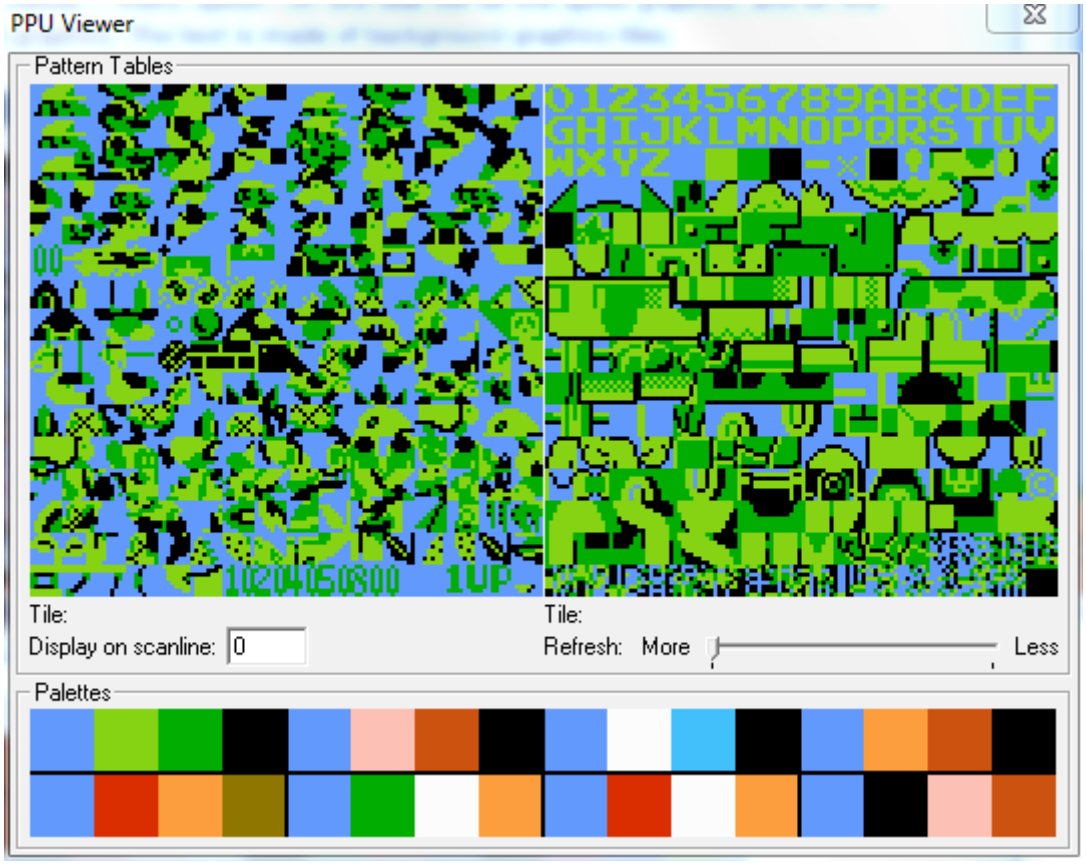
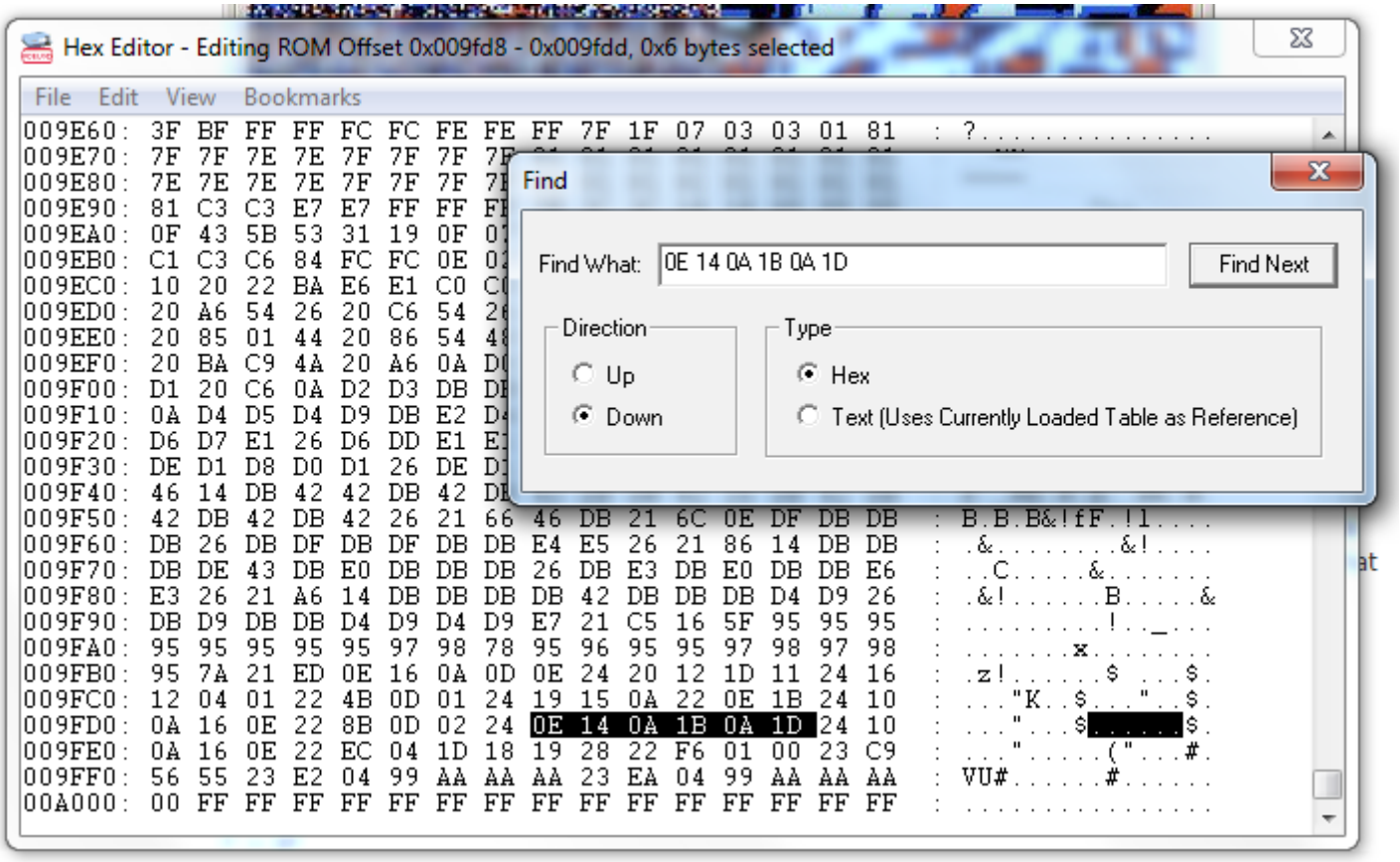
1. Hacking (a game) ROM. (i) Learn how to hack a game ROM from this link http://www.nintendoage.com/forum/messageview.cfm?catid=22&threadid=19733 (ii) Change 2 PLAYER GAME in menu to 2 Your Name GAME, e.g. I change the 2 PLAYER GAME to 2 EKARAT GAME. Capture and paste your change. * You can download the target game ROM (Super Mario Adventure (SMB1 Hack).nes) HERE.

→Just follow the instructions on the website.


→From the PPU Viewer, I found out that A = 0A, B = 0B, C = 0C, D = 0D, E = 0E, F = 0F, G = 10, H = 11, I = 12, J = 13, K = 14, L = 15, M = 16, N = 17, O = 18, P = 19, Q = 1A, R = 1B, S = 1C, T = 1D, U = 1E, V = 1F, W = 20, X = 21, Y = 22, Z = 23.


PPU Viewer
Pattern Tables
Tile:
Display on scanline: 0
Tile:
Refresh: More Less
Palettes


Hex Editor - Editing ROM Offset 0x009fd8 - 0x009fdd, 0x6 bytes selected
File Edit View Bookmarks
009E60: 3F BF FF FF FC FC FE FE FF 7F 1F 07 03 03 01 81 : ?...............
009E70: 7F 7F 7E 7E 7F 7F 7F 7F
