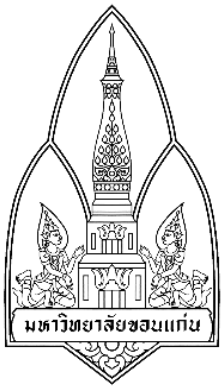


คู่มือการใช้ Security Tool

Cain and Abel

โดย

1. นางสาวธารดา	เหมือนโพธิ์	563020211-7
2. นางสาวมิตติมา	ไชยอุป	563020224-8
3. นางสาวรัศมิมัต	ทองมีค่า	563020226-4
4. นางสาวสุกัญญา	บุญพันธ์	563020232-9
5. นางสาวธารทิพย์	เพ็งปาน	563020764-6
6. นายอุบล	เกตุนอก	573021177-7

เสนอ

ผศ. ดร.จักรชัย โสอินทร์

รายวิชา 322376 ความมั่นคงทางเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคเรียนที่ 1 ปีการศึกษา 2558

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

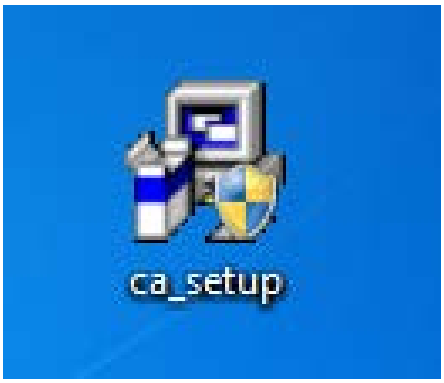
มหาวิทยาลัยขอนแก่น

Security Tool Cain and Abel

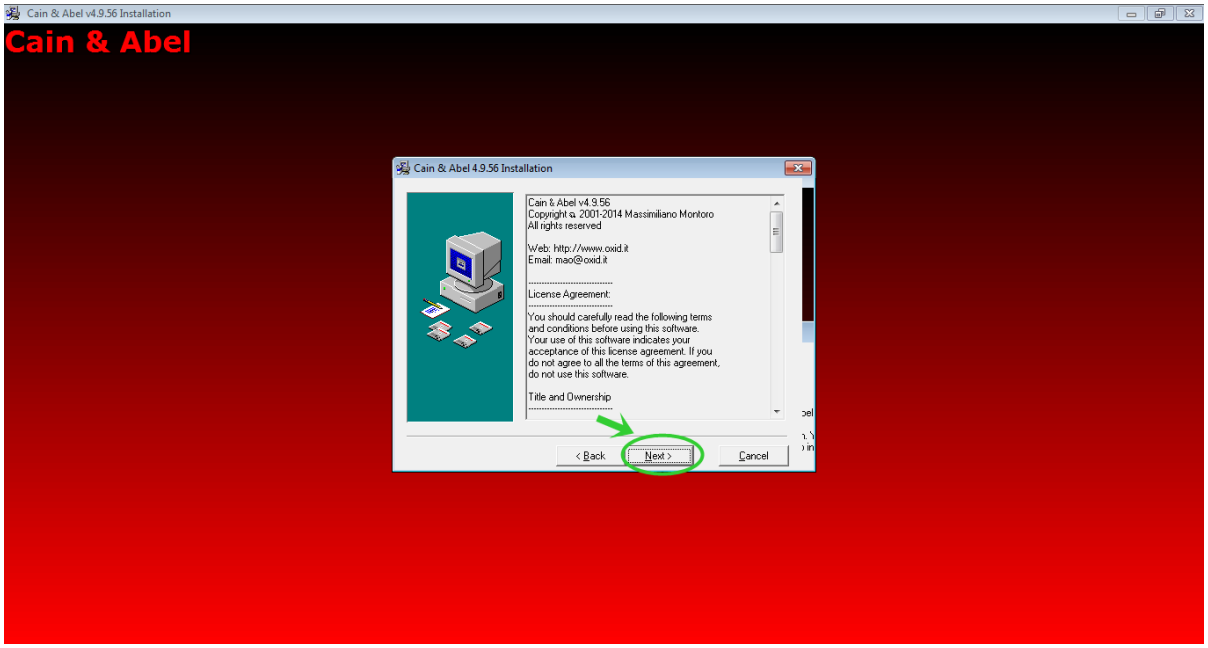
Cain & Abel เป็นเครื่องมือสำหรับใช้ในการกู้คืนรหัสผ่าน สำหรับเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการวินโดวส์ และสามารถทำการถอดรหัสผ่านได้หลากหลายรูปแบบ เช่น ทำการดักข้อมูลรหัสผ่านจากเครือข่าย, การแครกรหัสผ่านโดยใช้ Dictionary, การแครกรหัสผ่านแบบ Brute-Force, และการแครกรหัสผ่านแบบ Cryptanalysis attacks นอกจากนี้ยังสามารถทำการบันทึกการสนทนาแบบ VoIP, ทำการถอดรหัส scrambled passwords, ทำการแสดงรหัสผ่านใน password boxes, ทำการค้นหารหัสผ่านต่างๆ ที่เก็บอยู่ใน cache ได้

การติดตั้งโปรแกรม Cain and Abel

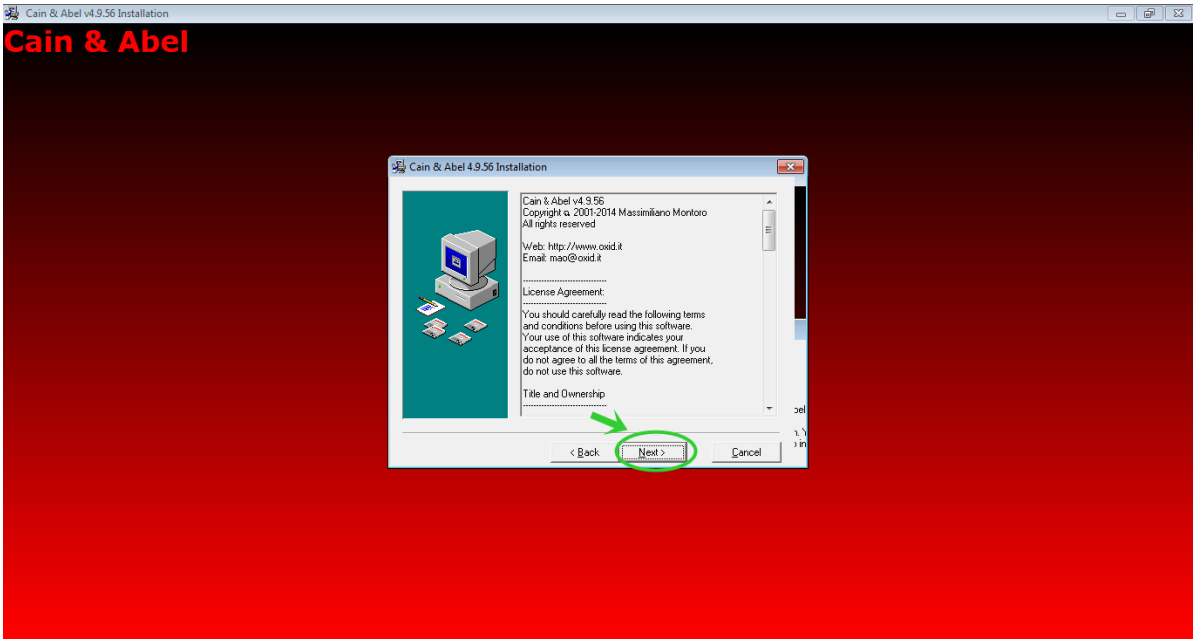
1.ให้ทำการดับเบิ้ลคลิกที่ไฟล์ ca_setup.exe



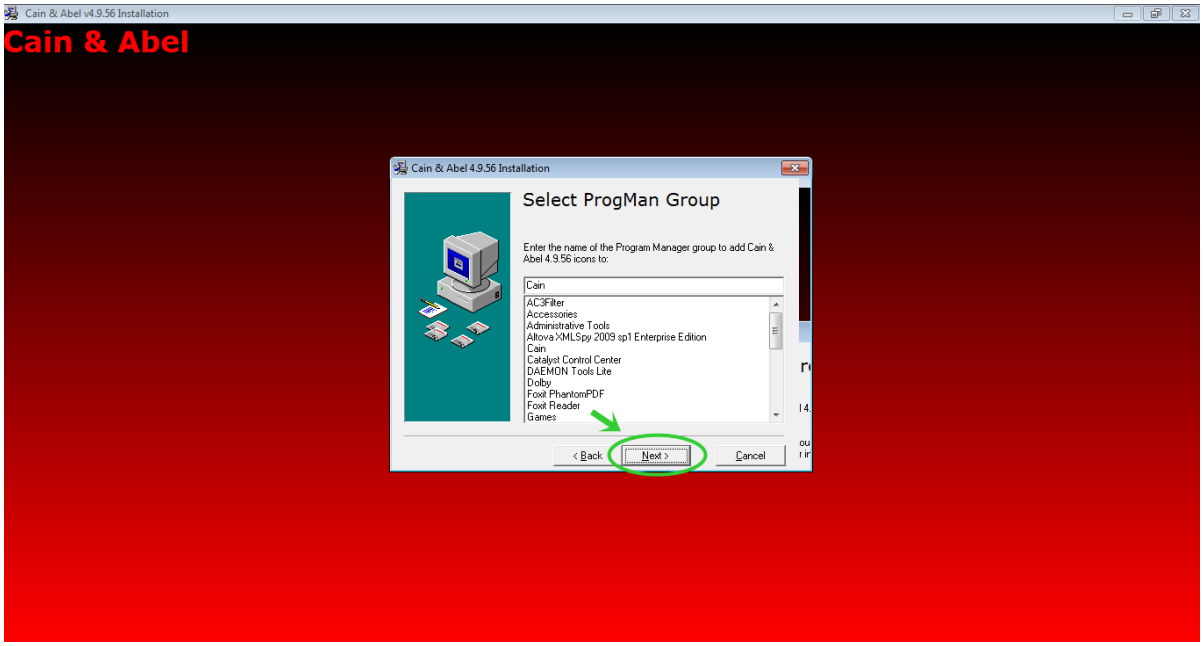
2. จะปรากฏหน้าต่างดังภาพ ให้คลิก Next



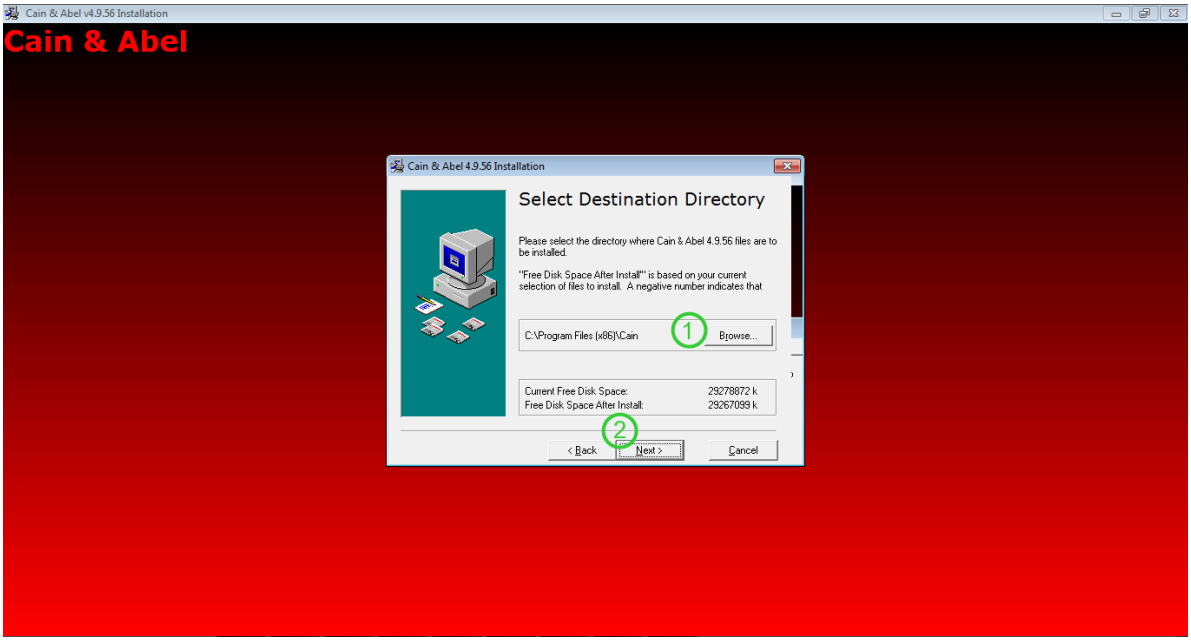
3. แสดงเกี่ยวกับ License Agreement ให้คลิก Next



