

# 한세사이버고 해킹 대회 문제풀이

신암중학교 2학년 1반 박인성  
Nickname : MacintoshClassic

# 문제 2번: HTML 코드 이해

<http://www.hsoc.codns.com/JC/>



```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="utf-8">
5     <title>Adray</title>
6   </head>
7   <body>
8     <link rel="stylesheet" href="sim.css">
9     <a href="index.html">돌아가기</a>
10    <div class="Good">
11      <p>안녕 난 'Adray'라고 해. 문앞에 있는 아저씨의
12        이름을 맞춰야 flag을 받을 수 있겠지? 그 아저씨의 이름은
13        <span>Mr.Ahong</span>이야. 가서 이름을 말하고 flag
14        값을 얻어내자!</p>
15    </div>
16    <pre>
17      0000000000000000
18      0 0
19      0 0 0 0
20      0 0 0 0 0 0
21      0 0 0 0 0 0 0
22      0 0 0 0 0 0 0 0
23      0 0 0 0 0 0 0 0 0
24      0 0 0 0 0 0 0 0 0
25      0 0 0 0 0 0 0 0 0
26      0 0 0 0 0 0 0 0 0
27      0 0 0 0 0 0 0 0 0
28      0 0 0 0 0 0 0 0 0
29      0 0 0 0 0 0 0 0 0
30      0 0 0 0 0 0 0 0 0
31      0 0 0 0 0 0 0 0 0
32      0 0 0 0 0 0 0 0 0
33      0 0 0 0 0 0 0 0 0
34      0 0 0 0 0 0 0 0 0
35      0 0 0 0 0 0 0 0 0
36    </pre>
37
38  </body>
39 </html>
```

Mr.Ahong

## 나의 접근 방식

### Name에서 답을 찾아 Flag에서 Flag 값을 얻는 방식의 문제

1. 웹페이지의 Name 을 클릭하면, "Adray" 라는 사람이 먼저 힌트를 알려준다. 이 힌트를 가지고 Name 페이지의 HTML 코드 내에서 아저씨의 이름을 확인
2. 아저씨 이름은 “**Mr.Ahong**”이라는 것을 확인 후, 이 값을 갖고 Flag 페이지에서 아저씨의 이름을 알아 내려고 함
3. Flag 페이지는 코드 확인하여, 0.1초 마다 계속 새로 고침하도록 설정된 것을 확인하고, **브라우저의 새로고침 취소 버튼** 이용하여 새로 고침하지 않도록 설정함
4. Mr.Ahong을 입력하여 Flag 값 확인 [**Mango**]

# 문제 3번: 이미지 속성 이해 및 분석

<http://www.goo.gl/uvNWUt>



|                               |                                    |
|-------------------------------|------------------------------------|
| Aperture Value                | 2.275                              |
| Brightness Value              | 1.682                              |
| Color Space                   | sRGB                               |
| Components Configuration      | 1, 2, 3, 0                         |
| Date Time Digitized           | 18 Feb 2017 at 3:04:32 PM          |
| Date Time Original            | 18 Feb 2017 at 3:04:32 PM          |
| Exif Version                  | 2.2.1                              |
| Exposure Bias Value           | 0                                  |
| Exposure Mode                 | Auto exposure                      |
| Exposure Program              | Normal program                     |
| Exposure Time                 | 1/30                               |
| Flash                         | Auto, Did not fire                 |
| FlashPix Version              | 1.0                                |
| FNumber                       | 2.2                                |
| Focal Length                  | 4.15                               |
| Focal Length In 35mm Film     | 29                                 |
| ISO Speed Ratings             | 125                                |
| Lens Make                     | Apple                              |
| Lens Model                    | iPhone 6s back camera 4.15mm f/2.2 |
| Lens Specification            | 4.15-4.15, 2.2-2.2                 |
| Metering Mode                 | Pattern                            |
| Pixel X Dimension             | 4,032                              |
| Pixel Y Dimension             | 3,024                              |
| Scene Capture Type            | Standard                           |
| Scene Type                    | A directly photographed image      |
| Sensing Method                | One-chip color area sensor         |
| Shutter Speed Value           | 1/30                               |
| Subject Area                  | 2,015, 1,511, 2,217, 1,330         |
| Sub-second Time Digitized     | 389                                |
| Sub-second Time Original      | 389                                |
| White Balance                 | Auto white balance                 |
| Altitude                      | 29.18 m (95.75 ft)                 |
| Altitude Reference            | above sea level                    |
| Date Stamp                    | 18 Feb 2017                        |
| Destination Bearing           | 98.804                             |
| Destination Bearing Reference | True direction                     |
| Horizontal Positioning Error  | 65                                 |
| Image Direction               | 98.804                             |
| Image Direction Reference     | True north                         |
| Latitude                      | 37° 33' 34.932" N                  |
| Longitude                     | 126° 50' 24.342" E                 |
| Speed                         | 0                                  |
| Speed Reference               | Kilometers per hour                |
| Time Stamp                    | 21:04:28 UTC                       |

