**\* 과제내용**

-> 사진에 들어가 있어야 할 정보, GPS 정보, JPG 형태로 저장합니다.

-> 해당 사진의 GPS 정보를 해당 BOB 센터가 아닌, 다른 지역(서울 제외) 으로 조작합니다.

**-> 분석 내용**

1) JPG 파일에 들어가 있는 GPS 관련 정보, 형식 및 자신의 사진에서 실제 GPS가 있는 파일에서의 Offset 등을 꼭 포함해서 조사합니다.

2) 디지털 포렌식 관점에서 어떻게 하면 조작할 수 있는지 논리적인 근거하에 작성합니다.

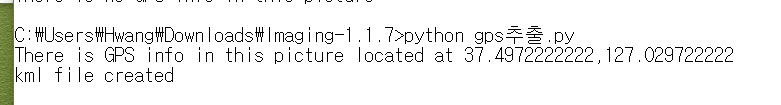
**[사진] 취약점 트랙 6기 교육생 황상두**

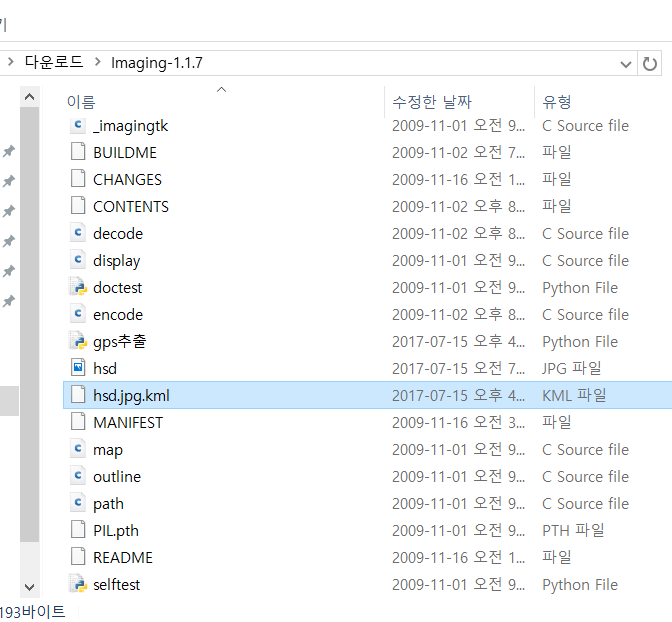


**[위치정보]대한민국 서울 특별시 강남구 역삼1동**



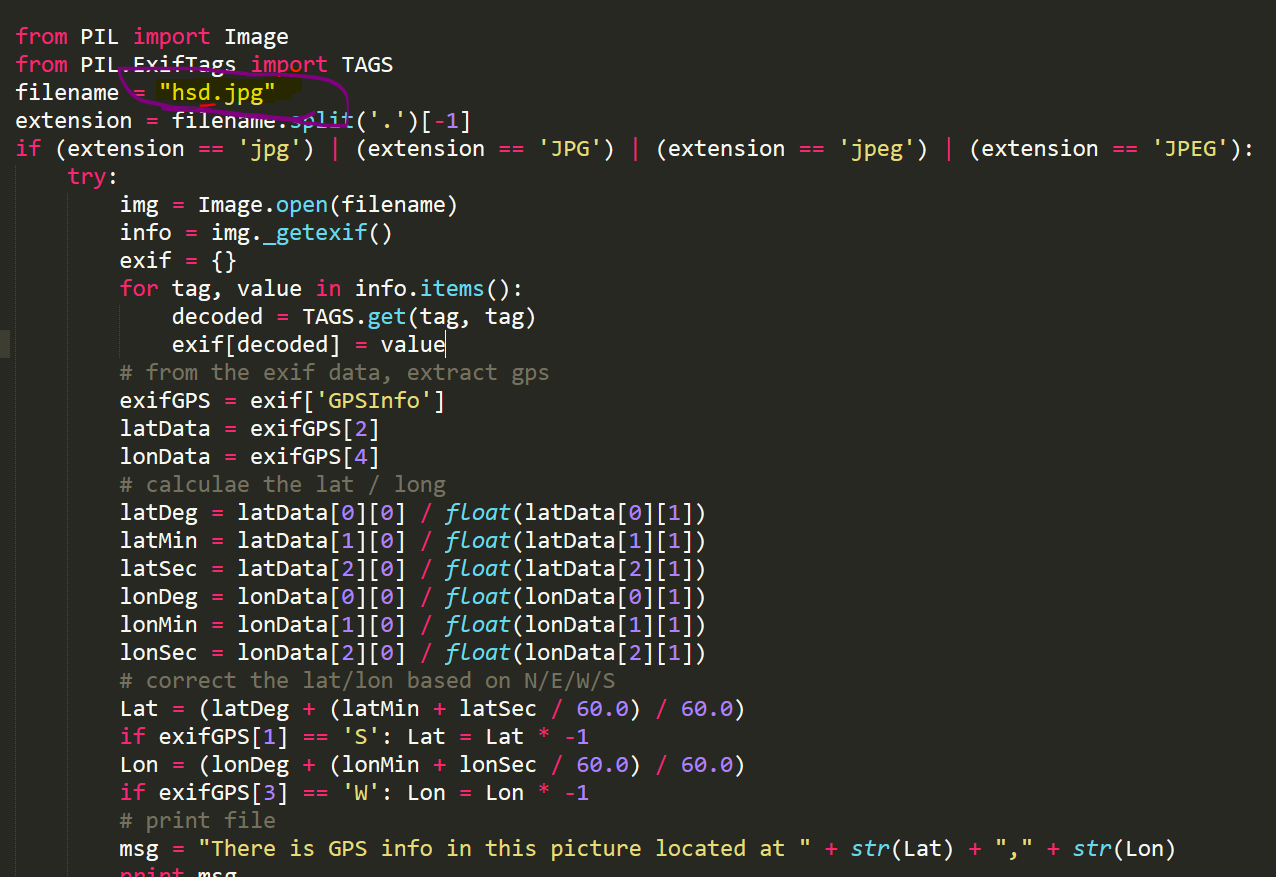
**Python 라이브러리를 이용**

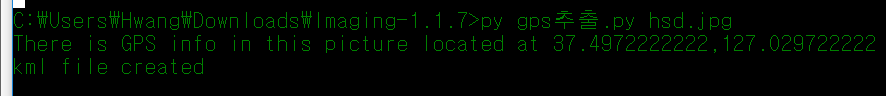






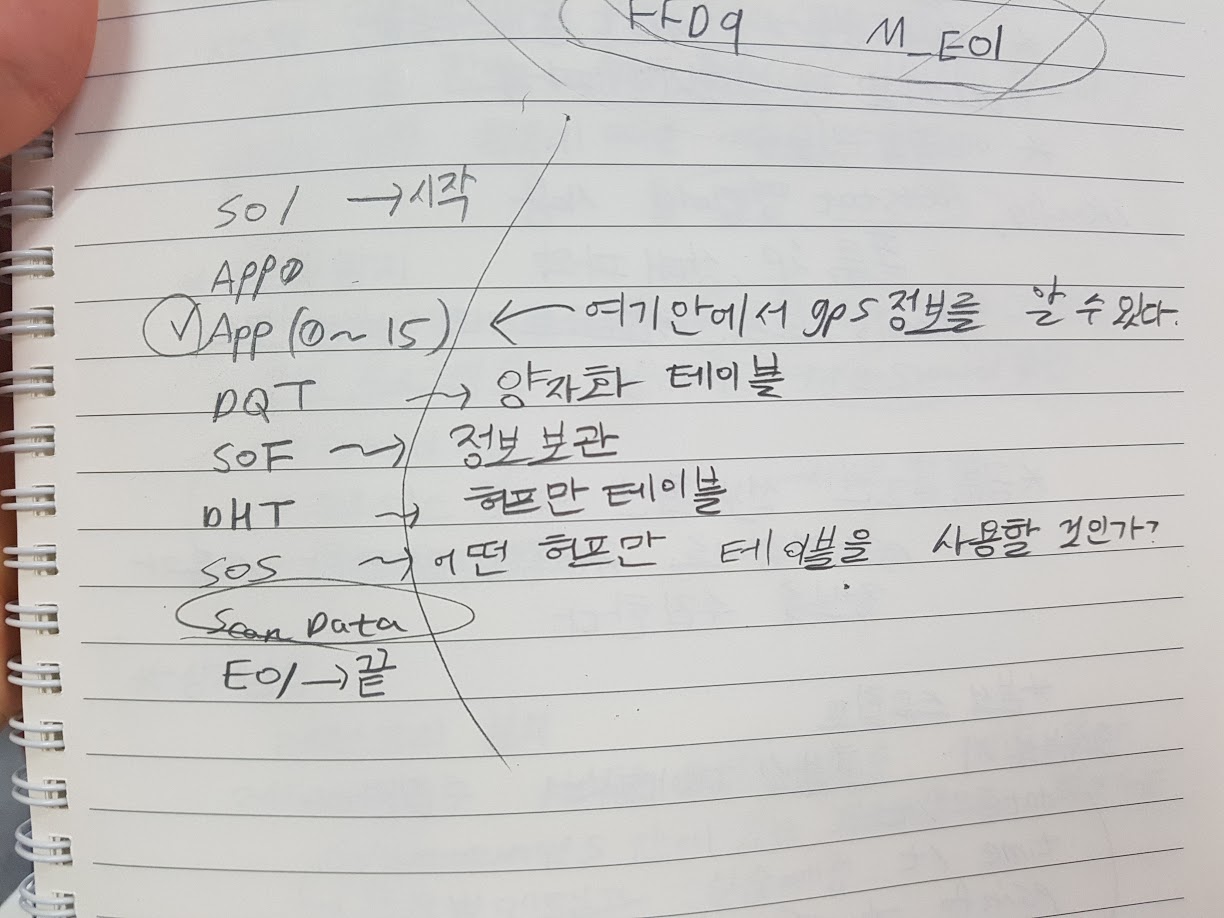
