



## รายงานวิชา Computer Security

### Assignment III

#### จัดทำโดย

นายปณิธาน ดวงขวัญ

รหัส 5735512036 Section 02

#### เสนอ

อาจารย์ฐิตินันท์ เกלי่งสุวรรณ

รหัสวิชา 242-312 Computer Security

คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

มหาวิทยาลัยสงขลานครินทร์

## Assignment III

เลือกหนึ่งหัวข้อจากที่กำหนดให้ ทำการค้นคว้าข้อมูลจากอินเทอร์เน็ต แล้วทำการทดลองตามหัวข้อที่เลือก เขียนรายละเอียดวิธีการที่ได้ศึกษาการทดลองเป็นรายงาน

### หัวข้อที่กำหนด

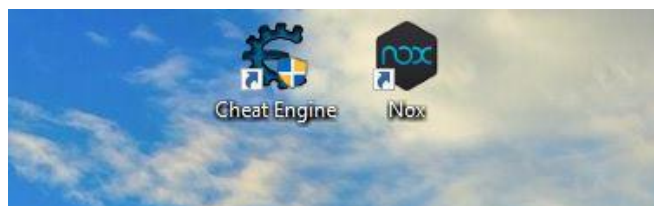
1. Port Scanning
2. Session Hijacking
3. หัวข้ออื่นๆ เช่น game hacking , password related issues, ARP spoof , MAC address spoof , sniffing tool เช่น Aircrack , cookies related issues , SQL injection

### 1.ข้อมูลพื้นฐานของ hack game โดยใช้ Cheat Engine

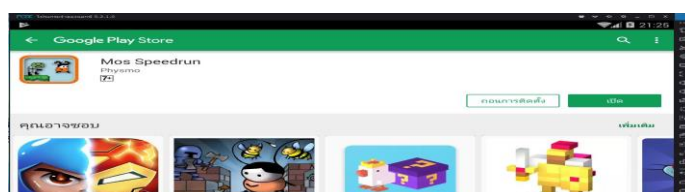
โปรแกรม **Cheat Engine 6.2** จะค้นหาค่า address ของค่าต่างๆ ในเกมส์เพื่อให้เราสามารถเปลี่ยนแปลงแก้ไขได้ เช่นการเพิ่มเงิน เพิ่มเลือด เพิ่มค่า EXP เพิ่มค่าสเตตัสต่างๆ หรือค่าที่เป็นตัวเลขภายในเกมส์ได้เกือบทั้งหมด โดยมีขั้นตอนที่เข้าใจได้ง่าย ไม่ยากนัก ซึ่งตัวโปรแกรมสามารถแก้ไขความเร็วของเกมส์ได้ด้วย เรียกว่า Speed hack เพียงแค่เข้าโปรแกรมแล้วเช็คที่ช่อง enable speed hack แล้วปรับความเร็วตามที่ต้องการแค่นี้ก็เรียบร้อยแล้ว