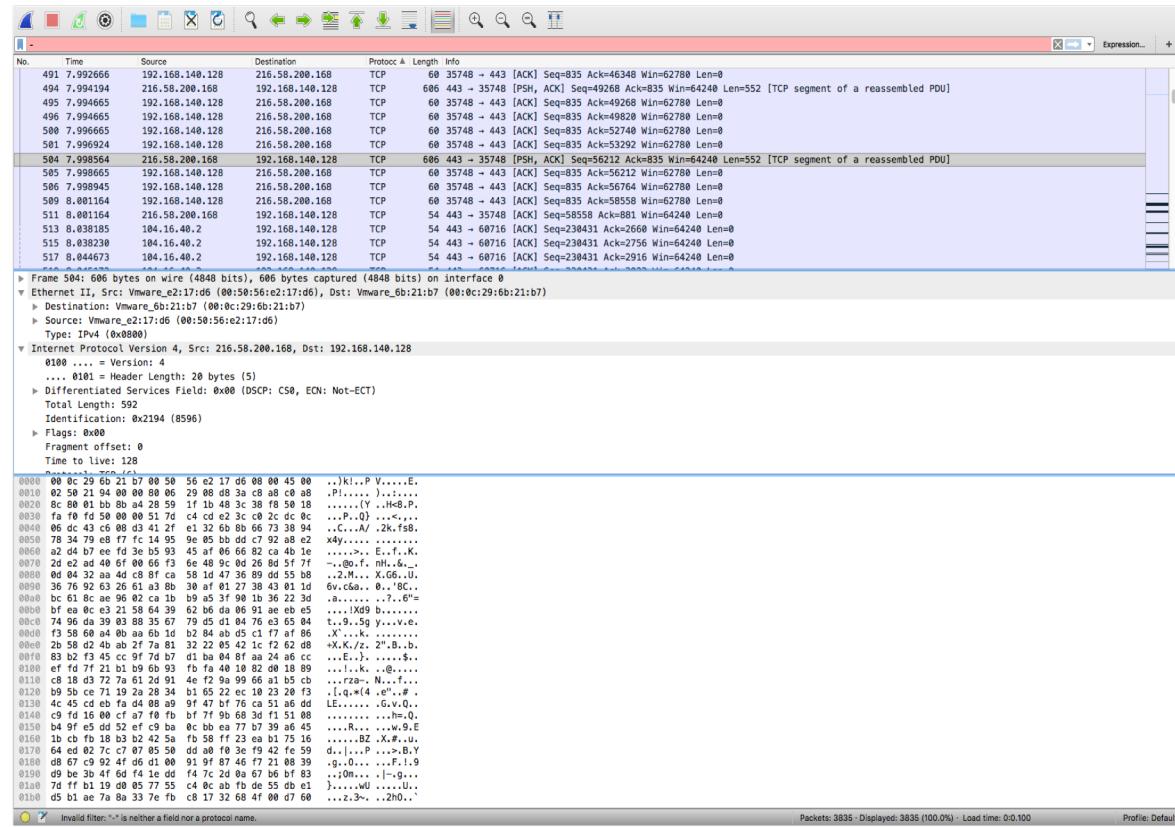
## 나의 접근 방식

이미지의 속성값을 확인하여, 사진촬영기기와 좌표값을 확인

1. 주어진 사진을 다운로드하여 Exif 파일의 속성을 확인
2. 사진을 찍은 기계의 정보와 조리개, 플래시 사용, 컬러, 모드 설정 등 사진과 관련된 정보에서 도둑의 핸드폰은 **iPhone 6s**라는 정보 확인
3. 사진의 위치 정보에서 위도와 경도 정보 확인하여, Google map 에서 확인
4. 경도와 위도로 NC 백화점으로 Flag 확인,  
**iphone6s\_ncqorghkwja**

# 문제 4번: 서버 로그의 이해

<http://www.goo.gl/YWYP6x>



## 나의 접근 방식

서버로그에서 파일전송 관련된 로그를 검색하여  
파일전송 로그 중, FTP 전송 로그에서 파일명 확인

1. 주어진 서버 로그에는 많은 형태의 서버로그 정보들이 있어, 파일 전송과 관련된 로그를 찾기 시작 함
2. 검색 중, FTP 로그 정보를 확인하고, 이 로그에서 hansei라는 유저가 P@ssw0rd 라는 비밀번호를 입력한후 flag\_is\_welcome\_to\_network.txt 라는 13byte 파일의 전송을 확인
3. flag 값 welcome\_to\_network

