Information and communication Technology Security

ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร

ผู้จัดทำ

1.นายจิรวัฒน์	สกุลวานิชเจริญ	573021386-8
2.นายพงศธร	กาบจันทร์	573020812-2
3.นางสาวสุภัทธา	เภกะสุต	573020829-5
4.นางสาวเอื้อมเดือน	ฮาดดา	573020835-0
5.นางสาวอรทัย	ประเสริฐโส	573020832-6

อาจารย์ที่ปรึกษา รศ.ดร.จักรชัย โสอินทร์

ภาคเรียนที่ 1 ปีการศึกษา 2559

ภาควิชาวิทยาการคอมพิวเตอร์ สาขาเทคโนโลยีสารสนเทศและการสื่อสาร

คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

หลักการและเหตุผล

ในปัจจุบันมีการเข้าถึงอินเตอร์เน็ตได้ง่ายมากขึ้น โดยทั่วทุกมุมโลกสามารถใช้อินเตอร์เน็ตในหลายด้านแตกต่างกันออกไปทั้งถูกทางและไม่ถูกทาง อินเตอร์เน็ตทำให้เกิดความสะดวกและรวดเร็วมากขึ้นสำหรับผู้ใช้งาน อีกทั้งยังมีการพัฒนาซอฟต์แวร์และฮาร์ดแวร์ขึ้นอย่างมากมายที่ใช้เป็นเครื่องมือในหลายๆด้านรวมถึงในด้านการรักษาความปลอดภัยของระบบ การถูกคุกคาม ซอฟต์แวร์ที่ติดตั้งเป็นระบบรักษาความปลอดภัยมีการเริ่มใช้อย่างแพร่หลายในปัจจุบัน หากใช้ในทางที่ผิดก็อาจจะทำให้เกิดความผิดพลาดและเกิดความเสียหายได้ ซึ่งปัจจุบันมีอาชญากรแอบแฝงมากมายอาจจะไล่ตามข้อมูลไปทำสิ่งที่ไม่ดี อย่างเช่น พวกเขามักจะใช้คอมพิวเตอร์จำนวนมากเพื่อทำให้เว็บไซต์ล่มหรือละเมิดระบบรักษาความปลอดภัยของเว็บไซต์ หรือแม้แต่ดึกจับรหัสของเราเพื่อค้นเอาข้อมูลลับอีกด้วย

วัตถุประสงค์

1. เพื่อศึกษาวิธีการหรือขั้นตอนการทำงานของโปรแกรม Cain & Abel
2. เพื่อศึกษาการโจมตี web Security
3. เพื่อตรวจสอบความแข็งแกร่งของรหัสผ่าน
4. เพื่อทำการทดสอบการดักจับข้อมูลรหัสผ่านจากเครือข่าย
5. เพื่อใช้ในรายวิชา 322376 Information and communication Technology Security

งานวิจัยที่เกี่ยวข้อง

1. **โปรแกรม : Saf etyPass**

ผู้จัดทำ นางสาวทันยา เสมอภาค และคณะ

ที่มา : http://csperson.kku.ac.th/chakchai/images/322376_2015/g17_safe_password.jpg

2. **โปรแกรม : KKU Internet Authen**

ผู้จัดทำ นายศรัณย์ พงโสภณ และคณะ

ที่มา : http://csperson.kku.ac.th/chakchai/images/322376_2015/g10_kku_authen.jpg

ขั้นตอนการติดตั้งโปรแกรม Cain & Abel

ทำการดาวน์โหลดโปรแกรม Cain & Abelที่ http://www.oxid.it/cain.html

การติดตั้ง Cain and Abel นั้น จะแบ่งออกเป็น 2 ขั้นตอนด้วยกัน คือ ติดตั้งโปรแกรม Cain and Abel และติดตั้ง WinPCAP (จะรวมอยู่ในชุดติดตั้ง Cain and Able อยู่แล้ว) ซึ่งจำเป็นสำหรับการใช้งานในแบบ sniffer เพื่อทำการดักข้อมูลจากเครือข่าย โดยวิธีการติดตั้ง มีดังนี้