**실제와 동일하게 나옴.**

  
**\* 실행결과**



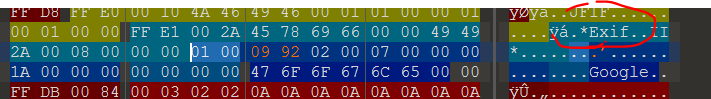
gps정보가 추출된 것을 볼 수 있습니다.

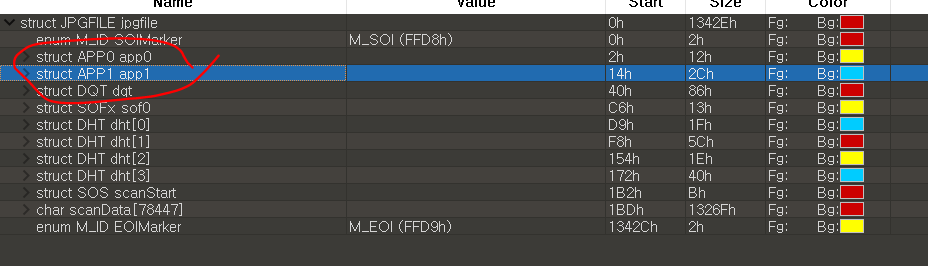
* **Jpg 헤더 분석**

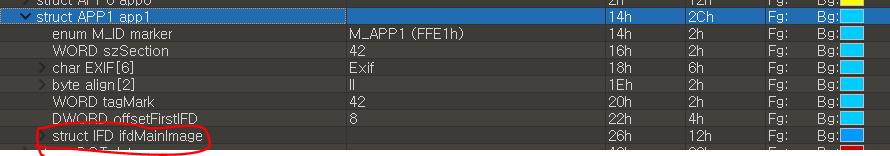


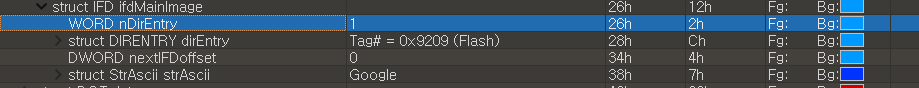
[참조] <http://fl0ckfl0ck.tistory.com/253>

Exif Format 🡨 GPS정보가 있는 곳입니다.





