



## รายงาน

### โปรแกรม Ophcrack

โดย

กลุ่มที่ 4

563020473-7	นางสาวจุฑาชนม์	บุษบงก์
563020956-7	นายเกียรติประวัติ	น้อยฟุ้ง
563020960-6	นายณัฐกิตต์	บุญเรือง
563020962-2	นายณัฐวุฒิ	อินทา
563020968-0	นางสาวพุทธชาติ	คำวงษา
563020972-8	นายสรวิษฐ์	โคตรนรินทร์

อาจารย์ที่ปรึกษา : ดร.จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของการศึกษารายวิชา 322 376  
Information and Communication Technology Security  
ภาคเรียน 1 ปีการศึกษา 2558  
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์  
มหาวิทยาลัยขอนแก่น

## โปรแกรม OPHCRACK LiveCD

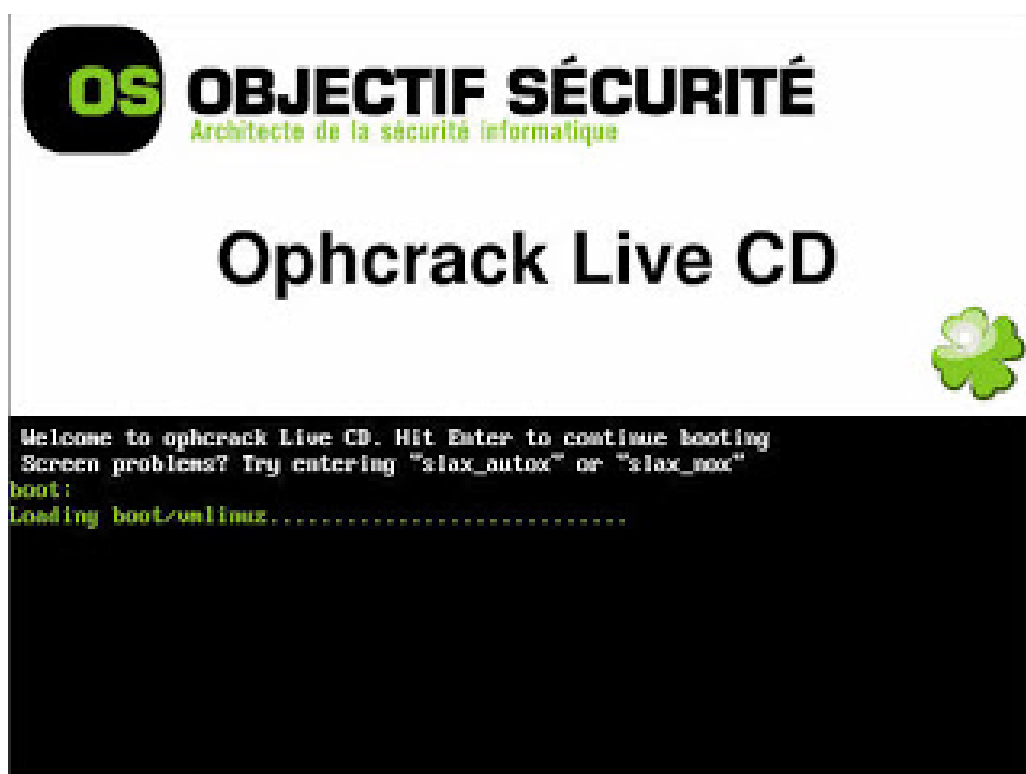
โปรแกรม OPHCRACK LiveCD เป็นเครื่องมือฟรีแวร์สำหรับการตรวจสอบรหัสผ่านผู้ดูแลระบบและผู้ใช้บนระบบปฏิบัติการ Windows ซึ่งก็สามารถรันจากแผ่นซีดีได้เลยโดยไม่ต้องทำการติดตั้งลงเครื่อง สำหรับวิธีการใช้งานก็ไม่ยุ่งยาก การทำงานค่อนข้างเร็วโดยใช้เวลาไม่นานก็สามารถถอดรหัสได้

### วิธีป้องกัน

1. ตั้ง Password ไม่น้อยกว่า 8 ตัวอักษร
2. ใช้อักขระ ตัวพิมพ์ใหญ่ พิมพ์เล็ก สลับกันไป
3. ล็อค Bios ด้วยเลย

### วิธีการใช้งาน OPHCRACK LiveCD

1. ทำการดาวน์โหลดดิมเมจ OPHCRACK LiveCD แล้วเบิร์นลง CD
2. ทำการบูตระบบด้วย CD ที่ทำในขั้นตอนที่ 1 ลักษณะหน้าจอของการบูต OPHCRACK LiveCD

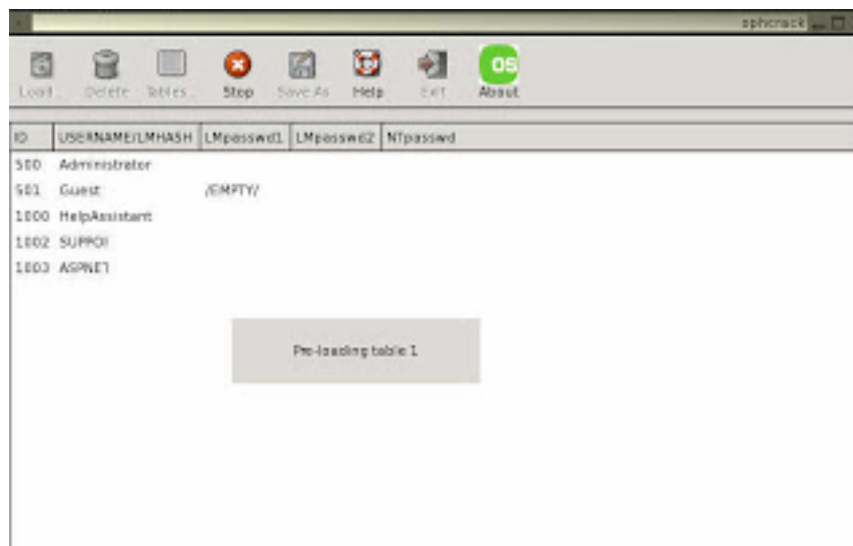


รูปที่ 1 OPHCRACK Live CD

3. หากเครื่องคอมพิวเตอร์ที่ทำการบูตนั้นมีหลายพาร์ติชัน OPHCRACK LiveCD จะให้เลือกว่าจะต้องการพาร์ติชันไหน ก็ให้ทำการเลือกพาร์ติชันที่ต้องการ จากนั้น OPHCRACK LiveCD ก็จะทำการโหลดหน้า Dumping hashes ดังรูปที่ 2 แล้วทำการถอดรหัสผ่านของ account ที่พบในไฟล์ SAM ลักษณะการทำงานจะเป็นดังรูปที่ 3