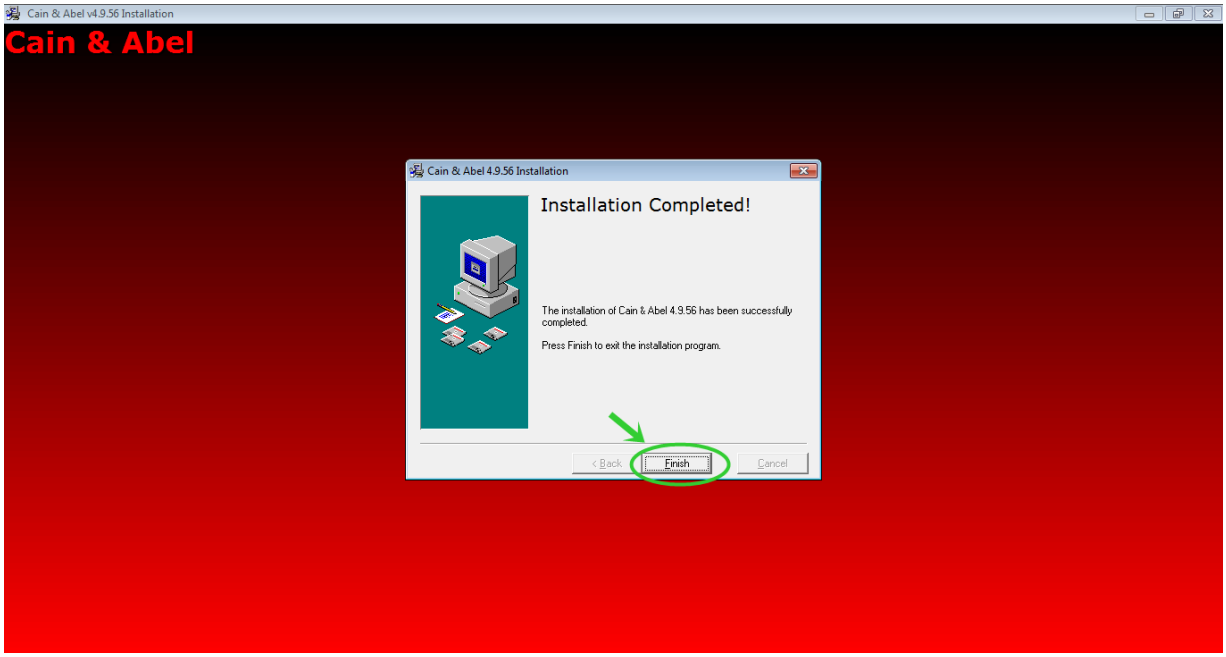
4. ให้เลือกตำแหน่งที่เก็บไฟล์ของโปรแกรม หลังจากเลือกเสร็จแล้ว ให้คลิก Next



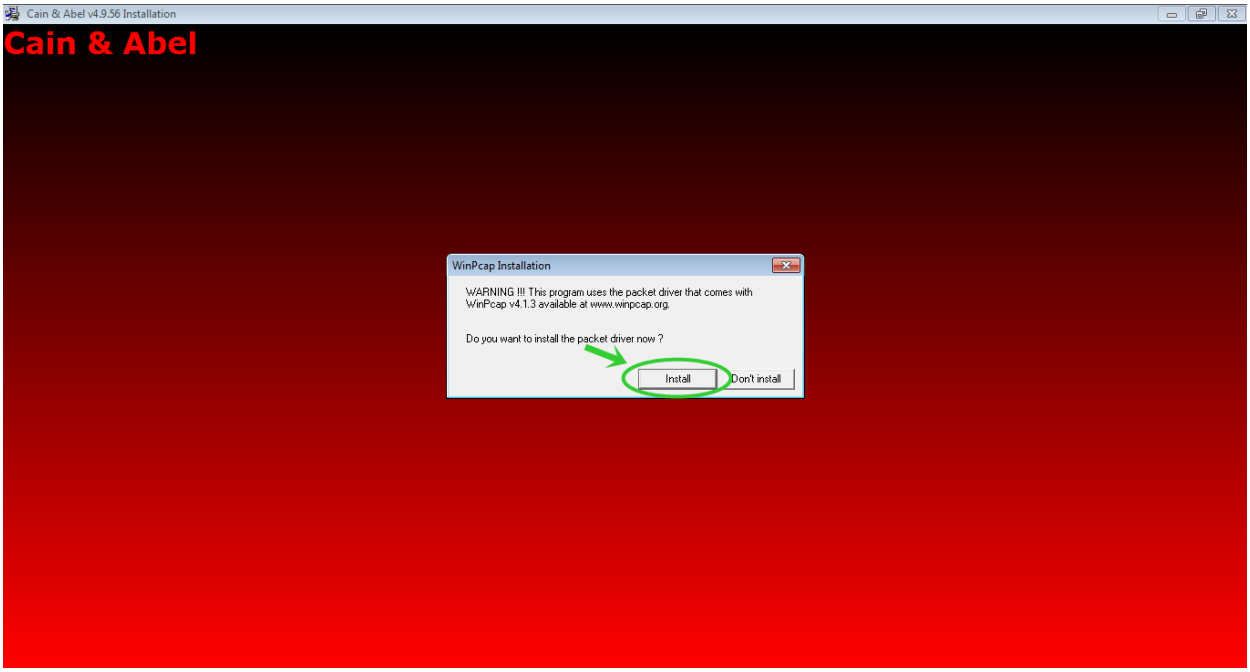
5. ให้คลิก Next เพื่อทำการติดตั้งโปรแกรม รอจนการติดตั้งแล้วเสร็จ



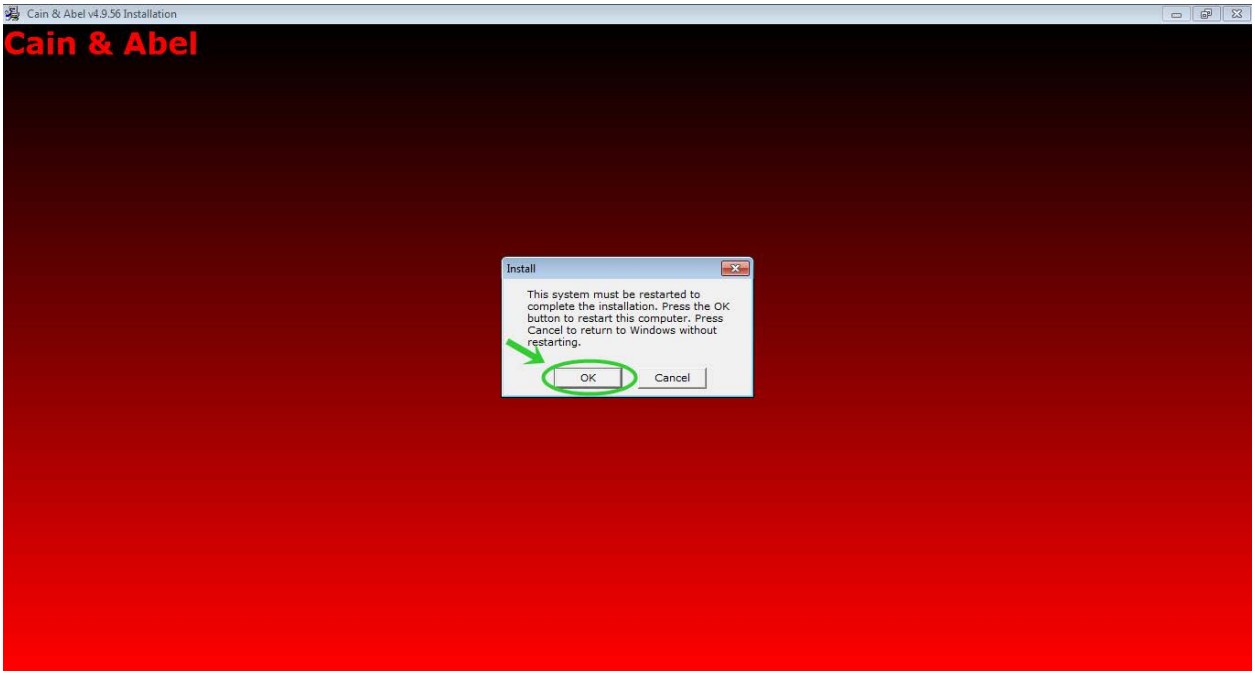
6. คลิกที่ Finish เพื่อจบการติดตั้งโปรแกรม



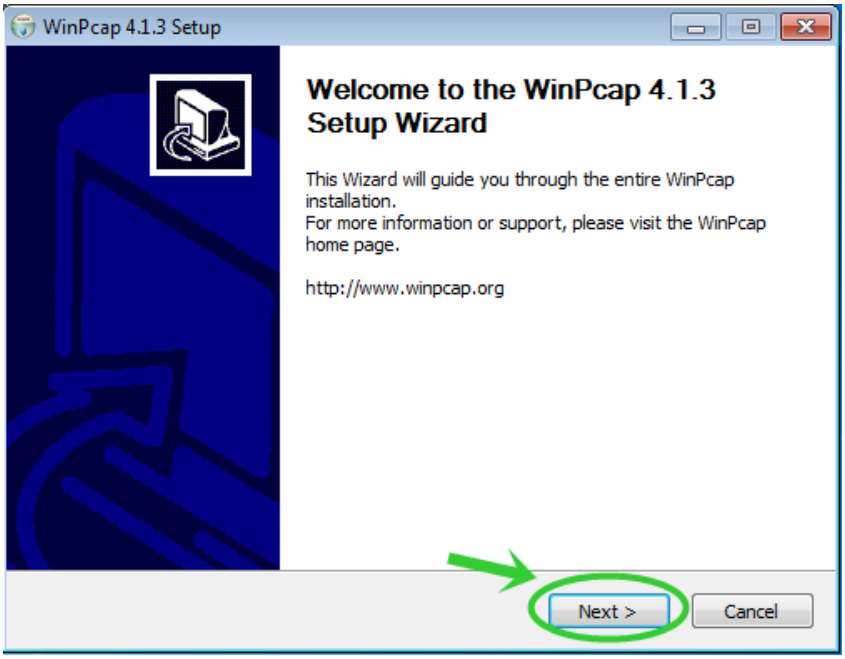
7. จากนั้นระบบจะถามว่าต้องการติดตั้ง WinPcap หรือไม่ ถ้าต้องการติดตั้ง ให้คลิกที่ Install หากต้องการใช้งานแบบการดักจับข้อมูลจากเครือข่าย



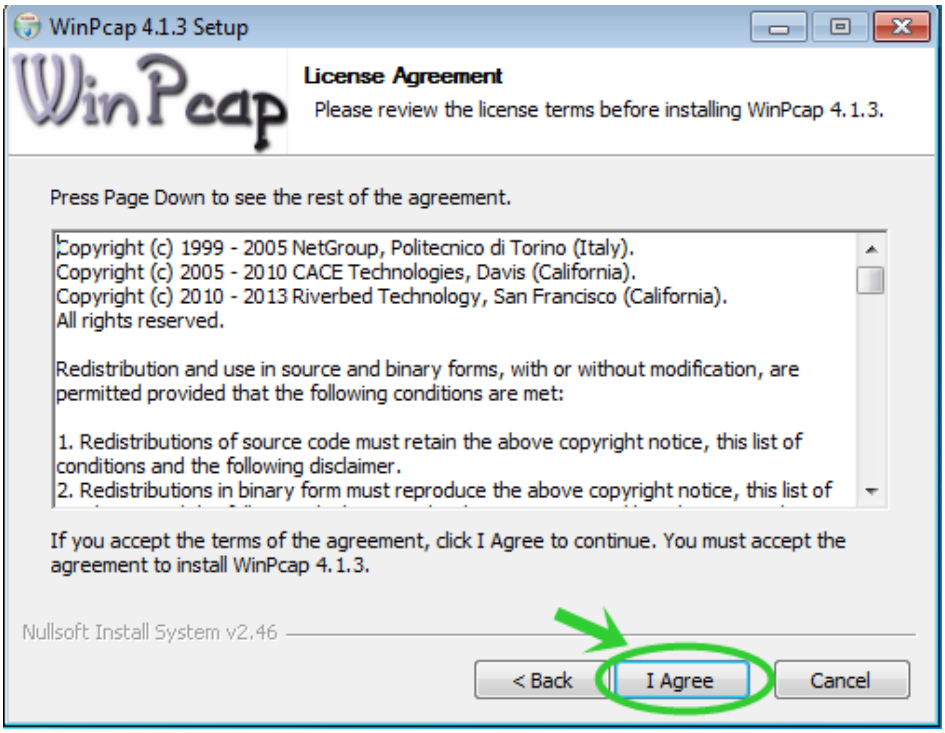
8. ระบบจะถามอีกครั้ง เพื่อยืนยันว่าจะติดตั้งโปรแกรมหรือไม่ ให้คลิกที่ปุ่ม OK