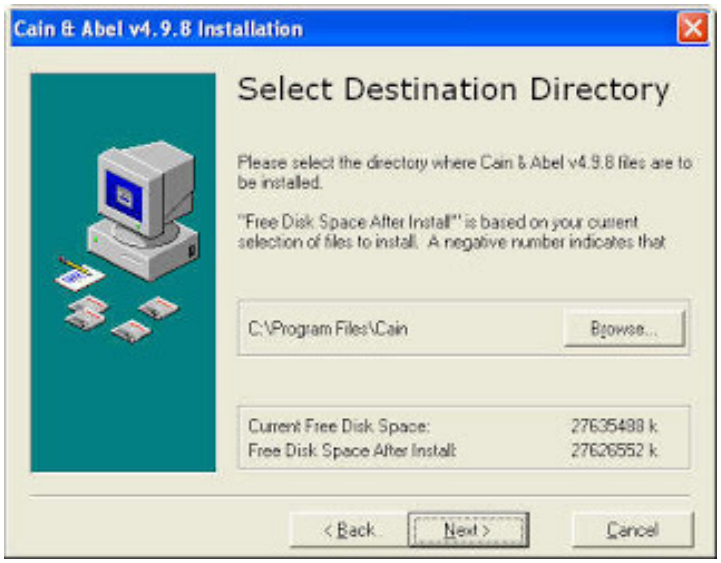
1. ที่โฟลเดอร์ซึ่งเก็บไฟล์ที่ดาวน์โหลดมา ให้ทำการดับเบิลคลิกไฟล์ CA_Setup.exe ซึ่งจะได้หน้าไดอะล็อกดังรูปที่ 1

รูปที่ 1 Cain and Abel Installation

2.ที่หน้าไดอะล็อกดังรูปที่ 1 ให้คลิก Next เพื่อเริ่มทำการติดตั้งโปรแกรม ซึ่งจะได้หน้าไดอะล็อกดังรูปที่ 2

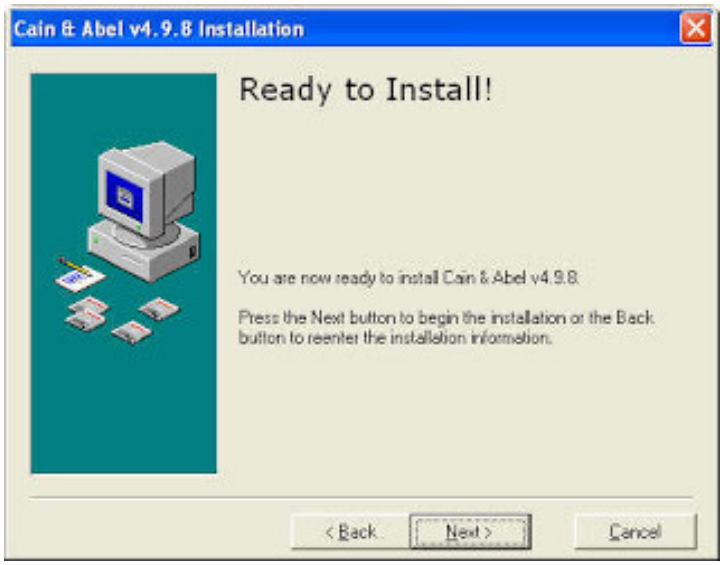
รูปที่ 2 License Agreement

3. ทีหน้าไดอะล็อก License Agreement ดังรูปที่ 2 ให้คลิก next



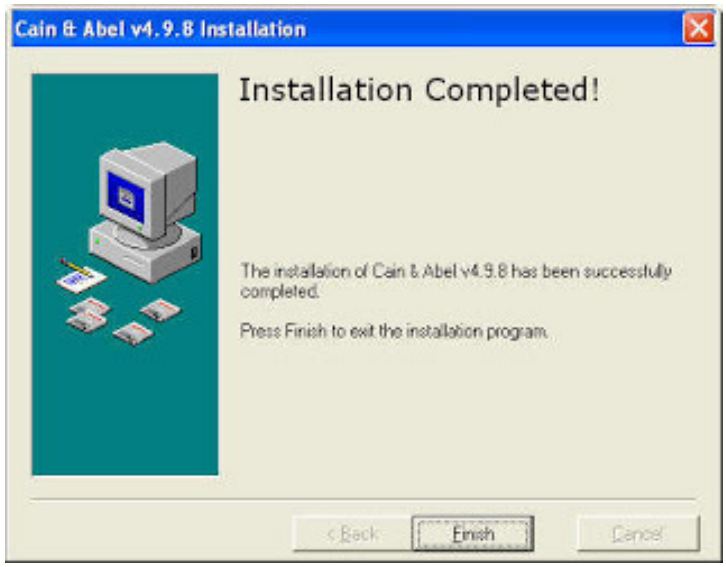
รูปที่ 3 Select Destination

4. ที่หน้าไดอะล็อกดังรูปที่ 3 ให้เลือกตำแหน่งที่จะติดตั้งโปรแกรม (ค่าดีฟอลท์เป็น C:\Program Files\Cain) เสร็จแล้วให้คลิก Next



