ICT 2557/5

คู่มือการ Hack Windows Account โดยใช้ Hiren's boot

โดย

553020009-1 นางสาวเกษมศรี คงยิ่ง

553020304-9 นางสาวปิยะพร พะนะสิทธิ์

553020729-7 นางสาวจิฬาภัณฑ์ หอมจันทร์

553020731-0 นางสาวเจนจิรา เจิมขุนทด

553020733-6 นางสาวธนาพร จังหวัดสุข

553020746-7 นายวุฒิชัย โนนสาคู

อาจารย์ประจำรายวิชา : ผศ.ดร.จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา 322 376 Information And Communication Technology Security ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคเรียน 1 ปีการศึกษา 2557

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

มหาวิทยาลัยขอนแก่น

(เดือนตุลาคม พ.ศ. 2557)

โปรแกรมที่ใช้งาน

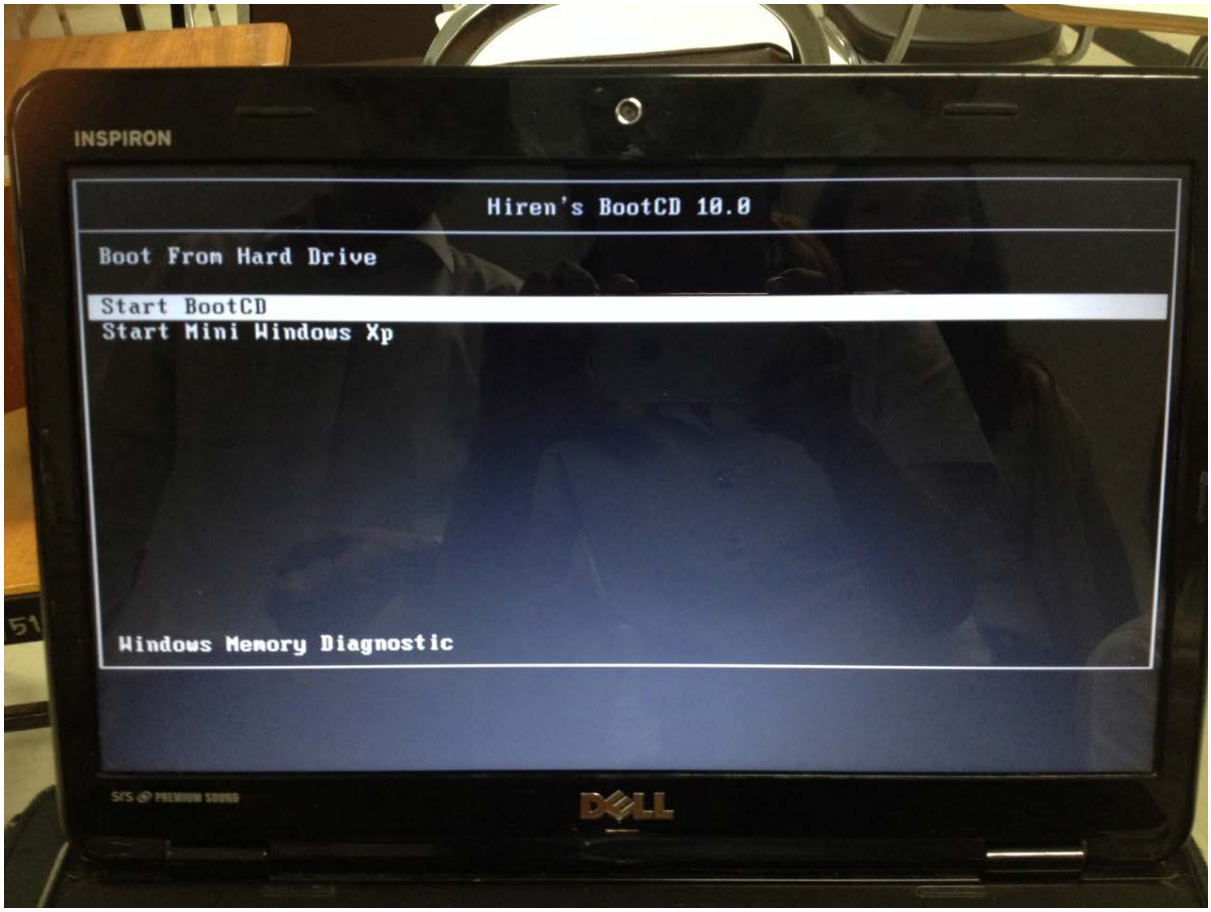
- Hiren’s boot Version 2008

อุปกรณ์ที่ใช้งาน

- เครื่องคอมพิวเตอร์ PC หรือ Notebook ที่สามารถใช้งานแผ่น CD และ USB ได้

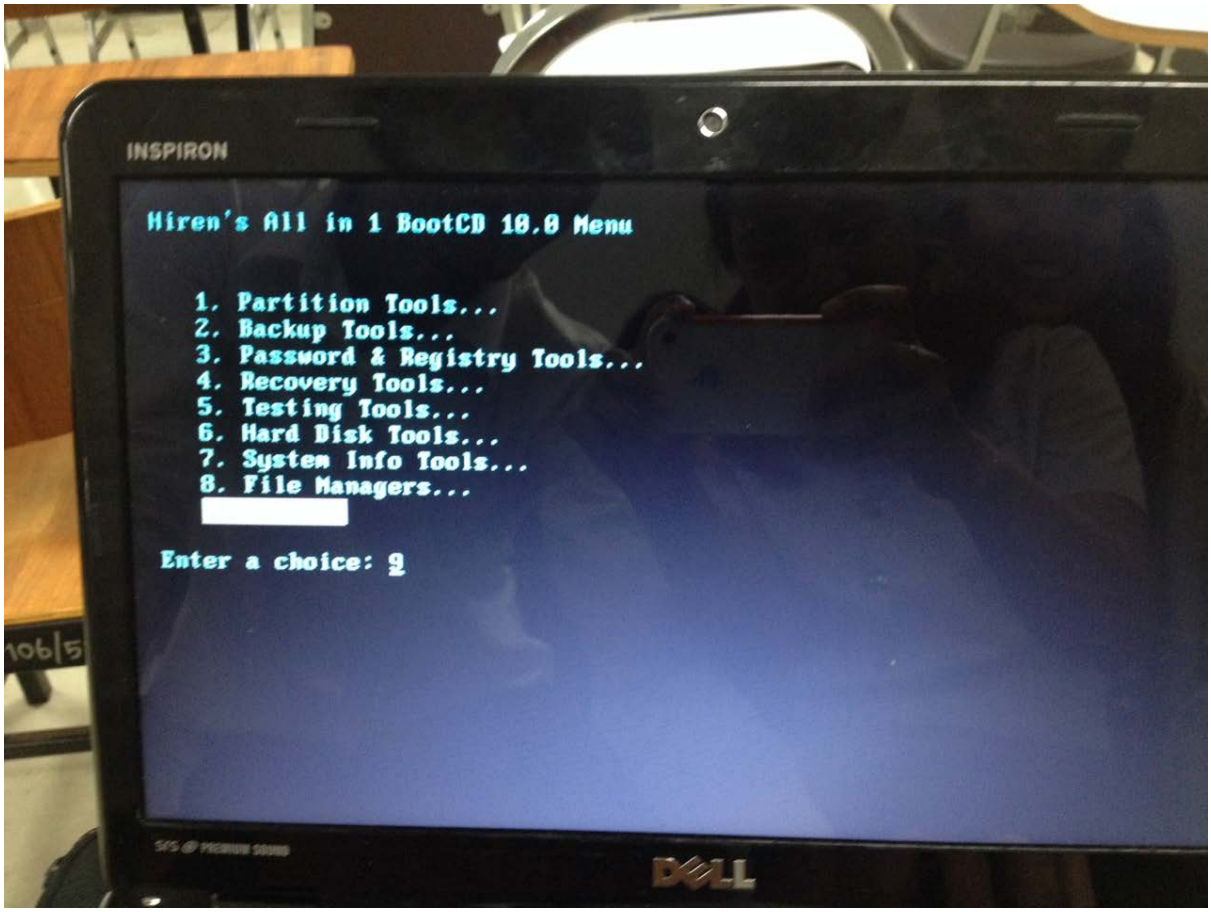
ขั้นตอนการใช้งาน Hiren’s boot

