OpenEMR Analysis

Name: Junhyuk Kang

Professor: Chowdhury, Omar Haider

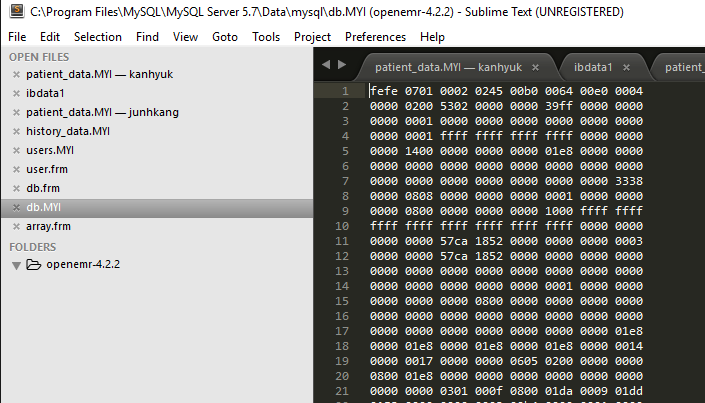
Date: 6.Sep.2016 ~ 13.Sep.2016

1. Where are the patient’s data stored? It is likely to be in a MySQL database

Tried to search from C:\xampp\mysql\data

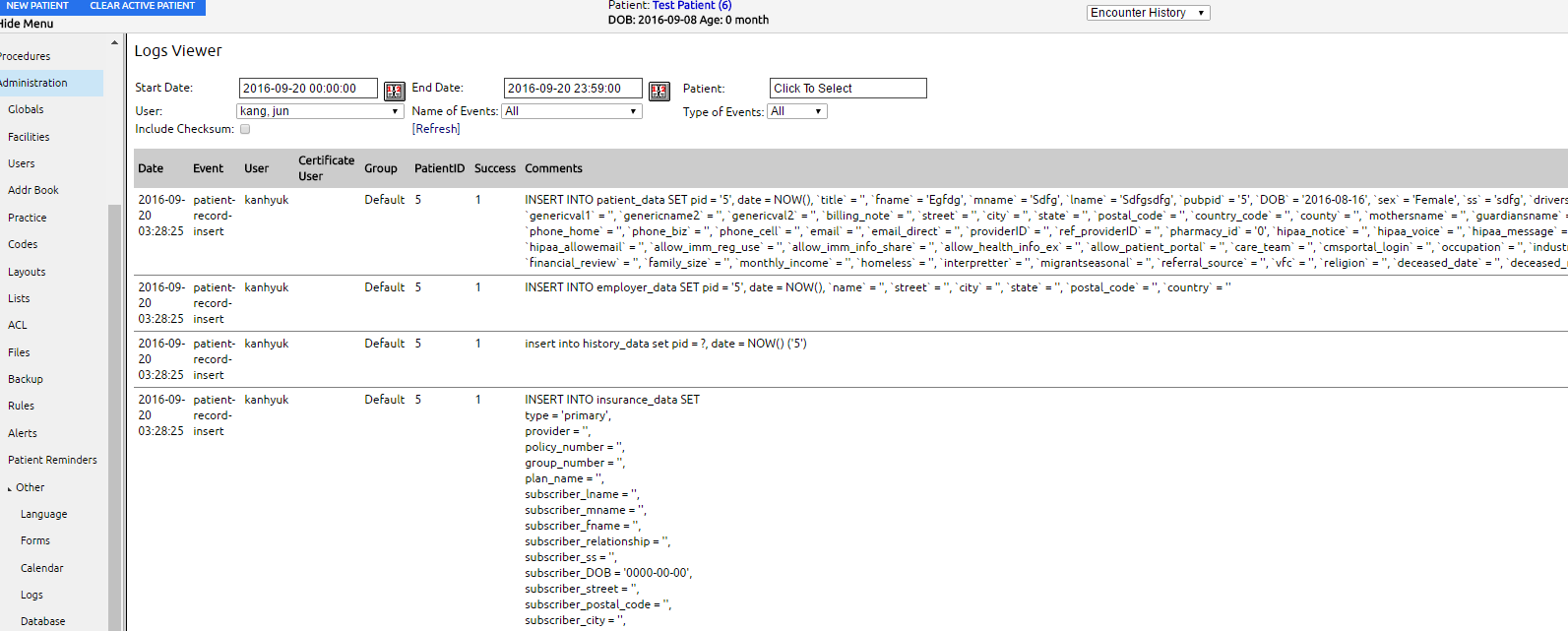
* Opened Db.opt, nothing was there
* Opened Patient\_data.frm, patient\_data.myd, patient\_data.MYI