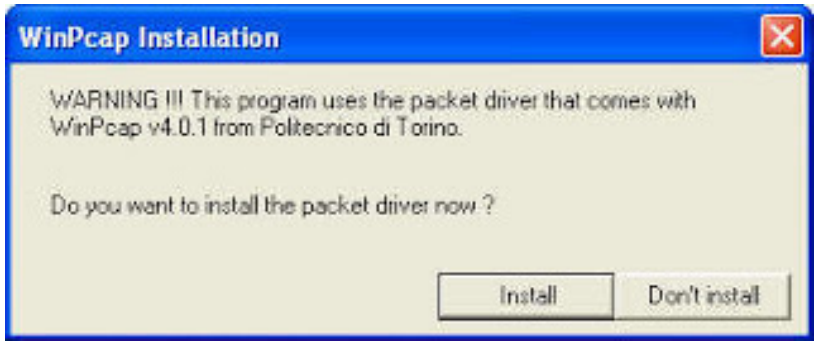
รูปที่ 4 Ready to Install

5. ที่หน้าไดอะล็อกดังรูปที่ 4 ให้คลิก Next เพื่อทำการติดตั้งโปแกรม รอจนการติดตั้งแล้วเสร็จ ซึ่งจะได้หน้าไดอะล็อกดังรูปที่ 5 ให้คลิก Finish เพื่อจบการติดตั้งโปรแกรม Cain and Abel



รูปที่ 5 Install Completed

6. จากนั้นระบบจะถามว่าต้องการติดตั้ง WinPcap หรือไม่ ดังไดอะล็อกรูปที่ 6 ให้คลิกปุ่ม Install หากต้องการใช้งานแบบการดักจับข้อมูลจากเครือข่าย หากไม่ต้องการให้คลิกปุ่ม Don't Install

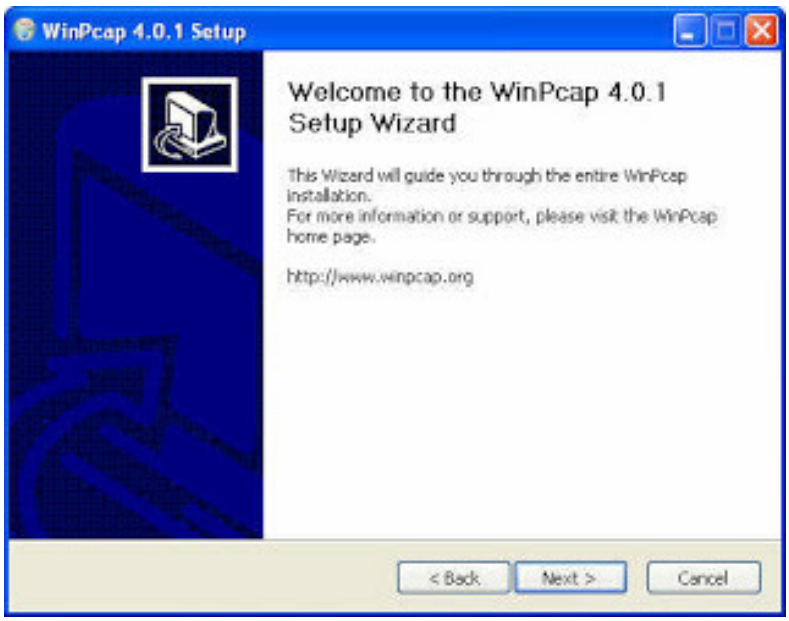


รูปที่ 6 WinPcap Installation

7. ที่หน้าไดอะล็อก WinPcap 4.0.1 Setup ดังรูปที่ 7 ให้คลิก Next เพื่อทำการติดตั้ง WinPcap