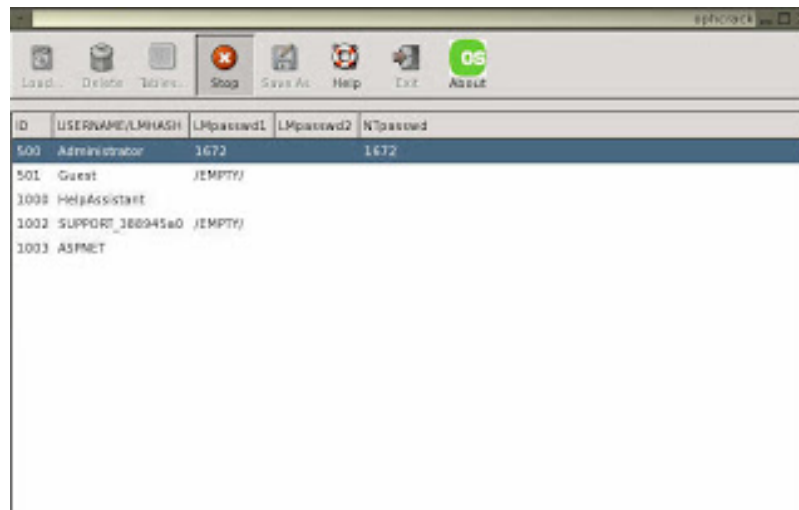


รูปที่ 2 Dumping hashes



รูปที่ 3 Starting Ophcrack

4. เมื่อถอดรหัสผ่านของ account ได้แล้วก็จะแสดงให้เห็นดังรูปที่ 4 โดยเวลาที่ใช้นั้นก็ขึ้นอยู่กับว่ารหัสผ่านที่ตั้งนั้น มีความซับซ้อนมากน้อยแค่ไหน สำหรับการทดสอบนี้ใช้เวลาประมาณไม่ถึง 5 นาที นับตั้งแต่บูตเครื่องด้วย OPHCRACK LiveCD จนถึงการถอดรหัสผ่านของ Administrator ได้ (ในการทดสอบนี้ ได้ทำการตั้งรหัสผ่านเป็นแบบอย่างง่าย เพื่อใช้ในการแสดงให้เห็นการทำงานของโปรแกรมเท่านั้น ไม่แนะนำให้ท่านตั้งรหัสผ่านตามตัวอย่างนี้)



The screenshot shows the OPHCRACK LiveCD interface. At the top, there is a menu bar with options: Load..., Delete, Titles..., Stop, Save As, Help, Exit, and About. Below the menu bar is a table with the following data:

ID	USERNAME/LMHASH	LMpassword1	LMpassword2	NTpassword
500	Administrator	1672		1672
501	Guest	(EMPTY)		
1008	HelpAssistant			
1002	SUPPORT_386945a0	(EMPTY)		
1003	ASPNET			

รูปที่ 4 Password cracked

5. จากนั้นก็ให้ทำการบูตระบบตามปกติ แล้วใช้รหัสผ่านที่ได้ในขั้นตอนที่ 4 ในการล็อกออนเข้าระบบวินโดวส์ (ในการใช้งานจริงนั้น ขอแนะนำให้ทำการเปลี่ยนรหัสผ่านทันทีเมื่อทำการล็อกออนเข้าระบบได้สำเร็จ)

### ข้อดี


- รหัสผ่านของผู้ดูแลระบบจะไม่ถูกเปลี่ยนแปลง
- สามารถใช้งานได้โดยไม่ต้องติดตั้งลงเครื่อง
- สามารถใช้งานได้ฟรี

### ข้อเสีย

- หากมีการตั้งรหัสผ่านของผู้ดูแลระบบแบบซับซ้อนมากๆ อาจใช้เวลาในการถอดรหัสนานมาก

โปรแกรม Ophcrack สามารถถอดรหัสได้แค่ 4 ตัวเท่านั้น จึงมีการโหลด Rainbow tables มาเป็นตัวช่วยในการถอดรหัสได้มากกว่า 4 ตัว ซึ่งตัวที่เราใช้คือ XP free fast (703MB)


Rainbow tables มีให้เลือกดาวน์โหลดหลายตัวตามความต้องการในการใช้งาน มีทั้งแบบฟรีและเสียค่าใช้จ่าย

 **XP free fast (703MB)**  
formerly known as SSTIC04-5k


Success rate: 99.9%  
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ  
md5sum: f6f5536975b57c891ed5f2de702a02bd

- ความยาวรหัส 8 ตัว , ถอดรหัสที่เป็นตัวเลข ภาษาอังกฤษพิมพ์เล็ก-ใหญ่ได้ (เราใช้ตัวนี้)


Rainbow tables แบบต่าง ๆ

 **XP free small (380MB)**  
formerly known as SSTIC04-10k

Success rate: 99.9%  
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ  
md5sum: 17cfa3fc613e275236c1f23eb241bc86

 **XP free fast (703MB)**  
formerly known as SSTIC04-5k

Success rate: 99.9%  
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ  
md5sum: f6f5536975b57c891ed5f2de702a02bd

 **XP special (7.5GB)**  
formerly known as WS-20k

Success rate: 96%  
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~ (including the space character)



### Vista free (461MB)

Success rate: 99%

Based on a dictionary of 64k words, 4k suffixes, 64 prefixes and 4 alteration rules for a total of  $2^{38}$  passwords (274 billion).

md5sum: 403cf58178d7272a48819b47ca8b2e6b



### Vista proba free (581MB)

Success rate: n/a

Passwords of length 5-10

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~ (including the space character)

$2^{39}$  passwords selected according to the most probable password patterns and the most probable character sequences (2nd order Markov Model) within the patterns. Trained on the Rocky password set.

md5sum: e0718aaf085980e0884ea5d09c7b856e



### Vista special (8.0GB)

formerly known as NTHASH

Success rate: 99%

Passwords of length 6 or less

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~ (including the space character)

Passwords of length 7

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

Passwords of length 8

Charset: 0123456789abcdefghijklmnopqrstuvwxyz



### Vista num (3.0GB)

Success rate: 99.9%

Passwords of length 1 to 12

Charset: 0123456789



### Vista proba 60G (60GB)

Success rate: n/a

Passwords of length 5-12

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ  
!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~ (including the space character)



### Vista specialXL (107GB)

Success rate: 99%

Passwords of length 1-7

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ  
!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~ (including the space character)



### Vista eight (134.6GB)

Success rate: 99%

Passwords of length 8

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!



