Activity 1: Hex Hacking

Group No: 55

Group Member:

1. Prangthip Buatongthanakarn
2. Nuttamas Udomsantitham
3. Kritsada Limsripraphan
4. Supanut Udompataikul
5. Tarmeesee Daoh

Part 0: Preparation

- Download “Activity 1 Resources” from CourseVille.
- In Part 2, each group is assigned to work with the files: [YOUR_GROUP_NO].bmp, and [YOUR_GROUP_NO].gif in “02 Pic” folder
- Answer the questions in the box given and submit this file (.docx format) to CourseVille.

Part 3: Data Representation in the Memory

Introduction

- The folder “03 Part 3” contains *fceux.exe* which is an NES (Nintendo’s game console) emulator.
- Execute the program. Then, open “Super Mario” ROM (Files > Open ROM). The ROM file is in the subfolder “roms”.
- If you are not familiar with the games, play the games for 5 minutes. (Use the arrow keys, ‘f’ for the ‘A’ (jump) button, ‘d’ for the ‘B’ (run,fireball) button, ‘s’ for the ‘SELECT’ button, and ‘Enter’ for the ‘START’ button.

Activity 1: Hex Hacking

Activity: Super Mario Hack

0. While playing the games, pause the games by hitting the “Enter” key. Open the built-in hex editor. (Debug > Hex Editor). The hexadecimal numbers displayed in the hex editor is the real-time memory of the program (NES memory).
1. The values at the position 0x0754 and at the position 0x0756 are known to be the data determining the “states” of Mario (short/tall, Normal Mario/Super Mario/Fire Mario).
    - Normally, Mario starts in the “Normal Mario” state (he looks short) and when he takes a “Mushroom” item, he grows into the “Super Mario” state (and he looks taller). In the “Super Mario” state, he can take a “Flower” item to go to the “Fire Mario” state in which he can throw fireballs with the “B” button.
    - When a “Fire Mario” or a “Super Mario” is hit by an enemy, he is downgraded to “Normal Mario”. When a “Normal Mario” is hit by an enemy, he dies.
    - Try changing the values in both positions to have a “short” Mario that can throw fireballs. What are the values?

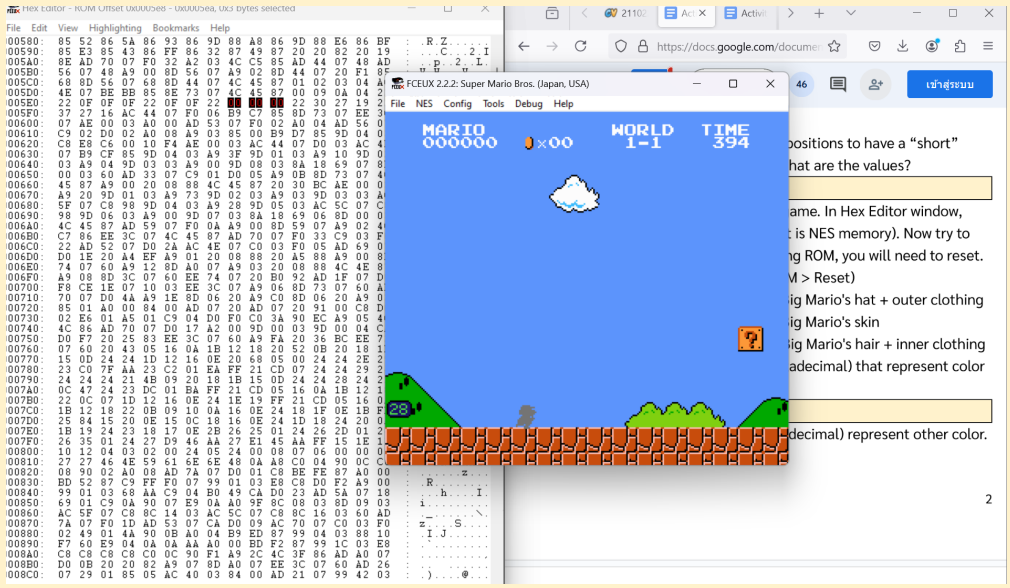
- Change the values at the position 0x0754 to 01
- Change the values at the position 0x0756 to 02

2. Now we will modify the ROM of the game. In Hex Editor window, select View > ROM File. (Hint: default is NES memory). Now try to edit the Mario character. (After editing ROM, you will need to reset. On the main screen menu, select ROM > Reset)
    - Byte : 0x05E8 = Color of Small/Big Mario's hat + outer clothing
    - Byte : 0x05E9 = Color of Small/Big Mario's skin
    - Byte : 0x05EA = Color of Small/Big Mario's hair + inner clothing
    - What’s the original value (in Hexadecimal) that represent color of Mario?

