BEST OF BEST 7TH OTG

[Pharming]

[Pharming을 통해 얻은 ip, 공인 인증서 데이터 파싱]

[담당 : 최원영 멘토님]

개요

|  |
| --- |
|  |

개발환경

* Windows 10
* Python 3.6
* MS office Excel
* Mysql Workbench

프로젝트 구현

1. Pharming Server zip파일 다운로드

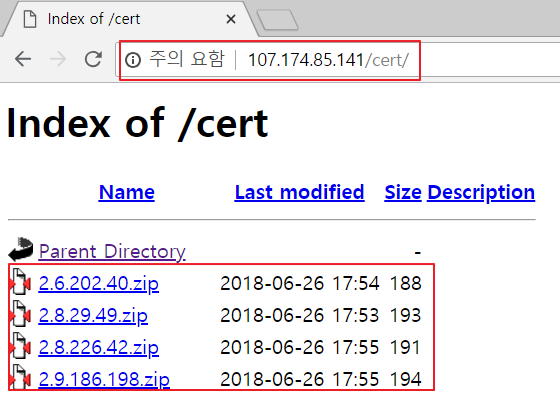


Figure 1 공인 인증서 서버 파일

공인 인증서가 저장되어 있는 (아이피).zip 파일이 저장되어 있는 서버를 확인할 수 있다. 해당 파일을 selenium을 사용해서 36833개의 인증서를 다운로드 하였다.

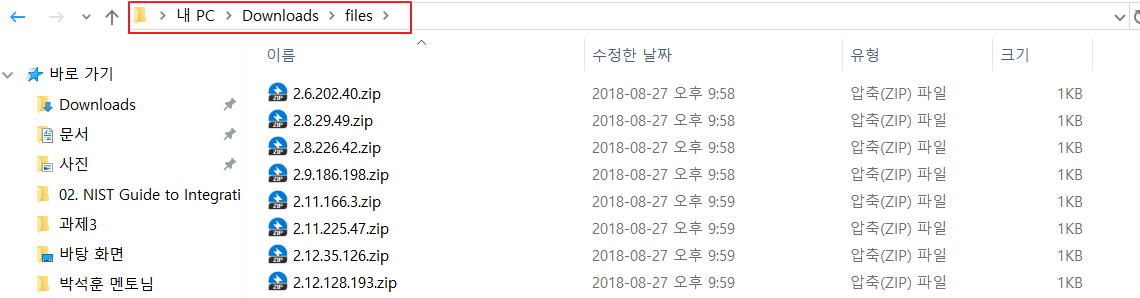


Figure 2 파일 다운로드

Selinium을 이용해서 다운로드 한결과 10시간이 걸렸다. 직접 클릭하듯 해당 URL에 접속하여 다운로드 하였다. 시간적으로 비효율적인 방법으로 생각되었다. 다음부터는 대용량의 파일을 다운로드 받는경우 urllib, urlopen과 같은 방법으로 사용하려 한다.

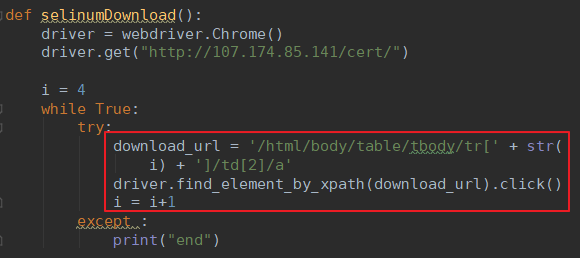


Figure 3 파일 다운로드

Selinum을 사용하여 (아이피).zip 파일을 다운로드 한다.