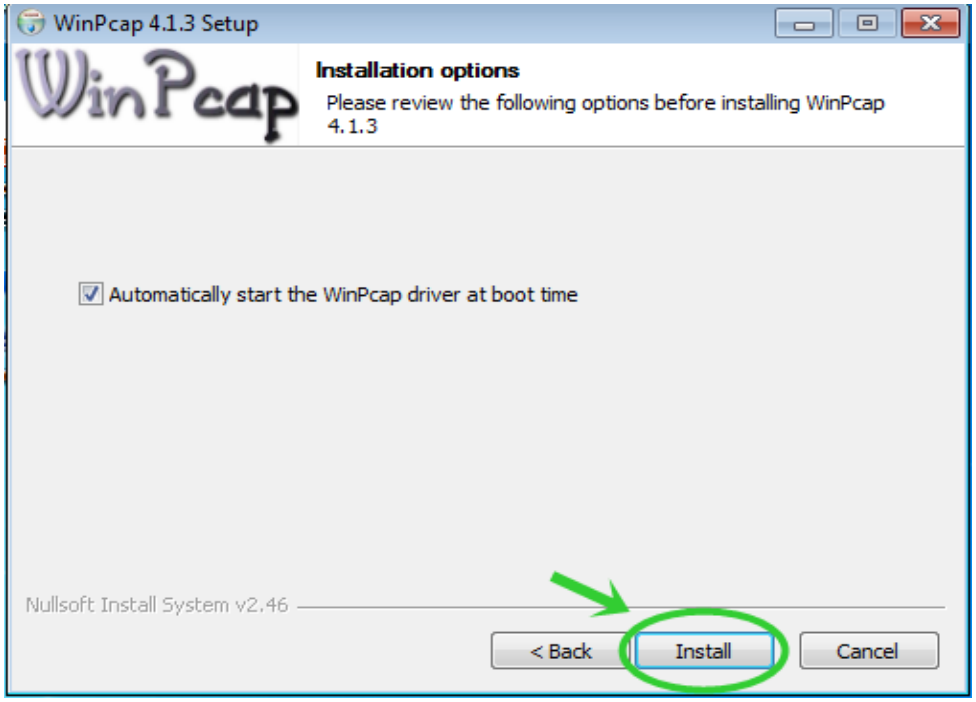
9. ให้คลิก Next เพื่อเริ่มการติดตั้งโปรแกรม



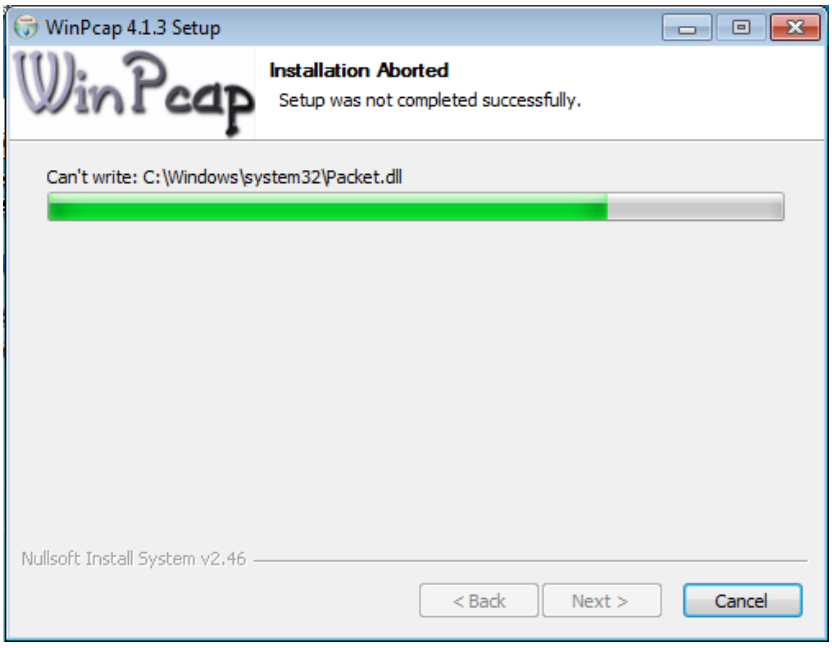
10. ให้คลิกที่ปุ่ม I Agree หากยอมรับเงื่อนไขของ License Agreement



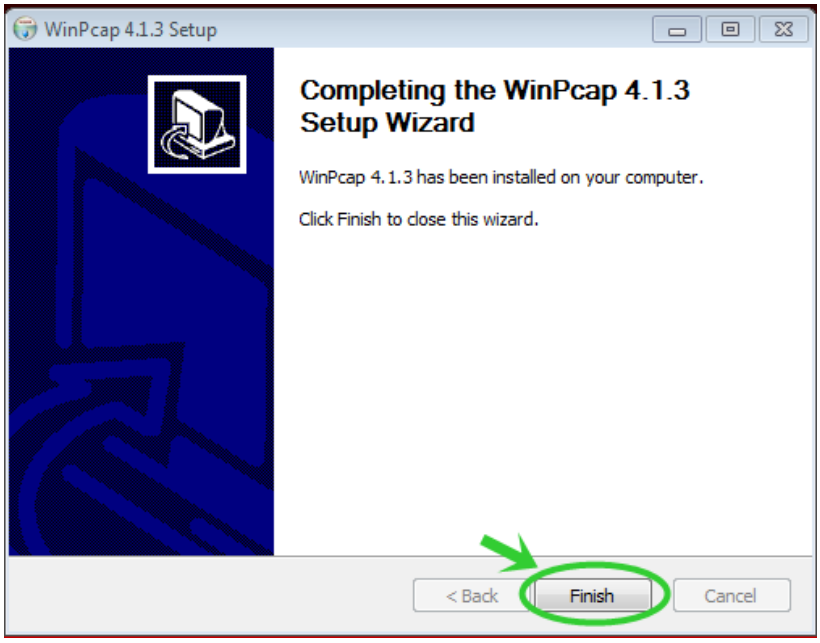
11. เลือกที่ Check box (Automatically start the WinPcap driver at boot time) ถ้าต้องการให้เมื่อติดตั้งโปรแกรมเสร็จแล้วให้รันโปรแกรมในทันที แล้วคลิกที่ปุ่ม Install