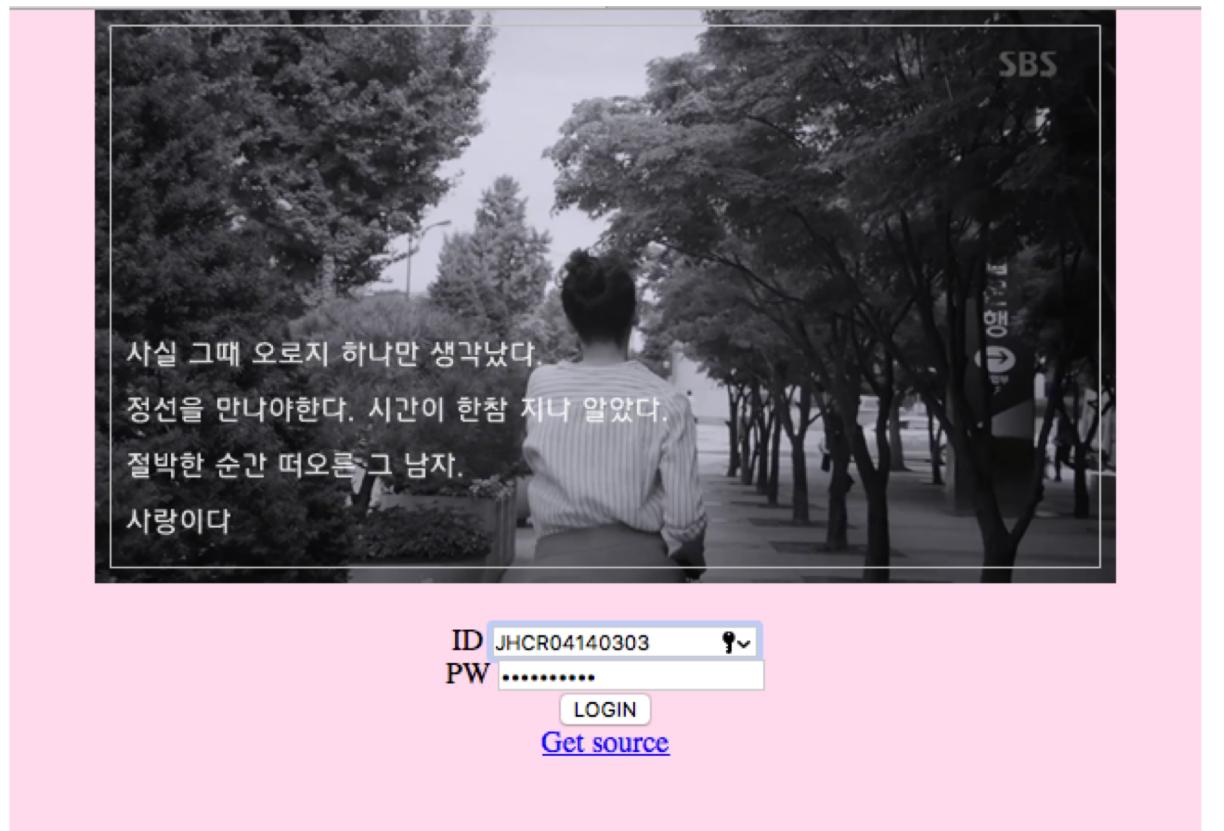
# 문제 4번: 서버 로그의 이해

<http://www.goo.gl/YWYP6x>

|      |           |                 |                 |          |  |
|------|-----------|-----------------|-----------------|----------|--|
| 3778 | 20.272969 | 192.168.140.128 | 192.168.140.1   | FTP      | 74 Response: 220 (vsFTPD 2.2.2)  |
| 3781 | 22.645619 | 192.168.140.1   | 192.168.140.128 | FTP      | 67 Request: USER hansei  |
| 3783 | 22.646472 | 192.168.140.128 | 192.168.140.1   | FTP      | 88 Response: 331 Please specify the password.  |
| 3785 | 24.537804 | 192.168.140.1   | 192.168.140.128 | FTP      | 69 Request: PASS P@ssw0rd  |
| 3789 | 24.640208 | 192.168.140.128 | 192.168.140.1   | FTP      | 77 Response: 230 Login successful.   |
| 3811 | 38.523106 | 192.168.140.1   | 192.168.140.128 | FTP      | 81 Request: PORT 192,168,140,1,201,95  |
| 3813 | 38.523601 | 192.168.140.128 | 192.168.140.1   | FTP      | 105 Response: 200 PORT command successful. Consider using PASV.                                      |
| 3814 | 38.527141 | 192.168.140.1   | 192.168.140.128 | FTP      | 91 Request: RETR flag_is_welcome_to_network.txt  |
| 3818 | 38.528878 | 192.168.140.128 | 192.168.140.1   | FTP      | 142 Response: 150 Opening BINARY mode data connection for flag_is_welcome_to_network.txt (13 bytes). |
| 3822 | 38.529998 | 192.168.140.128 | 192.168.140.1   | FTP      | 78 Response: 226 Transfer complete.  |
| 3829 | 40.171381 | 192.168.140.1   | 192.168.140.128 | FTP      | 60 Request: QUIT   |
| 3830 | 40.171968 | 192.168.140.128 | 192.168.140.1   | FTP      | 68 Response: 221 Goodbye.  |
| 3819 | 38.528878 | 192.168.140.128 | 192.168.140.1   | FTP-DATA | 79 FTP Data: 13 bytes  |