009E80: 7E 7E 7E 7E 7F 7F 7F 7F
009E90: 81 C3 C3 E7 E7 FF FF FF
009EA0: 0F 43 5B 53 31 19 0F 07
009EB0: C1 C3 C6 84 FC FC 0E 02
009EC0: 10 20 22 BA E6 E1 C0 C0
009ED0: 20 A6 54 26 20 C6 54 26
009EE0: 20 85 01 44 20 86 54 48
009EF0: 20 BA C9 4A 20 A6 0A D0
009F00: D1 20 C6 0A D2 D3 DB DB
009F10: 0A D4 D5 D4 D9 DB E2 D4
009F20: D6 D7 E1 26 D6 DD E1 E1
009F30: DE D1 D8 D0 D1 26 DE D1
009F40: 46 14 DB 42 42 DB 42 DB
009F50: 42 DB 42 DB 42 26 21 66 46 DB 21 6C 0E DF DB DB : B.B.B&!fF.!l....
009F60: DB 26 DB DF DB DF DB DB E4 E5 26 21 86 14 DB DB : .&.........&!....
009F70: DB DE 43 DB E0 DB DB DB 26 DB E3 DB E0 DB DB E6 : ..C.....&.......
009F80: E3 26 21 A6 14 DB DB DB DB 42 DB DB DB D4 D9 26 : .&!.....B.....&
009F90: DB D9 DB DB D4 D9 D4 D9 E7 21 C5 16 5F 95 95 95 : .........!._...
009FA0: 95 95 95 95 95 97 98 78 95 96 95 95 97 98 97 98 : .......x........
009FB0: 95 7A 21 ED 0E 16 0A 0D 0E 24 20 12 1D 11 24 16 : .z!......$ ...$.
009FC0: 12 04 01 22 4B 0D 01 24 19 15 0A 22 0E 1B 24 10 : ...."K..$...."..$.