ขั้นตอนที่ 1 ใส่แผ่น Hiren’s boot ที่ไดร์ฟ CD หลังจากนั้นเริ่มต้นการทำงานโดย ก่อนที่เครื่องจะทำการ Start Windows ให้กดปุ่ม F12 บนแป้นพิมพ์ (เครื่องคอมพิวเตอร์บางเครื่องอาจจะเป็นปุ่มอื่นบนแป้นพิมพ์) เพื่อทำการ Boot Setup หลังจากนั้นจะปรากฏหน้าจอดังรูปที่ 1 ให้กดเลือก Start Boot CD



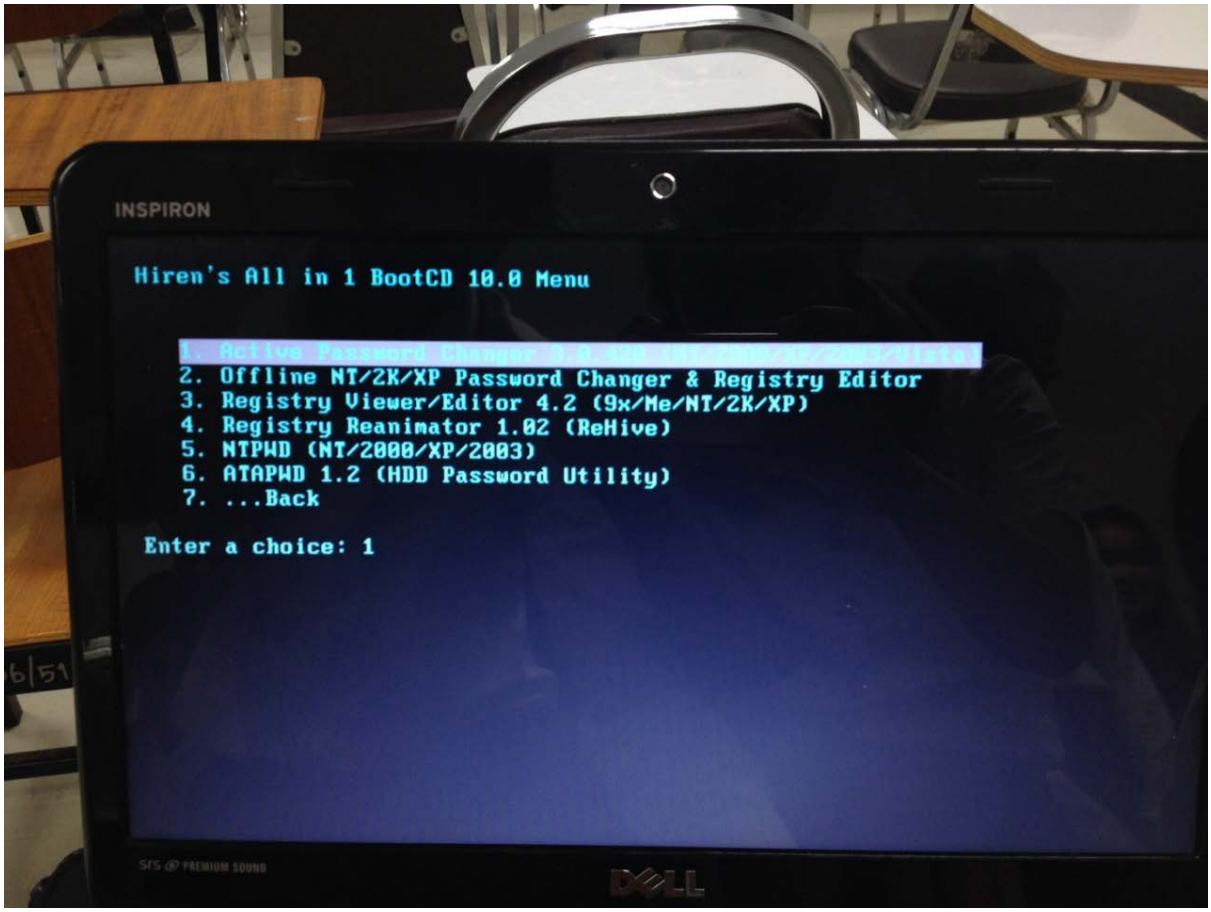
รูปที่ 1 การเริ่มต้น Start Boot CD

ขั้นตอนที่ 2 หลังจากที่กดเลือกปุ่ม Start Boot CD แล้ว จะปรากฏหน้าต่างดังรูปที่ 2 ให้เราเลือกหมวดหมู่ของ Tools ที่จะใช้งาน ให้กดเลือกข้อที่ 3 Password & Registry Tools โดยการพิมพ์เลขบนแป้นพิมพ์ได้เลย หลังจากนั้นก็กดปุ่ม Enter



รูปที่ 2 การเลือกหมวดหมู่ของ Tools ที่ต้องการจะใช้งาน

ขั้นตอนที่ 3 หลังจากที่กดเลือกปุ่ม 3 Password & Registry Tools แล้ว จะปรากฏหน้าต่างดังรูปที่ 3 ให้เราเลือกใช้เครื่องมือ(Tools) ในการทำงาน ให้กดเลือกข้อที่ 1 Active Password Changer โดยการพิมพ์เลขบนแป้นพิมพ์ได้เลย หลังจากนั้นก็กดปุ่ม Enter