1. 다운로드 파일 압축 해제 및 DB 업로드

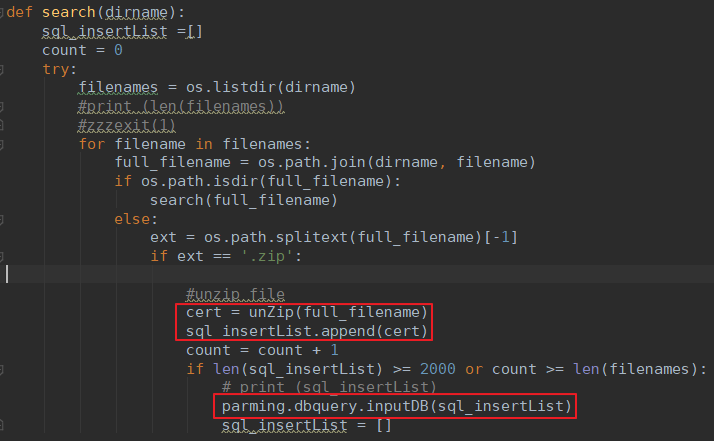


Figure 4 압축해제 및 DB 업로드

다운로드 한 파일의 압축을 풀고 입력된 IP, 은행명, 업로드 날짜 정보를 DB에 입력한다.

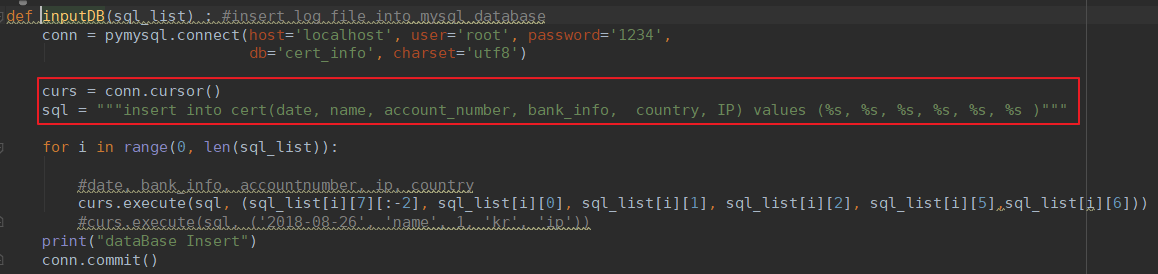


Figure 5 DB 파일 저장

DB에 signCert.txt 파일의 내용을 파싱해서 저장한다.

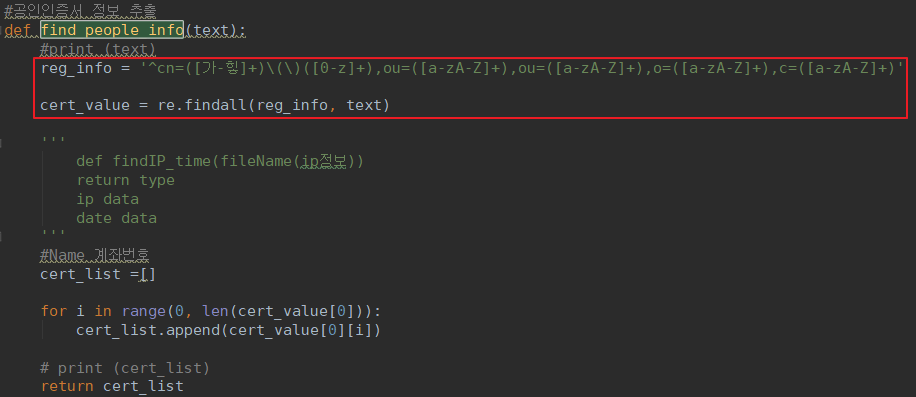


Figure 6 signCert.txt 파싱

DB에 signCert.txt 파일을 파싱한다.

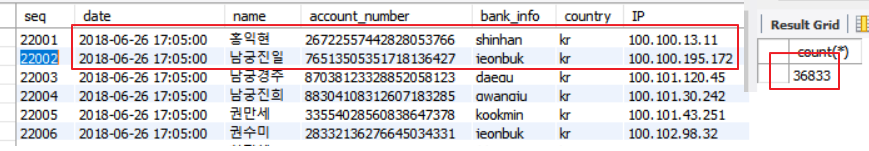


Figure 7 저장된 DB

DB에 입력된 signCert.txt 정보를 확인하였다.

