

2014 - 2015

G.M.D.

REPORT

3417 - 박성호

감재흠에게 바침.

1. IP 주소를 따라가보자

IP 주소를 통해 위치를 추적해 보았다.

‘해커의 언어, 치명적 파이썬(TJ 오코너)’이란 책의 도움을 많이 받았다.

※ IP 주소 추적 자체는 불법이 아니다. 추적하는 과정에서 불법 행위를 하지 않으면 된다.

프로그램은 Python 으로 제작했으며 대략적인 원리는 다음과 같다.



TJ 오코너 씨, 많이 배워가요~~

1. IP 주소에 대응하는 위치 정보가 담겨있는 파일을 인터넷에서 다운 받는다.
2. 내 노트북이 주변으로 퍼트리는 무선 패킷을 잡아낸다.
3. 잡아낸 패킷에서 출발 IP 주소와 도착 IP 주소를 뽑아낸다.
4. 이를 Google Earth 에 표시한다.

약용의 여지가 있으므로 코드는 다음과 같이 공개한다.

```
import pygeopip
import dpkt
import socket

gi = pygeopip.GeoIP('d:\\GeoLiteCity.dat')

#ip -> XML
def retXML(ip):
    rec = gi.record_by_name(ip)
    try:
        longitude = rec['longitude']
        latitude = rec['latitude']
        kml = (
            '<Placemark>\n'
            '  <name>X</name>\n'
            '  <Point>\n'
            '    <coordinates>X,Y,Z</coordinates>\n'
            '  </Point>\n'
            '</Placemark>\n'
        )(ip, longitude, latitude)
        return kml
    except:
        return ''

#Return all of XML's Data
def plotIPs(pcap):
    kmlPts = ''
    #call function 'retXML' from each IP Address
    for (ts, buf) in pcap:
        try:
            eth = dpkt.ethernet.Ethernet(buf)
            ip = eth.data

            #Extract IP
            src = socket.inet_ntoa(ip.src)
            srcXML = retXML(src)

            #Destination IP
            dst = socket.inet_ntoa(ip.dst)
            dstXML = retXML(dst)

            #Build XML data
            kmlPts = kmlPts + srcXML + dstXML
        except:
            pass
```

```
return kmlPts

f = open('test.pcap', 'rb')
pcap = dpkt.pcap.Reader(f)
kmlheader = '<?xml version="1.0" encoding="UTF-8">\n<?xml xmlns="http://www.opengis.net/kml/2.2">\n<Document>\n'
kmlfooter = '</Document>\n</kml>\n'

print plotIPs(pcap)

kmlDoc = kmlheader + plotIPs(pcap) + kmlfooter
kmlDoc = kmlheader + plotIPs(pcap)
srcXML = retXML('119.215.137.64')

t = open('iptrace.kml', 'w')
t.write(kmlDoc)
t.write(srcXML)
t.write(kmlfooter)

sock = socket.inet_ntoa('119.215.137.64')
```

프로그램을 실행시키면 다음과 같이 Google Earth 에 내 노트북에서 보내고 받은 패킷들의 출발 지점과 도착 지점들을 찾을 수 있다.

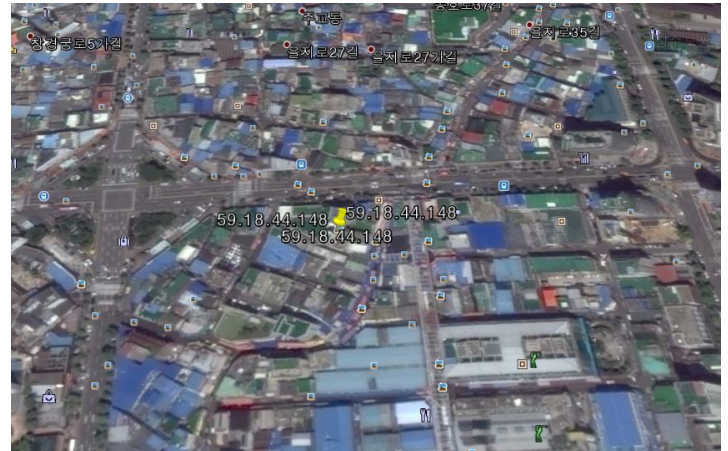
활동 보고서

www.stackoverflow.com 에 접속하게 되면 내 노트북이 송수신한 패킷은 다음과 같은 곳을 지난다.



US Post Office (72.10.193.111)

747 Broadway, Albany, NY 12207 (518) 426-2287



서울특별시 을지로 5가(59.18.44.148)



Life Sciences Library (173.194.126.191)

Mark Avenue, Mountain View, CA 94043



북위 53 도 59 초, 서경 1 도 59 초

(94.31.29.230)

다음과 같이 프로그램은 Google Earth 에 위치를 표시해주었다.

2. PDF 메타 데이터로 범인을 밝혀보자

옛날 옛날 이야기

2012 년 12 월 10 일 어나니머스(Anonymous)는 Operation Payback 이라는 공격의 의도에 대한 발표문을 포스팅했다. 어나니머스는 위키릭스의 지원이 중단되자 관련되어 있는 그룹에 대한 DDoS 공격을 감행했다. 어나니머스의 해커는 발표문을 아무런 속성 없이 포스팅했지만 메타데이터가 포함된 PDF 파일로 배포했다. 문서를 생성하는데 사용된 프로그램은 문서의 작성자인 Alex Tapanaris 의 이름을 메타데이터에 입력해 놓았다. 그리고 며칠 뒤 그리스 경찰은 그를 체포했다.