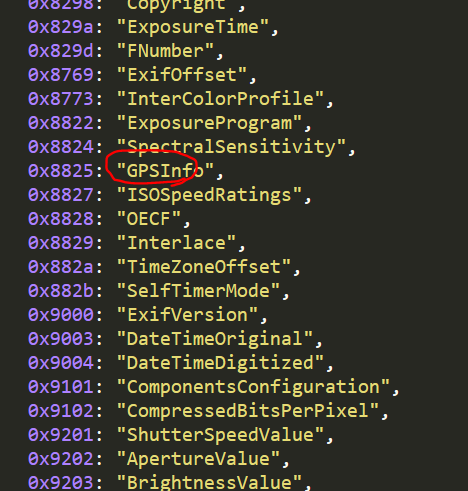


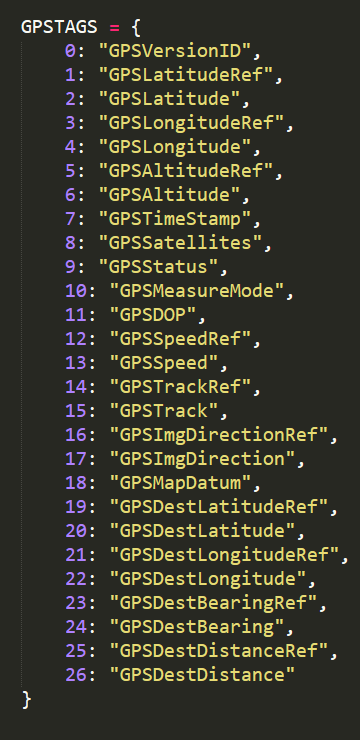
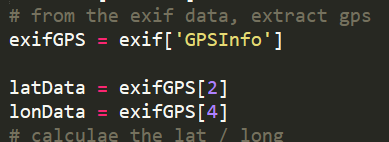




간단히 요약하자면

1. jpg헤더의 Maker를 통해 APP0의 위치를 알아낸다. (FFEx)의 형태를 가지고 있습니다.
2. 안에서 Exif를 찾아냅니다.
3. 이후 태그값으로 접근한다면 ‘GPSinfo’의 정보를 알아낼 수 있습니다.

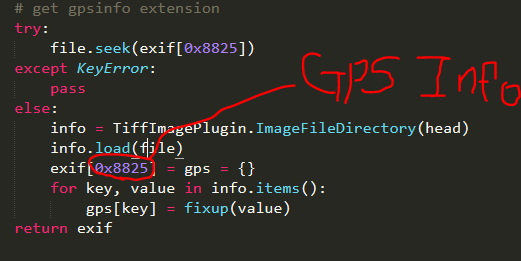


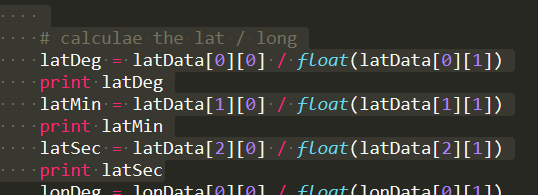
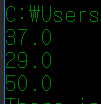
2번과 4번이 위도와 경도를 나타낸다 것을 알 수 있습니다.

조작을 시작하겠습니다.