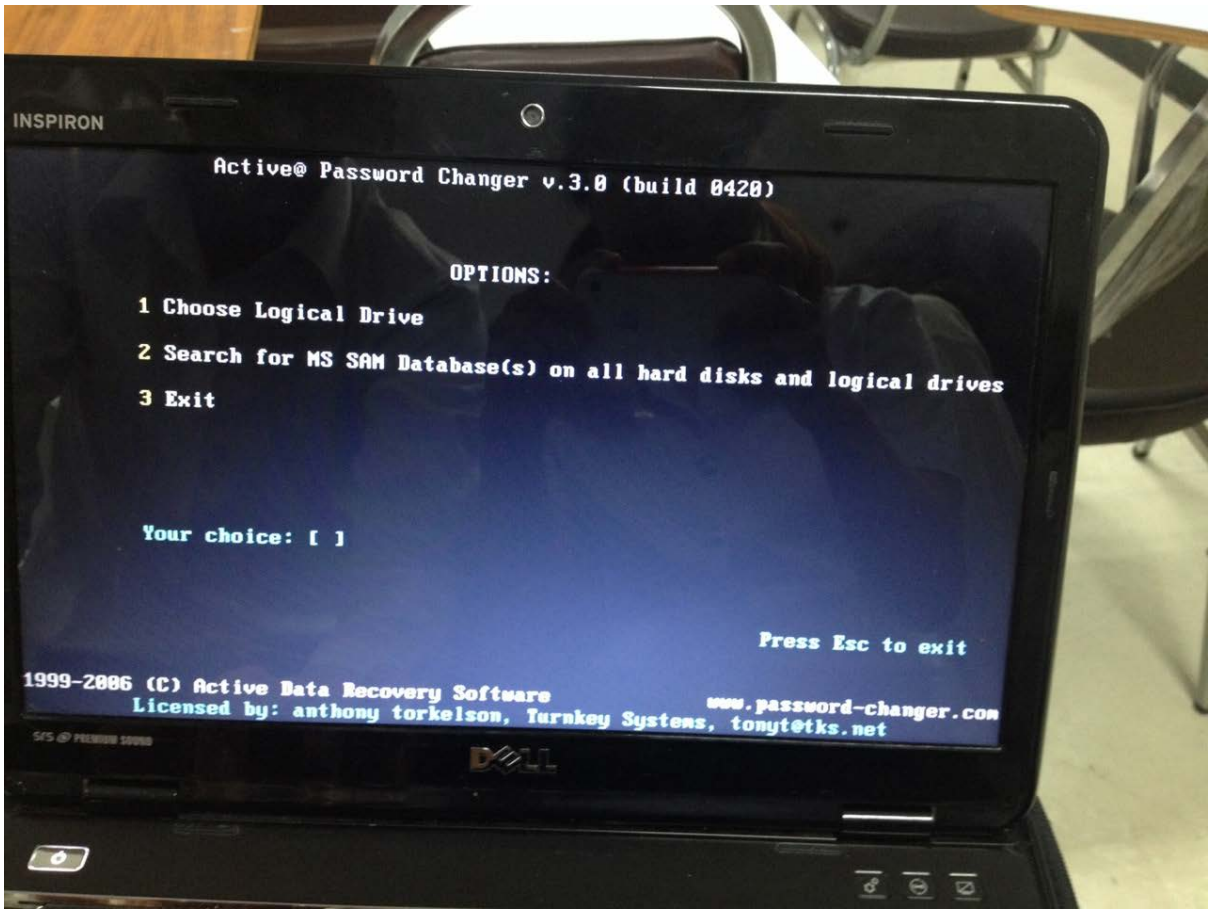
รูปที่ 3 การเลือก Tools ที่ต้องการใช้งาน

ขั้นตอนที่ 4 แสดงเมนูของ Tools ดังรูปที่ 4 โดยมีรายละเอียดดังนี้

ตัวเลือกที่ 1 Choose Logical Drive กรณีที่เราทราบว่า Windows ถูกติดตั้งที่ไดร์ฟใด

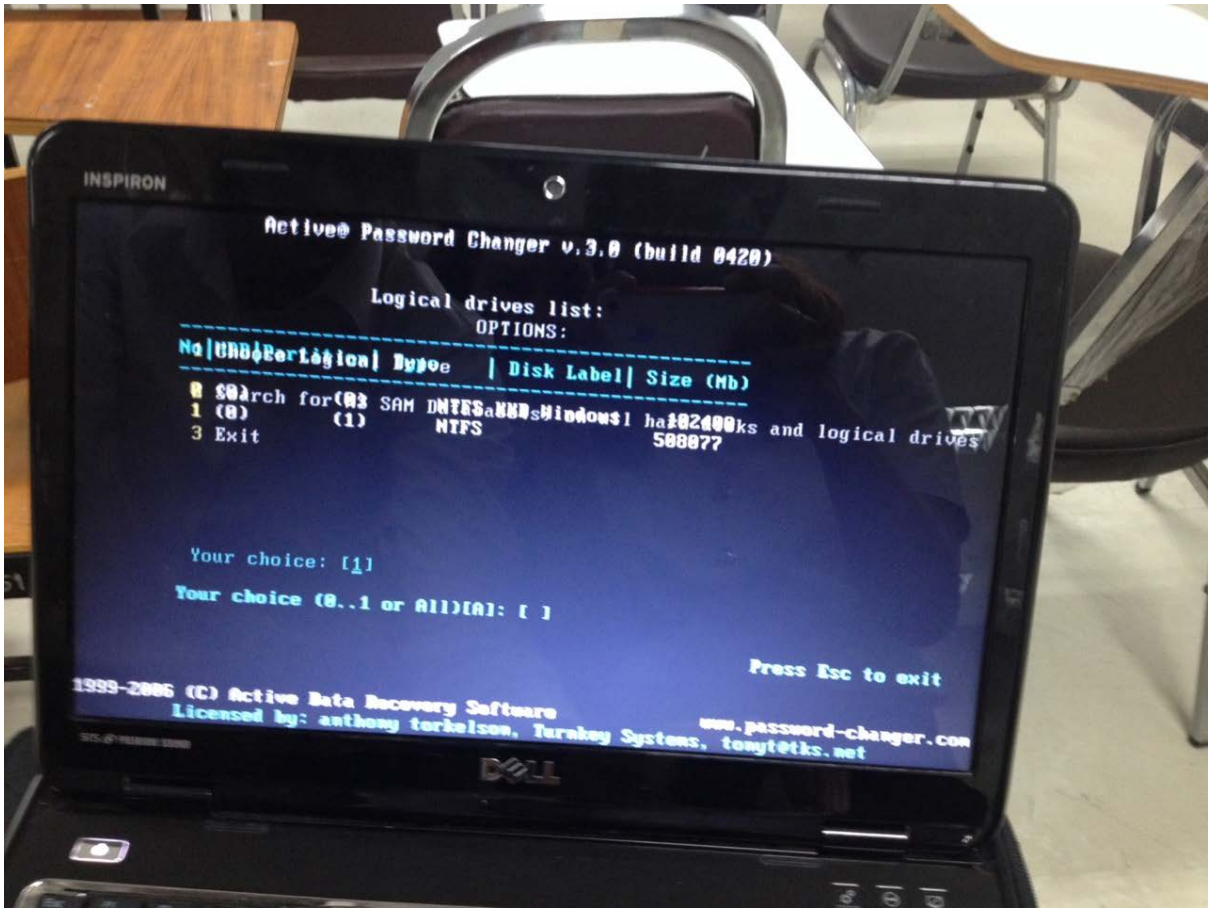
ตัวเลือกที่ 2 Search for MS SAM Database(s) on all… เป็นการค้นหาไฟล์ที่เก็บ Password ของ Windows ในทุกๆไดร์ฟ