★ 메타데이터란? -> 파일에 대한 정보 ★

경찰들이 멋있었다. 나도 해보고 싶어서 해봤다.

프로그램은 Python 으로 제작했으며 **대략적인** 원리는 다음과 같다.

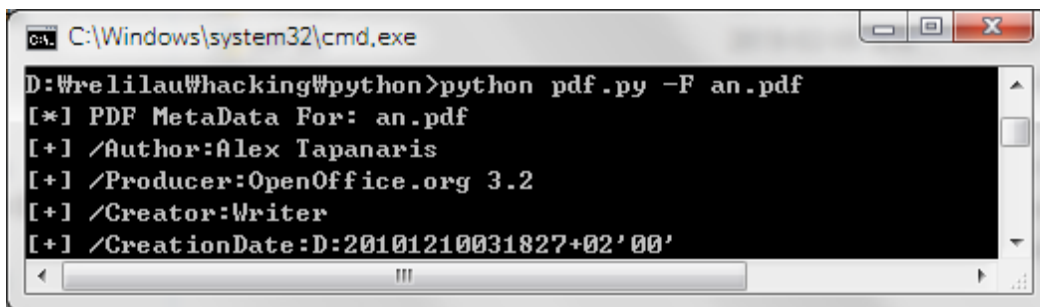
1. PDF 파일의 메타 데이터를 뽑는다.
2. 끝

코드는 다음과 같다. 악용의 여지는 없지만 다음과 같이 공개한다. Python 에 대해서 간단하게 소개도 하겠다.

```
1 import pyPdf
2 import optparse
3 from pyPdf import PdfFileReader
4
5 def printMeta(fileName):
6     pdfFile = PdfFileReader(file(fileName, 'rb'))
7     docInfo = pdfFile.getDocumentInfo()
8
9     print '[*] PDF MetaData For: ' + str(fileName)
10
11     for metaItem in docInfo:
12         print '[*] ' + metaItem + ':' + docInfo[metaItem]
13
14 parser = optparse.OptionParser('usage %prog "%s" -F <PDF File Name>!\n')
15 parser.add_option('-F', dest='fileName', type='string', help='specify PDF File Name')
16 (options, args) = parser.parse_args()
17 fileName = options.fileName
18
19 if fileName == None:
20     print parser.usage
21     exit(0)
22 else:
23     printMeta(fileName)
```



Python : 비단뱀과(Pythonidae)는 뱀목에 속하는 파충류 뱀 과의 하나이다. 학명은 그리스어 "피톤"(*python*, πύθων)에서 유래했다. 독이 없으며, 아프리카와 아시아 그리고 오스트레일리아에서 발견된다. 세계에서 가장 큰 뱀의 일부도 이 과에 속해 있다. 현재, 8 속 26 종으로 분류하고 있다.^[2]



프로그램을 실행시켜보면 Alex Tapanaris 가 OpenOffice 로 문서를 작성했다는 것을 알 수 있다. 참고로 OpenOffice 는 Copyleft 진영의 대표적인 문서 작성 프로그램이다.

3. 대한민국 도시들 간의 최단 거리와 최단 경로 탐색

시작하기 전에 하는 말



그많은 활동을 기반으로 강병관과 필자는 이 주제를 통해 ‘수학 교과서 심층 탐구 대회’에서 은상(2 위)를 수상했다. 이것에 대해서 ‘컴퓨터 모르는 선배들하고 선생님들 상대로 프로그래밍 덕분에 상을 탔네’라는 말이 나오는 등 일부 굵지 않은 시선을 가진 학생들이 있었는데 ‘사실이 아니다.’라고 말해주고 싶다.

먼저 우리는 수학의 그래프 이론을 컴퓨터로 활용함으로써 수학과 컴퓨터를 접목시키는 것이 주된 탐구 주제임을 말해주고 싶다. 또한 심사에 참여하신 선배들 중에는 카이스트 전산학과에 재학 중이신 선배님과 일반인에 비해 컴퓨터에 대한 깊은 조예를 가지신 **이진성 선생님**께서 참여하셨다. (선생님께서 배열의 저장공간에 대해 질문하실 때 알게 되었다.) 두 분 모두 우리의 탐구 주제가 수학과

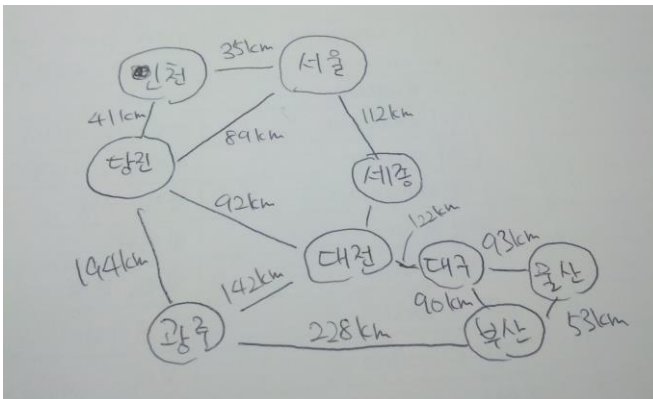
밀접한 관련이 있음을 인지하시고 수학과 프로그래밍의 측면에서 날카로운 질문을 많이 하셨다. 우리 팀이 다른 팀들에 비해 상당히 긴 질의응답 시간을 가졌다는 것 또한 주목할 점이다.