with txt, but can’t read.

* Opened with sublimetext, and found over 60 lines of keys
  + Hypothesis: This keys may contain data for patients
* On openemor, under patient reminders, we can find every changes we made on “Log” tab

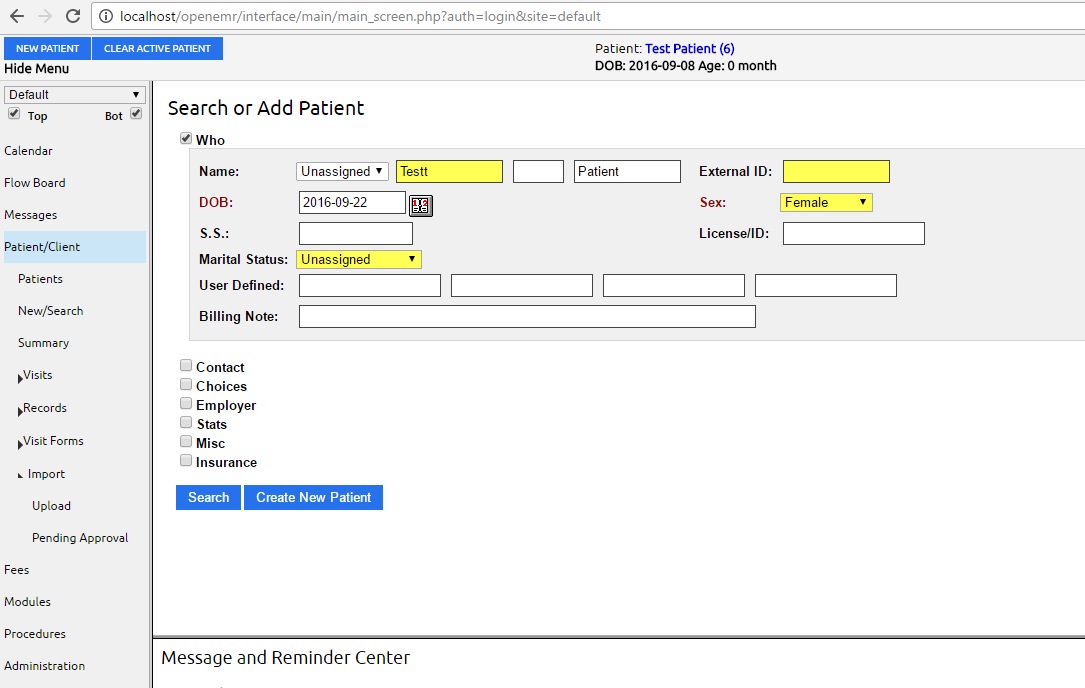
1. Location of the database

On “Log” tab,

provider = '', 

on database tab under “other” tab, there is employer\_data, and it has id, name, street, postal\_code, city, state, country, date, and pid

1. User-name, password for the database u:admin, p: password

* Add new user under Administration tab
* give “Front Office” access control
  + when I first relogged with other account, it keeps pop up that “network changed” but it still works
  + front office has authority on adding patient, appointment, fees, and patients records
  + 
  + tried to find any new file added after add new account, but there was no change
  + so I tried to make new user and gave “Accounting” access