สำหรับการทดสอบนี้ให้เลือกตัวเลือกที่ 1 เพราะเราทราบว่า Windows ถูกติดตั้งอยู่ที่ไดร์ฟใดซึ่งจะประหยัดเวลาในการค้นหามากกว่าตัวเลือกที่ 2 โดยการพิมพ์เลขบนแป้นพิมพ์ได้เลย หลังจากนั้นก็กดปุ่ม Enter



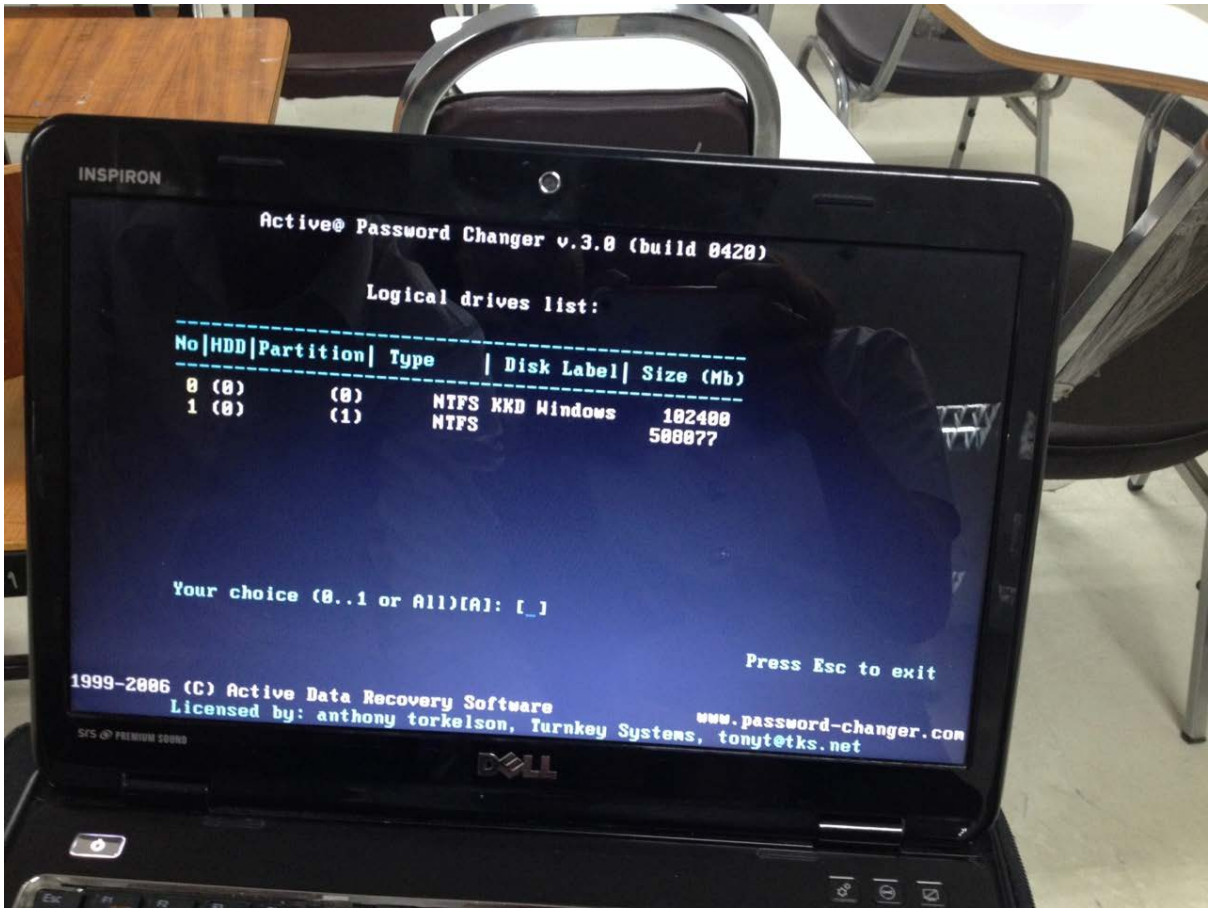
รูปที่ 4 การแสดงเมนูของ Tools

ขั้นตอนที่ 5 เข้าสู่หน้าจอเลือกไดร์ฟที่ติดตั้ง Windows โดยสังเกตที่ Type ที่เป็น SAM กรณีคือหมายเลข 0 โดยการพิมพ์เลขบนแป้นพิมพ์ได้เลย หลังจากนั้นก็กดปุ่ม Enter