### 2.วิธีการทดลอง

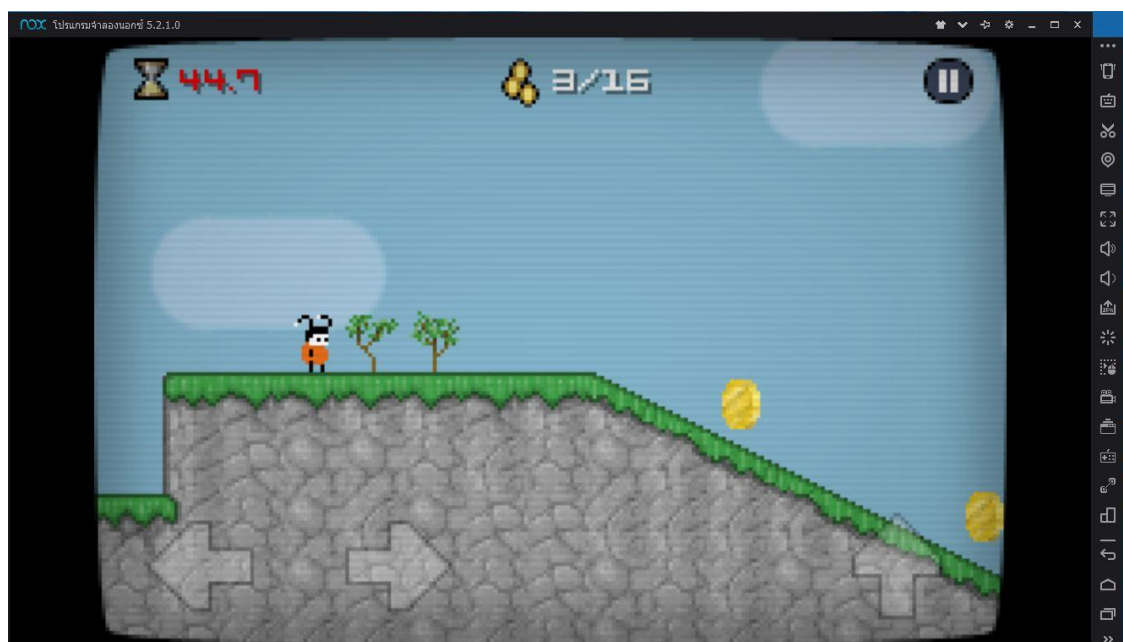
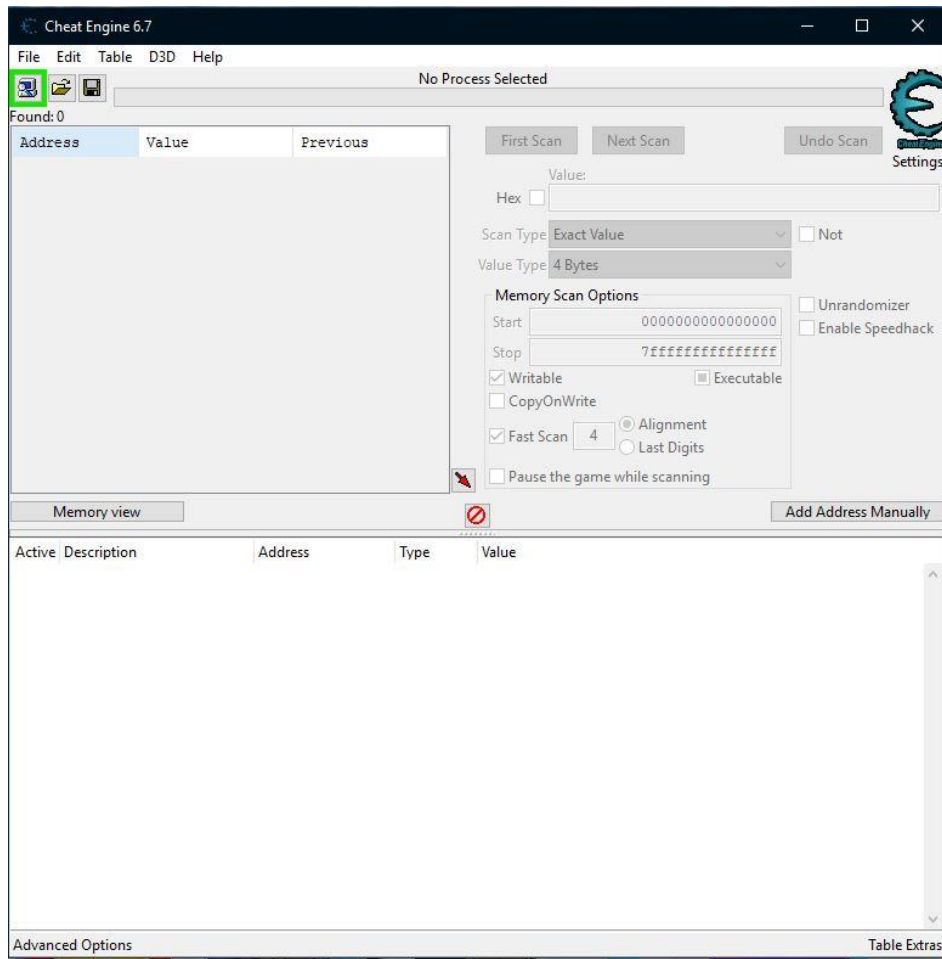
1. ทำการดาวน์โหลดโปรแกรม Cheat engine และ Nox ลงสู่คอมพิวเตอร์



2. ทำการเปิด Nox และดาวน์โหลดเกมส์ที่ต้องการจะใช้ในการทดลองในส่วนของการทดลองนี้จะเป็นเกมส์ Mos Speedrun