# 문제 7번: HTML 코드의 이해와 맥락 이해

<http://www.hsoc.codns.com/sql/>



## 나의 접근 방식

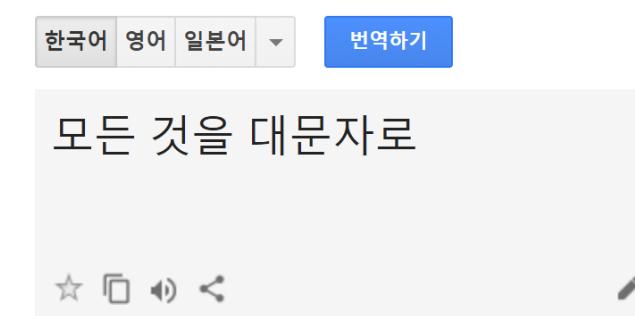
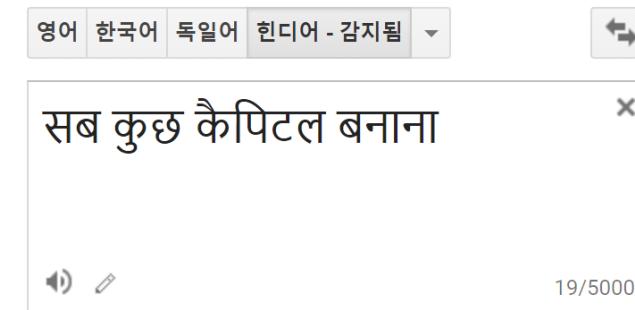
### HTML 소스 코드 내에 숨겨진 로그인 정보를 확인

1. <Get Source> 링크로 확인하는 PHP-HMTL 코드에서 주석 처리된 **ID와 Password 정보 확인**
2. ID와 Password 입력으로 확인된 문자를 구글 번역기로 확인
3. 힌디어로 확인된 한국어 번역 내용은 “**모든 것을 대문자로**”라고 확인
4. ID가 모두 소문자인것에 착안하여 **ID를 대문자로 입력하고 비밀번호는 그대로 입력하여 Flag 확인**
5. **tempoflove100**

# 문제 7번: HTML 코드의 이해와 활용

<http://www.hsoc.codns.com/sql/>

```
<?php  
  
if (isset($_GET['view-source'])) {  
    show_source(__FILE__);  
    exit();  
}  
  
if(isset($_POST['id']) && isset($_POST['ps'])){  
    include("../check.php"); // include for auth_code function.  
  
    mysql_connect("localhost","root","login");  
    mysql_select_db ("info");  
    mysql_query("set names utf8");  
  
    $key = "fIag is ilovey0u(please check this source use your editor)";  
  
    $id = mysql_real_escape_string(trim($_POST['id']));  
    $ps = mysql_real_escape_string(trim($_POST['ps']));  
  
    $row=mysql_fetch_array(mysql_query("select * from user where id='".$id.' and ps=md5('.$ps.')"));  
  
    if(isset($row['id'])){  
        if($id=='jhcr04140303'){  
            echo "your account is blocked";  
        }else{  
            echo "login ok". "<br />";  
            echo "Password : ".$key;  
        }  
    }else{  
        echo "wrong...";  
    }  
}  
?  
<!DOCTYPE html>  
<style>  
    * {margin:0; padding:0;}  
    body {background-color:#FDE9E6;}  
    input[type=text],input[type=password] {width:150px;}  
    td {text-align:center;}  
</style>  
  
<body>  
  
<form method="post" action="insertdb.php">  
<center></center><br>  
<center>ID <input type="text" name="id"></center>  
<center>PW <input type="password" name="ps"/></center>  
<center><input type="submit" value="LOGIN"></center>  
<center><a href="?view-source">Get source</a></center>  
  
</form>  
</body>  
<!--  
use this  
jhcr04140303 / bigorsmall  
-->
```



[www.hsoc.codns.com](http://www.hsoc.codns.com) says:  
Flag is tempoflove100