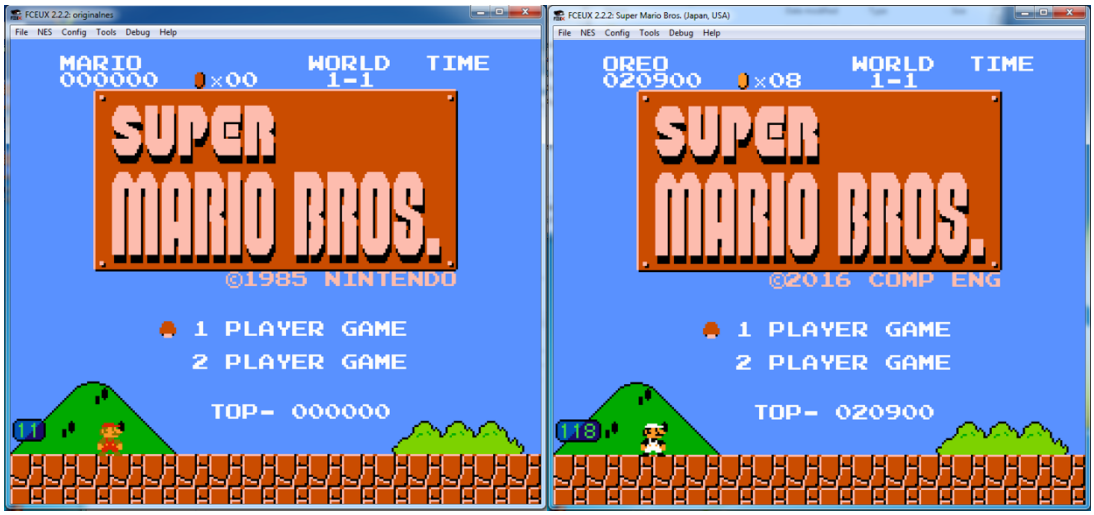
Activity 1: Hex Hacking

- Color of Small/Big Mario's hat + outer clothing is 16
- Color of Small/Big Mario's skin is 27
- Color of Small/Big Mario's hair + inner clothing is 18

- Try changing the values (in Hexadecimal) represent other color. Capture the result.



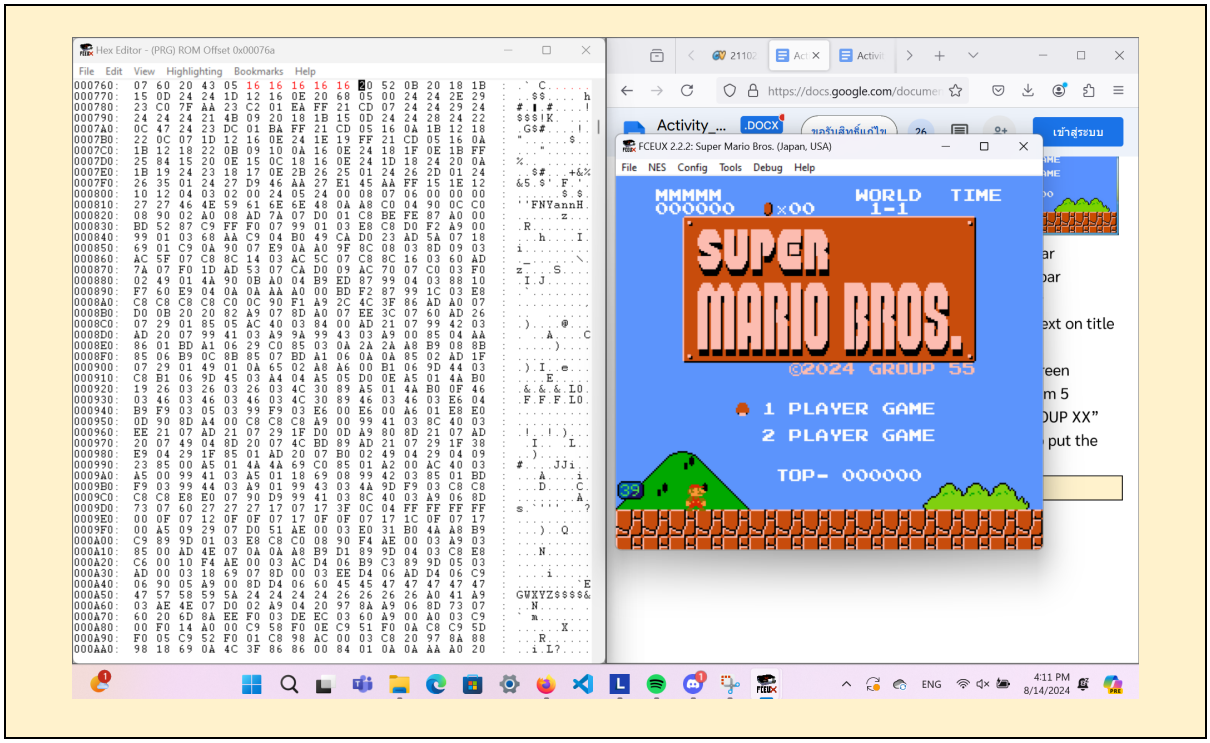
3. Now try to edit the text on the welcome screen.