### Vista eightXL (2.0TB)

Success rate: 99%

Passwords of length 8

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ  
!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~ (including the space character)



### Vista nine (52.0GB)

Success rate: 99%

Passwords of length 8

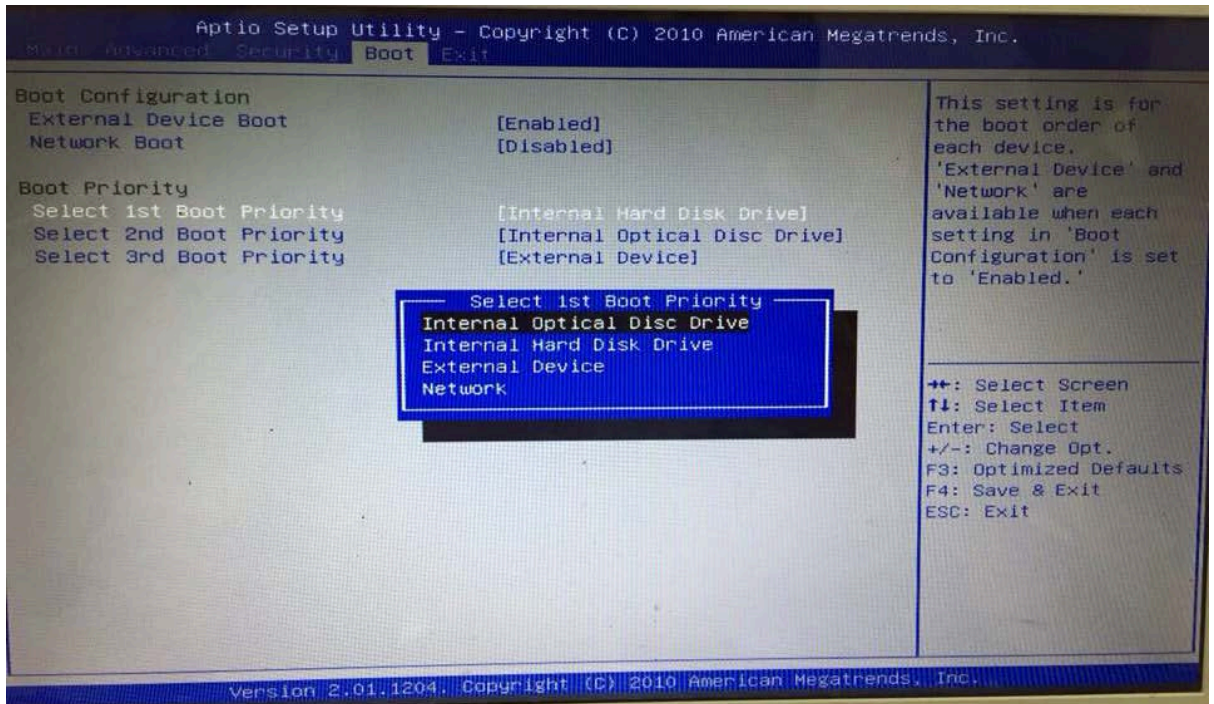
Charset: 0123456789abcdefghijklmnopqrstuvwxyz with the first letter capitalized

Passwords of length 9

Charset: 0123456789abcdefghijklmnopqrstuvwxyz

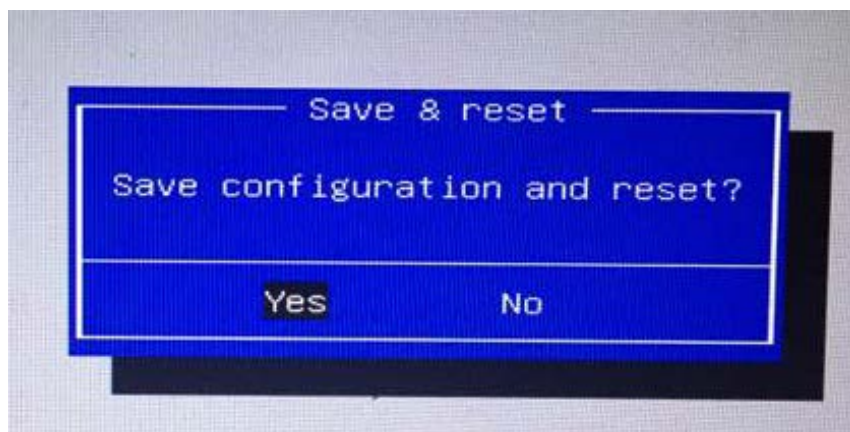
## ขั้นตอนการติดตั้งและใช้งาน OPHCRACK USB

1. เปิดเครื่องทำการกด F2 ย้ำๆแล้วจะขึ้นดังรูปที่ 1 แล้วคลิก boot กด internal optical disc drive เพื่อเซตค่าคอมพิวเตอร์ให้ทำการอ่านจาก disc หรือ usb