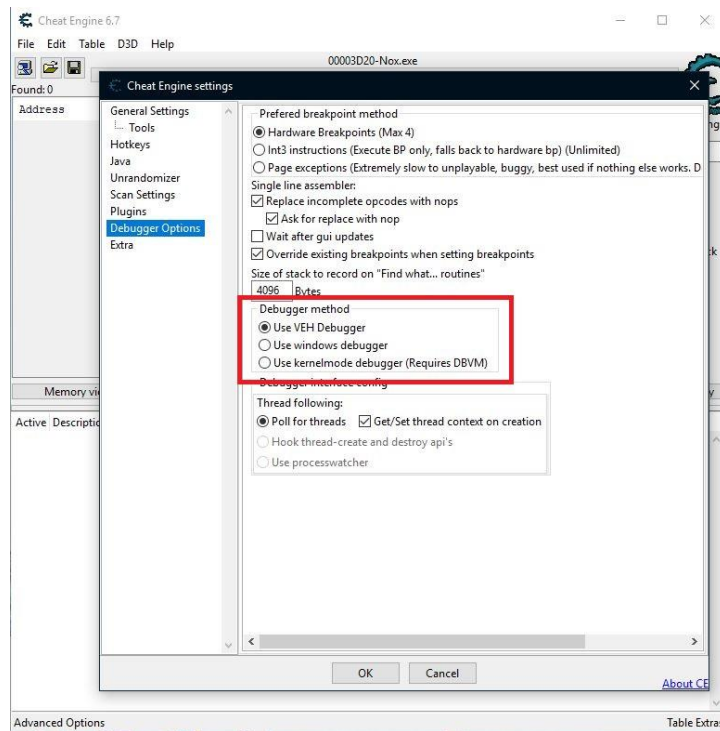


### 3. เปิด Cheat Engine และ เกมส์ขึ้นมา

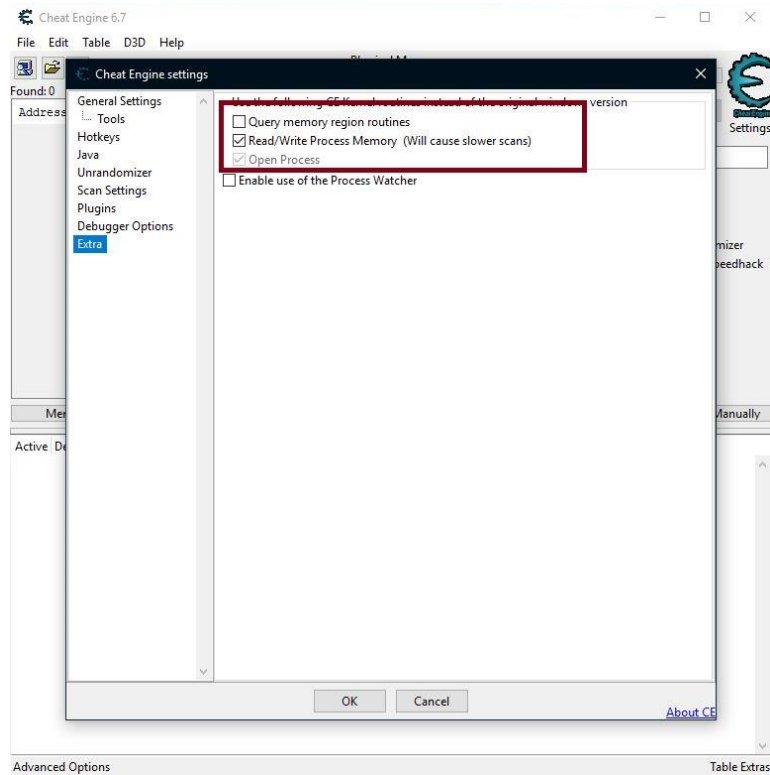


4. ทำการ set ค่าให้กับ cheat