- Bytes : 0x00765 to 0x00769 = "MARIO" text on top bar
- Bytes : 0x0076D to 0x00771 = "WORLD" text on top bar
- Bytes : 0x00774 to 0x00777 = "TIME" text on top bar

Activity 1: Hex Hacking

- Bytes : 0x09FB5 to 0x09FC2 = "©1985 NINTENDO" text on title screen
- Bytes : 0x09FE6 to 0x09FE9 = "TOP-" text on title screen
- Try to edit the word “MARIO” to your name (maximum 5 characters) and “©1985 NINTENDO” to “©2024 GROUP XX” (XX is your group number). How do you do that? Also put the screenshot here.



Activity 1: Hex Hacking

A Chance for the "Outstanding Factor"

Super Mario "Open" Hack

Some of the "best hack" will be awarded this week's "Outstanding Factor"

For example, you can control the timer on the top right of the screen by changing memory at 0x07F8-0x07FA to your decided value. Try changing 0x07F8-0x07FA to 09 09 09 to get more idea.

Another example is to control your score by changing memory at 0x07D8-0x7DD to any value. Good Luck!

With the information given below, do something fun on your own. Call TA and explain what changes you made. (At least five additional changes are needed to be considered outstanding. Only some groups will be given outstanding, so imagination is preferred.)

Here's the information.

===== In ROM File =====
05E0 = Background (sky) color for Overworld levels 1-1, 1-3, 2-1, 2-3, 4-1, 4-3, 5-3, 7-3, 8-1, 8-2 and 8-3.
05E1 = Background color for Underground levels 1-2 and 4-2. (Also used for New Level and Game Over screens.)
05E2 = Background color for Dungeon levels 1-4, 2-4, etc.
05E3 = Background color for Nighttime Overworld levels 3-3, 6-1 and 6-2.
05E4 = Background color for Winter Overworld levels 5-1, 5-2 and 7-1.
05E5 = Background color for Winter Nighttime Overworld levels 3-1 and 3-2 (and the cloud portion of 6-2).
05E6 = Background color for level 6-3.

Activity 1: Hex Hacking

===== In NES Memory =====

0024 - Fireball 1 Flag / Explosion Delay (00-01 / 80-86)
0025 - Fireball 2 Flag / Explosion Delay (00-01 / 80-86)

0030 - Point display 3 timeout
0031 - Point display 2 timeout
0032 - Point display 1 timeout

0057 - Player X Delta (Signed)

008D - Fireball 1 X Position (00-FF)
008E - Fireball 2 X Position (00-FF)

009F - Player Y Delta (Signed)

00A6 - Fireball 1 Status? (03, FD, FE)
00A7 - Fireball 2 Status? (03, FD, FE)

00CE - Player Y Position

00D5 - Fireball 1 Y Position (00-FF)
00D6 - Fireball 2 Y Position (00-FF)

0200-02FF - PPU Sprite Memory
0300-03FF - Sprite Values
03A0 - Unknown Value, Gets set to FF every time a map is loaded.