이번 기회를 통해 우리 팀은 프로그래밍이라는 분야의 특수성을 이용해 상을 날로 먹은 것이 아니란 것을 이야기 하고 싶다.

활동 보고서

진짜 하고 싶은 말

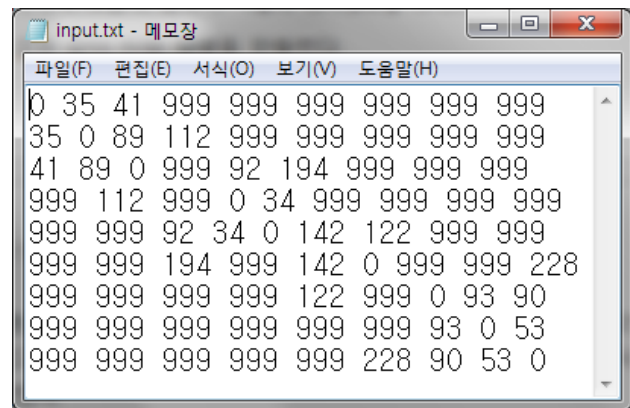
우리는 그래프를 활용해 대한민국 9 개 도시 간의 길이 정보를 바탕으로 최단 거리와 최단 경로를 탐색하는 알고리즘을 개발했다.



세종, 대전 간 거리는 34km 이다.

‘수학 1’에서 제시된 그래프와 인접행렬의 개념을 사용해 대한민국 도시들 간의 위치 정보가 표현된 그래프를 인접행렬의 형태로 컴퓨터에 저장했다. 단, 그래프의 정점들 사이의 거리를 표현한 것은 정규 교육 과정에서 제시되지 않은 우리 팀이 고안한 개념이고 이는 실제 그래프 이론에서 ‘가중치’라고 불리는 것을 알게 되었다.

최단 거리와 최단 거리 탐색 알고리즘은 C++로 구현했으며 코드는 다음과 같다. 원리는 생략한다.