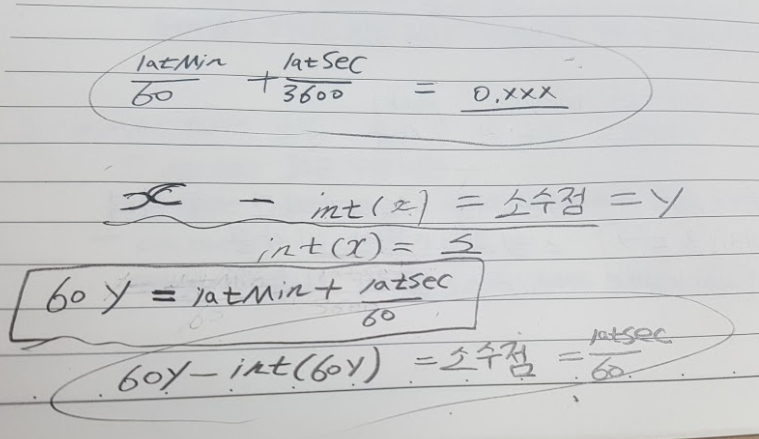


Exif[0x8825] 안에 조작된 gps값을 넣는다면 조작을 할 수 있겠군요!



Lat = (latDeg + (latMin + latSec / 60.0) / 60.0)

수식을 보니 각각 도 분 초를 의미하는 것을 알 수 있습니다. (DMS방식)

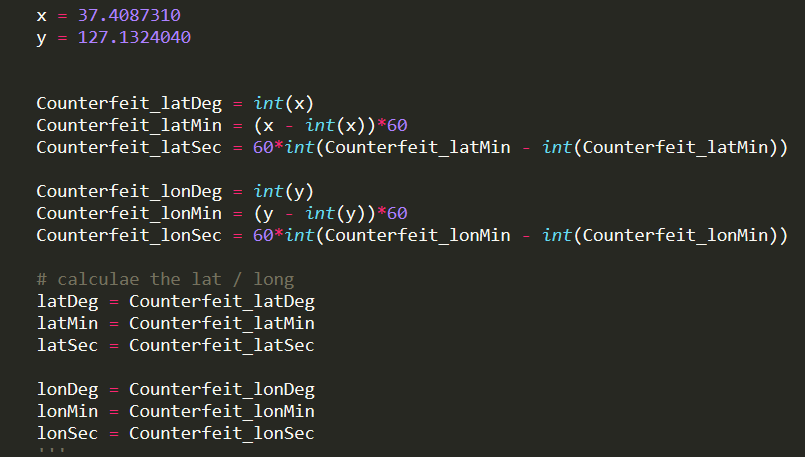


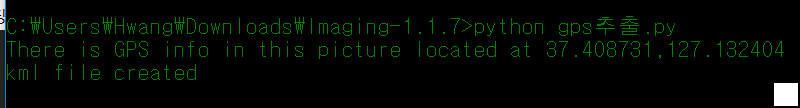
Degree를 DMS로 변환하기 위한 공식을 나름대로 세워보았습니다.

실제로 찾아보니 제가 생각한 게 맞는 듯 합니다.

[참조] <http://blog.naver.com/PostView.nhn?blogId=shoomi&logNo=90017563523>

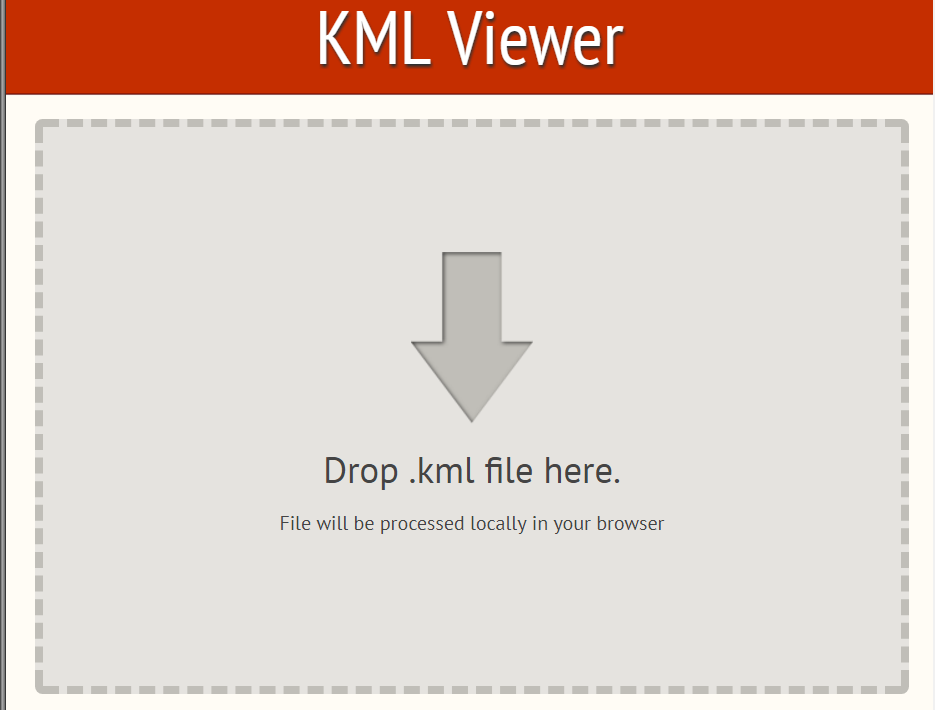
이제 코딩을 하겠습니다.