12. ระบบกำลังติดตั้งโปรแกรม WinPcap



13. เมื่อโปรแกรมติดตั้งเสร็จสมบูรณ์แล้ว ให้คลิกที่ปุ่ม Finish

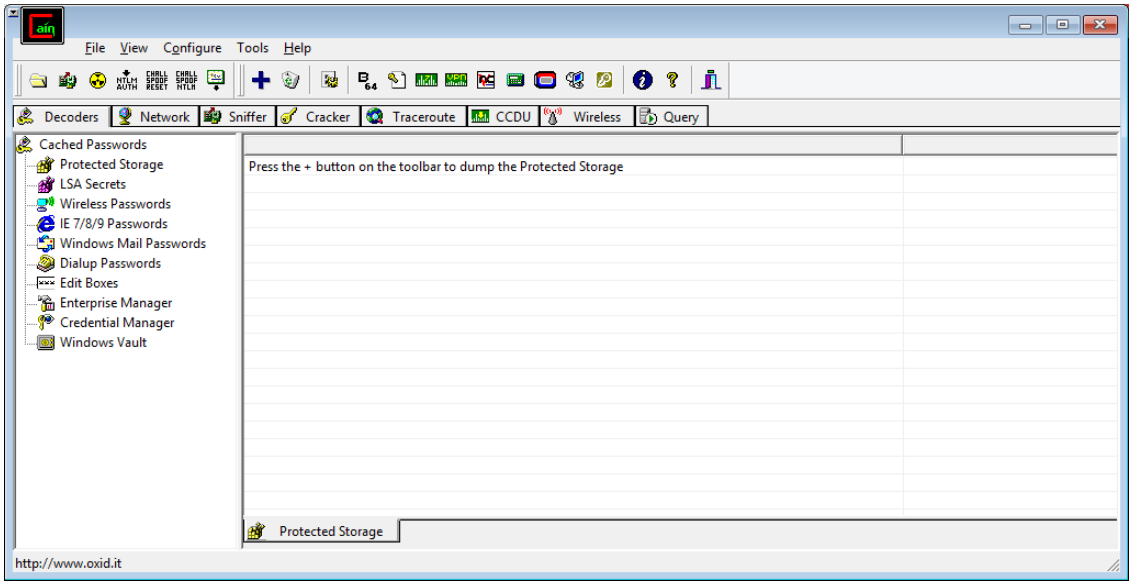


14. เมื่อติดตั้งเสร็จจะมีไอคอนของโปรแกรม Cain ปรากฏขึ้น

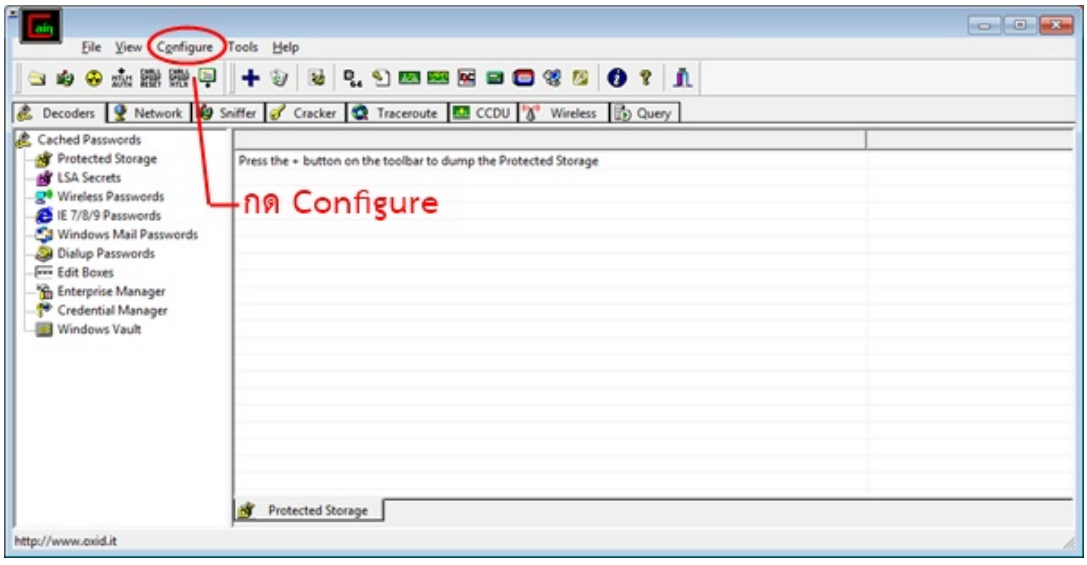
วิธีการใช้โปรแกรม Cain and Abel

1. Double Click ที่ไอคอนของโปรแกรม Cain and Abel

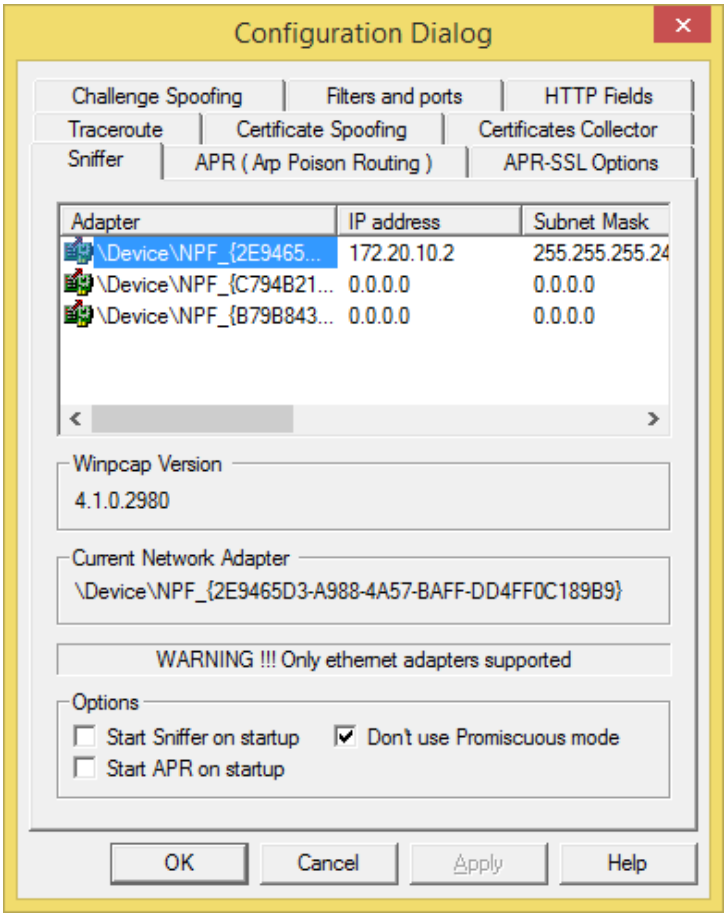
2. หน้าตาของโปรแกรม Cain & Abel



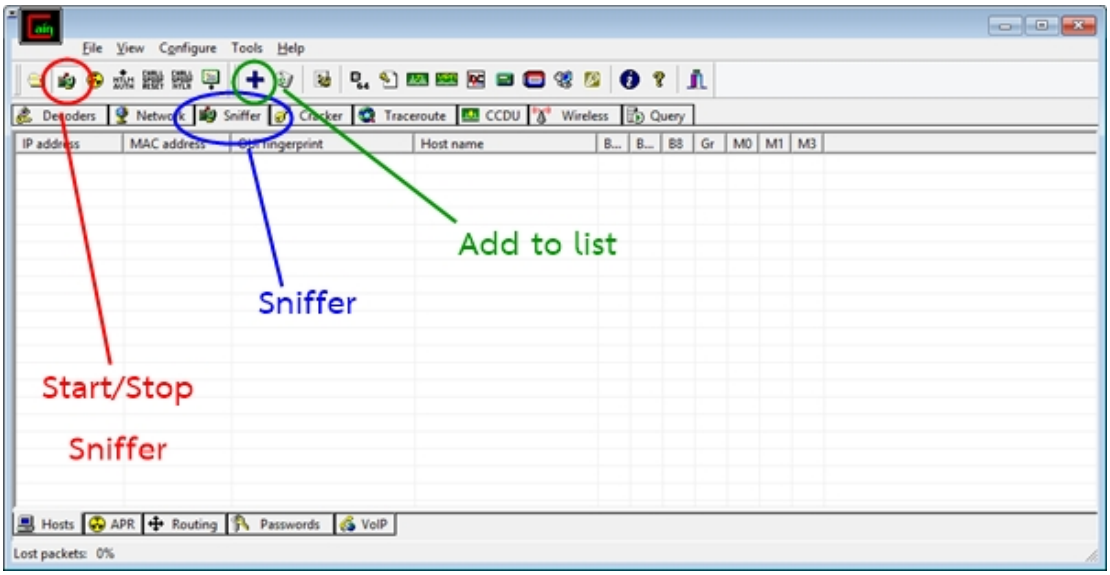
3. คลิกที่ Tab Configure



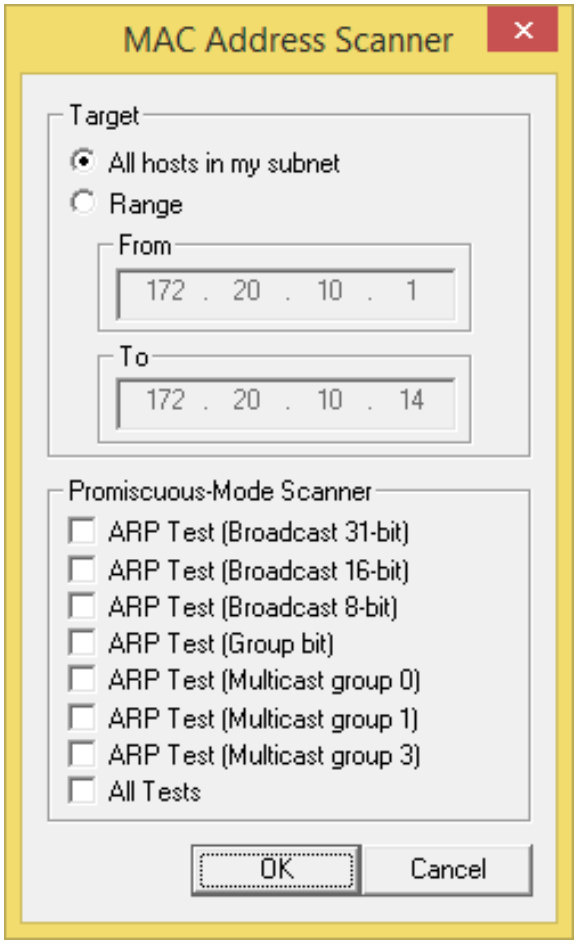
4. เลือก IP address ของเครื่องตัวเอง -> กดปุ่ม OK



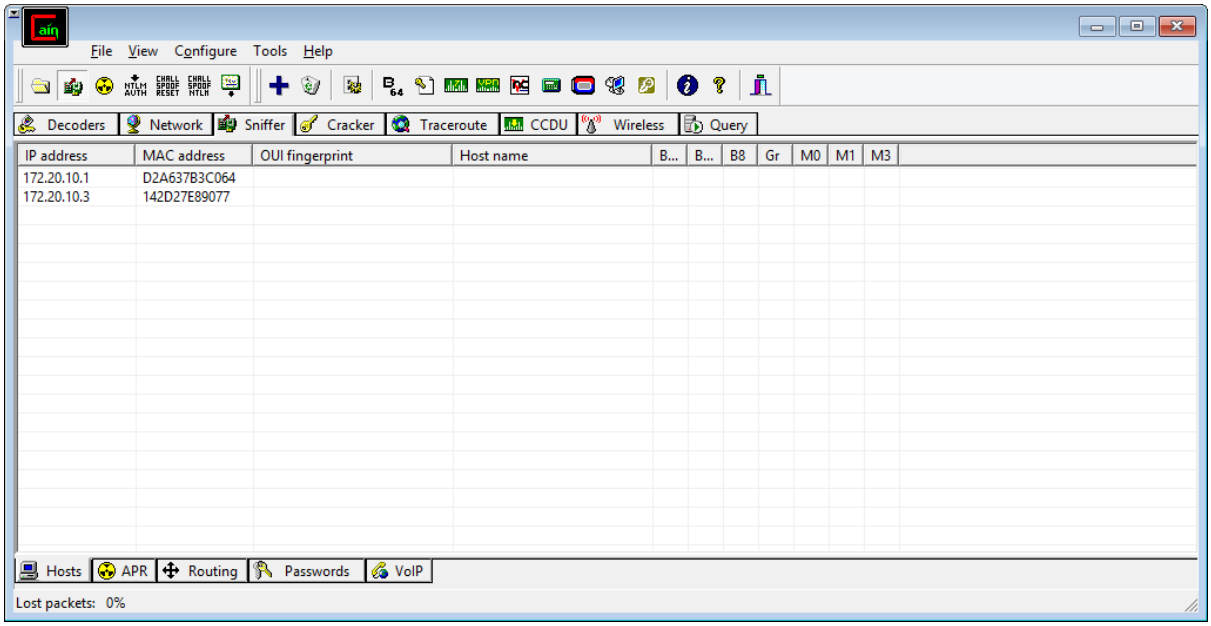
5. ไปที่ tab sniffer -> กดปุ่ม start/stop sniffer -> Add to list



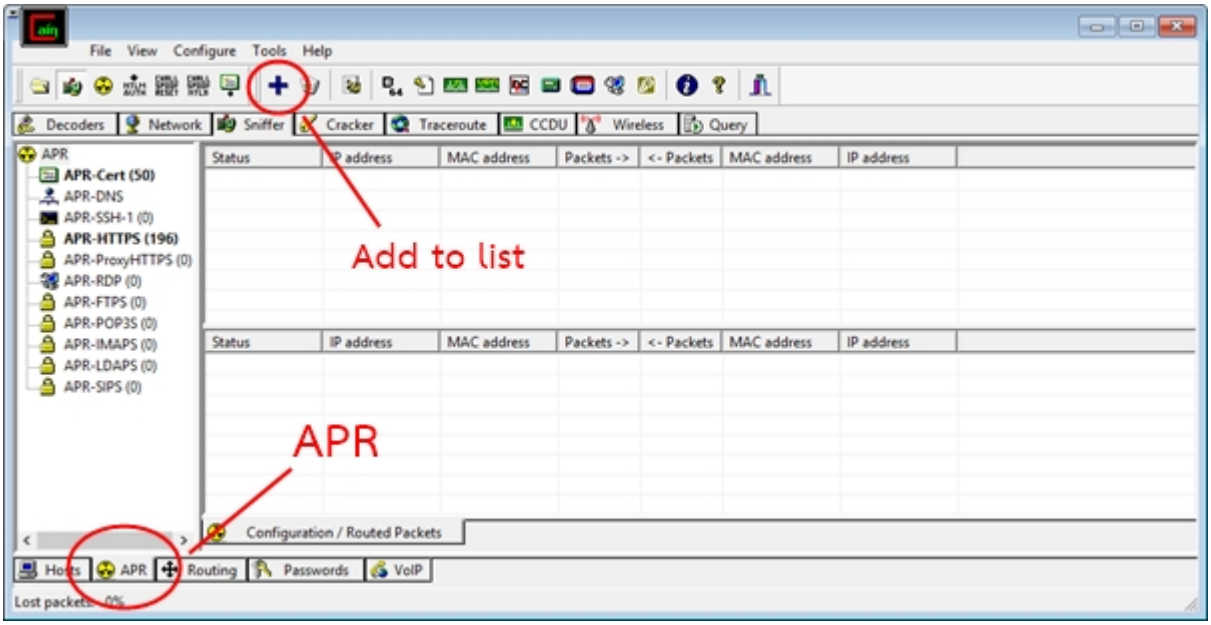
6. จะมีหน้าต่างปรากฏขึ้น ไม่ต้องปรับแต่งใดๆ คลิกปุ่ม OK



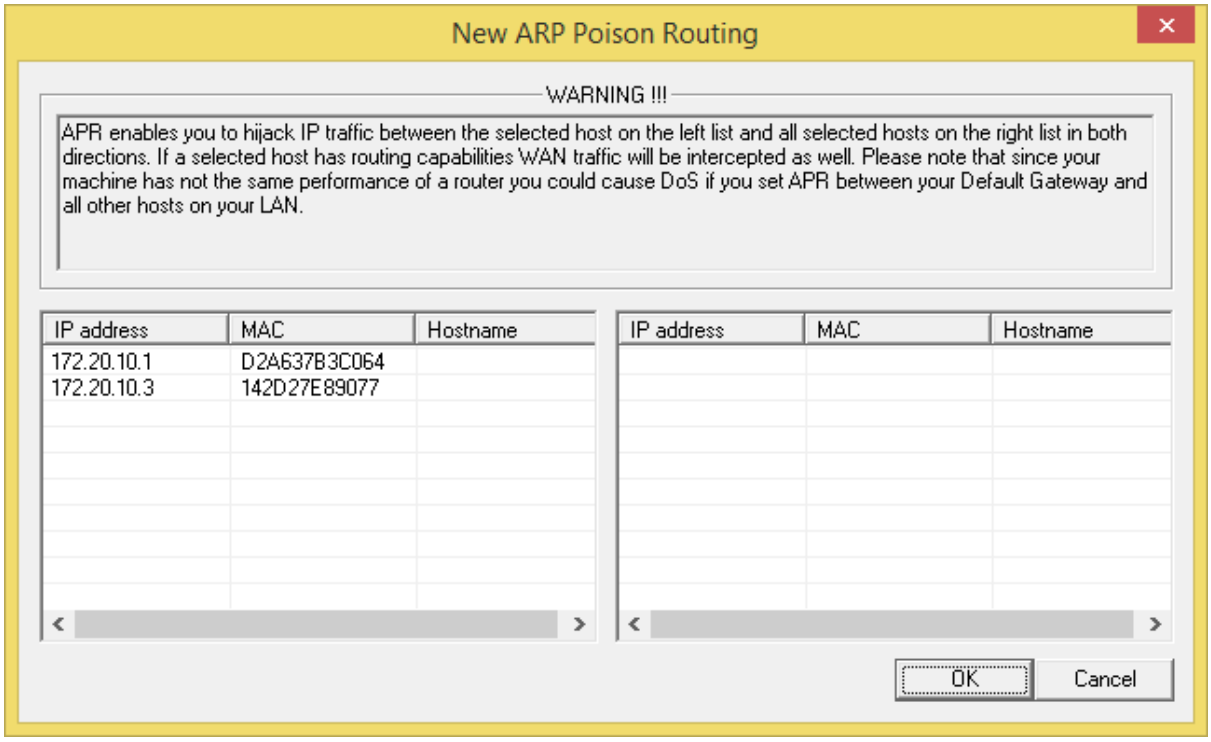
7. มี IP Address ของเครื่องที่เชื่อมต่อในวงแลนเดียวกันปรากฏขึ้น



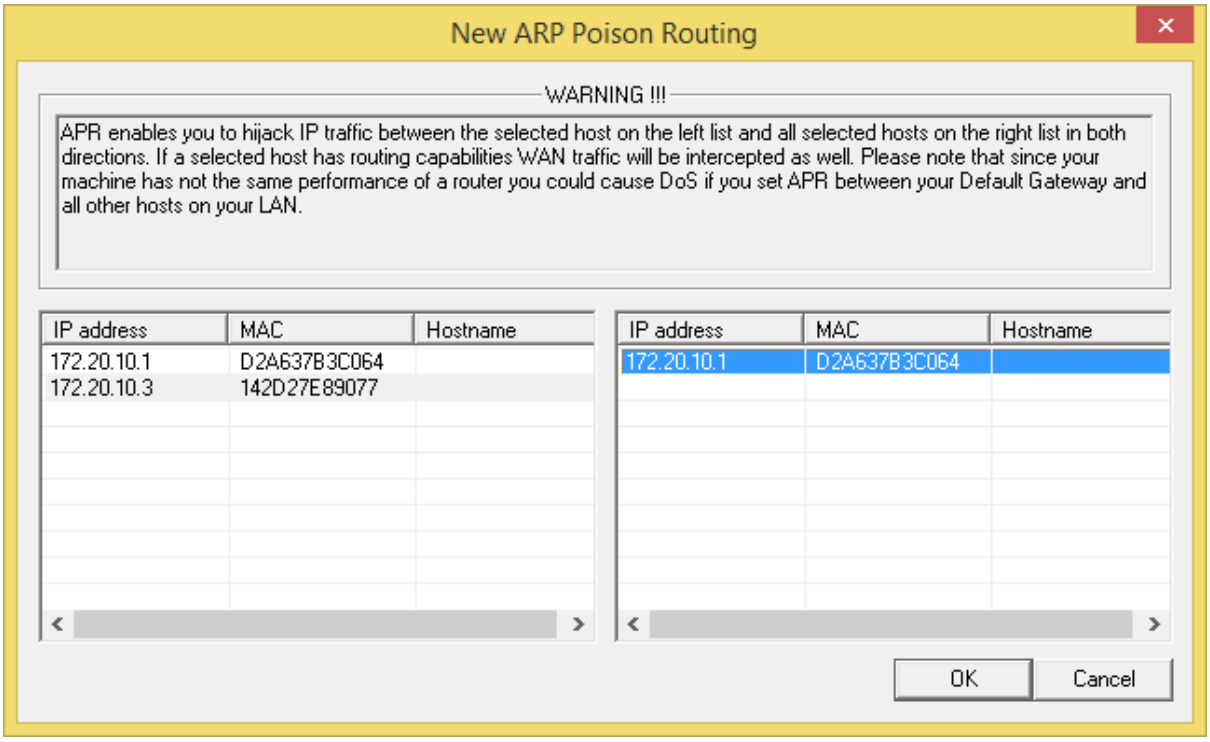
8. คลิกที่ Tab APR -> กดปุ่ม Add to list