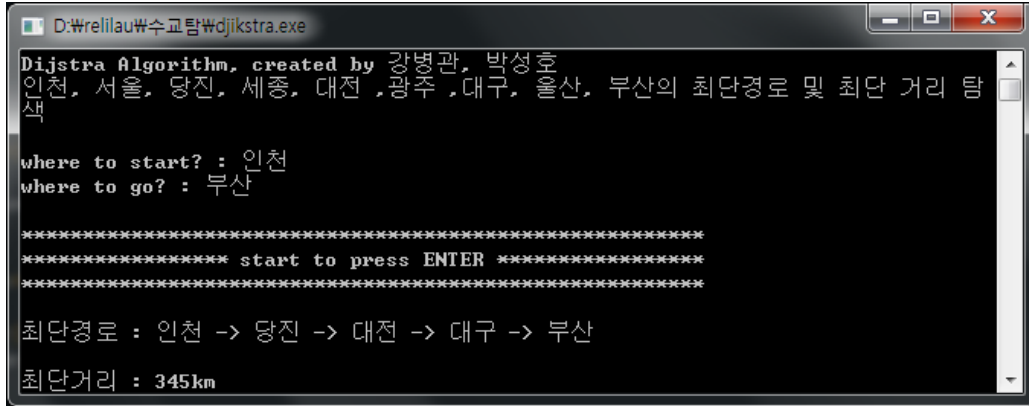


```

1 //scanf TIME 0
2 scanf("%d", &start);
3 scanf("%d", &MAX);
4
5 #include <stdio.h>
6 #include <string.h>
7 #include <conio.h>
8
9 using namespace std;
10
11 int arr[MAX][MAX]; //그래프
12 int dist[MAX][MAX]; //dist[i][j]은 i->j로 가는 최단 거리
13 const char *CITY[] = {"인천", "서울", "부산", "대전", "광주", "대구", "울산", "목포", "부산"}; //1에서 10로 가는 위치
14
15 void Dijkstra(int s, int b, int var[MAX], int found[MAX], int n);
16 void print_matrix(int n);
17 void dist_cal(int n);
18 void find(int start, int end, int m);
19 int choose(int var[MAX], int found[MAX], int n);
20
21 int main()
22 {
23     FILE *f;
24     f = fopen("input.txt", "r");
25     int n, a, b, temp;
26     int var[MAX], found[MAX];
27     char _start[5], _end[5];
28     char _start[5], _end[5];
29     printf("Dijkstra Algorithm, created by 김현철, 박재현\n");
30     printf("인천, 서울, 부산, 대전, 광주, 대구, 울산, 목포의 최단경로 및 최단 거리 출력\n");
31     n = 1;
32     a = b = -1;
33
34     while(1)
35     {
36         printf("where to start? ");
37         scanf("%s", _start);
38         printf("where to go? ");
39         scanf("%s", _end);
40         for(int i=0; i<n; i++)
41         {
42             if(strcmp(CITY[i], _start) == 0)
43             {
44                 a = i;
45             }
46             if(strcmp(CITY[i], _end) == 0)
47             {
48                 b = i;
49             }
50         }
51         if(a == -1 || b == -1)
52         {
53             printf("도시번호를 입력하세요\n");
54         }
55         else
56         {
57             print_matrix(n);
58             printf("start to goess (ENTER)");
59             printf("start to goess (ENTER)");
60             printf("start to goess (ENTER)");
61             printf("start to goess (ENTER)");
62             printf("start to goess (ENTER)");
63             printf("start to goess (ENTER)");
64             printf("start to goess (ENTER)");
65             printf("start to goess (ENTER)");
66             printf("start to goess (ENTER)");
67             printf("start to goess (ENTER)");
68             printf("start to goess (ENTER)");
69             printf("start to goess (ENTER)");
70             printf("start to goess (ENTER)");
71             printf("start to goess (ENTER)");
72             printf("start to goess (ENTER)");
73             printf("start to goess (ENTER)");
74             printf("start to goess (ENTER)");
75             printf("start to goess (ENTER)");
76             printf("start to goess (ENTER)");
77             printf("start to goess (ENTER)");
78             printf("start to goess (ENTER)");
79             printf("start to goess (ENTER)");
80             printf("start to goess (ENTER)");
81             printf("start to goess (ENTER)");
82             printf("start to goess (ENTER)");
83             printf("start to goess (ENTER)");
84             printf("start to goess (ENTER)");
85             printf("start to goess (ENTER)");
86             printf("start to goess (ENTER)");
87             printf("start to goess (ENTER)");
88             printf("start to goess (ENTER)");
89             printf("start to goess (ENTER)");
90             printf("start to goess (ENTER)");
91             printf("start to goess (ENTER)");
92             printf("start to goess (ENTER)");
93             printf("start to goess (ENTER)");
94             printf("start to goess (ENTER)");
95             printf("start to goess (ENTER)");
96             printf("start to goess (ENTER)");
97             printf("start to goess (ENTER)");
98             printf("start to goess (ENTER)");
99             printf("start to goess (ENTER)");
100             printf("start to goess (ENTER)");
101             printf("start to goess (ENTER)");
102             printf("start to goess (ENTER)");
103             printf("start to goess (ENTER)");
104             printf("start to goess (ENTER)");
105             printf("start to goess (ENTER)");
106             printf("start to goess (ENTER)");
107             printf("start to goess (ENTER)");
108             printf("start to goess (ENTER)");
109             printf("start to goess (ENTER)");
110             printf("start to goess (ENTER)");
111             printf("start to goess (ENTER)");
112             printf("start to goess (ENTER)");
113             printf("start to goess (ENTER)");
114             printf("start to goess (ENTER)");
115             printf("start to goess (ENTER)");
116             printf("start to goess (ENTER)");
117             printf("start to goess (ENTER)");
118             printf("start to goess (ENTER)");
119             printf("start to goess (ENTER)");
120             printf("start to goess (ENTER)");
121             printf("start to goess (ENTER)");
122             printf("start to goess (ENTER)");
123             printf("start to goess (ENTER)");
124             printf("start to goess (ENTER)");
125             printf("start to goess (ENTER)");
126             printf("start to goess (ENTER)");
127             printf("start to goess (ENTER)");
128             printf("start to goess (ENTER)");
129             printf("start to goess (ENTER)");
130             printf("start to goess (ENTER)");
131             printf("start to goess (ENTER)");
132             printf("start to goess (ENTER)");
133             printf("start to goess (ENTER)");
134             printf("start to goess (ENTER)");
135             printf("start to goess (ENTER)");
136             printf("start to goess (ENTER)");
137             printf("start to goess (ENTER)");
138             printf("start to goess (ENTER)");
139             printf("start to goess (ENTER)");
140             printf("start to goess (ENTER)");
141             printf("start to goess (ENTER)");
142             printf("start to goess (ENTER)");
143             printf("start to goess (ENTER)");
144             printf("start to goess (ENTER)");
145             printf("start to goess (ENTER)");
146             printf("start to goess (ENTER)");
147             printf("start to goess (ENTER)");
148             printf("start to goess (ENTER)");
149             printf("start to goess (ENTER)");
150             printf("start to goess (ENTER)");
151             printf("start to goess (ENTER)");
152             printf("start to goess (ENTER)");
153             printf("start to goess (ENTER)");
154             printf("start to goess (ENTER)");
155             printf("start to goess (ENTER)");
156             printf("start to goess (ENTER)");
157             printf("start to goess (ENTER)");
158             printf("start to goess (ENTER)");