03ad 307b 0000 0000 0000 0000 0000 0000

0000 0000 002e 09c9 0008 0000 0000 002d

da29 0000 0000 0000 0000 0000 0000 0000

1300 0000 0240 0000 0000 0000 0030 0000

0000 ffff ffff 0000 ffff ffff 0000 0000

0001 0000 0000 01de 0000 0000 01de 0000

0006 0000 0000 009e 0000 0000 01b6 0000

0000 0000 018f 0000 0004 0000 0002 0026

0000 019b 0026 0000 0001 0000 01f4 0026

0000 01f4 0026 0000 0000 0000 0000 ffff

ffff 0000 0000 0000 0116 0000 0003 aaaa

aaaa aaaa aaaa aaaa aaaa aaaa aaaa 0000

0000 0000 000f ffff ffff 0000 0000 0000

00ee 0000 0004 aaaa aaaa aaaa aaaa aaaa

aaaa aaaa aaaa 0000 0000 0000 000f 0000

* + but could not notice difference in keys in data file, so I tried again to make it sure
  + I made new account and gave “clinician” access
  + Checked ibdata1 file again and found no difference

03ad 307b 0000 0000 0000 0000 0000 0000

0000 0000 002e 09c9 0008 0000 0000 002d

da29 0000 0000 0000 0000 0000 0000 0000

1300 0000 0240 0000 0000 0000 0030 0000

0000 ffff ffff 0000 ffff ffff 0000 0000

0001 0000 0000 01de 0000 0000 01de 0000

0006 0000 0000 009e 0000 0000 01b6 0000

0000 0000 018f 0000 0004 0000 0002 0026

0000 019b 0026 0000 0001 0000 01f4 0026

0000 01f4 0026 0000 0000 0000 0000 ffff

ffff 0000 0000 0000 0116 0000 0003 aaaa

aaaa aaaa aaaa aaaa aaaa aaaa aaaa 0000

0000 0000 000f ffff ffff 0000 0000 0000

00ee 0000 0004 aaaa aaaa aaaa aaaa aaaa

aaaa aaaa aaaa 0000 0000 0000 000f 0000

* made new database and tried to compare with this.
  + New database named “junhkang” has no account or patient, and original database “kanhyuk” which has 1 patient, 1 admin, 1 clinician, and 1 officer.