รูปที่ 1

2. กด Exit แล้วกด yes



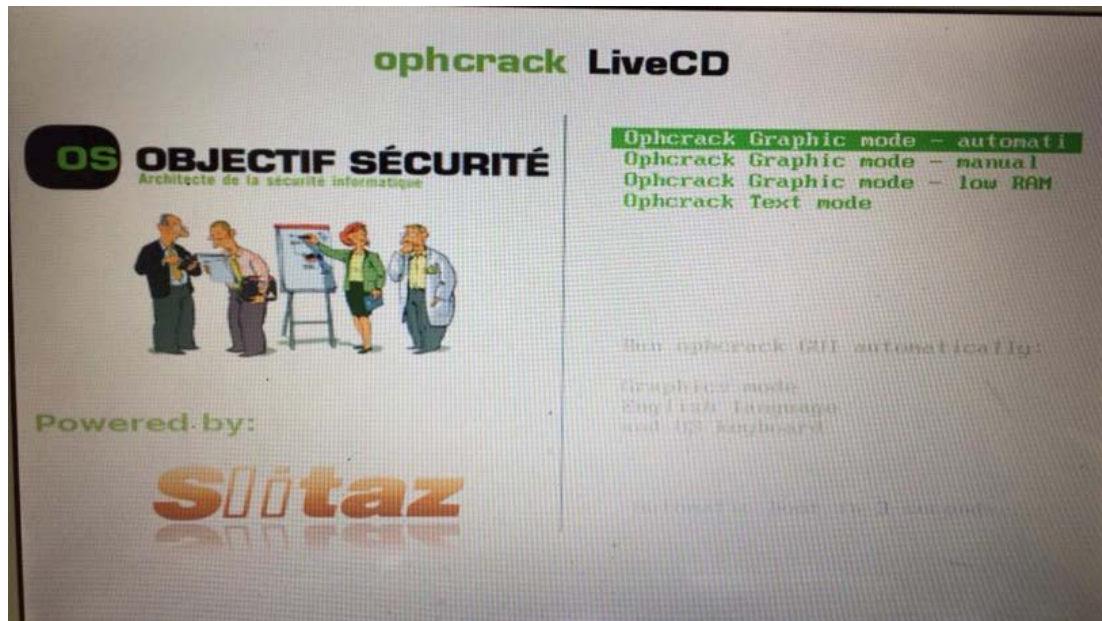
รูปที่ 2



3. โหมดของ Ophcrack ให้อยู่ 4 โหมด

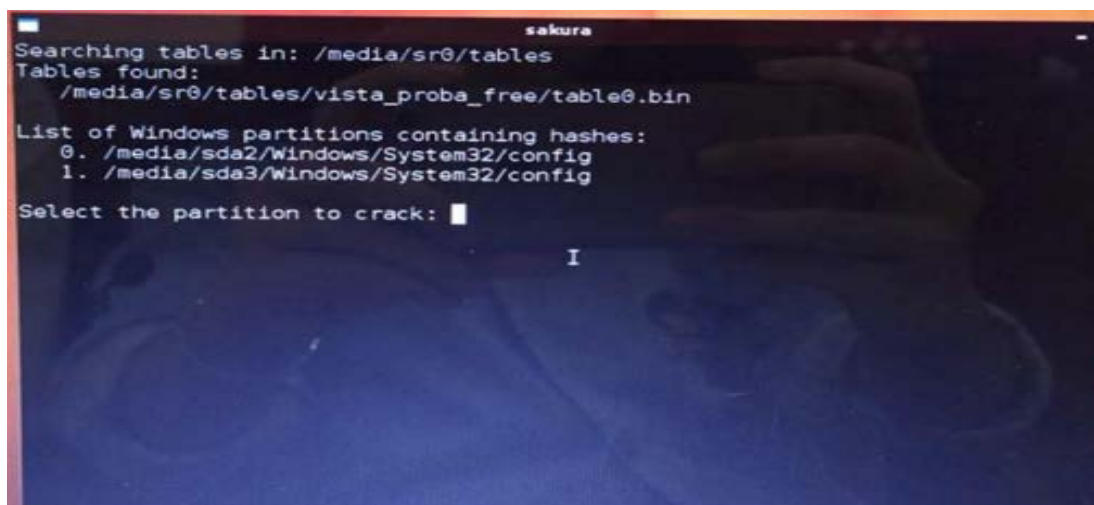
- Ophcrack Graphic mode – automatic
- Ophcrack Graphic mode – manual
- Ophcrack Graphic mode – low RAM
- Ophcrack Text mode

ซึ่งเราจะเลือกโหมดที่ 1 คือ Ophcrack Graphic mode – automatic เพื่อให้เข้าทำงานได้เลย