engine โดยการตรวจสอบดังนี้

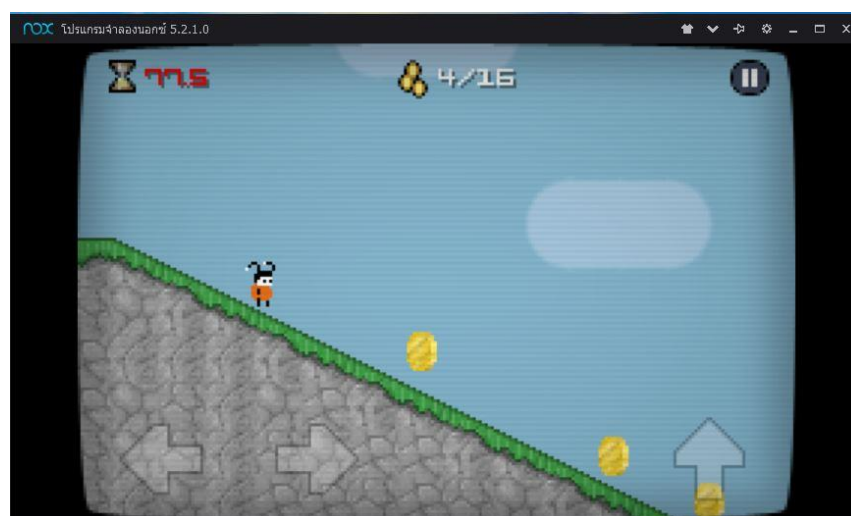
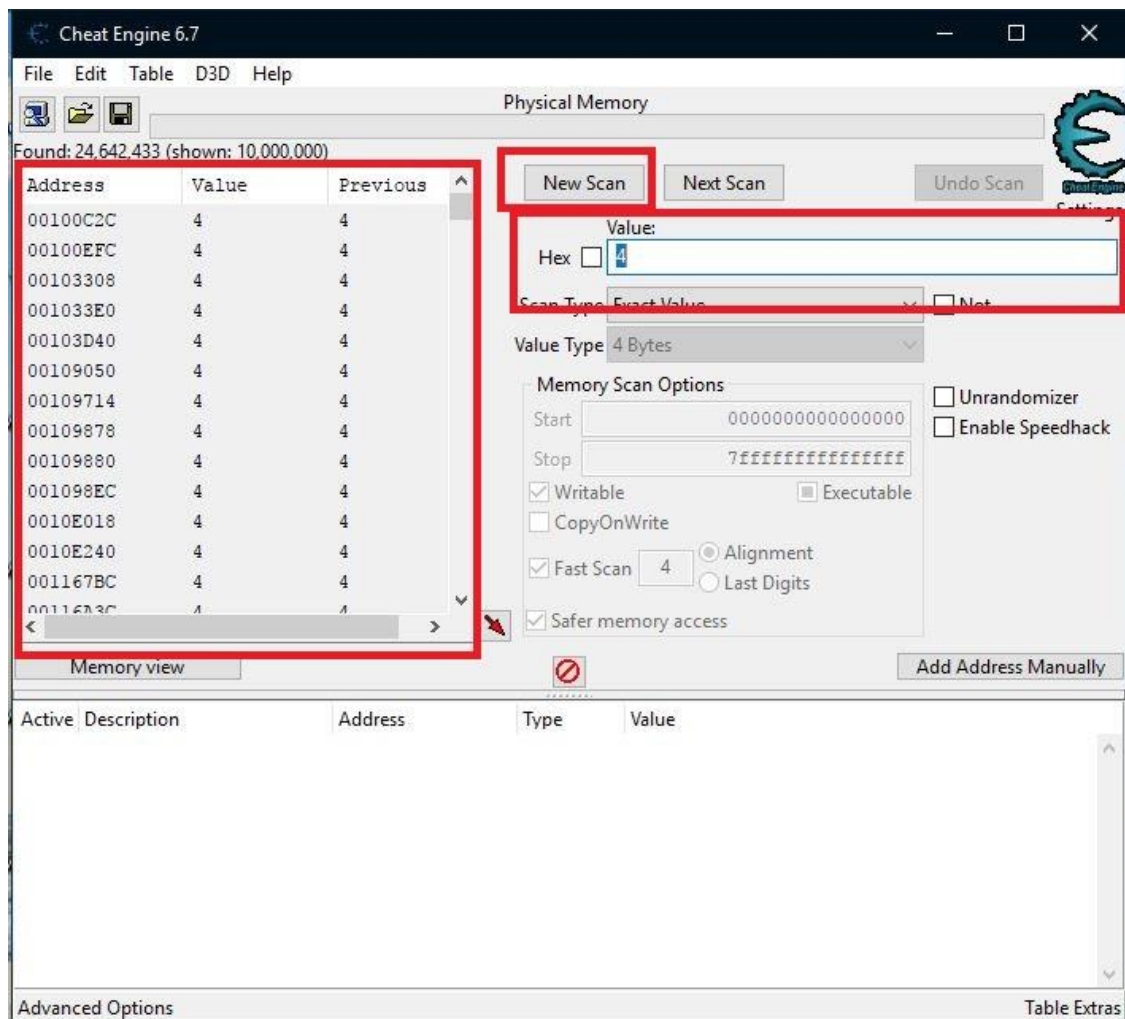
a. ทำการติ๊กถูกที่ช่อง Use VEH Debugger