009FD0: 0A 16 0E 22 8B 0D 02 24 0E 14 0A 1B 0A 1D 24 10 : ...".....$.....$.
009FE0: 0A 16 0E 22 EC 04 1D 18 19 28 22 F6 01 00 23 C9 : ...".....("...#.
009FF0: 56 55 23 E2 04 99 AA AA AA 23 EA 04 99 AA AA AA : VU#.....#.....
00A000: 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF : ................
Find
Find What: 0E 14 0A 1B 0A 1D
Find Next
Direction
Up
Down
Type
Hex
Text (Uses Currently Loaded Table as Reference)

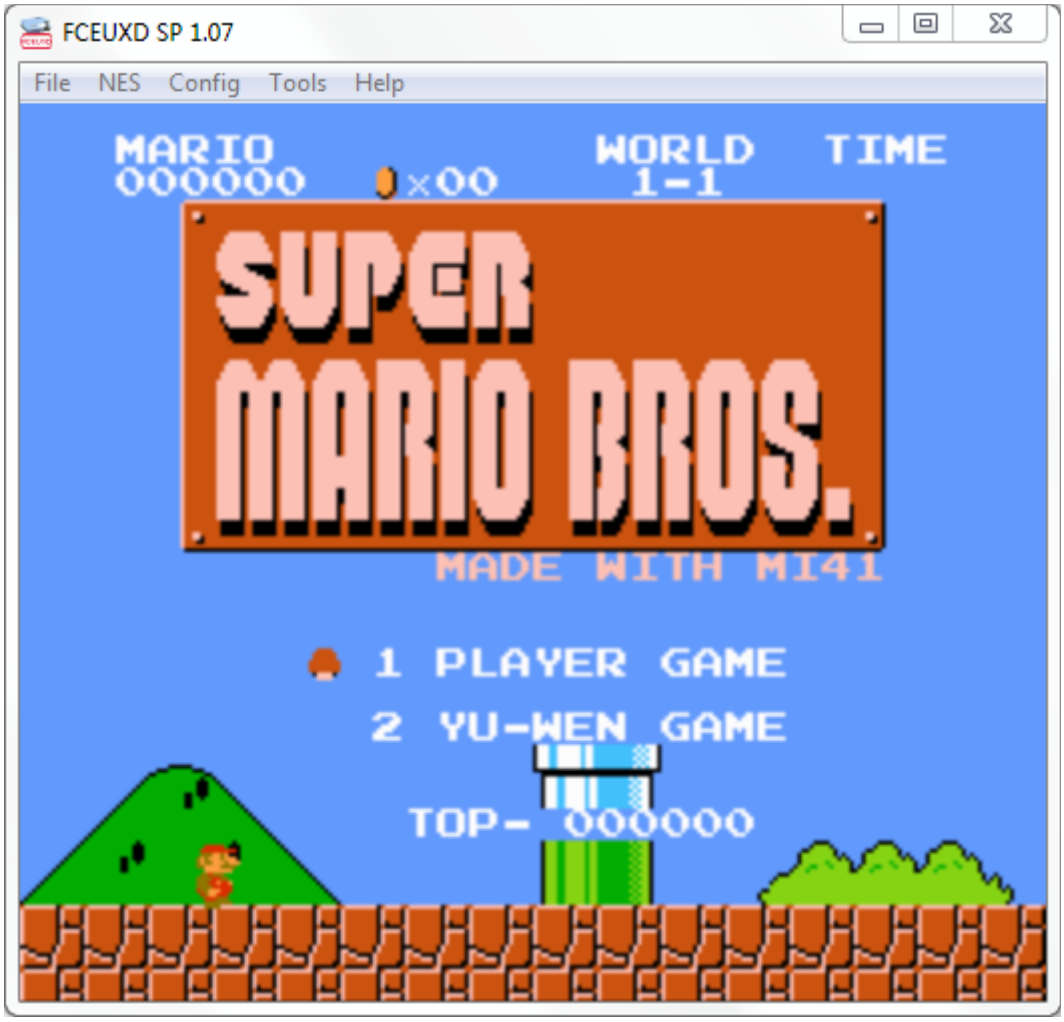
Hex Editor - Editing ROM Offset 0x009fde

File Edit View Bookmarks

```
009E60: 3F BF FF FF FC FC FE FE FF 7F 1F 07 03 03 01 81
009E70: 7F 7F 7E 7E 7F 7F 7F 7F 81 81 81 81 81 81 81 81
009E80: 7E 7E 7E 7E 7F 7F 7F 7F 81 81 81 81 81 81 81 81
009E90: 81 C3 C3 E7 E7 FF FF FF 7E 3C 3C 18 18 00 00 00
009EA0: 0F 43 5B 53 31 19 0F 07 F2 FE FE FF FF EF F7 F8
009EB0: C1 C3 C6 84 FC FC 0E 02 BF BE BD 7B 7B 07 F3 FD
009EC0: 10 20 22 BA E6 E1 C0 C0 FF FF FF 67 59 9E BF BF
009ED0: 20 A6 54 26 20 C6 54 26 20 E6 54 26 21 06 54 26
009EE0: 20 85 01 44 20 86 54 48 20 9A 01 49 20 A5 C9 46
009EF0: 20 BA C9 4A 20 A6 0A D0 D1 D8 D8 DE D1 D0 DA DE
009F00: D1 20 C6 0A D2 D3 DB DB DB D9 DB DC DB DF 20 E6
009F10: 0A D4 D5 D4 D9 DB E2 D4 DA DB E0 21 06 0A D6 D7
009F20: D6 D7 E1 26 D6 DD E1 E1 21 26 14 D0 E8 D1 D0 D1
009F30: DE D1 D8 D0 D1 26 DE D1 DE D1 D0 D1 D0 D1 26 21
009F40: 46 14 DB 42 42 DB 42 DB 42 DB DB 42 26 DB 42 DB
009F50: 42 DB 42 DB 42 26 21 66 46 DB 21 6C 0E DF DB DB
009F60: DB 26 DB DF DB DF DB DB E4 E5 26 21 86 14 DB DB
009F70: DB DE 43 DB E0 DB DB DB 26 DB E3 DB E0 DB DB E6
009F80: E3 26 21 A6 14 DB DB DB DB 42 DB DB DB D4 D9 26
009F90: DB D9 DB DB D4 D9 D4 D9 E7 21 C5 16 5F 95 95 95
009FA0: 95 95 95 95 95 97 98 78 95 96 95 95 97 98 97 98
009FB0: 95 7A 21 ED 0E 16 0A 0D 0E 24 20 12 1D 11 24 16