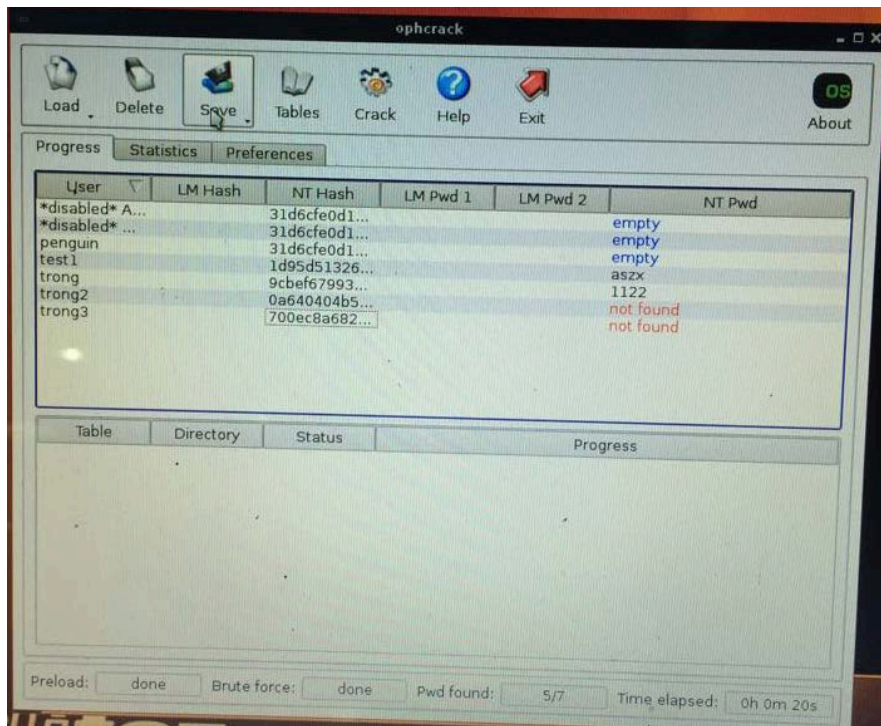
รูปที่ 3

4. จะได้หน้าต่างของดังรูปที่ 4 ขึ้นมาแล้วกด enter



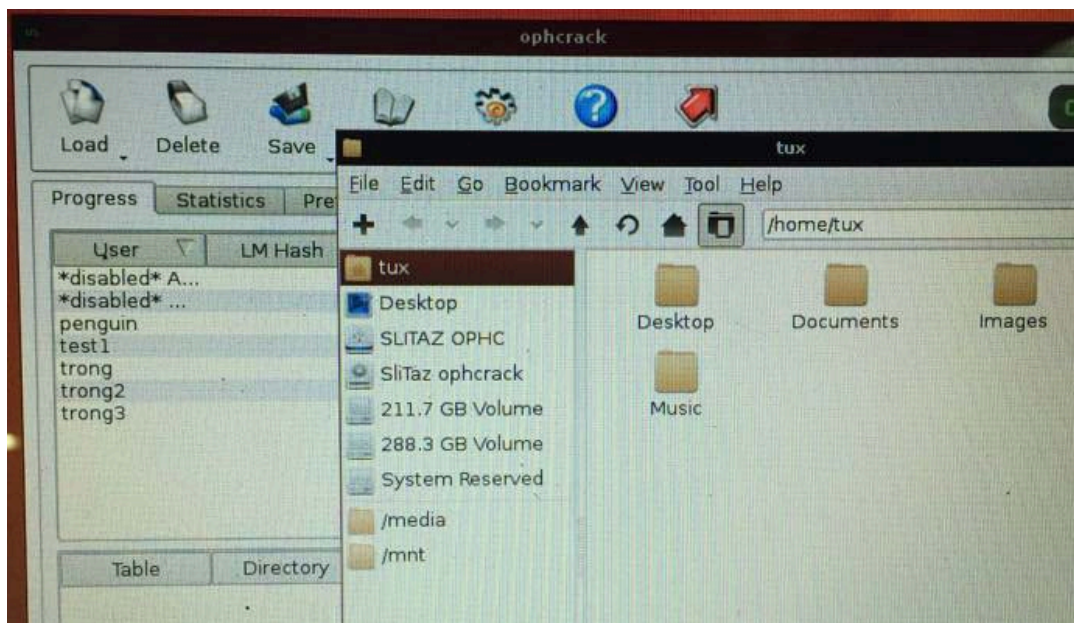
รูปที่ 4

5. โปรแกรมพื้นฐานจะทำการ Hack ได้สำเร็จได้แค่ password 4 ตัวเท่านั้น



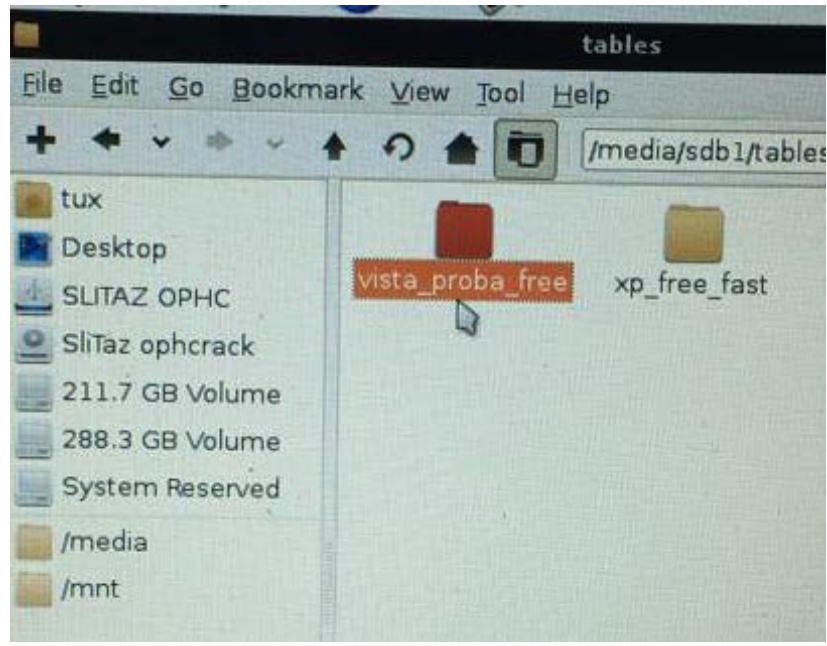
รูปที่ 5

6. จึงทำการเพิ่มในส่วนของ Rainbow Tables เข้ามาเพื่อให้ทำการ Hack password ได้มากขึ้นกว่าเดิม ให้ทำการคลิกที่ my document จะได้ดังรูป



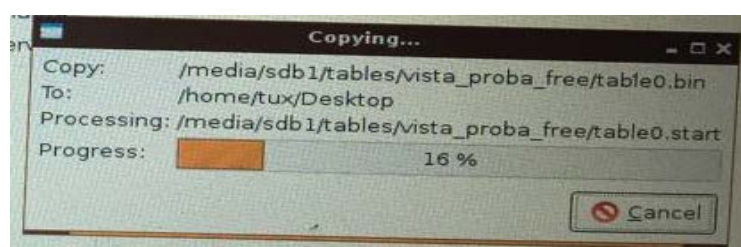
รูปที่ 6

7. ทำการเลือก slitaz ophc -> เลือก table -> คือไฟล์ของ Rainbow Tables ที่จะใช้ทำการ Hack เลือก vista\_proba\_free แล้วลากมาไว้ Desktop



