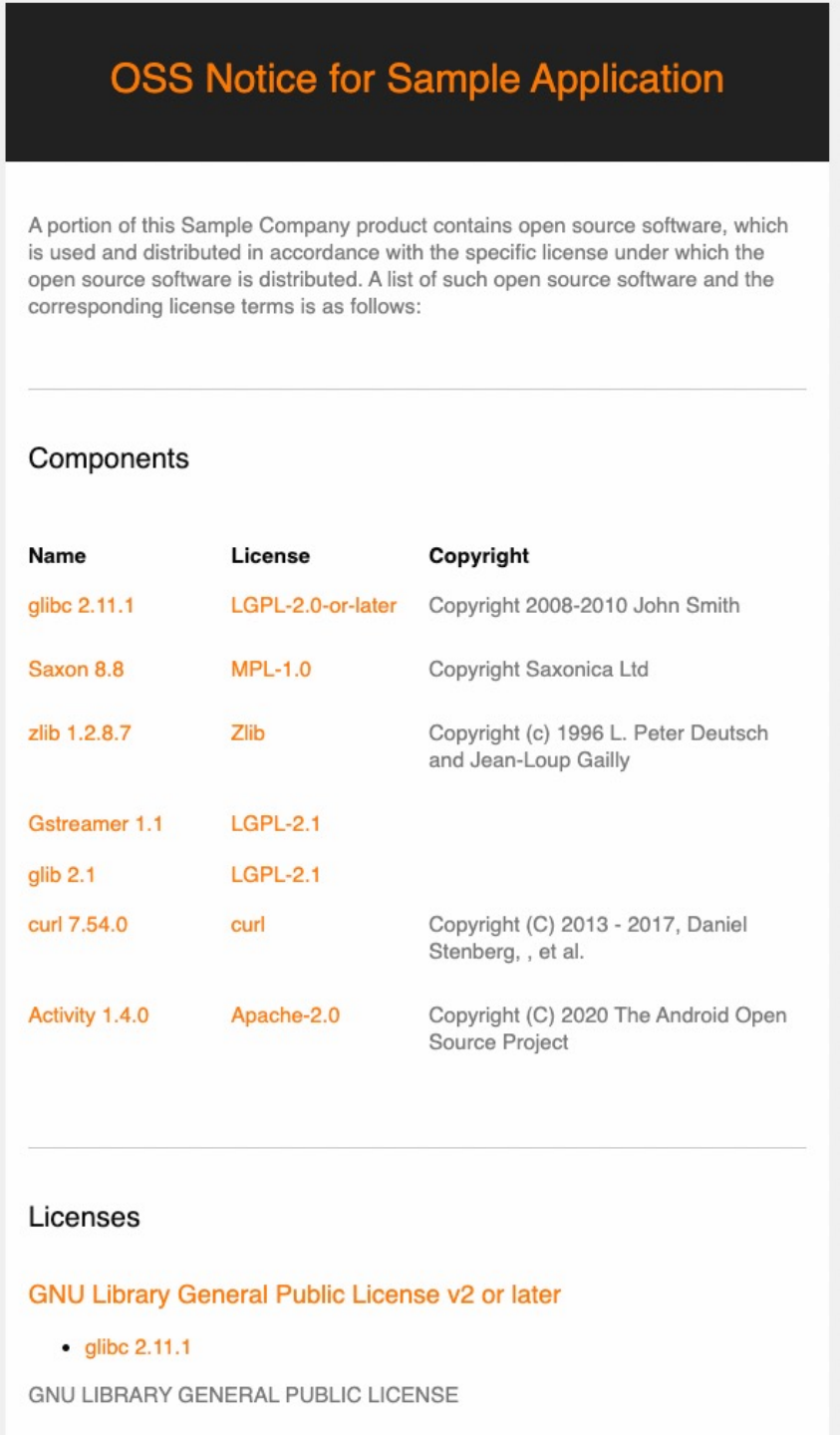
Usage

1. Prepare your input file. The input file is an Excel format SPDX document, and refer to the next page for how to prepare it.
2. Run onot command with two arguments.
    - `-i` or `--input` : SPDX document in Excel format containing open source information to be included in the OSS notice
    - `-o` or `--output_format` : File type of OSS notice to be generated (`html` or `text`)
    - Sample output : output/OSS_Notice_SPDX-Tools-v2.0_20221009_180948.html

```
$ onot --input sample/SPDXRdfExample-v2.1.xlsx --output_format html
```

onot 사용법 (3)

- Sample output
  - output/OSS_Notice_SPDX-Tools-v2.0.html



OSS Notice for Sample Application

A portion of this Sample Company product contains open source software, which is used and distributed in accordance with the specific license under which the open source software is distributed. A list of such open source software and the corresponding license terms is as follows:

Components

Name	License	Copyright
glibc 2.11.1	LGPL-2.0-or-later	Copyright 2008-2010 John Smith
Saxon 8.8	MPL-1.0	Copyright Saxonica Ltd
zlib 1.2.8.7	Zlib	Copyright (c) 1996 L. Peter Deutsch and Jean-Loup Gailly
Gstreamer 1.1	LGPL-2.1	
glib 2.1	LGPL-2.1	
curl 7.54.0	curl	Copyright (C) 2013 - 2017, Daniel Stenberg, , et al.
Activity 1.4.0	Apache-2.0	Copyright (C) 2020 The Android Open Source Project

Licenses

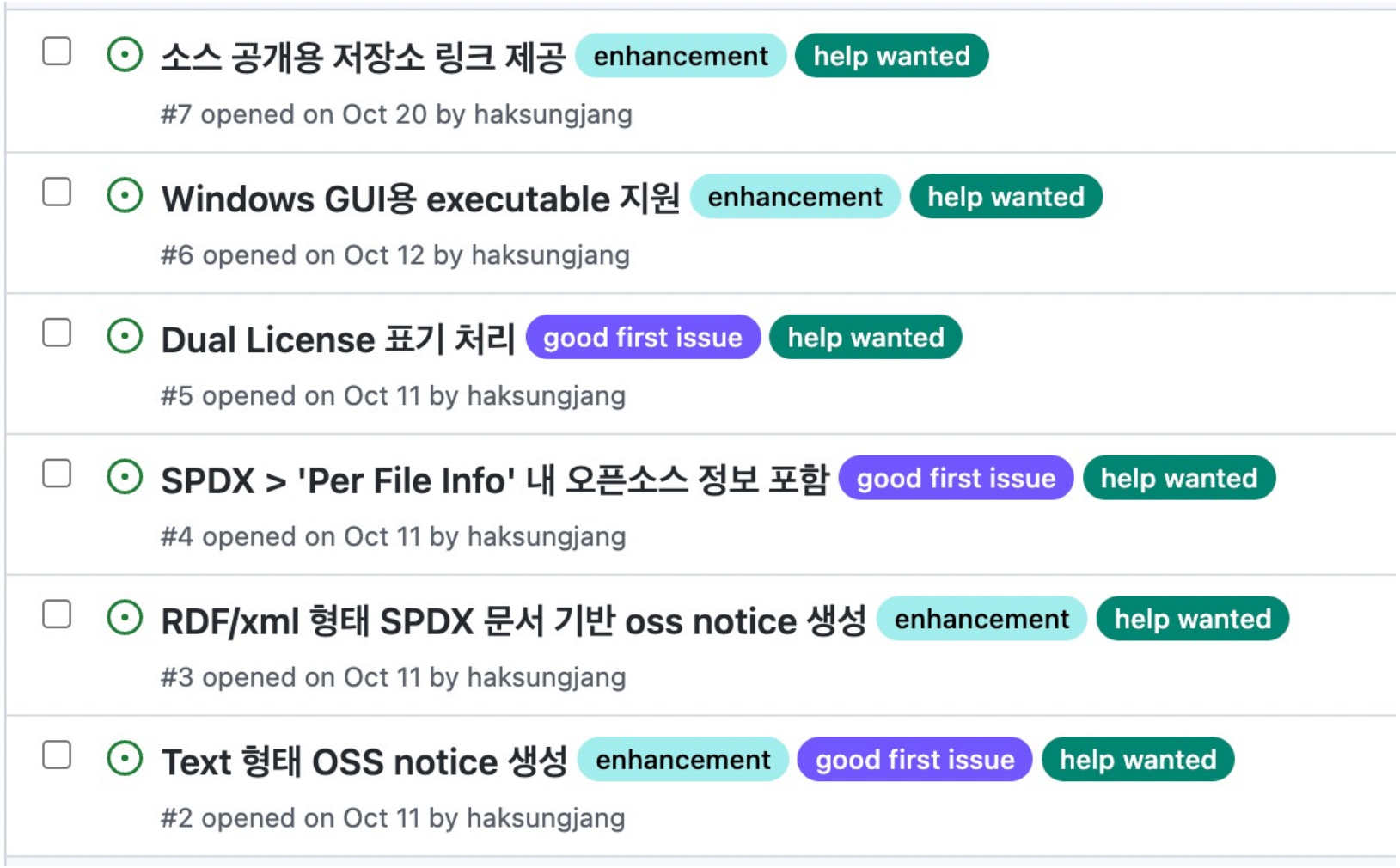
GNU Library General Public License v2 or later

- glibc 2.11.1

GNU LIBRARY GENERAL PUBLIC LICENSE

help wanted!

- https://github.com/sktelecom/onot/issues



감사합니다.

Thank you.