Patient\_data.MYI-kanhyuk

fefe 0701 0001 03f4 00b0 0064 00d0 0002

0000 0200 2101 0000 0001 39ff 0000 0000

0000 0003 0000 0000 0000 0000 0000 0000

0000 0003 ffff ffff ffff ffff 0000 0000

0000 0c00 0000 0000 0000 01b8 0000 0000

0000 0000 0000 0000 0000 0000 0000 0000

0000 0003 0000 0000 0000 0000 0000 19a0

0000 0832 0000 0000 0000 0002 0000 0000

0000 0400 0000 0000 0000 0800 ffff ffff

ffff ffff 0000 0000 0000 0000 57cc b863

Patient\_data.MYI-junhkang

fefe 0701 0001 03f4 00b0 0064 00d0 0002

0000 0200 2101 0000 0000 00ff 0000 0000

0000 0000 0000 0000 0000 0000 0000 0000

0000 0000 ffff ffff ffff ffff 0000 0000

0000 0400 0000 0000 0000 0000 0000 0000

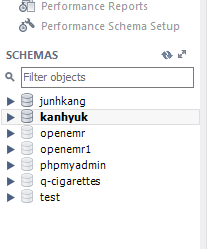
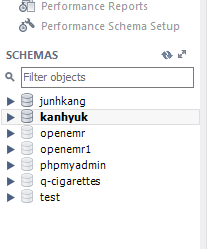
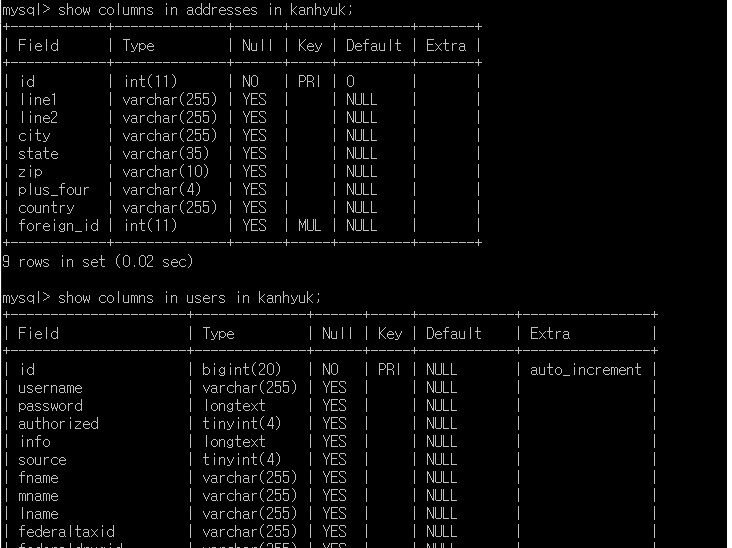
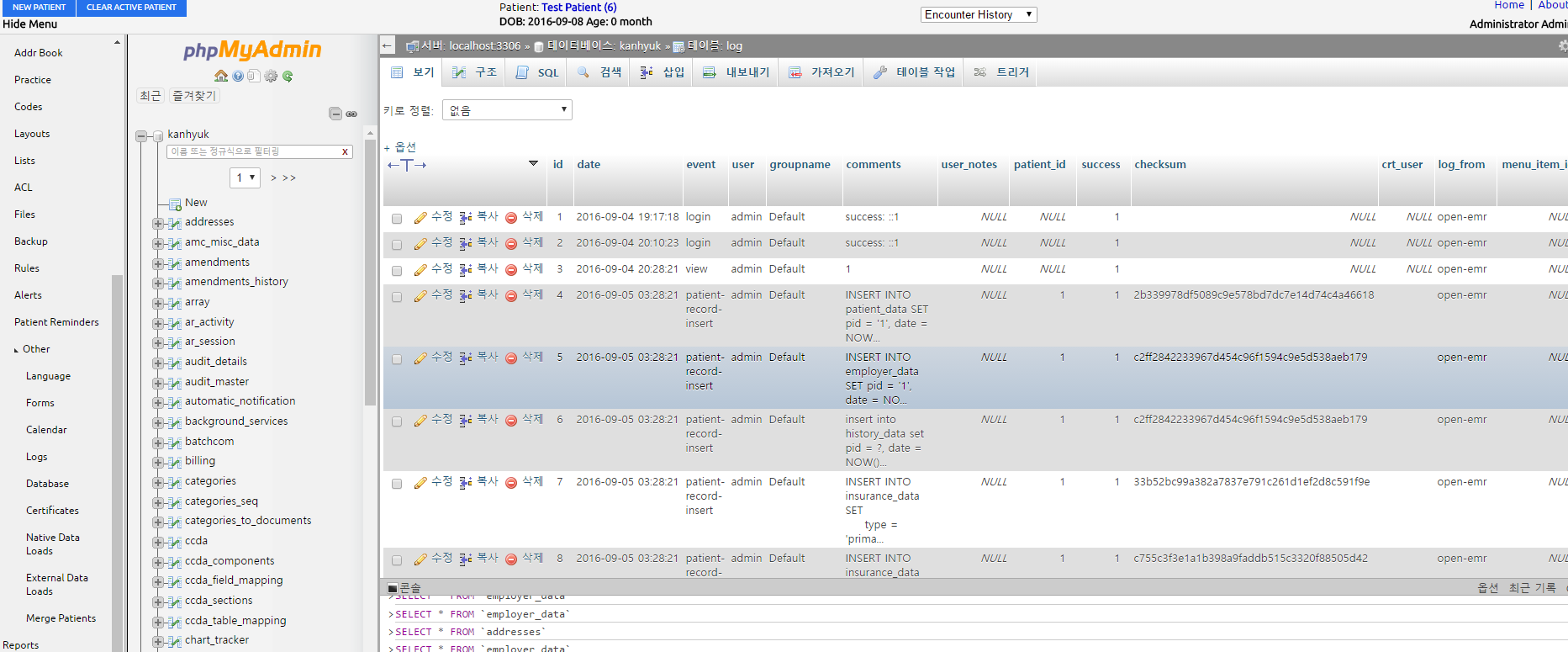
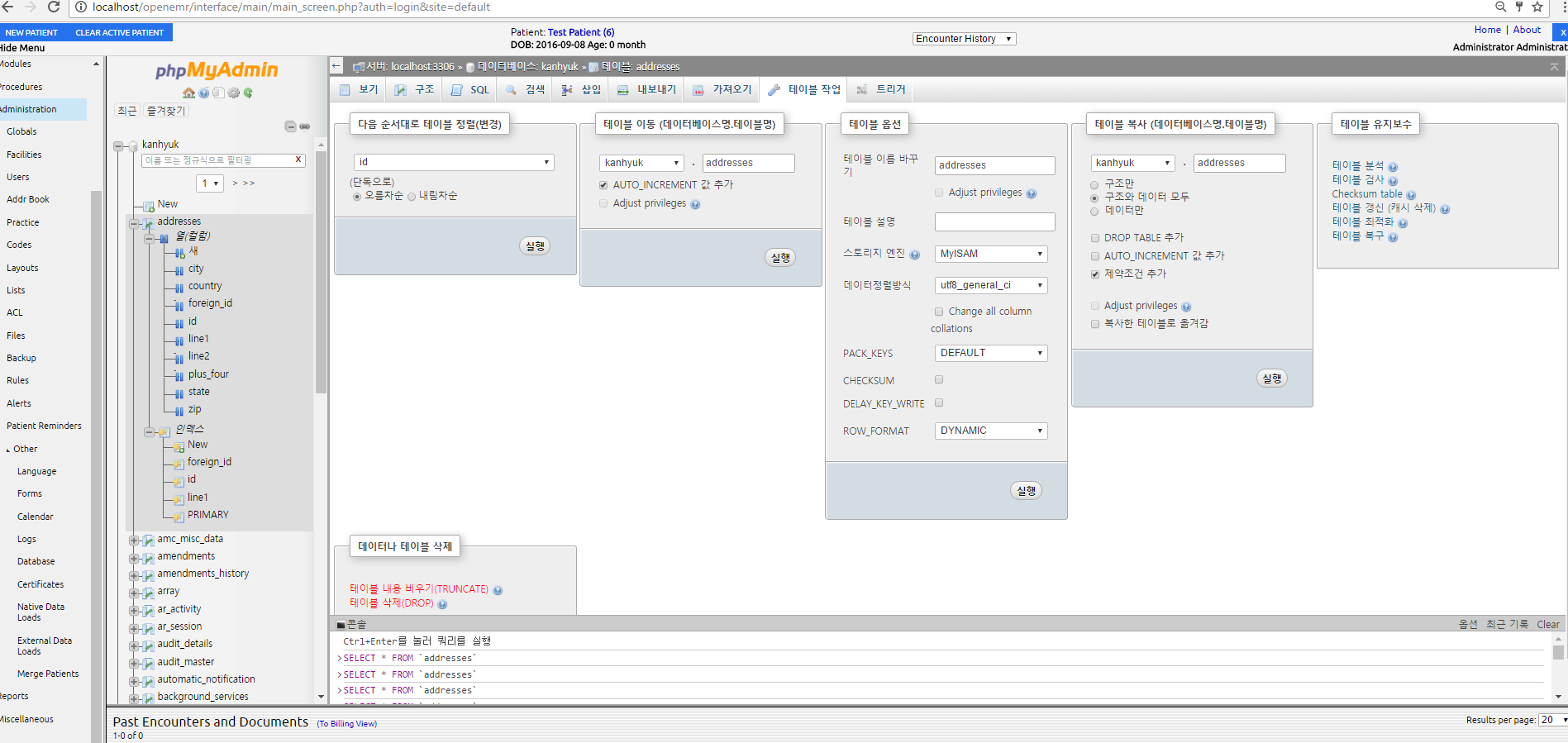
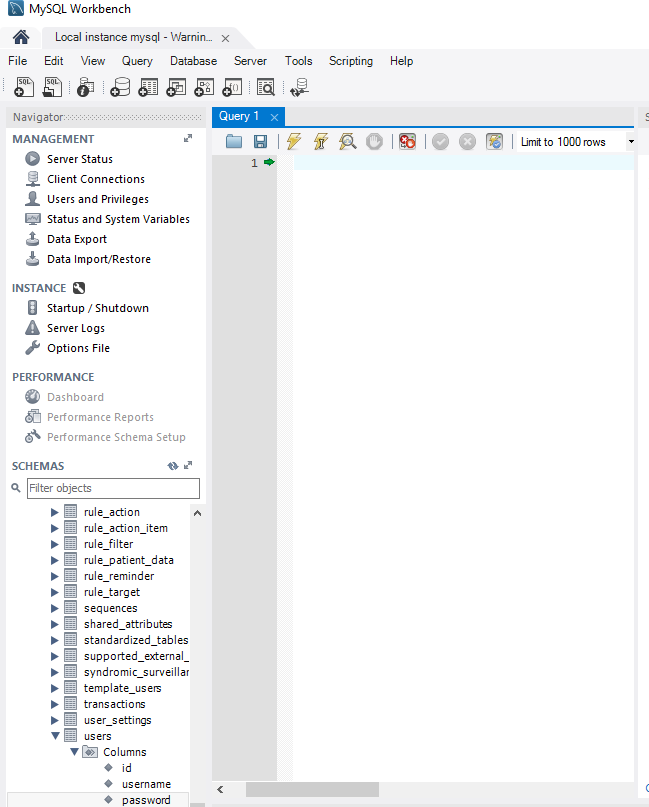
0000 0000 0000 0000 0000 0000 0000 0000