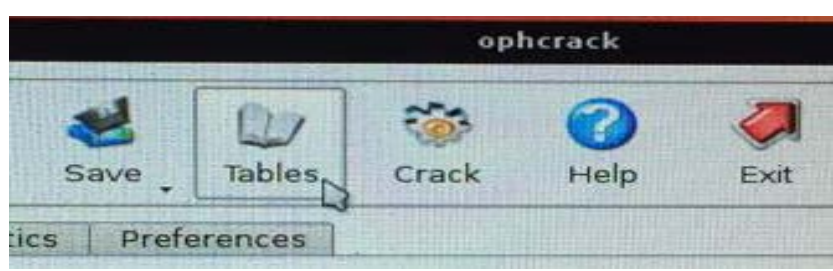
รูปที่ 7

8. จากนั้นมันจะทำการโหลดเพื่อใช้ไฟล์ในการ Hack



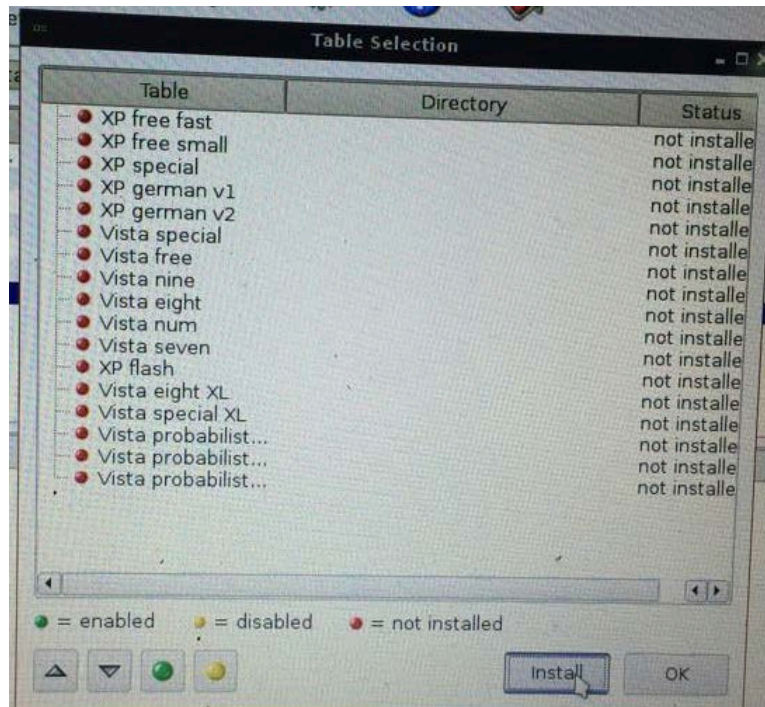
รูปที่ 8

9. คลิกtables



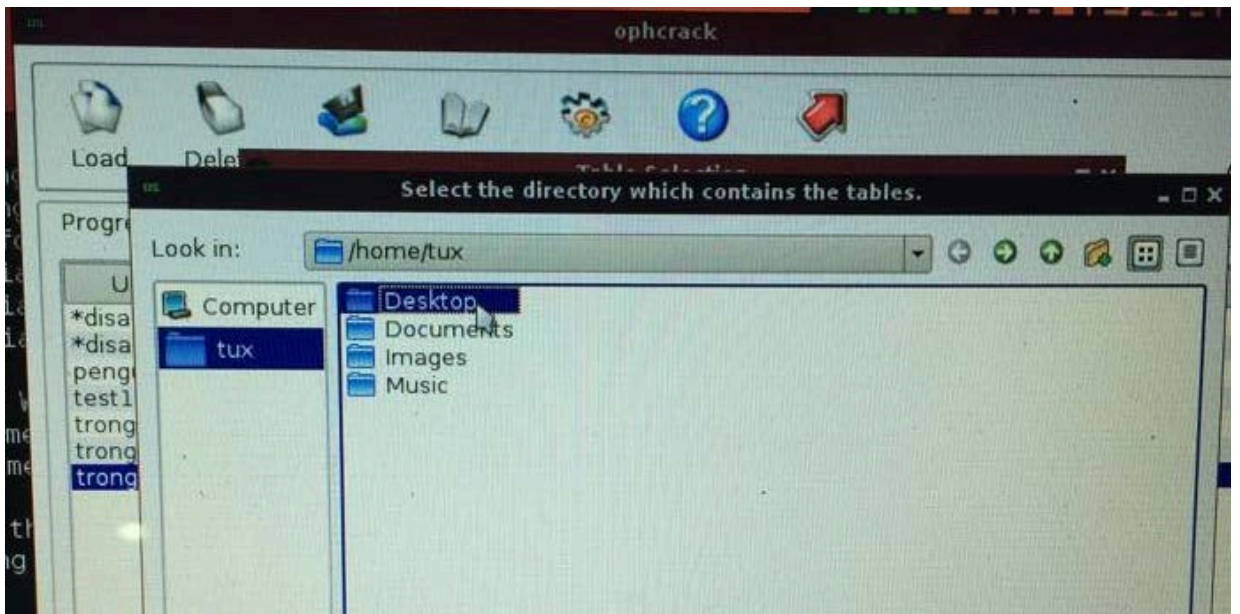
รูปที่ 9

10. ทำการ Install



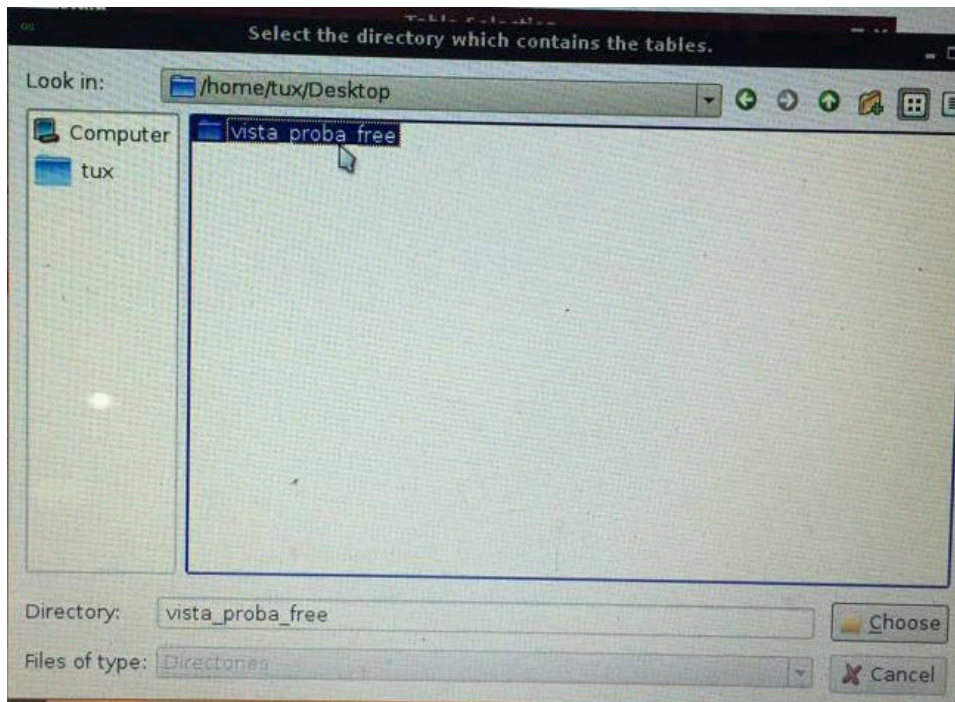