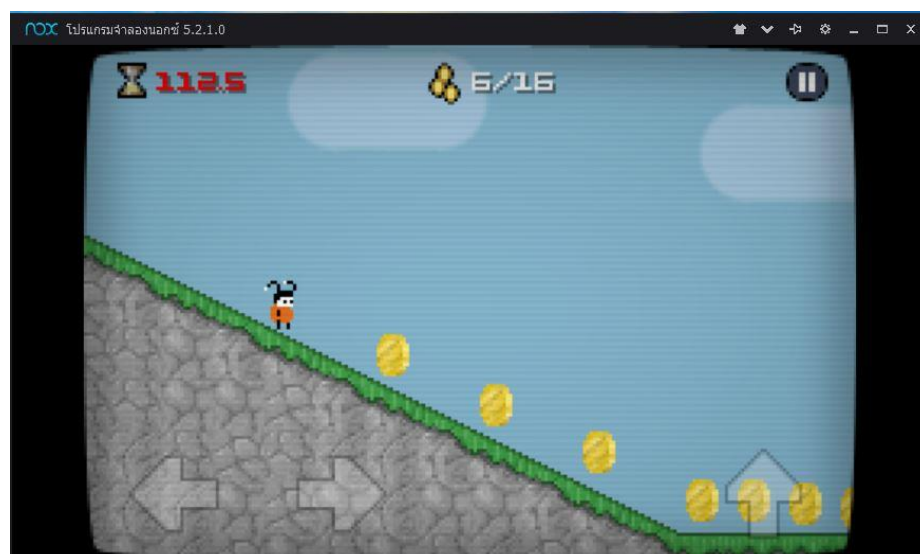
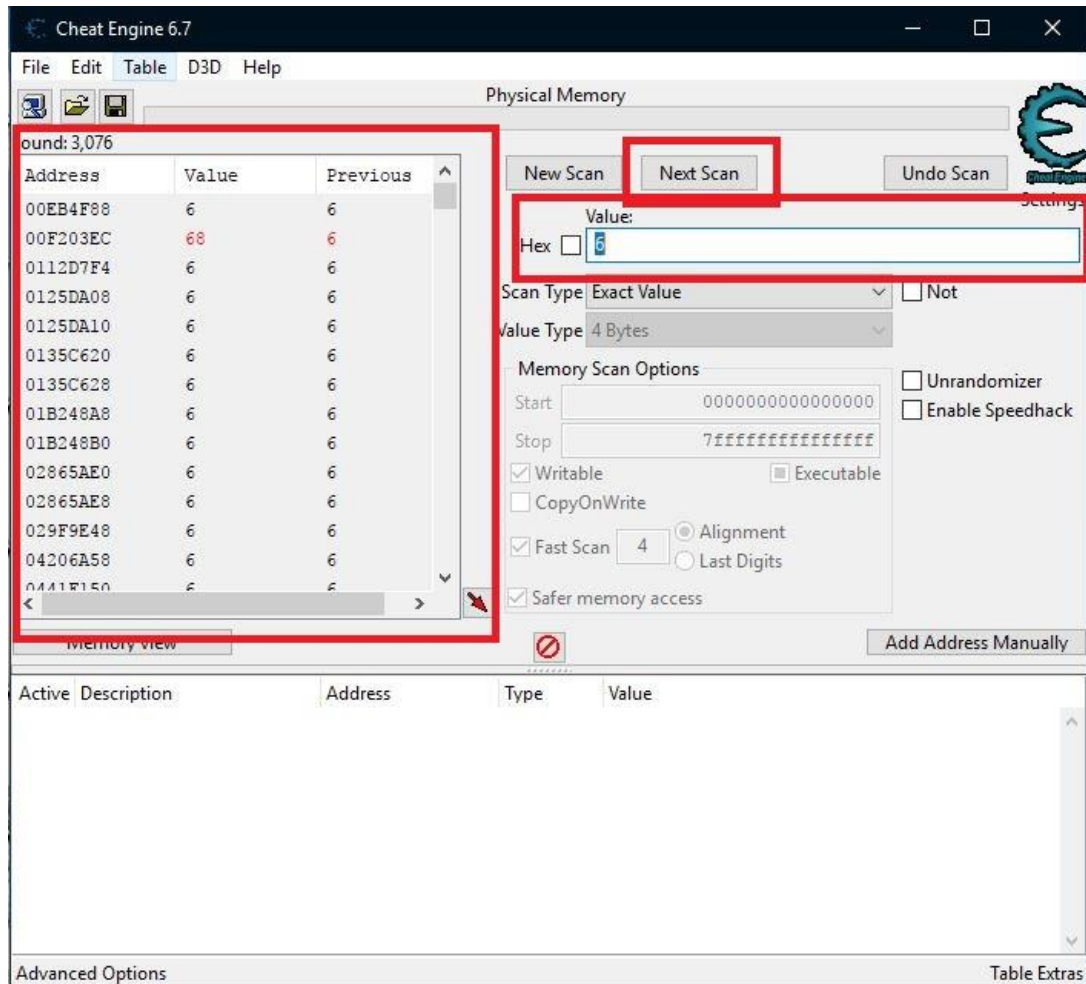
b. ติ๊กถูกที่ช่อง Read/Write Process Memory