1. IP별 국가 조회

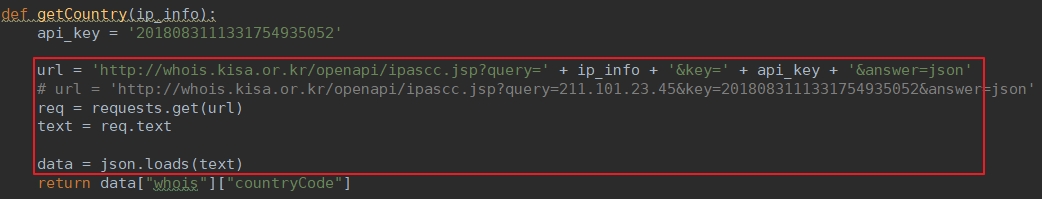


Figure 8 whois api로 국가코드 조회

내 Gmail 계정으로 로그인을 한다. 수신한 메일중 “fl0ckfl0ck@hotmail.com”으로부터 수신된 메일의 정보가 있는지 파악

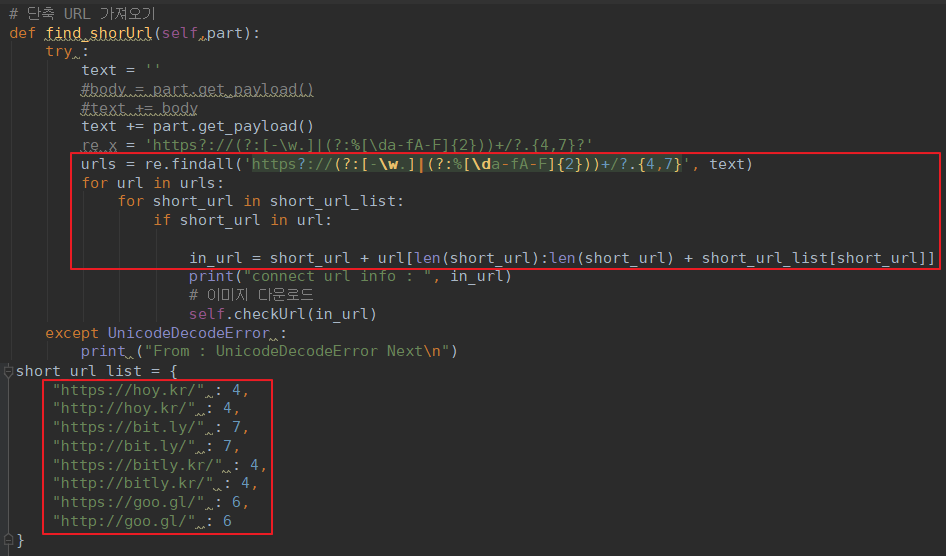


Figure 9 whois API 사용

Whois API를 이용하여 국가코드 검색

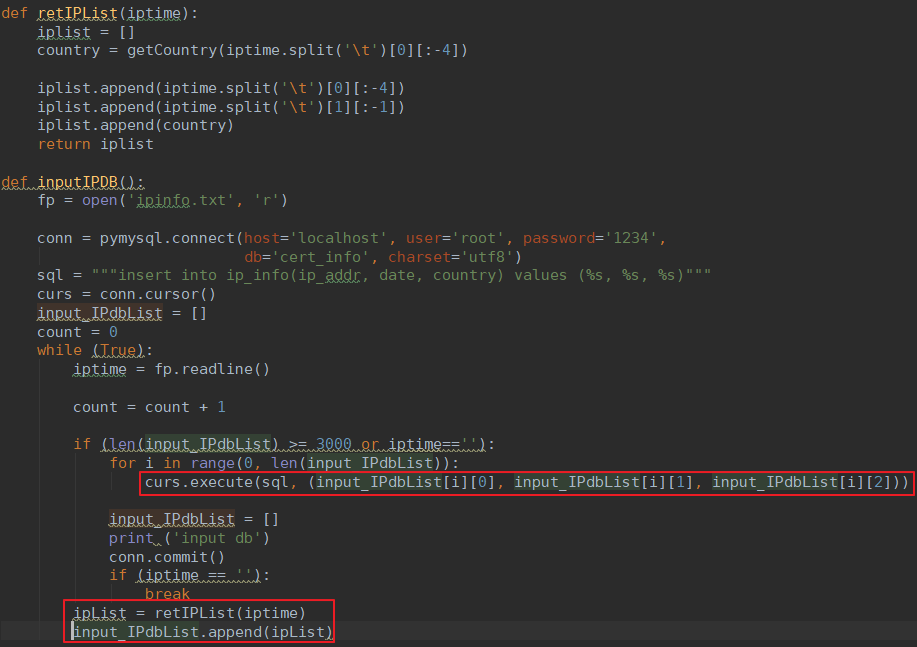


Figure 10 IP의 국가 정보 DB 입력