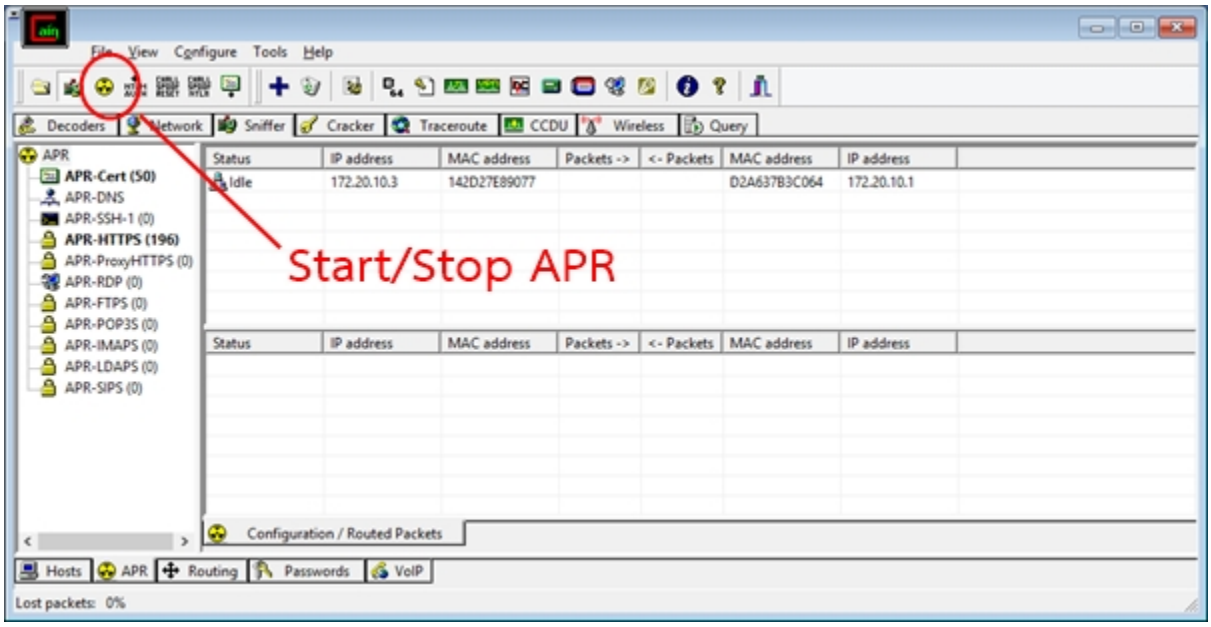
9. (ด้านซ้ายมือ) เลือก IP Address เครื่องเป้าหมาย



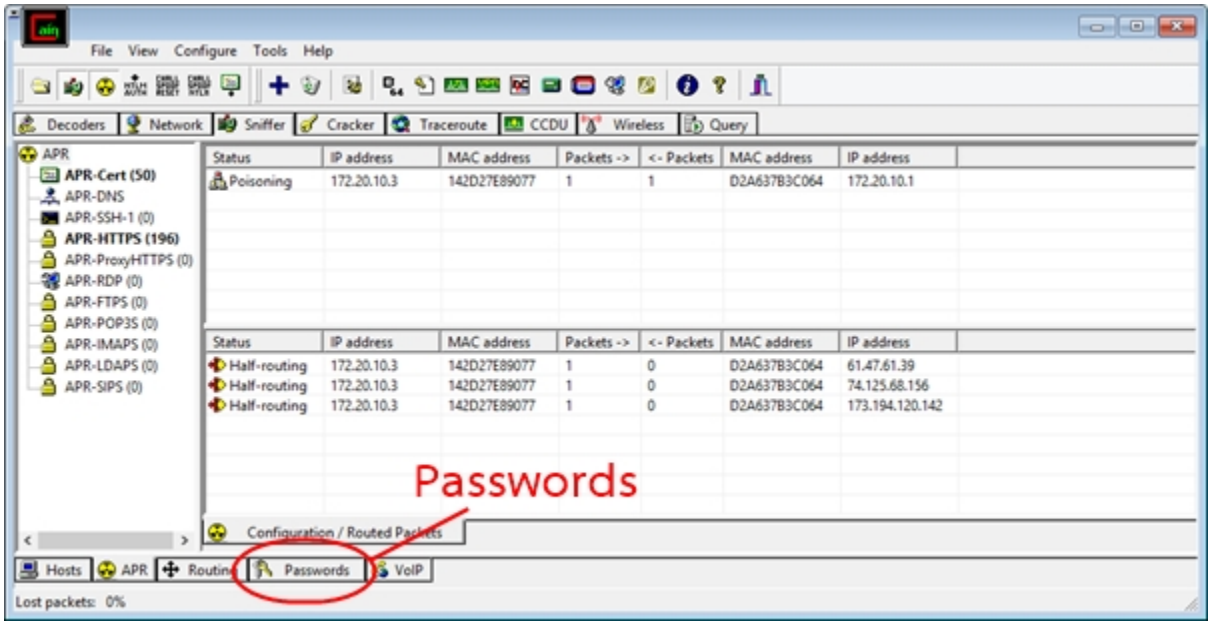
10. (ด้านขวามือ) เลือก IP Address เครื่องตัวเอง และกดปุ่ม OK



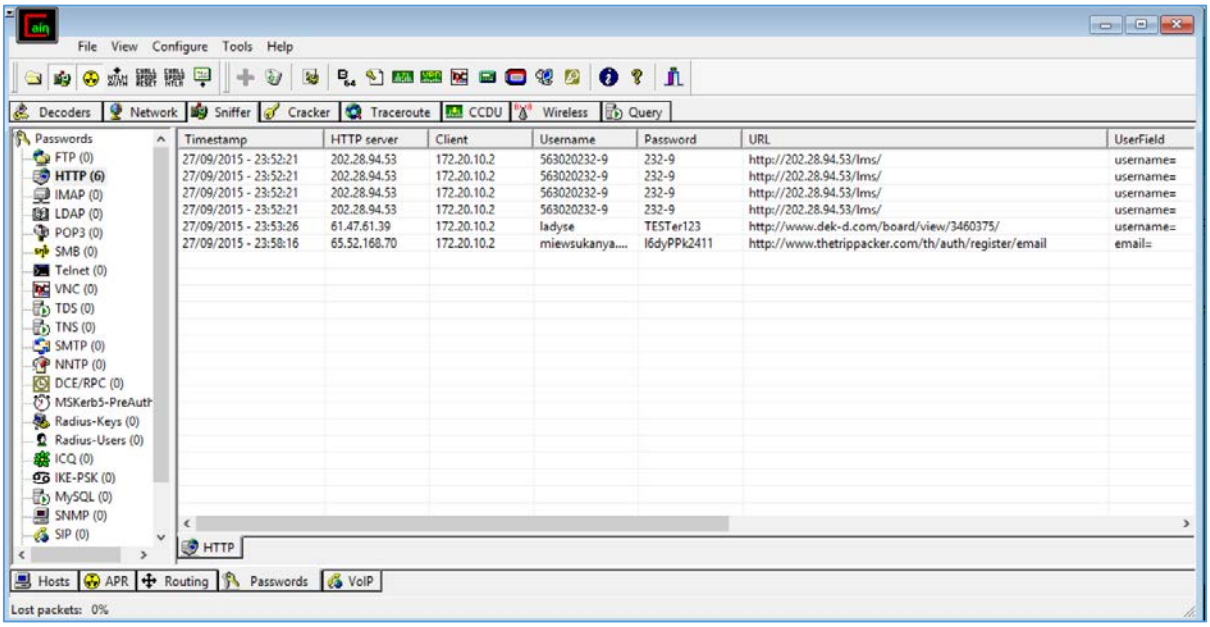
11. กดปุ่ม start/stop APR



12. ข้อมูลในเครื่องเป้าหมาย และกดที่ tab Password

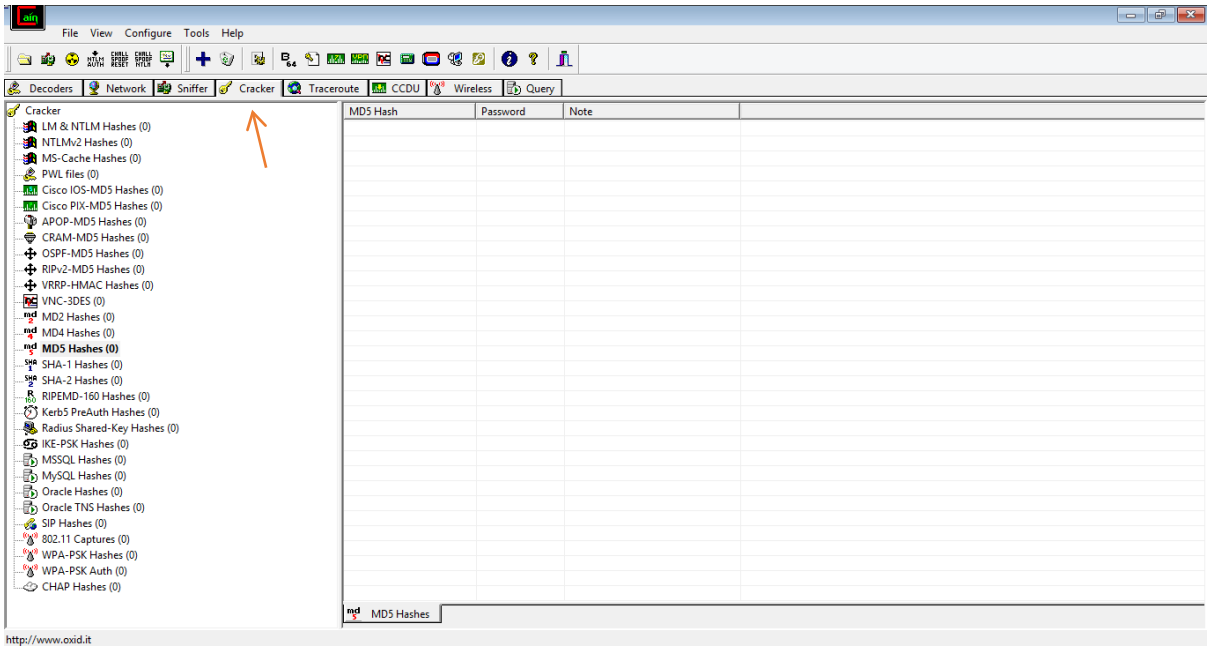


13. โปรแกรมจะแสดงข้อมูล username และ password ตามที่เครื่องเป้าหมายได้เข้าใช้ สามารถนำ username และ password นำไปเข้าสู่ระบบตามเว็บต่างๆที่แสดงได้