รูปที่ 10

11. คลิก Desktop



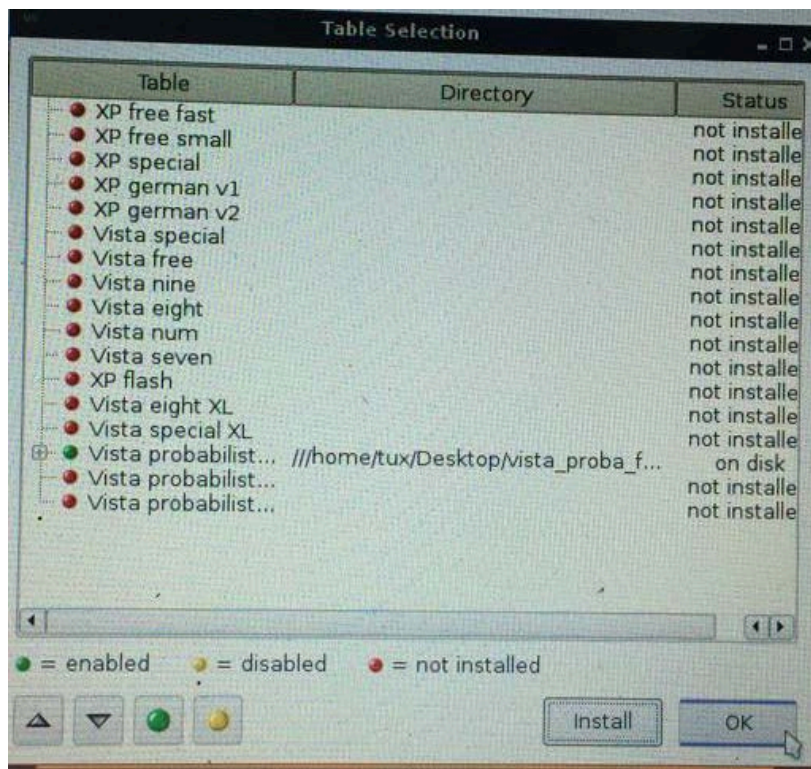
รูปที่ 11

12. คลิกชื่อไฟล์ดังรูปที่ 12 แล้วกด Chooses



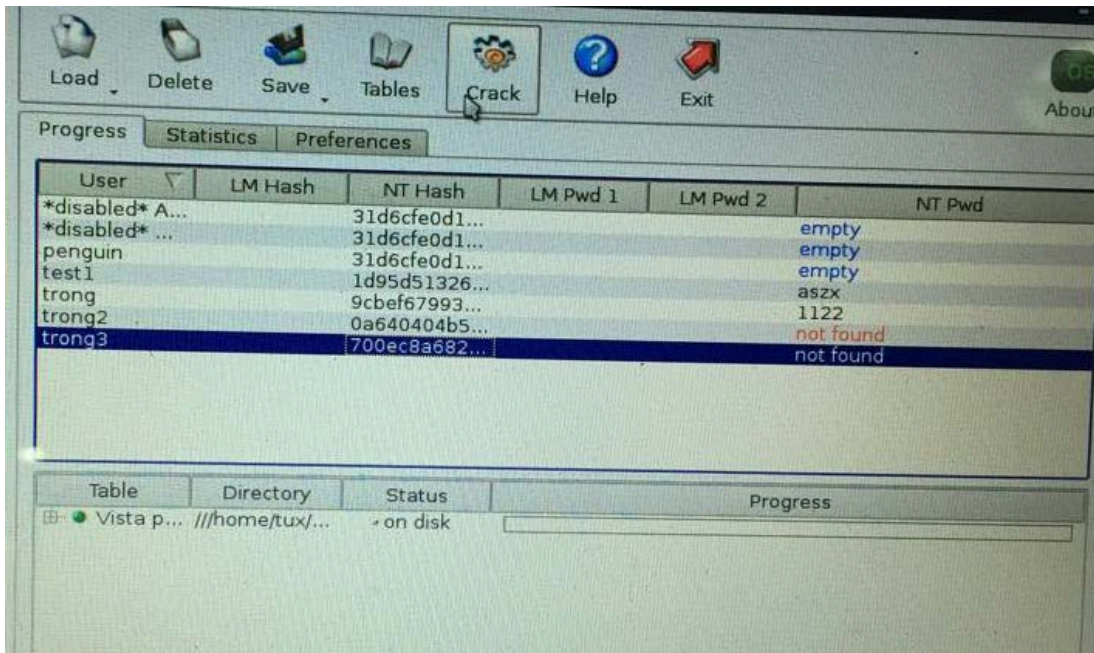
รูปที่ 12

13. คลิกที่ OK



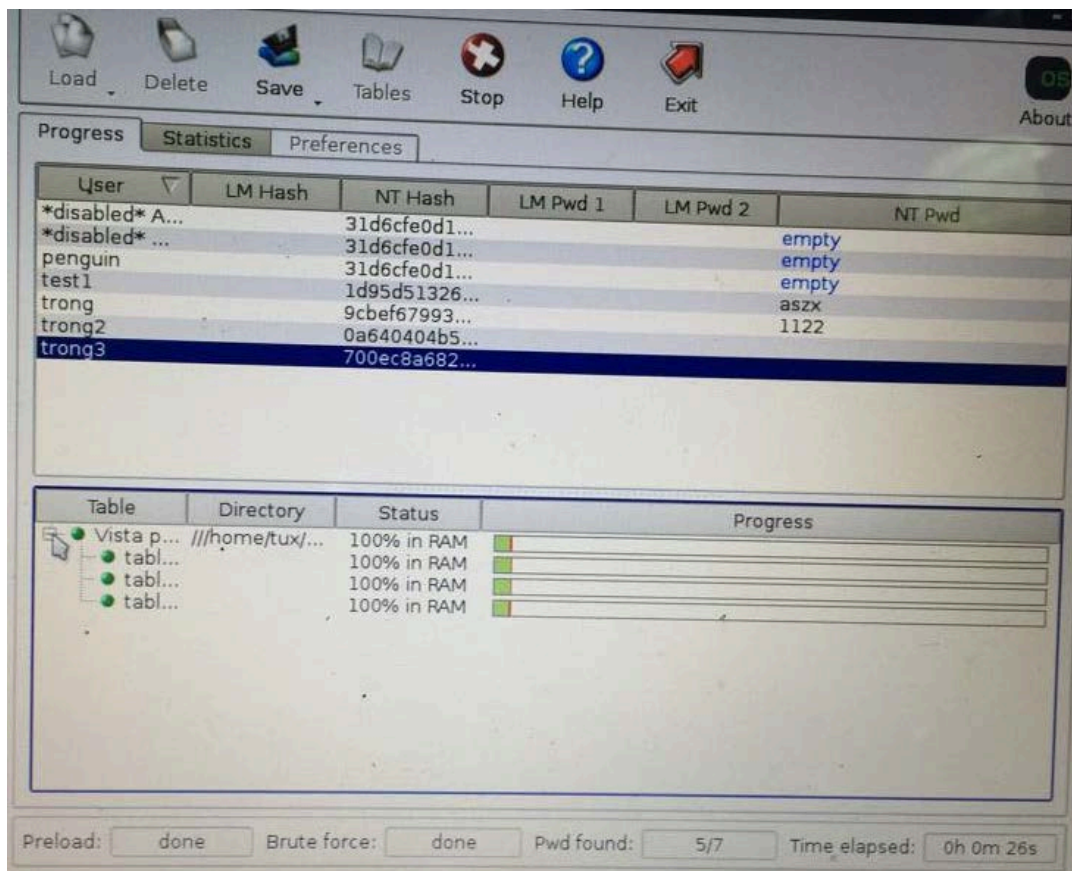
รูปที่ 13

14. คลิกที่ Crack