5. เล่นเกมและเก็บแต้มเหรียญในเกม 4 เหรียญหรือเท่าใดก็ตามที่ท่านต้องการและทำการใส่ค่า 4 ลงไปในช่องของโปรแกรม Cheat Engine และกด New scan จะได้ค่าทางช่องทางซ้าย ดังรูป

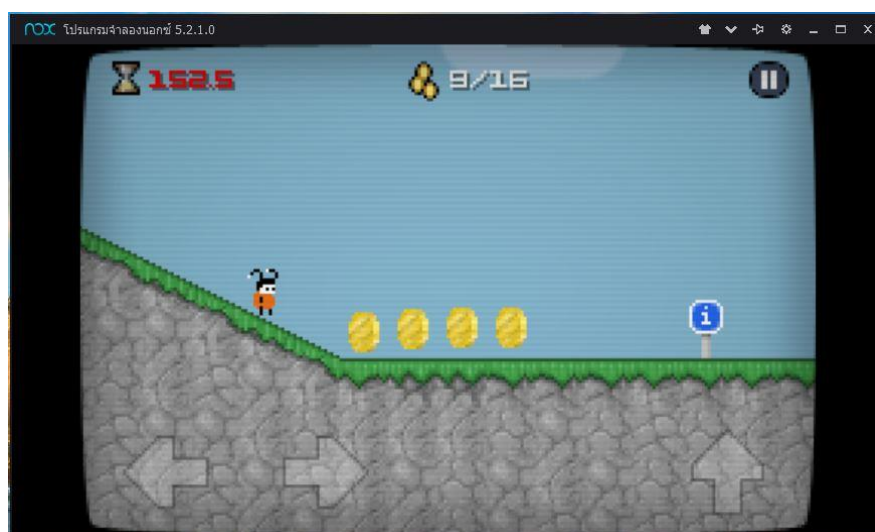
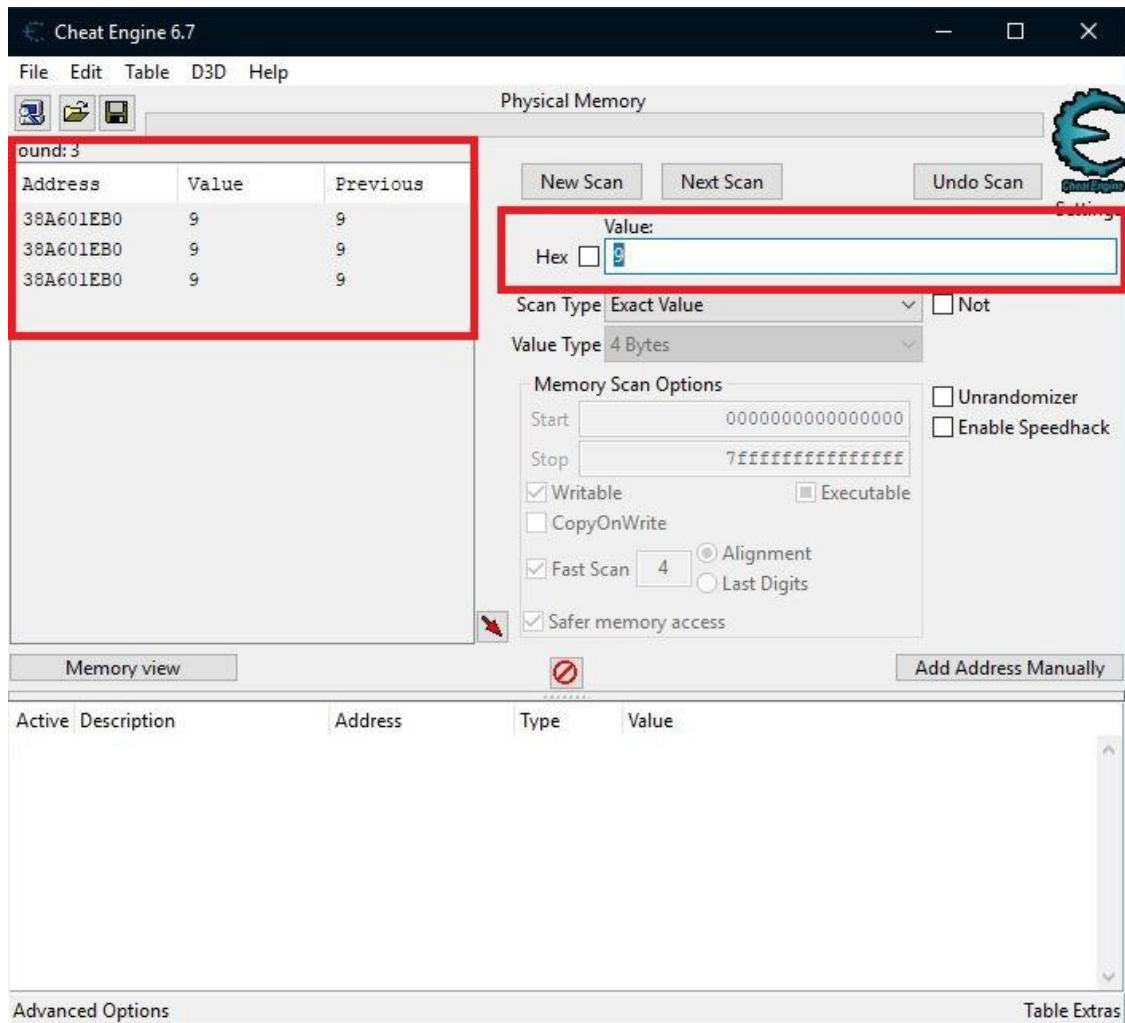