0500-05CF - Screen layout page 1
05D0-069F - Screen layout page 2

Activity 1: Hex Hacking

06A0 - Screen Memory Offset

06CE - Fireball Count (00-FF)

06D5 - Player Sprite Frame

06D7 - End of Level Fireworks (Firework position is determined by value)

06FC - Controller 1 Poll

0700 - Running Animation Speed (00-28)
0701 - Sliding Flag (00 - No, 01 - Yes)
0702 - Slide Length
0703 - Matches Running Animation Speed from 1C-28
0704 - Unused?
0705 - Cycles during walking animation
0706 - Minimum Jump Height (01)
0707 - Always 01?
0708 - Starting Jump Y Position (Affects max jump height)
0709 - Player Y Delta While Jumping
070A - Player Y Delta Change To
070B - Player Injured Flag
070C - Walking Frame Delay (04-07)
070D - Player Frame While Walking (00-02)
070E - ? When Not 00, Player can't move or jump
070F - ? When not 0, score at flag is visible before touched.
0710 - How Mario enters the level (00-07)
    00 - Fall from ceiling - Water (2-2)
    01 - Fall from ceiling - Underground (1-2)
    02 - On ground (1-1) Also, pipes and vines
    03 - Middle of screen for castles (1-4)

04 - Unused: Same as 01
05 - Unused: Same as 01 (maybe 02?)
06 - Unused: Same as 07
07 - On ground, Mario walks right (Between 1-1 and 1-2)
0711 - Delay (Used by throwing fireballs)
0712 - Unused?
0713 - Used during flag contact
0714 - Ducking Flag (00 - Walking, 04 - Ducking)

0747 - Object pause (When above zero, nothing but Mario can move. Used upon dieing)
0748 - Display Coins
074A - Controller 1 Poll
074B - Controller 2 Poll

074E - Bubble Flag (00 - Bubbles Visible, 01 - No Bubbles)

0754 - Tall Mario Flag (00 - Tall, 01 - Short)
0756 - Powerup Flag (00 - Mario, 01 - Super Mario, 02 - Fire Mario)
0757 - Player Lives Screen Flag (00 - Playing, 01 - Player Lives Screen)
0758 - Vine Growth Flag? Set to 1, die, restart, vine grows!
0759 - Time Up Flag (00-01) Doesn't take effect until after death
075A - Current Player Lives
075C - Display Level
075E - Display Coins
075F - World
0760 - Level
0761 - Waiting Player Lives

0770 - Gameplay Mode (00 - Demo, 01 - Playing, 02 - End of Level)

Activity 1: Hex Hacking

0772 - Gameplay Status (00 - Run to next status, 01 - Loading, 02 - Loading done, 03 - Playing)
0773-0774 - Counters for Gameplay Status

0778 - Affects Horizontal Scrolling
0779 - Color Mode? (1E - Color, 1F - Black & White)

077F - Delay (Used by demo, invincibility, and player lives screen)

0781 - Delay (Used by walking and throwing fireballs)
0782 - Delay (Used by jumping)

0787 - Timer Delay (00-18)

079F - Star Invincibility Timeout (00 - Not Invincible, 00-07 - Slow Flash, 08-FF - Fast Flash) - You can even kill Bowser's fireballs!

07A0 - Player Lives Countdown (00-07) At zero it starts the demo.
07A2 - Demo Countdown (00-07) At zero it starts the demo.

07ED - P1 Coins: 9x
07EE - P1 Coins: x9
07F3 - P2 Coins: 9x
07F4 - P2 Coins: x9

07FC - Beat Game Flag (00 - 1st Run, 01 - 2nd Run)

B424 - Standing Max Jump Height (20) Signed
B425 - Sliding Max Jump Height (20) Signed
B426 - Walking Max Jump Height (1E) Signed
B427 - Staring to Run Max Jump Height (28) Signed

Activity 1: Hex Hacking

B428 - Running Max Jump Height (28) Signed

B42B - Standing Gravity (70) Signed
B42C - Sliding Gravity (70) Signed
B42D - Walking Gravity (60) Signed
B42E - Starting to Run Gravity (90) Signed
B42F - Running Gravity (90) Signed

B432 - Standing Jump Y Delta (FC) Signed
B433 - Sliding Jump Y Delta (FC) Signed
B434 - Walking Jump Y Delta (FC) Signed
B435 - Starting to Run Jump Y Delta (FB) Signed
B436 - Running Jump Y Delta (FB) Signed

B440 - Left Running Speed Max (D8) Signed
B441 - Left Walking Speed Max (E8) Signed
B443 - Right Running Speed Max (28) Signed
B444 - Right Walking Speed Max (18) Signed

B447 - Running Acceleration (E4) Unsigned