Whois API로 확보한 국가코드 정보를 DB에 입력한다.

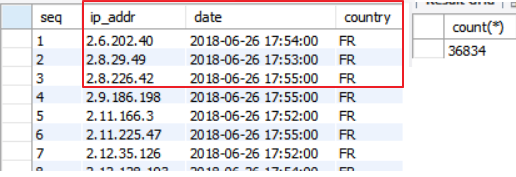


Figure 11 IP당 국가코드

인증서별 입력된 국가코드와 수를 확인 할 수 있다.

1. 유출국가 및 유출 은행수

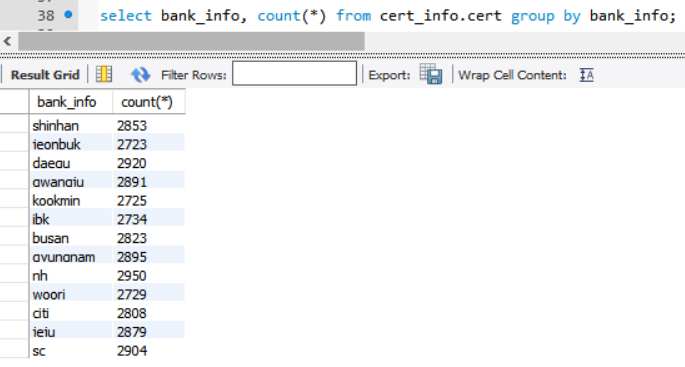


Figure 12 은행별 유출 건수

은행별 유출된 공인인증서 수가 다음과같이 DB로 확인 되었다.

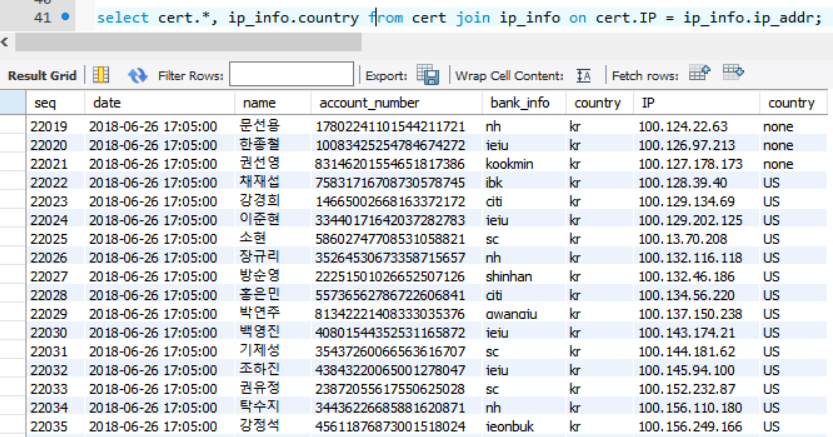


Figure 13 IP별 국가정보

IP별 국가정보를 조회한 결과를 확인 하였다.