009FC0: 12 04 01 22 4B 0D 01 24 19 15 0A 22 0E 1B 24 10
009FD0: 0A 16 0E 22 8B 0D 02 24 22 1E 28 20 0E 17 24 10
009FE0: 0A 16 0E 22 EC 04 1D 18 19 28 22 F6 01 00 23 C9
009FF0: 56 55 23 E2 04 99 AA AA AA 23 EA 04 99 AA AA AA
00A000: 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

FCEUXD SP 1.07

File NES Config Tools Help



2. Use your Hex editor to modify any programs you want, and tell us (i) What is the target program? (ii) What is your modification? Show the captured screen of the result.

→I wrote a simple program by myself.

```
vim hello.cpp
 1 #include <iostream>
 2 #include <string>
 3 using namespace std;
 4
 5 int main () {
 6         string test;
 7         cout << "Hello, World!" << endl;
 8         cin >> test;
 9         cout << "test = " << test << endl;
10         return 0;
11 }
12
```

```
~ ./hello
Hello, World!
tset
test = tset
```

```
~ vim hello.cpp
~ hexdump -C hello
00000000  7f 45 4c 46 02 01 01 00  00 00 00 00 00 00 00 00  |.ELF............|
00000010  02 00 3e 00 01 00 00 00  70 0b 40 00 00 00 00 00  |..>.....p.@.....|
00000020  40 00 00 00 00 00 00 00  40 2f 00 00 00 00 00 00  |@.......@/......|
00000030  00 00 00 00 40 00 38 00  09 00 40 00 1f 00 1c 00  |....@.8...@.....|
00000040  06 00 00 00 05 00 00 00  40 00 00 00 00 00 00 00  |........@.......|
00000050  40 00 40 00 00 00 00 00  40 00 40 00 00 00 00 00  |@.@.....@.@.....|
00000060  f8 01 00 00 00 00 00 00  f8 01 00 00 00 00 00 00  |................|
00000070  08 00 00 00 00 00 00 00  03 00 00 00 04 00 00 00  |................|
00000080  38 02 00 00 00 00 00 00  38 02 40 00 00 00 00 00  |8.......8.@.....|
00000090  38 02 40 00 00 00 00 00  1c 00 00 00 00 00 00 00  |8.@.............|
```

→I changed “Hello, World!” to “Hello, MY NAME!”