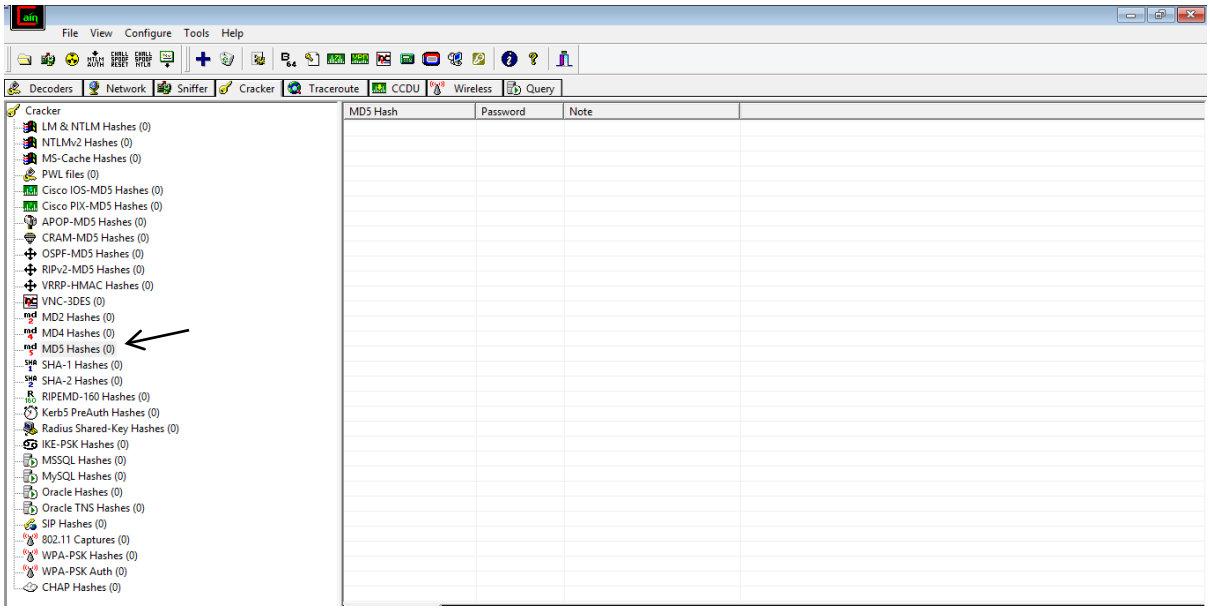


วิธีการ crack หา Plaintext โดย brute force attack

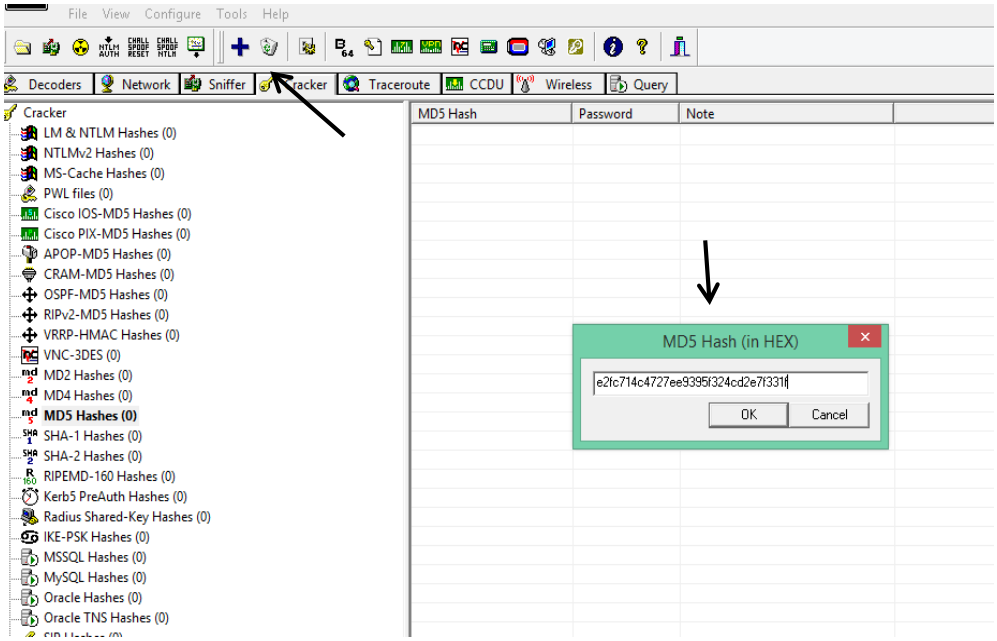
1. มาที่ tab cracker



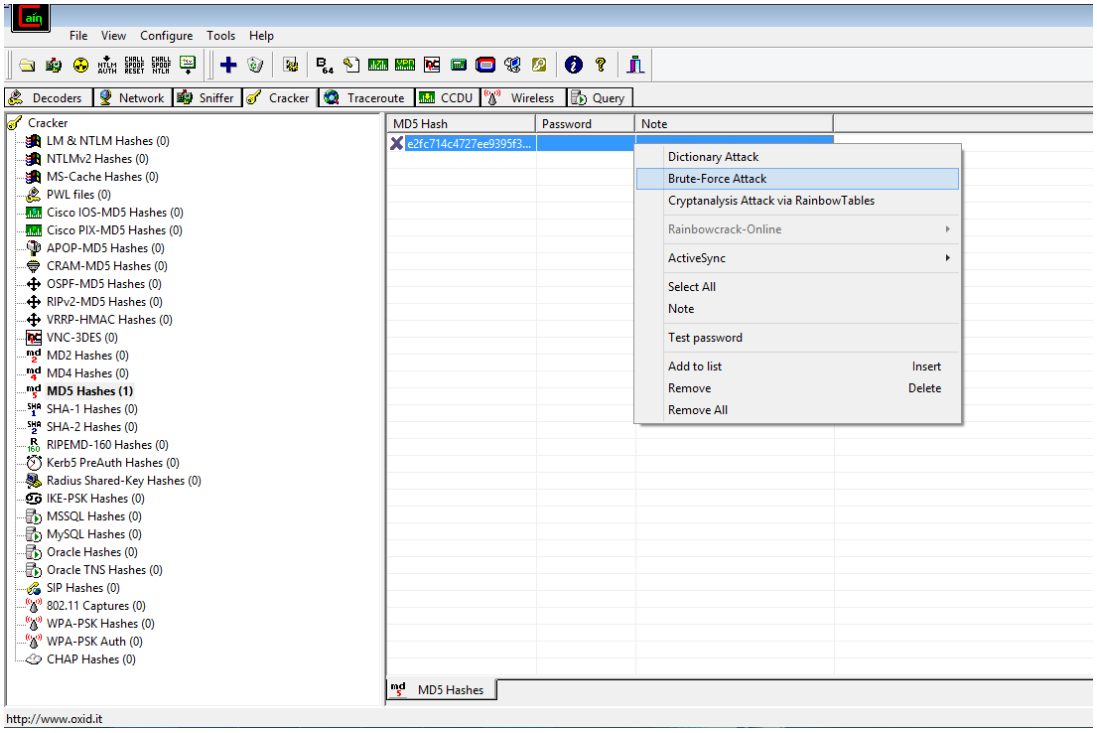
2. เลือกชนิดการเข้ารหัสที่ต้องการถอดหา Plaintext เช่น md5 hashes



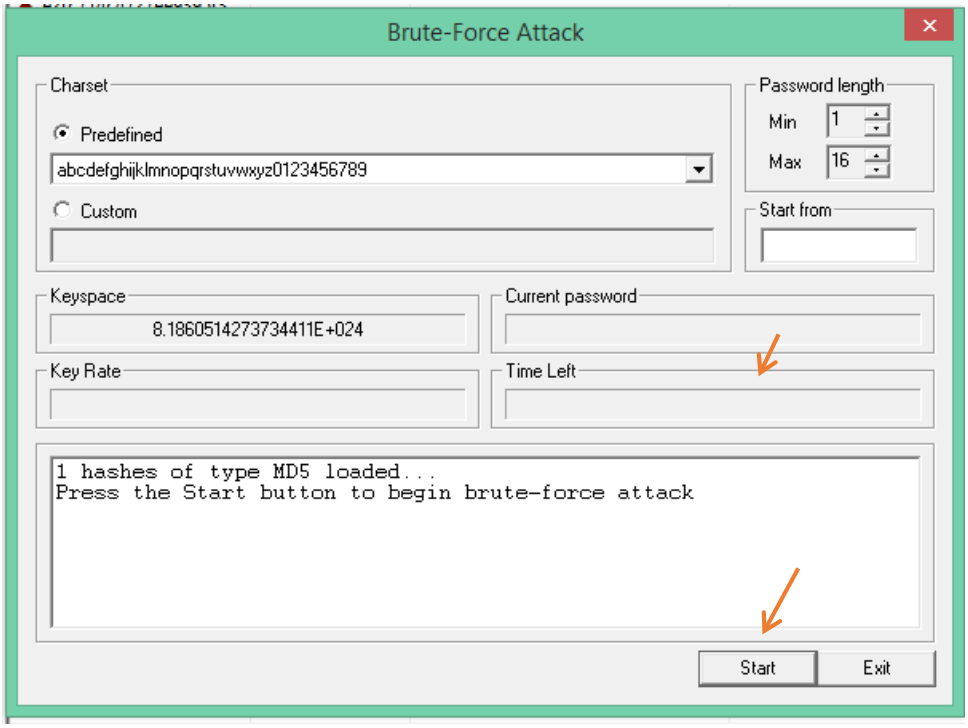
3. คลิกที่เครื่องหมายบวกก็จะมีกล่องข้อความขึ้นแล้วกรอกข้อความที่ต้องการถอดรหัส เช่น e2fc714c4727ee9395f324cd2e7f331f คลิก ok



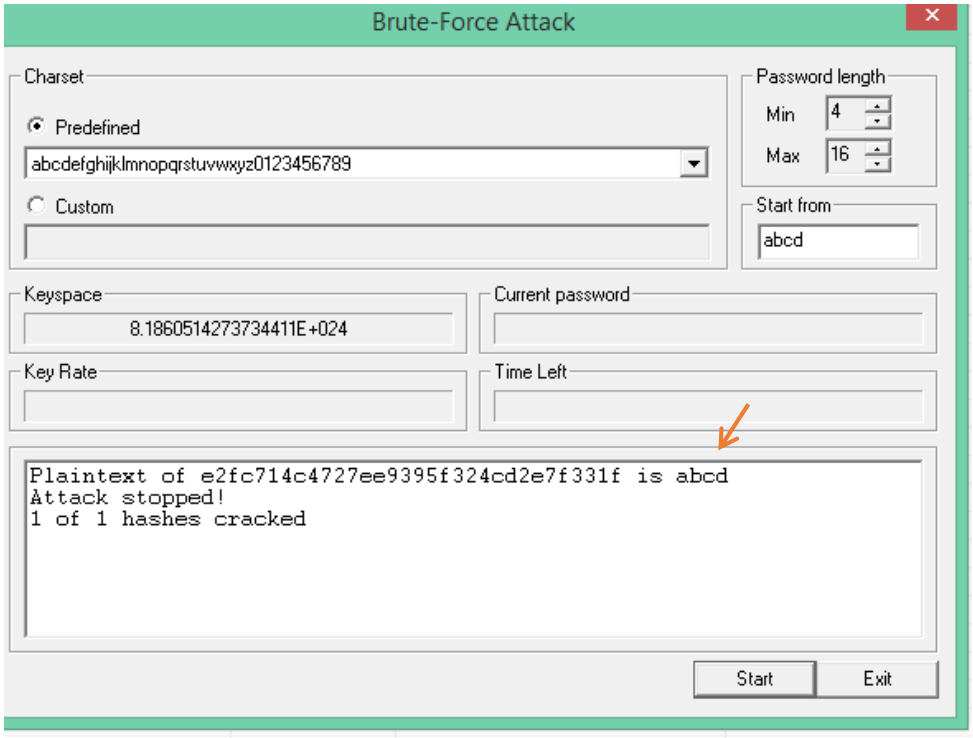
4. คลิกขวาที่ข้อความแล้วเลือก brute force attack



5. คลิกปุ่ม start



6. ก็จะได้Plaintext ของ e2fc714c4727ee9395f324cd2e7f331f ออกมาคือ abcd

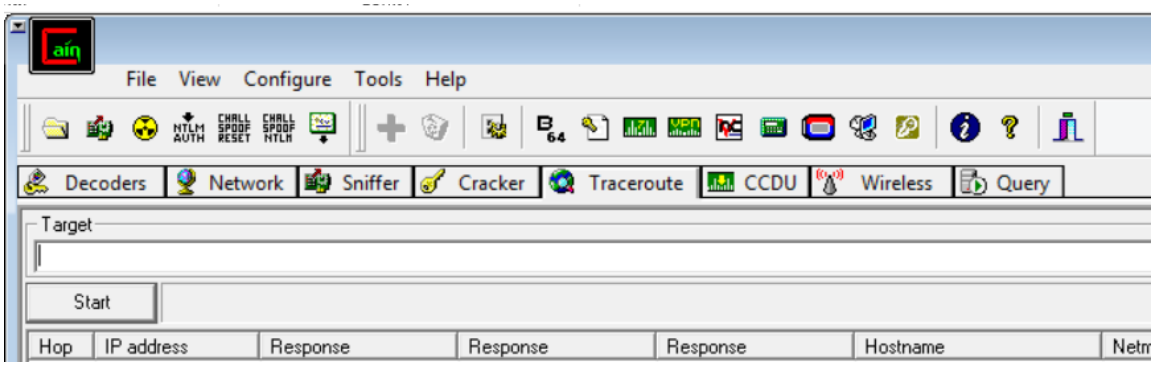


การติดตามดูเส้นทางโดย **Traceroute**

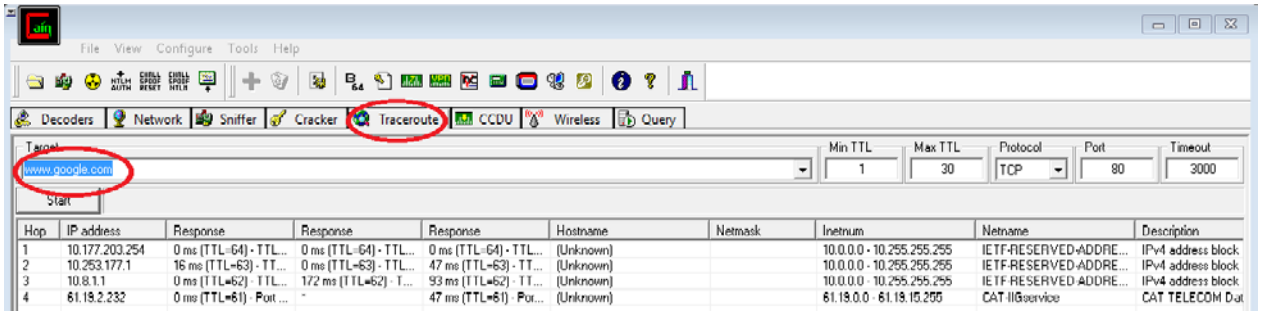
เป็นฟังก์ชันในการตรวจสอบการเส้นทางในการส่ง IP packets ระหว่างเครื่องคอมพิวเตอร์สองเครื่องและจำนวนเครื่อง routers ที่ IP packets ถูกส่งผ่าน โดยการใส่ IP Address หรือ ชื่อเว็บไซต์เป้าหมายที่ช่อง Target แล้วกดปุ่ม Start โดยจะแสดงข้อมูลดังนี้