159             printf("start to goess (ENTER)");
160             printf("start to goess (ENTER)");
161             printf("start to goess (ENTER)");
162             printf("start to goess (ENTER)");
163             printf("start to goess (ENTER)");
164             printf("start to goess (ENTER)");
165             printf("start to goess (ENTER)");
166             printf("start to goess (ENTER)");
167             printf("start to goess (ENTER)");
168             printf("start to goess (ENTER)");
169             printf("start to goess (ENTER)");
170             printf("start to goess (ENTER)");
171             printf("start to goess (ENTER)");
172             printf("start to goess (ENTER)");
173             printf("start to goess (ENTER)");
174             printf("start to goess (ENTER)");
175             printf("start to goess (ENTER)");
176             printf("start to goess (ENTER)");
177             printf("start to goess (ENTER)");
178             printf("start to goess (ENTER)");
179             printf("start to goess (ENTER)");
180             printf("start to goess (ENTER)");
181             printf("start to goess (ENTER)");
182             printf("start to goess (ENTER)");
183             printf("start to goess (ENTER)");
184             printf("start to goess (ENTER)");
185             printf("start to goess (ENTER)");
186             printf("start to goess (ENTER)");
187             printf("start to goess (ENTER)");
188             printf("start to goess (ENTER)");
189             printf("start to goess (ENTER)");
190             printf("start to goess (ENTER)");
191             printf("start to goess (ENTER)");
192             printf("start to goess (ENTER)");
193             printf("start to goess (ENTER)");
194             printf("start to goess (ENTER)");
195             printf("start to goess (ENTER)");
196             printf("start to goess (ENTER)");
197             printf("start to goess (ENTER)");
198             printf("start to goess (ENTER)");
199             printf("start to goess (ENTER)");
200             printf("start to goess (ENTER)");
201             printf("start to goess (ENTER)");
202             printf("start to goess (ENTER)");
203             printf("start to goess (ENTER)");
204             printf("start to goess (ENTER)");
205             printf("start to goess (ENTER)");
206             printf("start to goess (ENTER)");
207             printf("start to goess (ENTER)");
208             printf("start to goess (ENTER)");
209             printf("start to goess (ENTER)");
210             printf("start to goess (ENTER)");
211             printf("start to goess (ENTER)");
212             printf("start to goess (ENTER)");
213             printf("start to goess (ENTER)");
214             printf("start to goess (ENTER)");
215             printf("start to goess (ENTER)");
216             printf("start to goess (ENTER)");
217             printf("start to goess (ENTER)");
218             printf("start to goess (ENTER)");
219             printf("start to goess (ENTER)");
220             printf("start to goess (ENTER)");
221             printf("start to goess (ENTER)");
222             printf("start to goess (ENTER)");
223             printf("start to goess (ENTER)");
224             printf("start to goess (ENTER)");
225             printf("start to goess (ENTER)");
226             printf("start to goess (ENTER)");
227             printf("start to goess (ENTER)");
228             printf("start to goess (ENTER)");
229             printf("start to goess (ENTER)");
230             printf("start to goess (ENTER)");
231             printf("start to goess (ENTER)");
232             printf("start to goess (ENTER)");
233             printf("start to goess (ENTER)");
234             printf("start to goess (ENTER)");
235             printf("start to goess (ENTER)");
236             printf("start to goess (ENTER)");
237             printf("start to goess (ENTER)");
238             printf("start to goess (ENTER)");
239             printf("start to goess (ENTER)");
240             printf("start to goess (ENTER)");
241             printf("start to goess (ENTER)");
242             printf("start to goess (ENTER)");
243             printf("start to goess (ENTER)");
244             printf("start to goess (ENTER)");
245             printf("start to goess (ENTER)");
246             printf("start to goess (ENTER)");
247             printf("start to goess (ENTER)");
248             printf("start to goess (ENTER)");
249             printf("start to goess (ENTER)");
250             printf("start to goess (ENTER)");
251             printf("start to goess (ENTER)");
252             printf("start to goess (ENTER)");
253             printf("start to goess (ENTER)");
254             printf("start to goess (ENTER)");
255             printf("start to goess (ENTER)");
256             printf("start to goess (ENTER)");
257             printf("start to goess (ENTER)");
258             printf("start to goess (ENTER)");
259             printf("start to goess (ENTER)");
260             printf("start to goess (ENTER)");
261             printf("start to goess (ENTER)");
262             printf("start to goess (ENTER)");
263             printf("start to goess (ENTER)");
264             printf("start to goess (ENTER)");
265             printf("start to goess (ENTER)");
266             printf("start to goess (ENTER)");
267             printf("start to goess (ENTER)");
268             printf("start to goess (ENTER)");
269             printf("start to goess (ENTER)");
270             printf("start to goess (ENTER)");
271             printf("start to goess (ENTER)");
272             printf("start to goess (ENTER)");
273             printf("start to goess (ENTER)");
274             printf("start to goess (ENTER)");
275             printf("start to goess (ENTER)");
276             printf("start to goess (ENTER)");
277             printf("start to goess (ENTER)");
278             printf("start to goess (ENTER)");
279             printf("start to goess (ENTER)");
280             printf("start to goess (ENTER)");
281             printf("start to goess (ENTER)");
282             printf("start to goess (ENTER)");
283             printf("start to goess (ENTER)");
284             printf("start to goess (ENTER)");
285             printf("start to goess (ENTER)");
286             printf("start to goess (ENTER)");
287             printf("start to goess (ENTER)");
288             printf("start to goess (ENTER)");
289             printf("start to goess (ENTER)");
290             printf("start to goess (ENTER)");