```
00000dc0  fc ff ff 48 85 ed 74 1e  0f 1f 84 00 00 00 00 00  |...H..t.........|
00000dd0  4c 89 ea 4c 89 f6 44 89  ff 41 ff 14 dc 48 83 c3  |L..L..D..A...H..|
00000de0  01 48 39 eb 75 ea 48 83  c4 08 5b 5d 41 5c 41 5d  |.H9.u.H...[]A\A]|
00000df0  41 5e 41 5f c3 90 66 2e  0f 1f 84 00 00 00 00 00  |A^A_..f.........|
00000e00  f3 c3 00 00 48 83 ec 08  48 83 c4 08 c3 00 00 00  |....H...H.......|
00000e10  01 00 02 00 48 65 6c 6c  6f 2c 20 57 6f 72 6c 64  |....Hello, World|
00000e20  21 00 74 65 73 74 20 3d  20 00 00 00 01 1b 03 3b  |!.test = ......;|
00000e30  40 00 00 00 07 00 00 00  44 fc ff ff 8c 00 00 00  |@.......D.......|
00000e40  44 fd ff ff 5c 00 00 00  3a fe ff ff d4 00 00 00  |D...\...:.......|
00000e50  03 ff ff ff fc 00 00 00  41 ff ff ff 1c 01 00 00  |........A.......|
00000e60  64 ff ff ff 3c 01 00 00  d4 ff ff ff 84 01 00 00  |d...<...........|
```

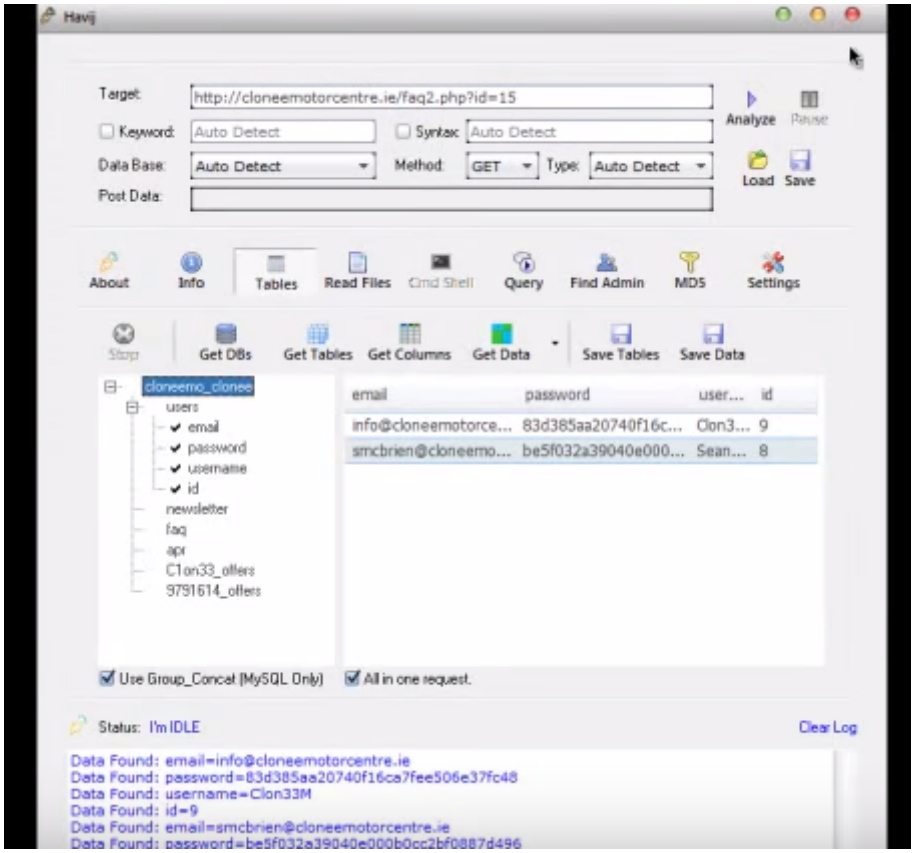
```
147  00000db0:  d531 db4c 29e5 4883 ec08 48c1 fd03 e88d fcff ff48 85ed 741e  :.1.L).H...H....t.
148  00000dc8:  0f1f 8400 0000 0000 4c89 ea4c 89f6 4489 ff41 ff14 dc48 83c3  :........L..L..D..A...H..
149  00000de0:  0148 39eb 75ea 4883 c408 5b5d 415c 415d 415e 415f c390 662e  :.H9.u.H...[]A\A]A^A_..f.
150  00000df8:  0f1f 8400 0000 0000 f3c3 0000 4883 ec08 4883 c408 c300 0000  :............H...H.......
151  00000e10:  0100 0200 4865 6c6c 6f2c 2057 6f72 6c64 2100 7465 7374 203d  :....Hello, World!.test =
152  00000e28:  2000 0000 011b 033b 4000 0000 0700 0000 44fc ffff 8c00 0000  : ......;@.......D.......
153  00000e40:  44fd ffff 5c00 0000 3afe ffff d400 0000 03ff ffff fc00 0000  :D...\...:.......
154  00000e58:  41ff ffff 1c01 0000 64ff ffff 3c01 0000 d4ff ffff 8401 0000  :A.......d...<.....
155  00000e70:  1400 0000 0000 0000 017a 5200 0178 1001 1b0c 0708 9001 0710  :.........zR..x.....
156  00000e88:  1400 0000 1c00 0000 e0fc ffff 2a00 0000 0000 0000 0000 0000  :............*.....
157  00000ea0:  1400 0000 0000 0000 017a 5200 0178 1001 1b0c 0708 9001 0000  :.........zR..x.....
158  00000eb8:  2400 0000 1c00 0000 b0fb ffff 0001 0000 000e 1046 0e18 4a0f  :$..............F..J.
159  00000ed0:  0b77 0880 003f 1a3b 2a33 2422 0000 0000 1c00 0000 0000 0000  :.w...?.;*3$"......
           Hex Inspector : Big Endian
byte       :  72                    short      :  72
word       :  18533                 int        :  18533
```

```
00dc8:  0f1f 8400 0000 0000 4c89 ea4c 89f6 4489 ff41 ff14 dc48 83c3  :........L..L..D..A...H..