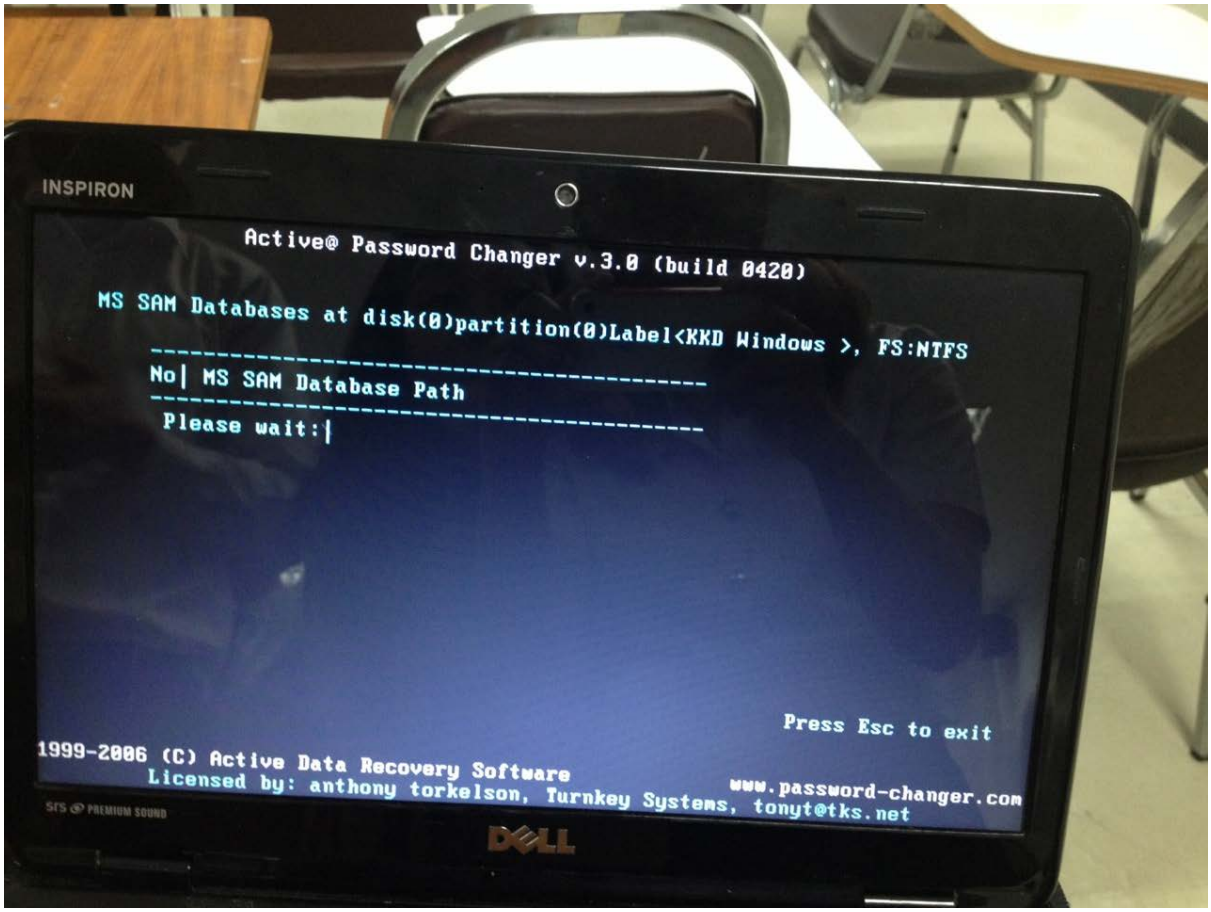
รูปที่ 5 การเลือกไดร์ฟ

ขั้นตอนที่ 6 เข้าสู่หน้าจอเลือก Partition ที่ติดตั้ง Windows โดยสังเกตที่ Disk Label ที่เป็น KKD Windows กรณีคือหมายเลข 0 โดยการพิมพ์เลขบนแป้นพิมพ์ได้เลย หลังจากนั้นก็กดปุ่ม Enter



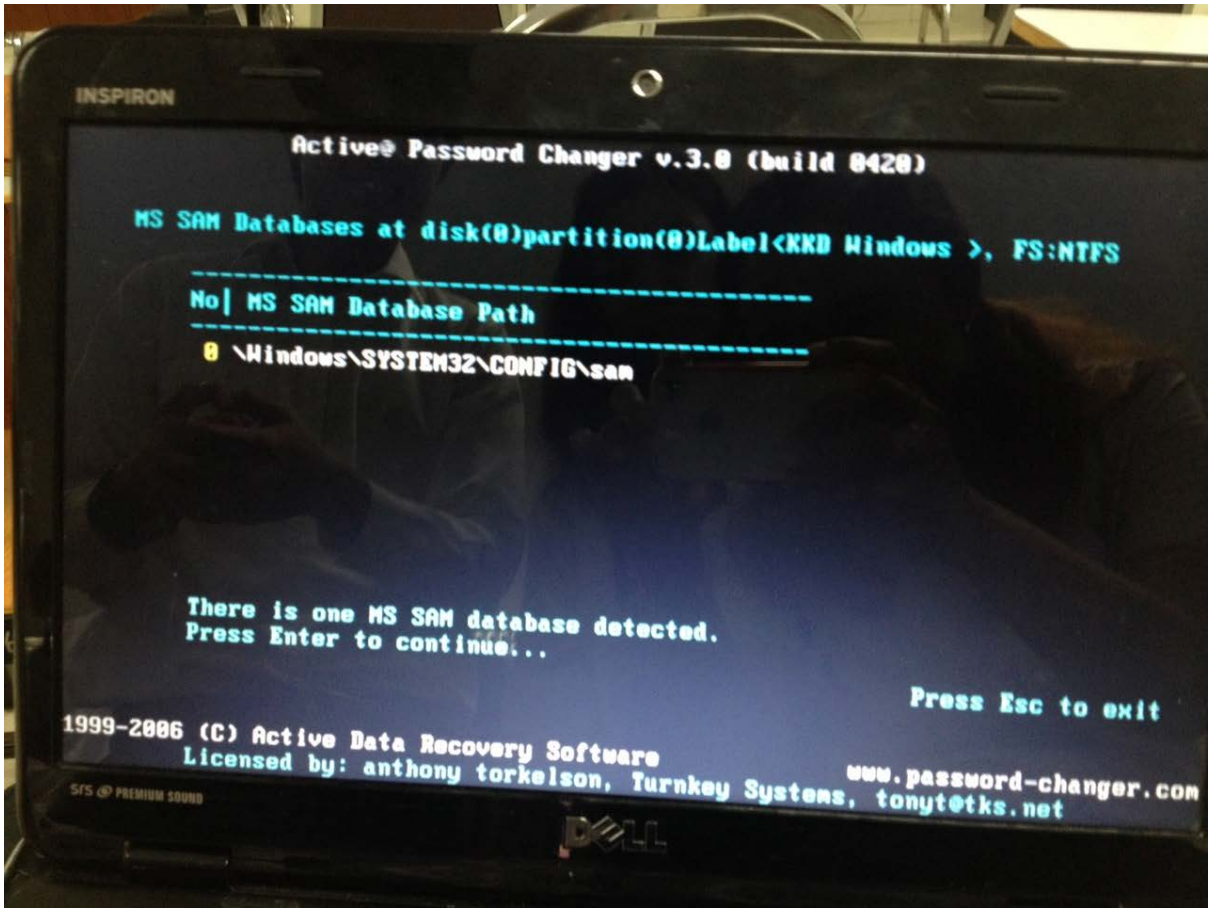
รูปที่ 6 การเลือก Partition

ขั้นตอนที่ 7 เป็นหน้าที่แสดงว่าระบบกำลังค้นหาไฟล์ Password อยู่ อาจใช้เวลาสักพักประมาณ 3-5 นาที ขึ้นอยู่กับความเร็วของคอมพิวเตอร์ (เช่น ความเร็วของ CPU หรือ ความเร็วของ Hard disk)