- Hop คือ ลำดับของ Router ที่ถูกส่งผ่าน
- IP Address คือ หมายเลขประจำเครื่องของแต่ละ Router
- Response จะแสดงค่า TTL (Time to Live) คือเวลาที่ packet หนึ่ง สามารถอยู่บนระบบได้ เพื่อไม่ให้มี packet ตกค้างอยู่บนระบบ โดยให้หมดอายุไปเอง ถ้าไม่ถึงปลายทาง
- Hostname ชื่อของ Router
- Net name คือสตริงของอักขระที่กำหนดไว้ เพื่อใช้พิสูจน์ตัวตน Public Key และ Private key ซึ่งถูกเก็บตาม per-net-name
- Description อธิบายถึงเวอร์ชันของ Internet Protocol ที่ใช้

1. คลิกที่ tab Traceroute และใส่ IP Address หรือ ชื่อเว็บไซต์เป้าหมายที่ช่อง Target

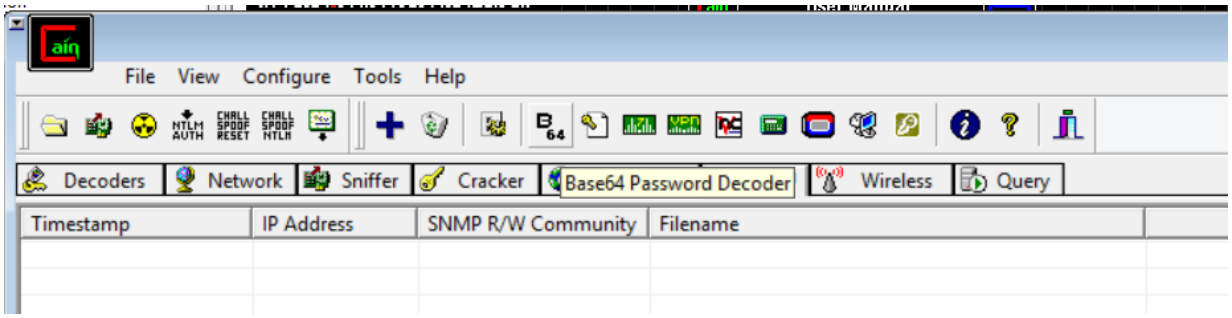


2. โปรแกรมจะแสดงข้อมูลต่างๆ ดังภาพ

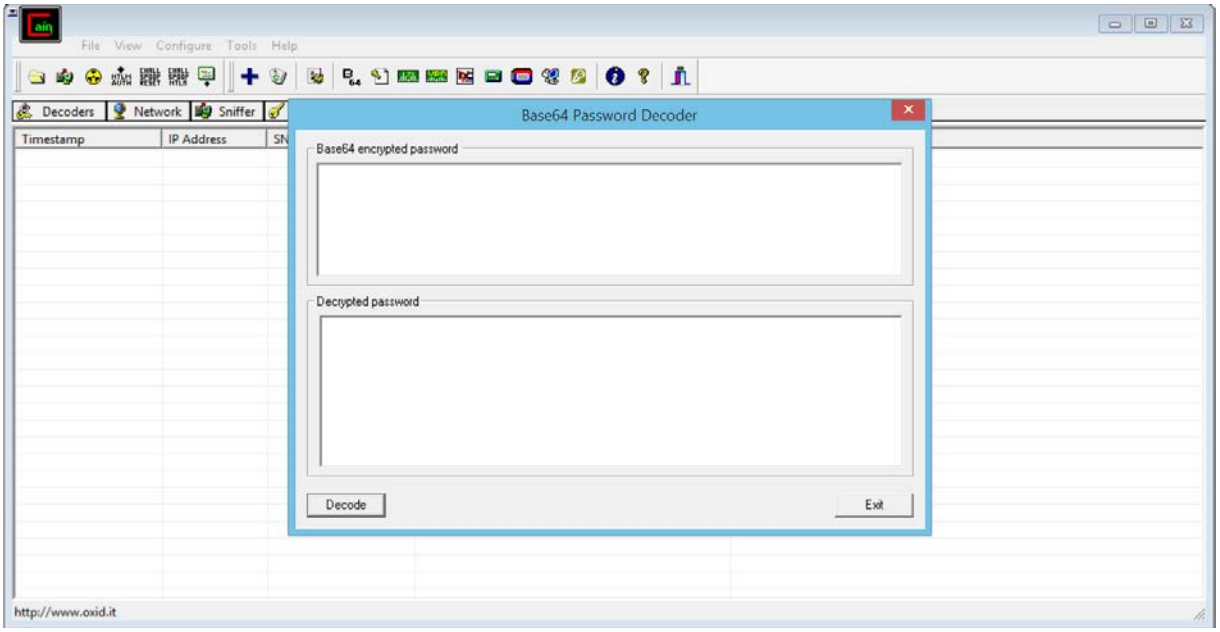


การเข้ารหัส ถอดรหัส

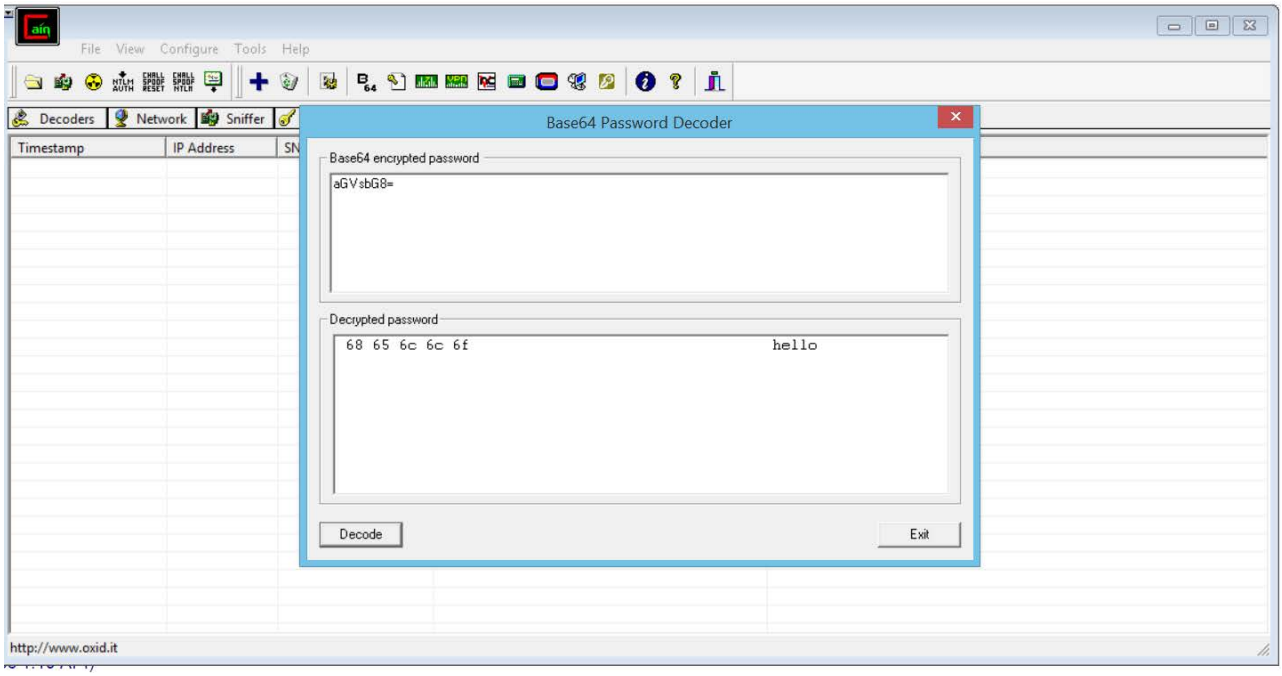
1.คลิกที่ปุ่ม Base64 Password Decoder



2.มีหน้าต่างขึ้นมาดังรูป

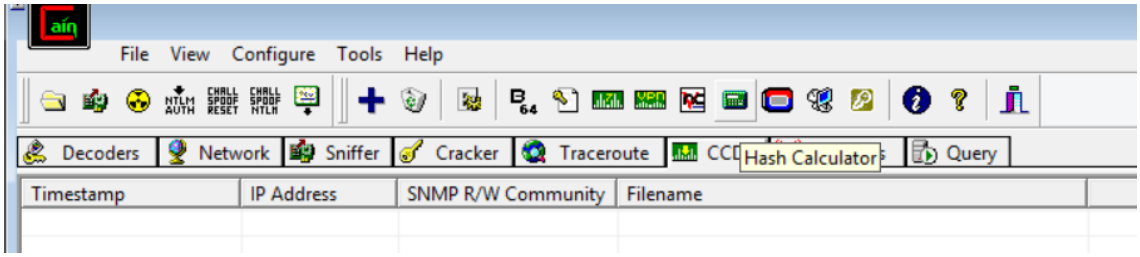


3. ใส่ text ที่จะ Encrypted ประเภท base64 เข้าไป และจะได้ข้อความออกมา

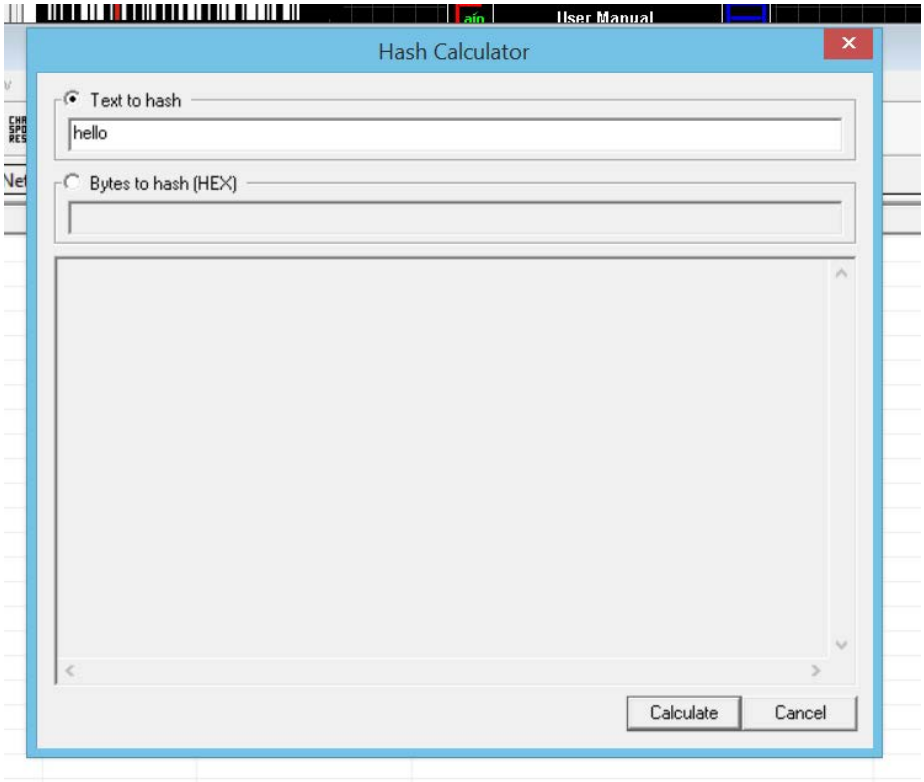