00de0:  0148 39eb 75ea 4883 c408 5b5d 415c 415d 415e 415f c390 662e  :.H9.u.H...[]A\A]A^A_..f.
00df8:  0f1f 8400 0000 0000 f3c3 0000 4883 ec08 4883 c408 c300 0000  :............H...H.......
00e10:  0100 0200 4865 6c6c 6f2c 2059 7577 656e 2100 7465 7374 203d  :....Hello, Yuwen!.test =
00e28:  2000 0000 011b 033b 4000 0000 0700 0000 44fc ffff 8c00 0000  : ......;@.......D.......
00e40:  44fd ffff 5c00 0000 3afe ffff d400 0000 03ff ffff fc00 0000  :D...\...:.......
00e58:  41ff ffff 1c01 0000 64ff ffff 3c01 0000 d4ff ffff 8401 0000  :A.......d...<.....
00e70:  1400 0000 0000 0000 017a 5200 0178 1001 1b0c 0708 9001 0710  :.........zR..x.....
```

```
~ ./hello2
Hello, Yuwen!
tset
test = tset
```

3. Havij. (i) Install Havij. (ii) Explain how to use this tool to crack a database.

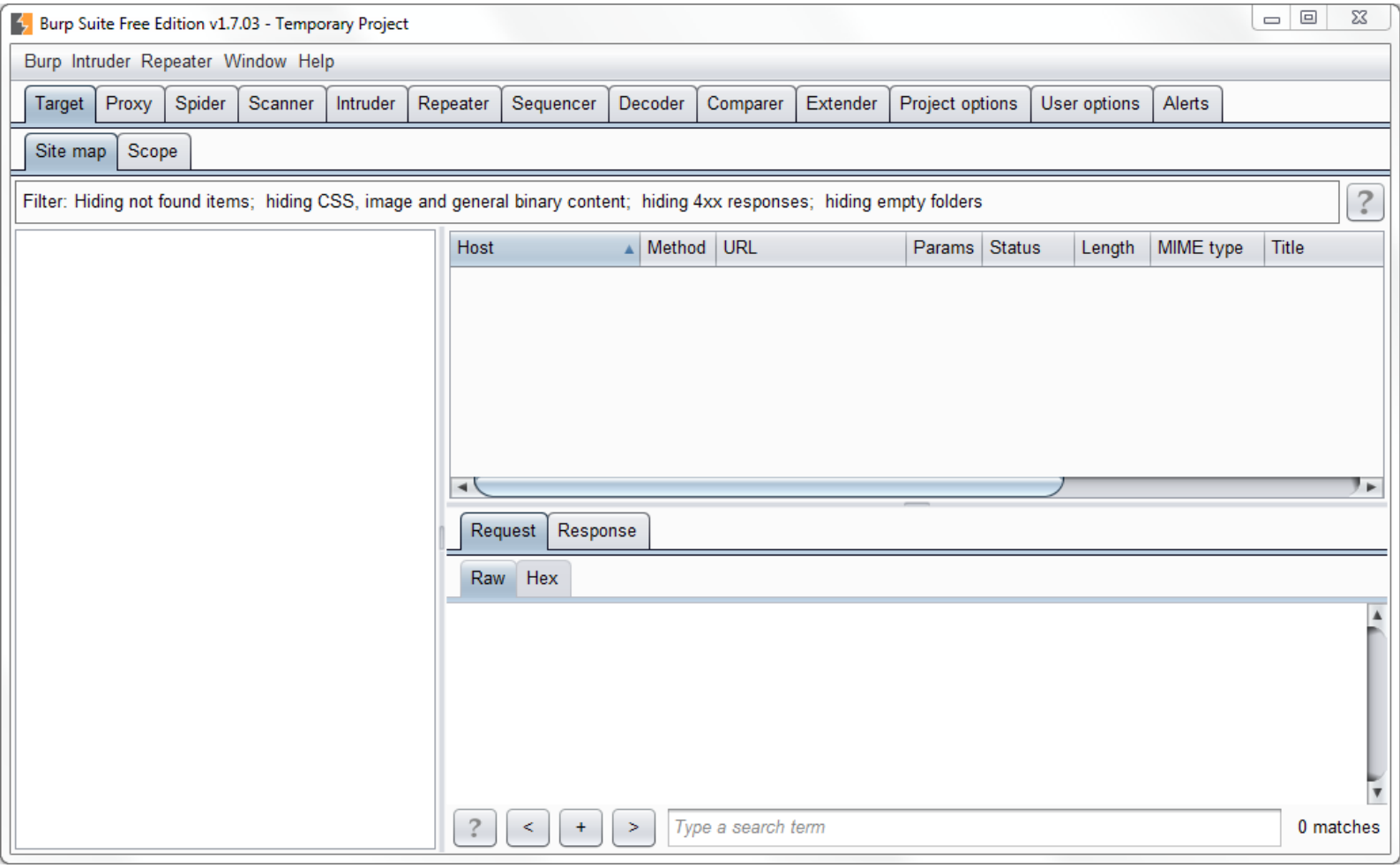
→I tried hard, but I still cannot find an effective link to download the program. The following image is taken from the Internet (by TheHallo80, under the CC BY License).