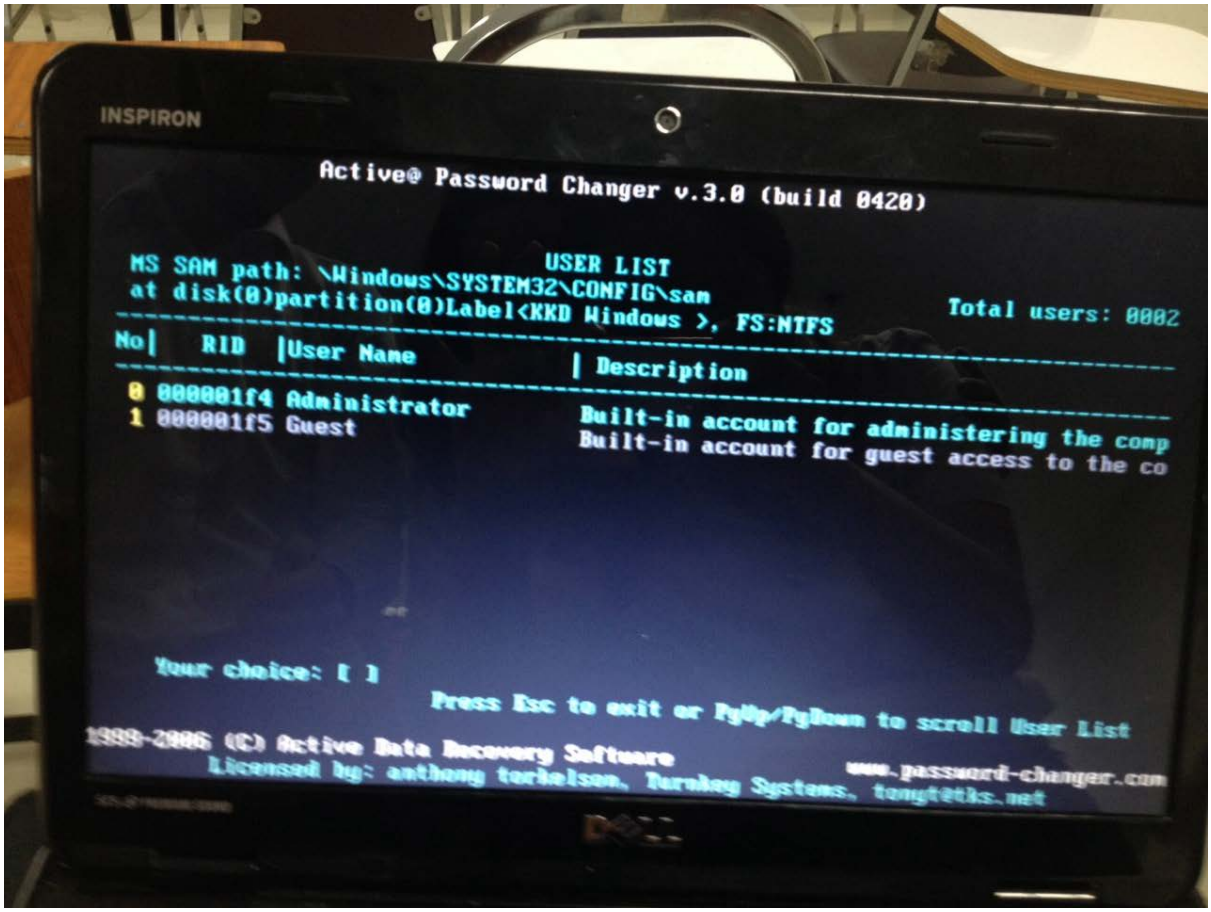
รูปที่ 7 การแสดงว่าระบบกำลังค้นหาไฟล์

ขั้นตอนที่ 8 แสดงผลการค้นหาว่าระบบได้ค้นหา Password พบแล้ว



รูปที่ 8 การแสดงผลการค้นหา

ขั้นตอนที่ 9 แสดงรายชื่อ User ของ Windows โดยเราสามารถเลือกที่จะดำเนินการกับบางบัญชีในแต่ละ Account ได้ ในกรณีนี้คือบัญชี Administrator หมายเลข 0 โดยการพิมพ์เลขบนแป้นพิมพ์ได้เลย หลังจากนั้นก็กดปุ่ม Enter