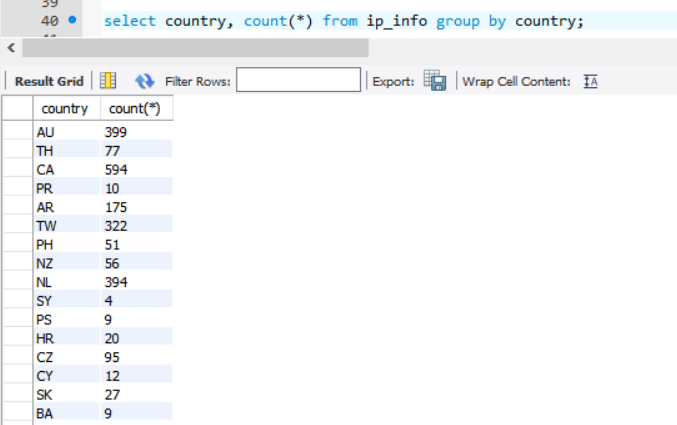


Figure 14 인증서가 유출된 국가

인증서가 유출된 국가정보를 확인 할 수 있다.

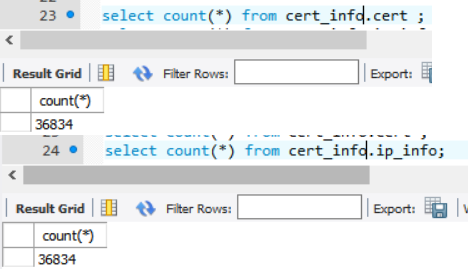


Figure 15 다운로드 받은 수 확인

저장한 파일수를 36834로 맞추었다. 처음 다운로드 받았던 파일을 실수로 종료하고 실행하는 경우가 발생하여 IP하나를 찾지 못하여 IP검색을 통한 1개의 IP를 찾아 내어 다시 입력하였다.

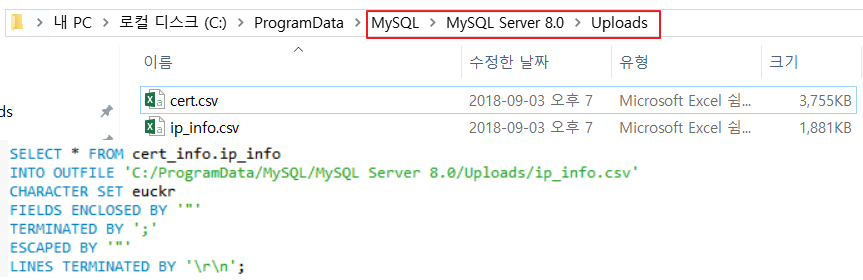


Figure mysql to csv 생성

SHOW VARIABLES LIKE 'secure\_file%'; 명령어로 얻은 경로에서 Mysql DB의 내용을 csv 파일로 생성하여 저장

프로젝트 결과 및 정리

1. 완성도 및 결과

이번 프로젝트의 완성도는 80% 정도로 생각 된다.

1. 파일 다운로드 방법 : Selinum을 사용한 .zip 파일 다운로드
2. Zip파일 압축 해제후 DB 업로드
3. WHOIS 국가 코드 조회 및 DB 업로드
4. DB 쿼리를 통한 유출 국가 정보 확인
5. 프로젝트를 통한 느낀점

이번 프로젝트를 통해서 지금까지 학습했던 , DB 쿼리 사용법, 파일을 반복적으로 입 출력하는 방법과, 새로운 WHOIS API 사용법을 학습 할 수 있었다. 앞의 과제를 통해서 학습한 내용덕에 간단하게 구현 할 수 있었다.