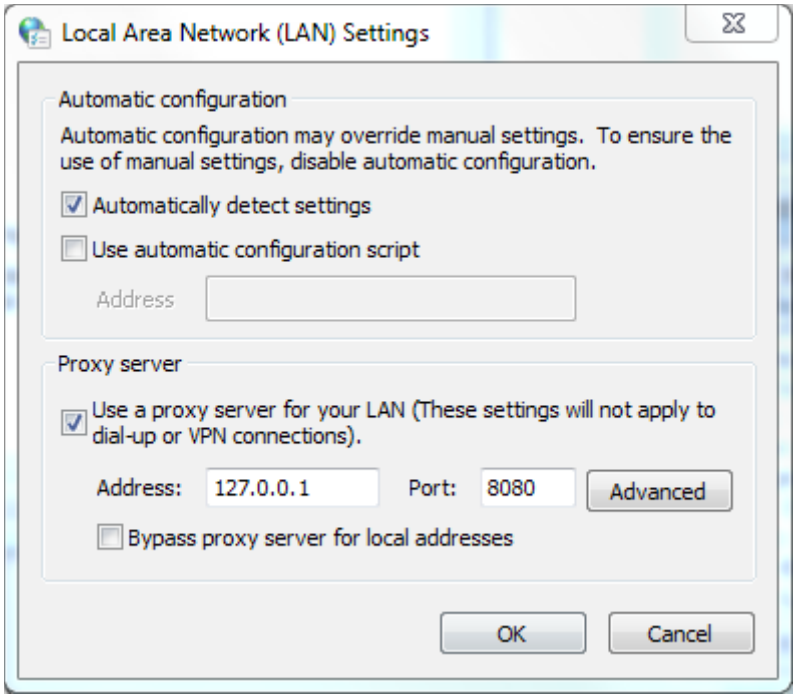

→First find a website that SQL injection can be applied. (Usually, when we modify the URL parameter of a vulnerable website to an arbitrary value, we will encounter some unexpected behavior, e.g. seeing some SQL error messages.) Then, just click analyze. It will try to inject the database behind the website. After succeeding, we can use the GUI to retrieve the table schema and content.

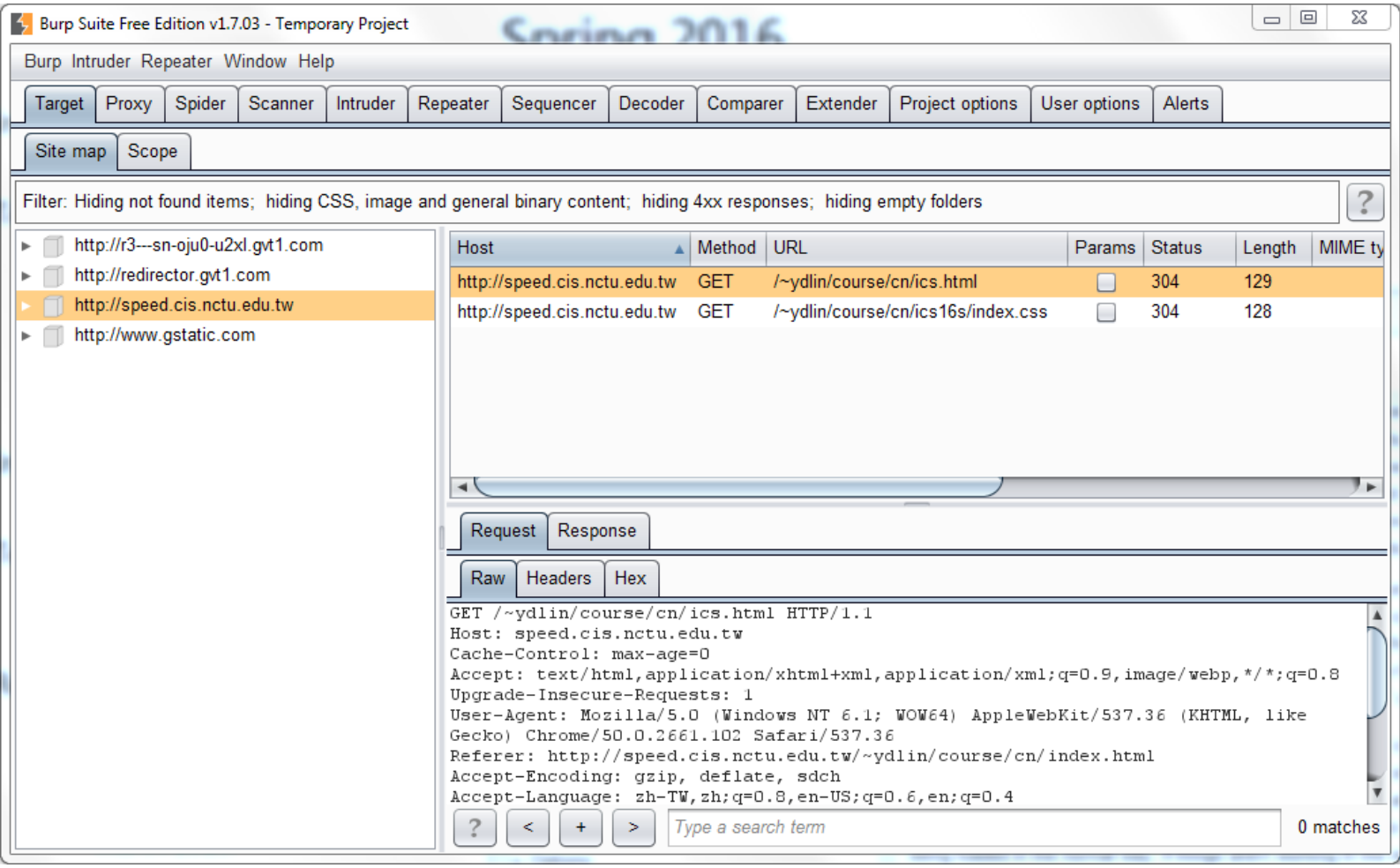
4. Burp Suite. (i) Install Burp Suite. (ii) Explain how to use this tool. (iii) Using Burp Suite to scan a target, what kind of information can you get?