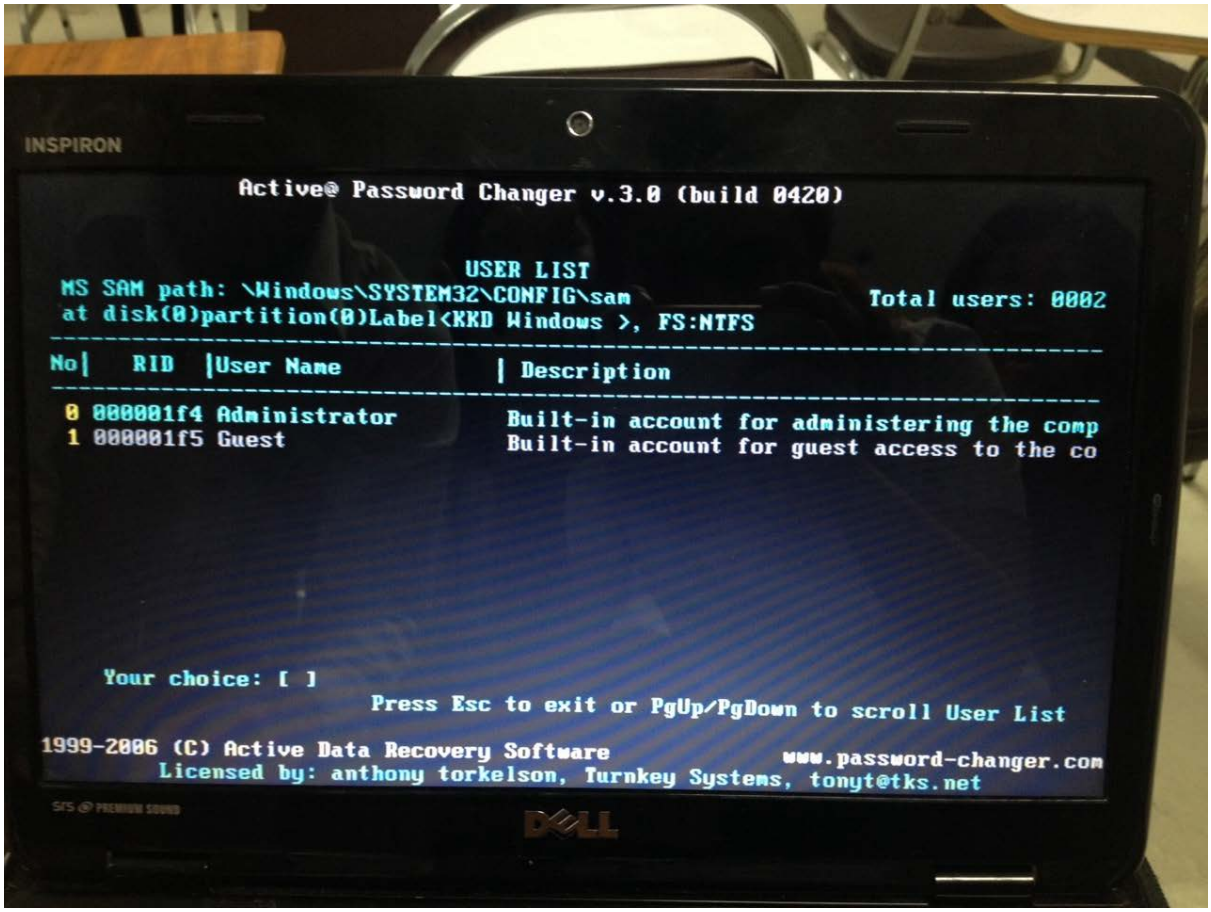


รูปที่ 9 การเลือกที่จะดำเนินการกับบางบัญชีในแต่ละ Account

ขั้นตอนที่ 10 เป็นหน้าที่แสดงรายละเอียดหรือยืนยันการดำเนินรายการโดยการพิมพ์ Y บนแป้นพิมพ์ได้เลย หลังจากนั้นก็กดปุ่ม Enter

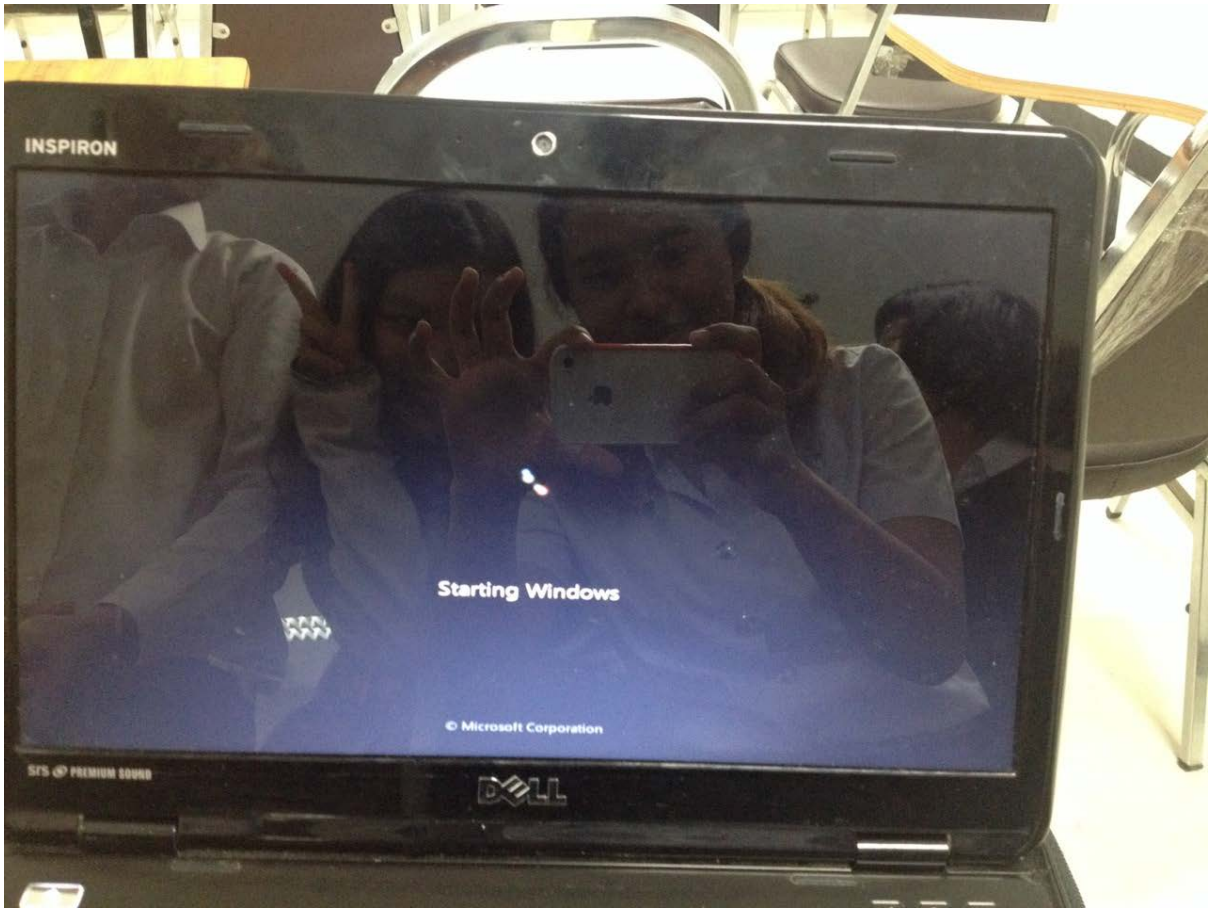
รูปที่ 10 การแสดงรายละเอียดหรือยืนยันการดำเนินรายการ

ขั้นตอนที่ 11 เมื่อระบบได้ทำการลบ Password จากขั้นตอนที่แล้ว ก็จะกลับมาหน้าจอเลือก User อื่นๆที่ต้องการจะลบ Password ในกรณีเราทำแค่บัญชี Administrator แต่ถ้าหากต้องการเลือกลบ Password จากบัญชีอื่นๆก็สามารถทำได้จากขั้นตอนที่ 9 ถึงขั้นตอนที่ 11 เมื่อเสร็จสิ้นขั้นตอนทุกอย่างแล้วให้กด Ctrl+Alt+Delete เพื่อทำการ Reboot เครื่องใหม่