6. เนื่องจากค่าทางช่องทางซ้ายมีเยอะมากเกินไป เราจึงเปลี่ยนค่าโดยการเก็บเหรียญในเกมเพิ่ม และทำการเปลี่ยนค่าลงในโปรแกรมหลังจากนั้นให้กดปุ่ม Next Scan จะได้ค่าข้อมูลทางซ้ายที่น้อยลง ดังรูป

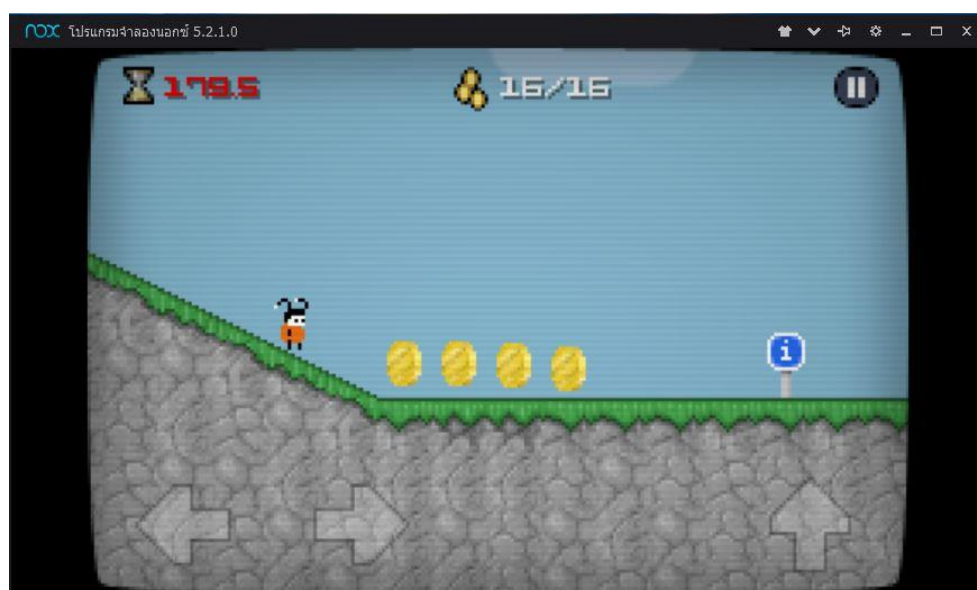
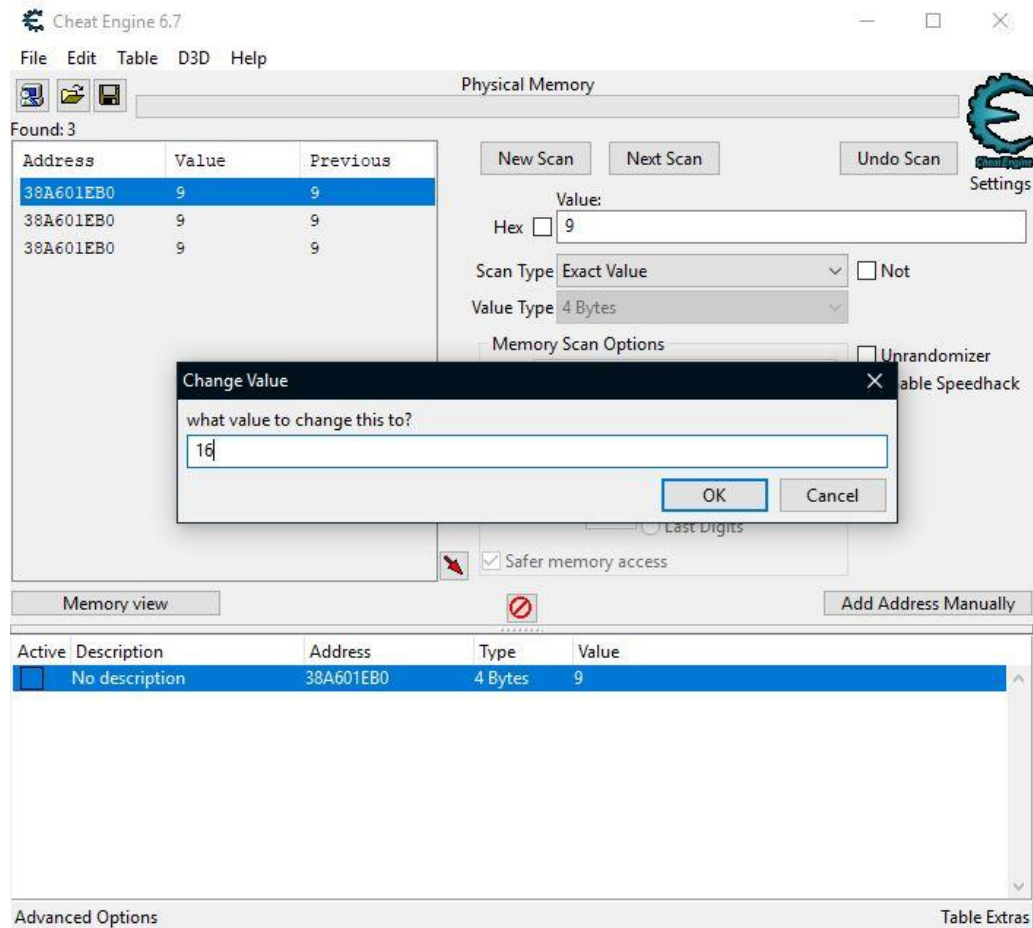