→ I can only get the Free Edition from its official website. It's a JAR program, so there is no need to install.

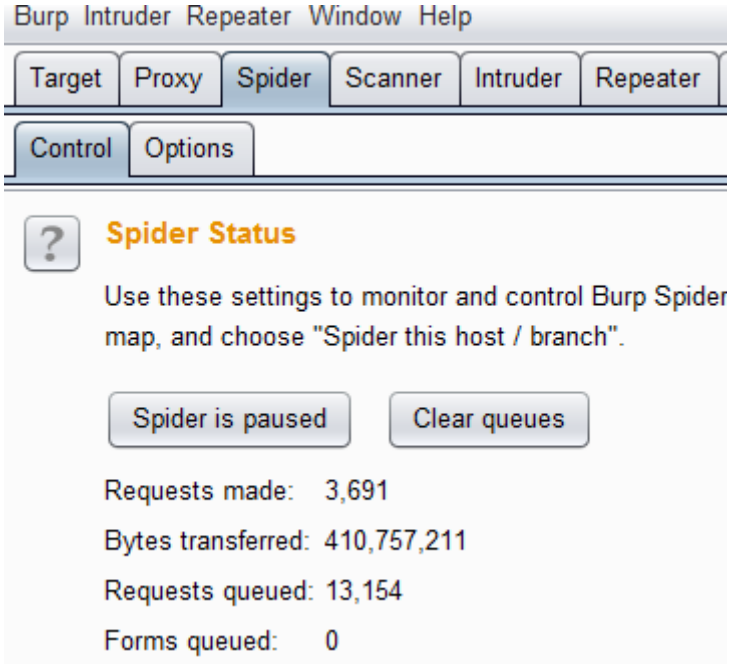



→ Simply change the proxy settings for your browser (or your OS), and it works.


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: 127.0.0.1
Port: 8080
Advanced
Bypass proxy server for local addresses
OK
Cancel


Burp Suite Free Edition v1.7.03 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://r3---sn-oju0-u2xl.gvt1.com
http://redirector.gvt1.com
http://speed.cis.nctu.edu.tw
http://www.gstatic.com
Host Method URL Params Status Length MIME ty
http://speed.cis.nctu.edu.tw GET /~ydlin/course/cn/ics.html 304 129
http://speed.cis.nctu.edu.tw GET /~ydlin/course/cn/ics16s/index.css 304 128
Request Response
Raw Headers Hex
GET /~ydlin/course/cn/ics.html HTTP/1.1
Host: speed.cis.nctu.edu.tw
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36
Referer: http://speed.cis.nctu.edu.tw/~ydlin/course/cn/index.html
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4
Type a search term
0 matches

→ Scanner can automatically find vulnerabilities in your website. However, Scanner is only available in the Professional Edition, so I used Spider. Then I found several interesting URLs, which are saying that they are “protected files.”




| Host | Method | URL | Params | Status | Length | MIME ty |
|---|---|---|---|---|---|---|
| http://speed.cis.nctu.edu.tw | GET | /phdStudyTip.html | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /photo/group/00-01.html | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /photo/group/98-99.html | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /photo/group/photo2002-01-25/index... | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /photo/group/ydlin.html | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /proposalTip.html | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /protected_files/final_scores.php | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /protected_files/hw1_scores.php | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /protected_files/hw2_scores.php | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /protected_files/hw3_scores.php | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /protected_files/hw4_scores.php | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /protected_files/hw5_scores.php | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /protected_files/hw6_scores.php | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /protected_files/midterm_scores.php | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /protected_files/total_scores.php | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /quarterly_m.doc | | | | HTML |
| http://speed.cis.nctu.edu.tw | GET | /quarterly_r.doc | | | | HTML |