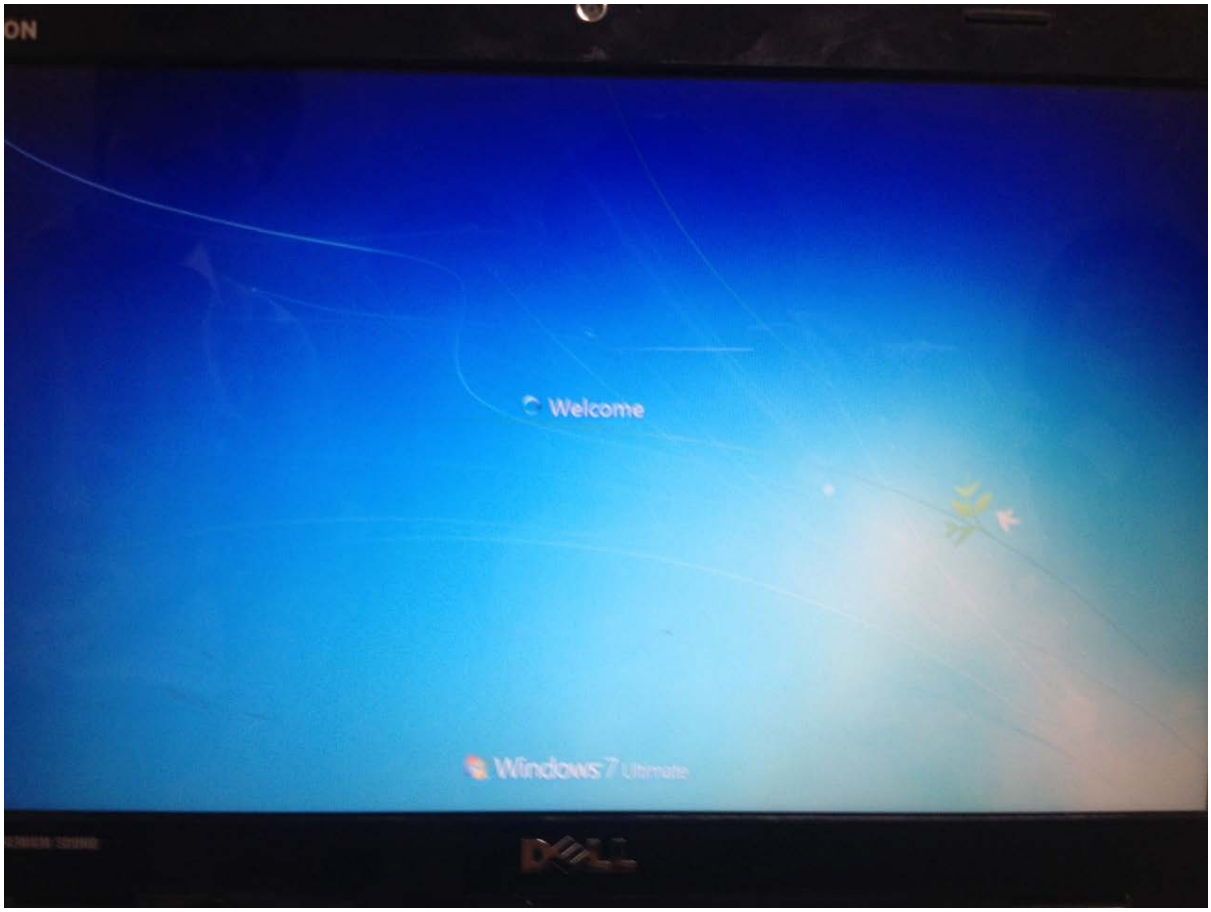
รูปที่ 11 ต้องการเลือกลบ Password จากบัญชีอื่นๆ

ขั้นตอนที่ 12 หลังจากที่ได้ Reboot เครื่องแล้วจะแสดงหน้าการ Start Windows ขึ้นมาใหม่



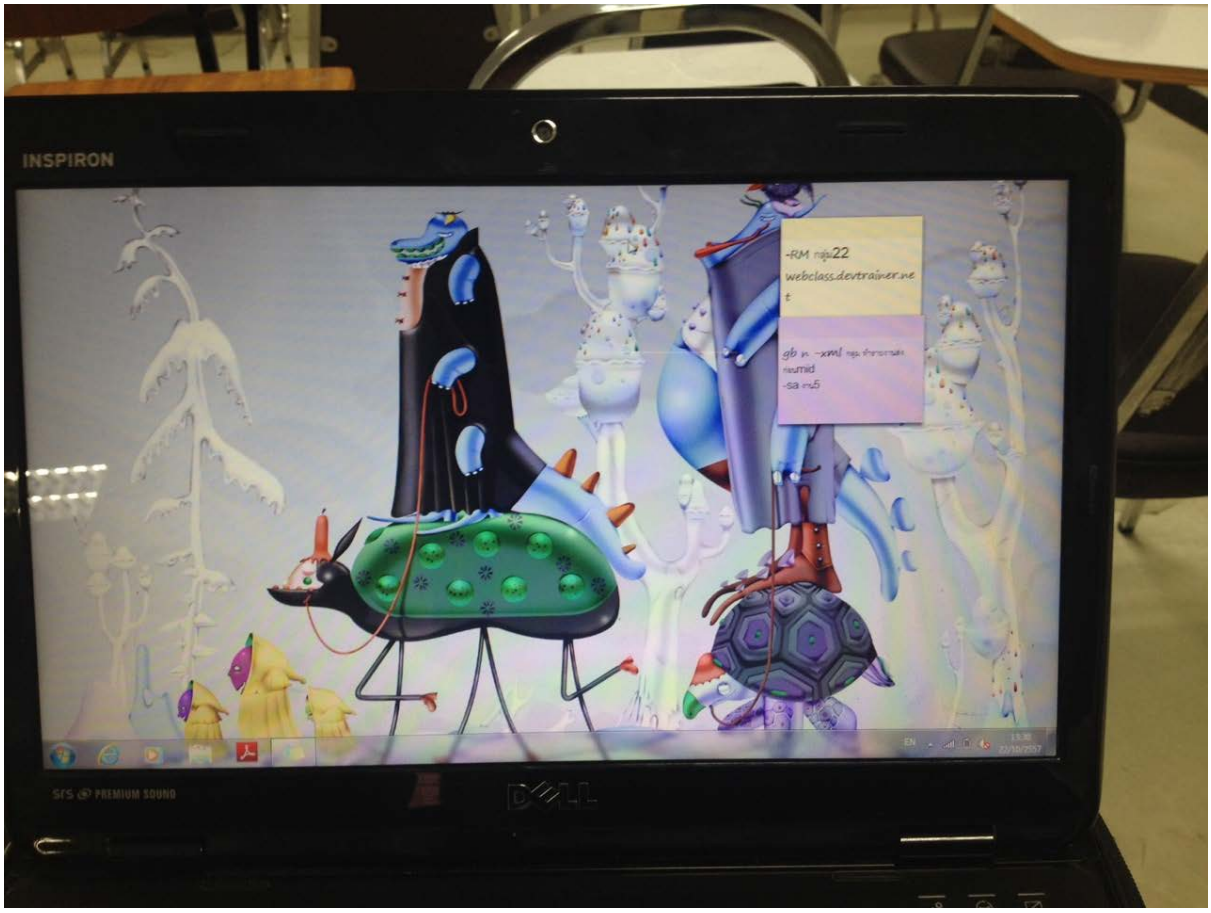
รูปที่ 12 การแสดงหน้าการ Start Windows ขึ้นมาใหม่

ขั้นตอนที่ 13 การเข้าสู่หน้าใช้งานคอมพิวเตอร์



รูปที่ 13 การแสดงการเข้าสู่หน้าใช้งานคอมพิวเตอร์

ขั้นตอนที่ 14 เริ่มต้นการใช้งานเครื่องคอมพิวเตอร์ได้ปกติ และการใช้งานในครั้งต่อไปไม่ต้องกรอก Password อีกเลย นอกจากนี้แล้วเรายังสามารถตั้งรหัสผ่านใหม่ได้อย่างสบายใจ



รูปที่ 14 การเริ่มต้นใช้งานเครื่องคอมพิวเตอร์