```

프로그램을 실행시키면 다음과 같은 결과를 얻을 수 있다.



```
D:\wreilau\수교탐\#dijkstra.exe
Dijkstra Algorithm, created by 강병관, 박성호
인천, 서울, 당진, 세종, 대전, 광주, 대구, 울산, 부산의 최단경로 및 최단 거리 탐색

where to start? : 인천
where to go? : 부산

*****
***** start to press ENTER *****
*****

최단경로 : 인천 -> 당진 -> 대전 -> 대구 -> 부산
최단거리 : 345km
```

4. 서버 구축

처음에 가장인 강재흠에게 제출한 서버 구축 기획서의 초안에서 그많데 서버의 역할은 다음과 같다. 아직까지 서버 PC 를 비축할 공간을 마련하지 못했기에 다음 중 가장 기본적인 1, 3 번 만을 구현했다. 나머지는 부원들 개인 노트북으로 구현 중에 있다.

1. 그많데 부원들의 활동 소개, 정리, 다운로드 가능한 서비스 제공
2. 그많데 부원들의 연구 활동 지원을 위해 원하는 시간 동안 프로그램 가동 가능한 환경 제공
3. 그많데 SNS 서비스 제공
4. 모의 해킹의 장
5. 그많데 파일 서버
6. 마인크래프트(?)

하드웨어

버려진 PC 3 대의 부품을 조합해서 다음과 같은 사양의 PC 를 조립했다.

CPU: 셀러론 2.6GHz

RAM: DDR 4GB

VGA: 뭔지 모르겠음

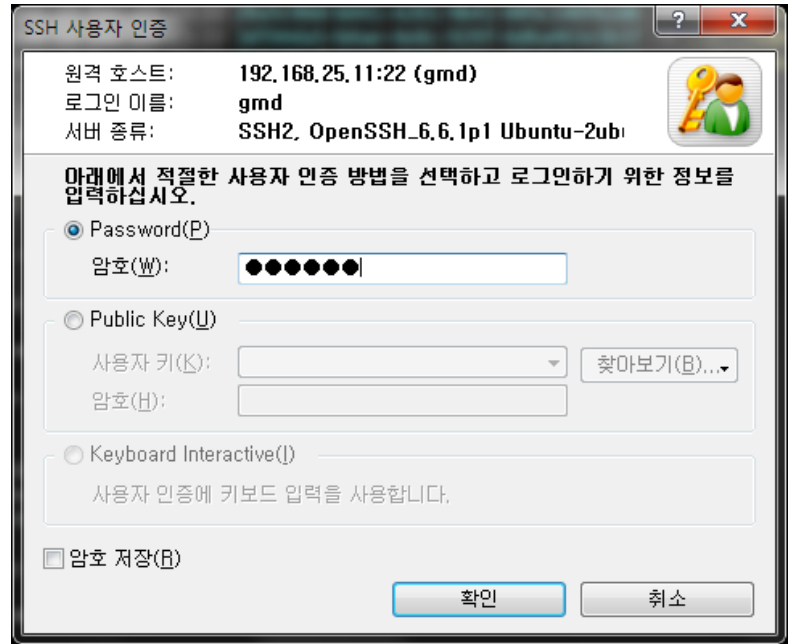
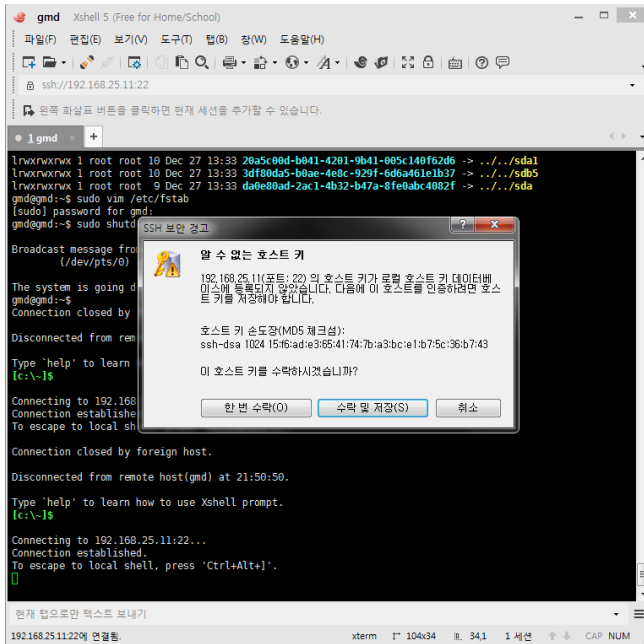
HDD: 80GB + 320GB