Hash Calculator

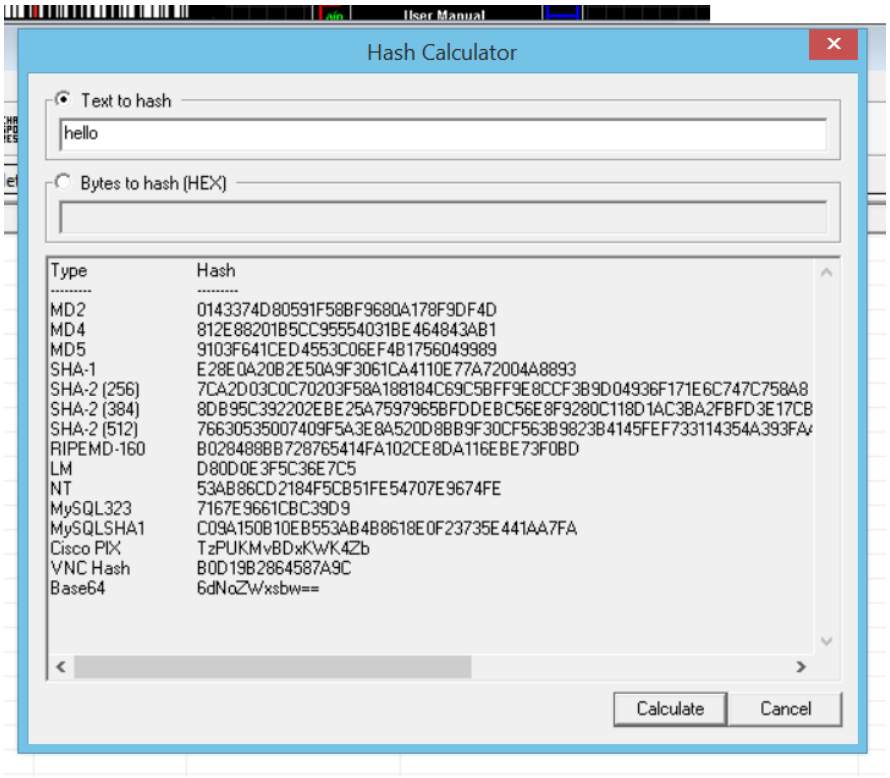
1.เข้าที่ปุ่ม Hash Calculator



2.พิมพ์ text เข้าไป

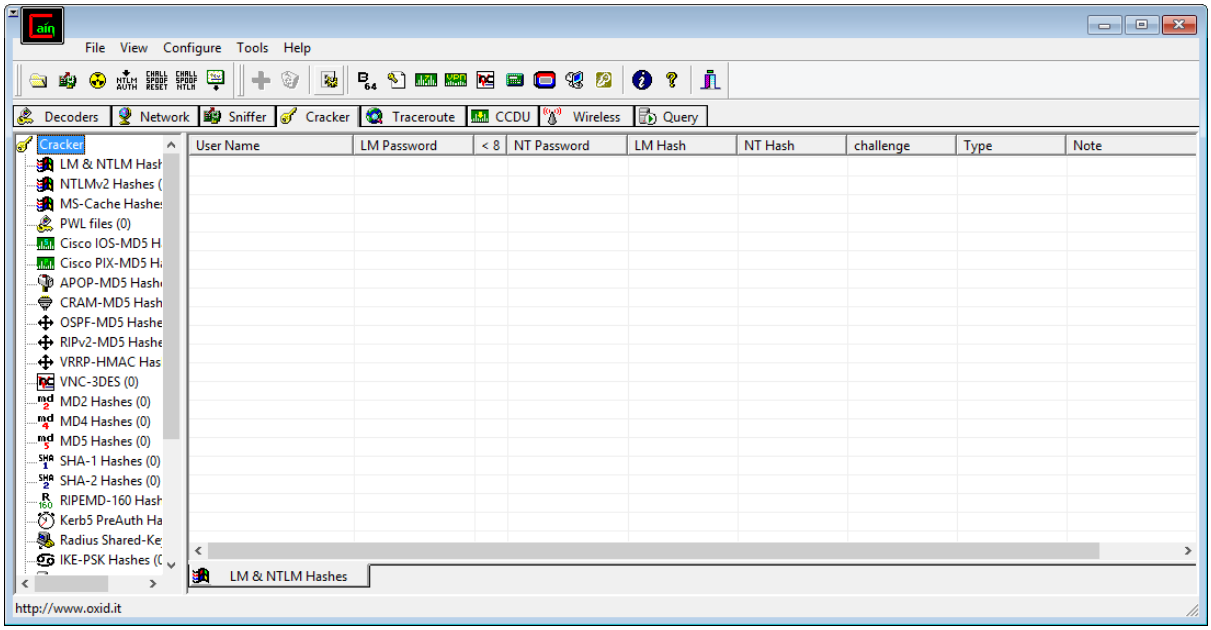


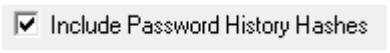
3.จะได้การเข้ารหัสแต่ละประเภทออกมา



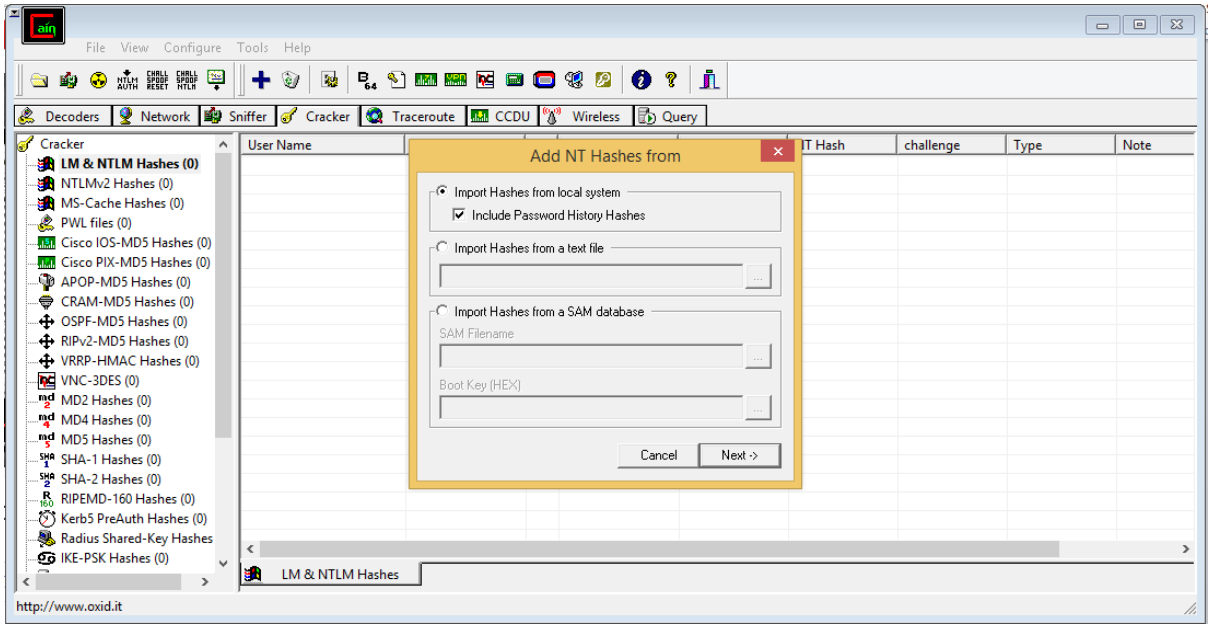
การทำ Password Recovery

1. เปิดโปรแกรม Cain and Abel เลือกที่ tab Cracker

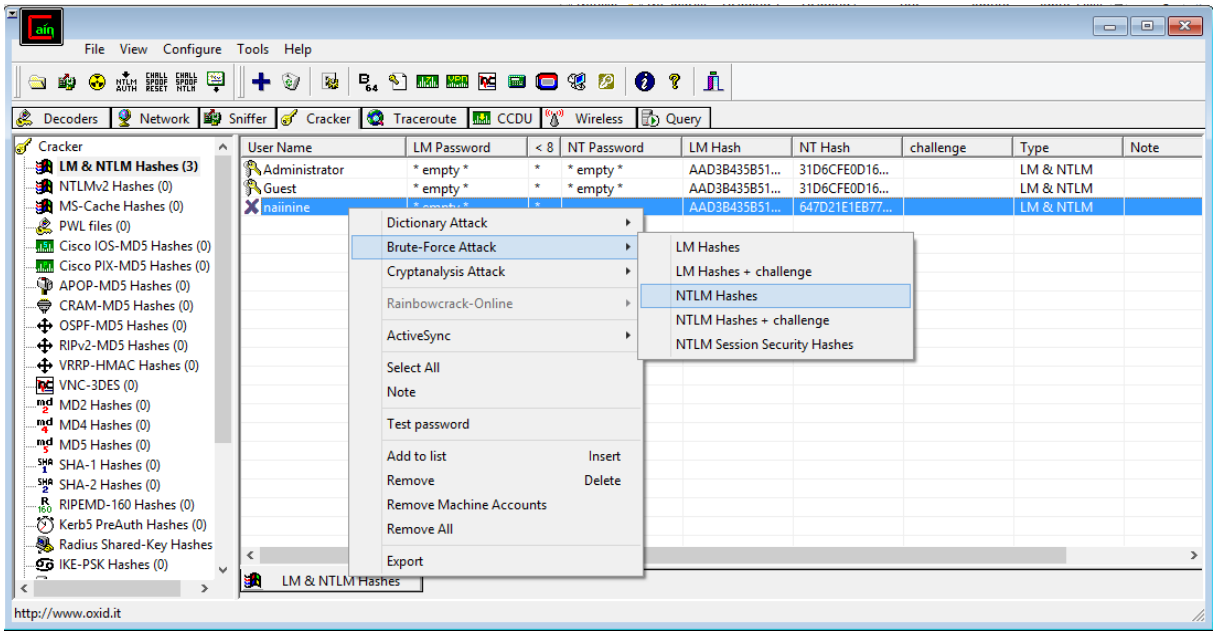


2. เลือกแถบเมนู LM & NTLM Hasher เลือกปุ่ม  จะปรากฏหน้าต่างดังรูป เลือกปุ่ม 

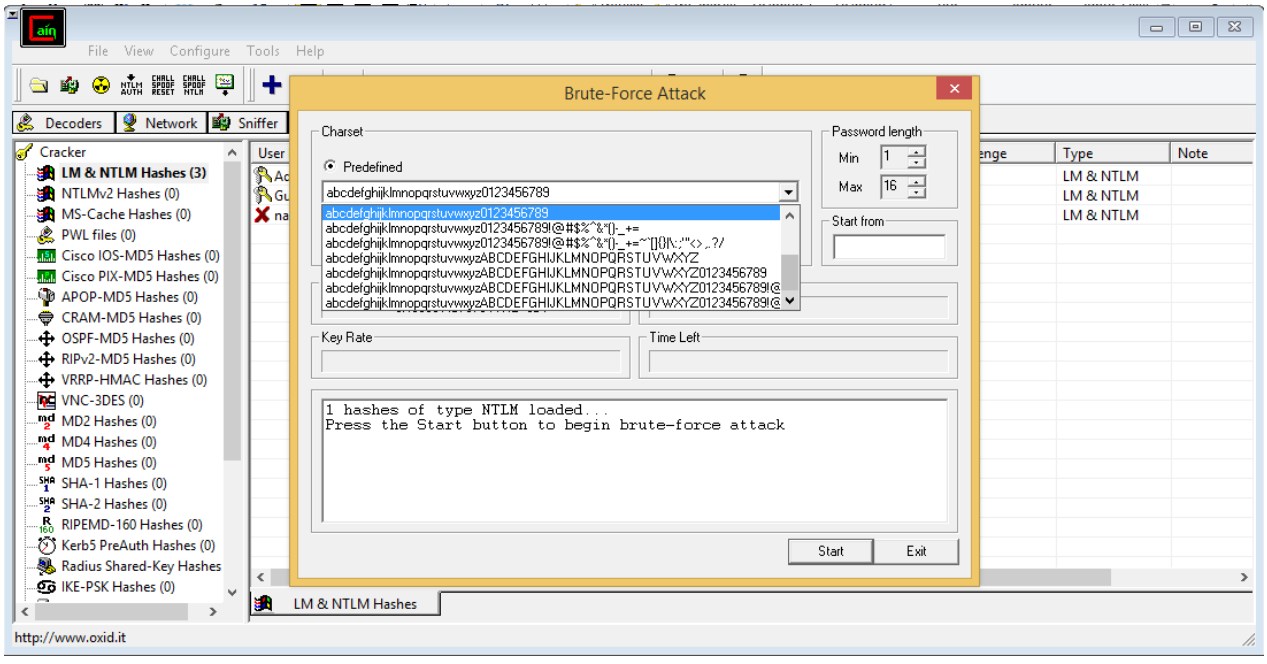
แล้วกด Next



3. จะปรากฏหน้าต่าง ของไฟล์ ของ dummy account ที่เก็บ password ที่เคยลบทิ้งไป โดยปรากฏเป็นรูป naiinine แล้วคลิกขวาที่รูปดังกล่าว เลือกแถบ Brute-Force Attack กด เลือก NTLM Hashes



4. จะปรากฏหน้าจอดังนี้ โดยสามารถเลือกชนิดข้อมูลของ password ที่ลบทิ้งไปได้ตามความต้องการ ในที่นี้เลือกแบบ acbdefghijklmnopqrstuvwxyz0123456789 แล้วกดปุ่ม start



5. จะปรากฏหน้าจอเดียวกัน ที่แสดงเป็นรหัสผ่าน ที่เราเคยลืมไว้