0000 0000 0000 0000 0000 0000 0000 1924

0000 0000 0000 0000 0000 0000 ffff ffff

ffff ffff ffff ffff ffff ffff ffff ffff

ffff ffff 0000 0000 0000 0000 57cc b6f7

* + found difference on 8th line of data keys -> Data stores in patient\_data
* workbench
  + names of databases
* log in to mysql workbench(Set mysql password on last assignment)
* found database under schemas
* 
* unser users\_secure/columns it stores password
* try to find login history.=? under instance/server logs
  + but it doesn’t show login history
* realized that I cant read files in detail so tried to find other way
* logged in to mysql with command shell
  + mysqladmin/log ->
  + typed show databases
  + <http://dev.mysql.com/doc/refman/5.7/en/show-engine.html> mysql shell commands
  + Show open tables shows that usable table entries in each database
  + Show tables in ‘database name’ shows every columns of that database
  + Show columns in tablename in databasename shows each columns of database
  + Also found phpmyadmin on localhost/openemr
  + Could found user history(login/out, create new user…) on log tab
  + Could find code when I press default value on datacolumn name
  + Can change database name or default values on phpmyadmin-tablework
  + Amendments -> history, and details(creator, created time, id,
  + Audit\_master -> ipaddress, created time, id, userid
  + Employer’s data -> employer id, date, country, city
  + On mysqlworkbench, under users/columns -> id, username, password, authorized…
  + 
  + Could check real code for the database on structure