기술적인 부분

초창기: Apache + PHP + Django + MySQL

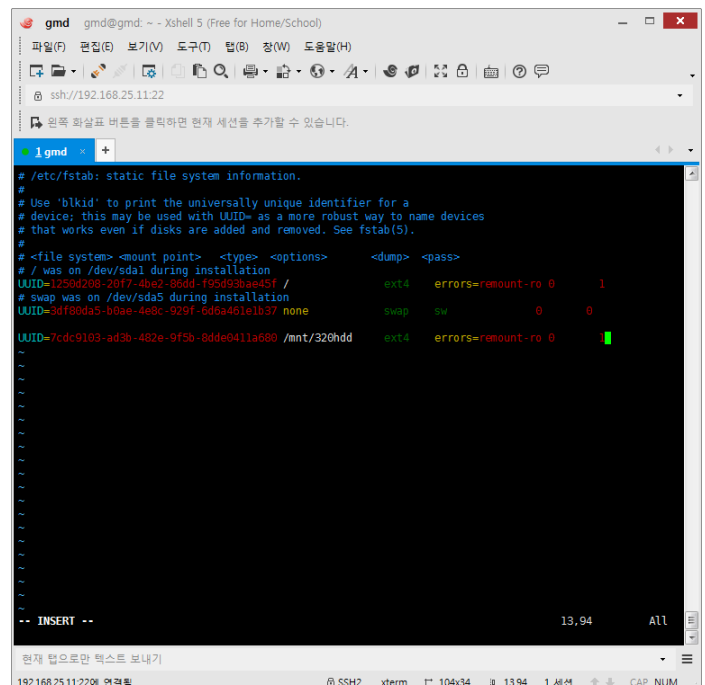
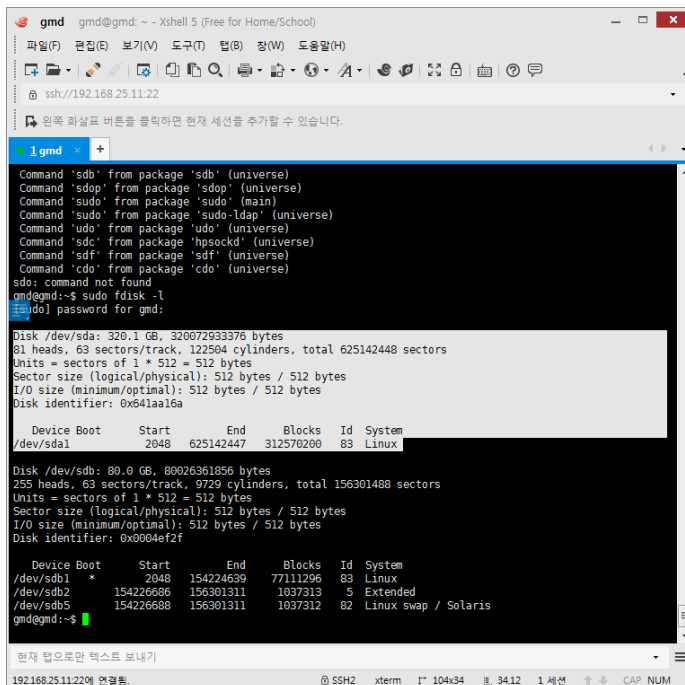
지금: Node.js + MariaDB

활동 보고서



서버 PC 를 위한 모니터와 키보드를 준비했기에 서버를 직접 조작할 수 도 있지만 많은 수의 그많은데 부원들이 동시에 원격으로 접속할 수 있는 환경을 제공하기 위해서 SSH 서버를 사용했다.

서버로의 접속은 다음과 같이 SSH 를 사용하여 무선 네트워크 해킹에 일차적으로 방어하기 위해서 암호화된 통신을 한다.