7. เนื่องจากยังมีค่ามากเกินไปทำตามข้อที่ 6 เข้าไปเรื่อยๆจนกว่าจะเจอชุดข้อมูลที่น้อยลง และ ค่า Address ชุดข้อมูลที่เหมือนกัน ( อาจจะมากกว่า 1 ชุดก็ได้แต่พยายามทำให้ Address ชุดข้อมูลเหมือนกันเยอะที่สุด ) สามารถดูได้ ดังรูป



8. ดับเบิลคลิกที่ช่อง Address ช่องใดช่องหนึ่ง ( ถ้ามีชุดข้อมูลที่ Address เหมือนกันมากกว่า 1 ชุดให้แก้ค่าทั้งหมดให้เหมือนกันทั้งหมด ) และทำการแก้ค่า Value ตามที่เราต้องการหลังจากนั้น ค่าเหรียญในเกมก็จะเปลี่ยนตามค่า Value ที่เราเขียนไว้นั่นเอง





### 3.สรุปผลการทดลอง

จากการทดลอง เราจะได้ทดลองในเรื่องของการ hack game เพื่อเข้าไปเปลี่ยนค่าต่างๆภายในเกมส์ จะสังเกตได้ว่า “ สามารถทำได้ “ แต่จากการทดลองนั้นจะทำได้เฉพาะเกมส์ที่มีความปลอดภัยต่ำเท่านั้น หรือเป็นเกมส์ออฟไลน์เท่านั้น เพราะ เกมส์พวกนี้จะเป็นเกมส์ที่เล่นเพียงคนเดียว ไม่ได้มีผลกระทบในส่วนของเซิร์ฟเวอร์เกมส์หรือระบบเกมส์นั่นเอง แต่การทำงานนั้นก็จะเป็นการหาค่า Address ที่ตรงกับค่า value ที่เราต้องการโดยการเลือกชุดข้อมูลที่เหมือนกันทั้งหมดและเปลี่ยนค่ามันให้เป็นไปตามที่ต้องการหลังจากนั้นค่าในเกมส์ก็จะเปลี่ยนไปตามค่าที่เราตั้งไว้นั่นเอง

เพราะฉะนั้นการทดลองนี้เป็นการทดลองในส่วนของ hack game โดยใช้ cheat engine พื้นฐานเท่านั้นโดยจะเป็นการ hack ค่าข้อมูลของภายในเกมส์เพื่อที่จะเปลี่ยนค่าไปเป็นค่าที่เราต้องการ

### 4.อ้างอิง

<http://proinw9.blogspot.com/2013/04/cheat-engine-62-edge-of-warriors.html>

<https://www.youtube.com/watch?v=Xo20nvppGm0>