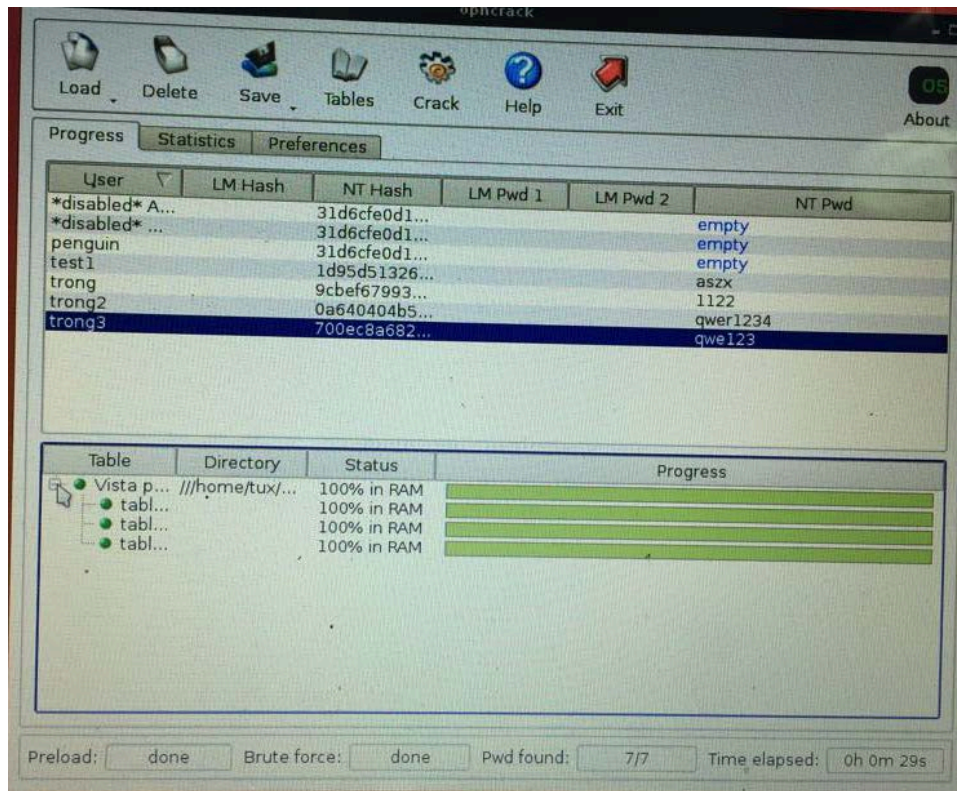
รูปที่ 14

15. ทำการประมวลผล และอ่านรหัสของ user



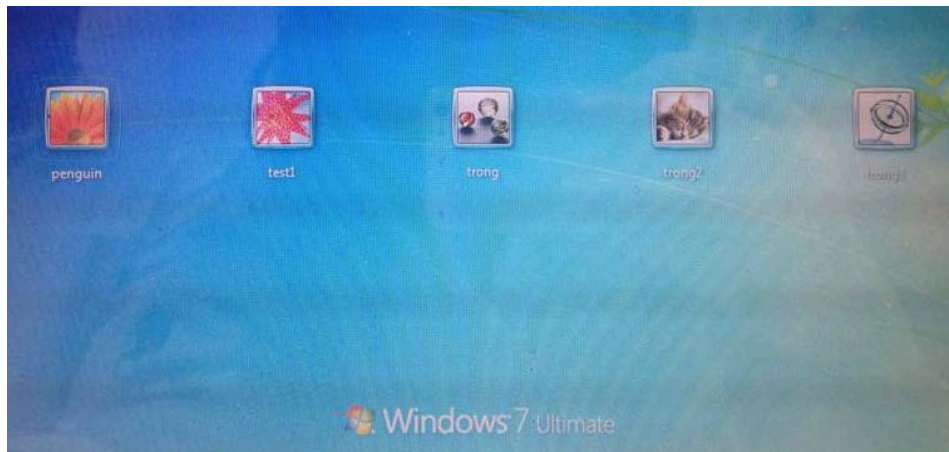
รูปที่ 15

16. ประมวลผลเสร็จได้รหัส



รูปที่ 16

17. เลือก account ที่จะใส่รหัส



รูปที่ 17

18. ทำการใส่รหัสที่ถอดมาได้



รูปที่ 18