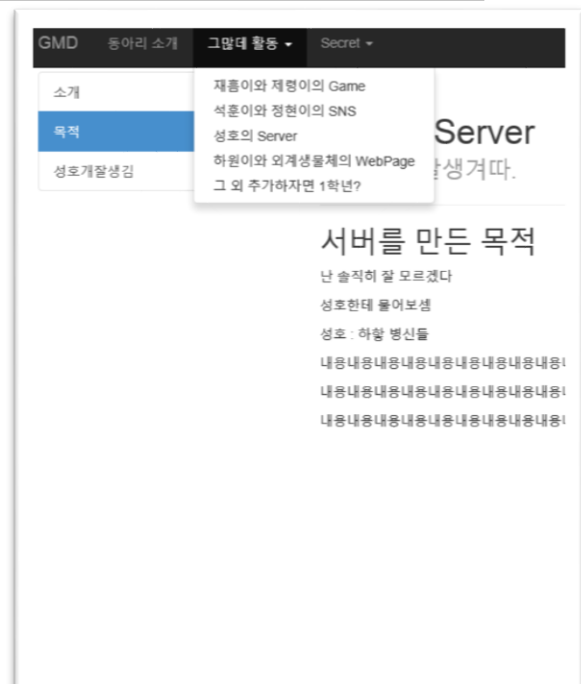
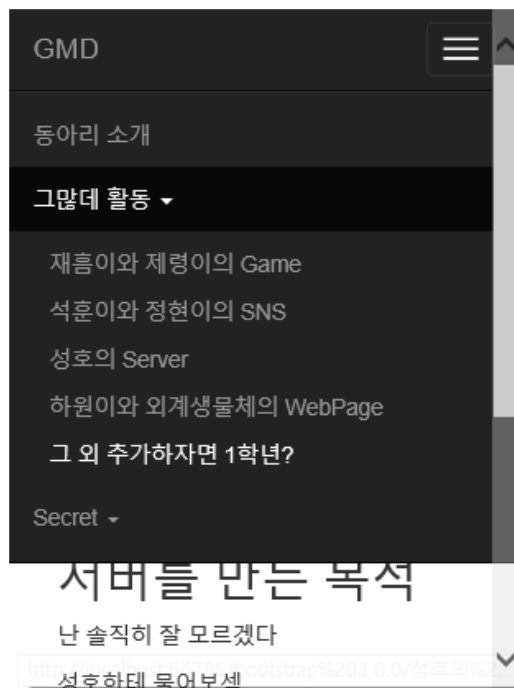
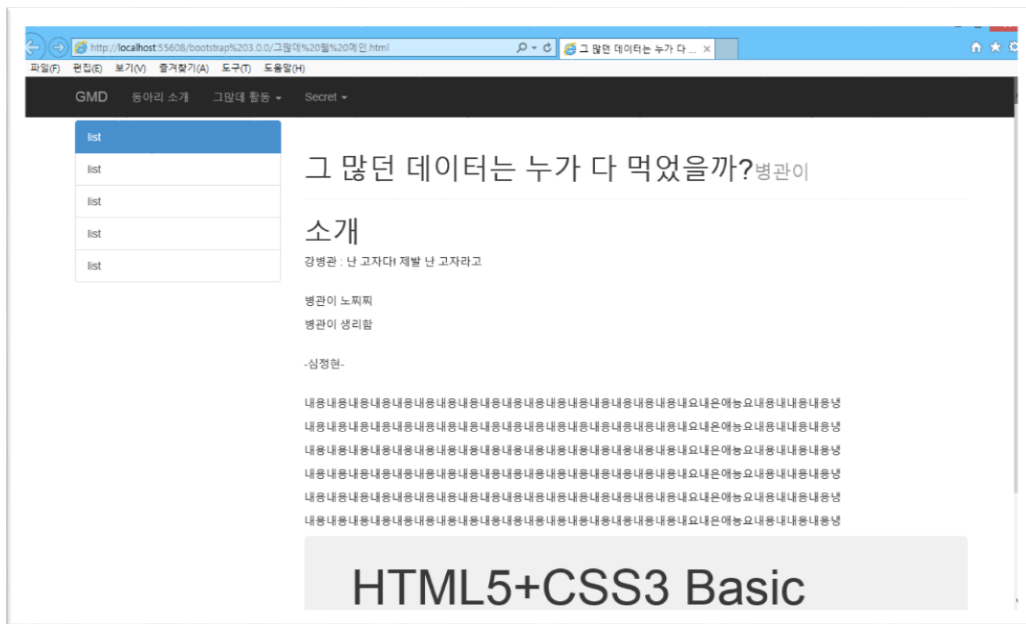


활동 보고서

다음과 같이 fdisk 와 mount 를 이용해 320GB 의 하드디스크도 추가했고 fstab 을 통해 부팅 시 자동으로 하드디스크를 추가시킬 수 있게 설정했다.

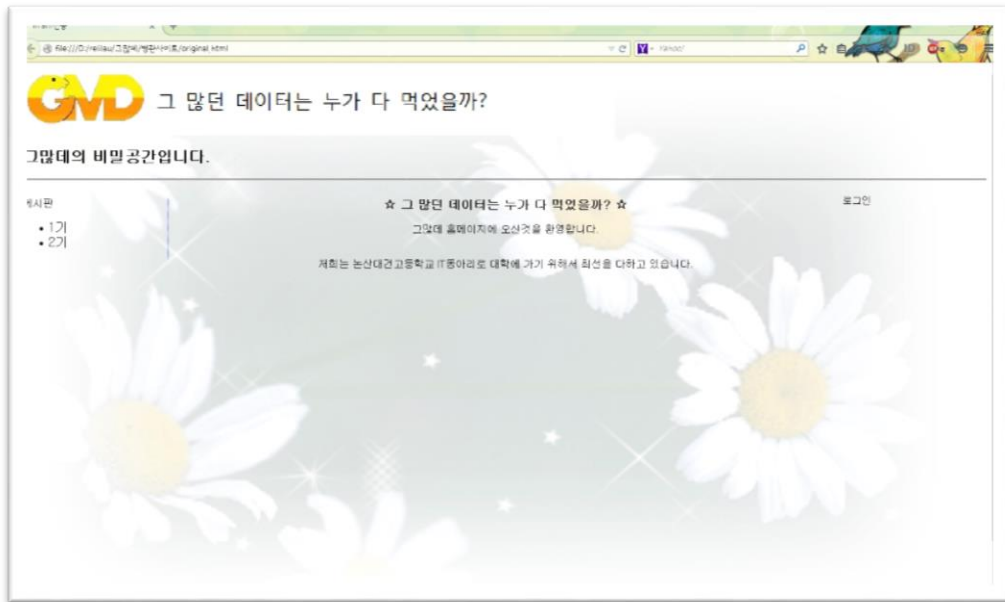
그렇데 부원인 병관이와 하원이가 제작한 웹 사이트는 다음과 같이 서버에 접속하면 볼 수 있다. 두 명 모두 제작 중에 있기 때문에 웹 사이트의 일부만 공개한다.

먼저 하원 作. 갑하원이 만든 것이라 그런지 빛이 난다.



병관 作

하도 해놓은 것이 없어서 메인 웹 사이트만 공개. 갠하원에 비해서 너무 허접하다.



활동 보고서 끝.