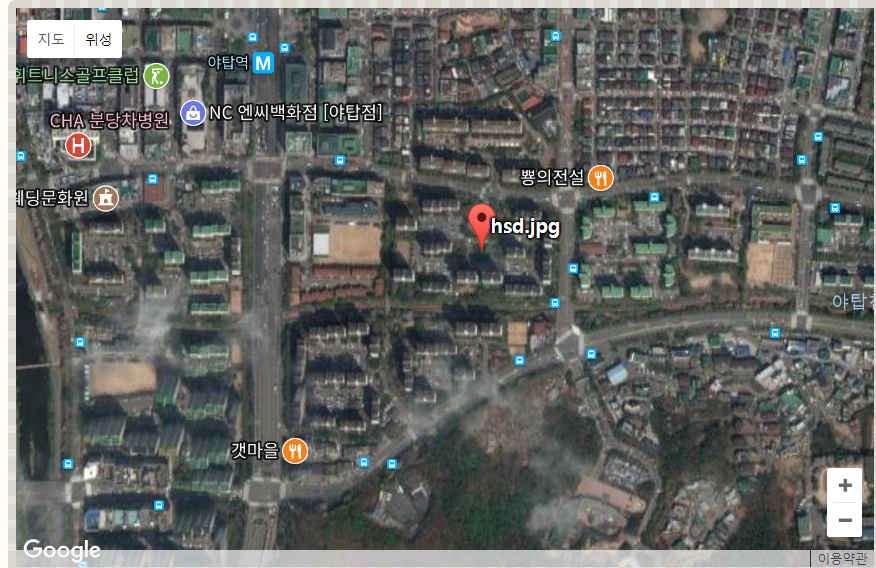




조작값과 일치하게 나온 것을 확인할 수 있습니다.

<http://ivanrublev.me/kml/>





저희 집 위치입니다.

변조에 성공하였습니다.

* **변조방법**

[참조] <http://fl0ckfl0ck.tistory.com/254>

1. 보여드린 방법처럼 위경도만 변경시키는 방법이 있습니다.
2. 툴(Exif Viewer , Exif Tool , Opanda PowerExif )등을 이용할 수도 있습니다.

그러나 **주의할 사항**이 있습니다.

Exif 필드를 변경했을 때 Modify-Time 필드시간이 변경됩니다. 즉 위경도를 변경한 이후에 Modify-time 필드값까지 변경해주어야 합니다.

바이너리를 조작함에 따라 SHA-1과 MD5의 값이 변경되게 됩니다. 다시 말하면 원본이 있다면 무결성 검증이 가능하게 되기 때문에 조작 후에 원본을 꼭 삭제해야 합니다.

단지 변조하는 것이 아닌 내가 보내고자 하는 수신자가 있다면 개인키와 공개키를 사용하는 PKI방식을 사용하는 것도 좋은 방법입니다.

다시 말하면 IFD를 개인키로 암호화하고 공개키로 열어볼 수 있도록 하는 것입니다. 공개키를 가지고 있지 않은 이들은 결코 열어볼 수 없을 것입니다.