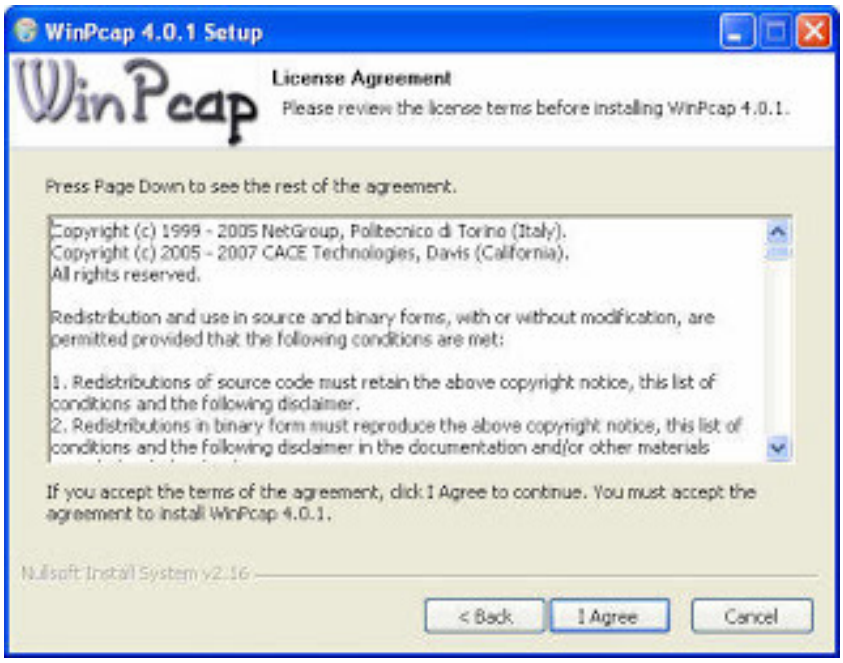
รูปที่ 7 WinPcap 4.0.1 Setup

8. ที่หน้าไดอะล็อก Setup wizard ดังรูปที่ 8 ให้คลิก Next เพื่อเริ่มทำการติดตั้ง WinPcap

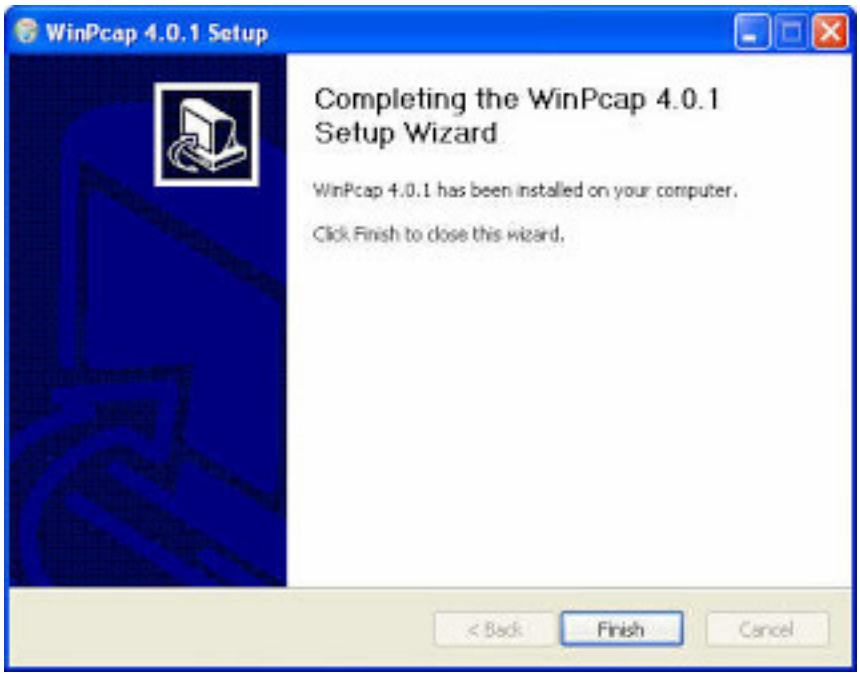


รูปที่ 8 WinPcap Setup wizard

9. ที่หน้าไดอะล็อก License Agreement ดังรูปที่ 9 ให้คลิก I Agree เพื่อเริ่มทำการติดตั้ง WinPcap แล้วรอจนการติดตั้งแล้วเสร็จ ซึ่งจะได้หน้าไดอะล็อกดังรูปที่ 10 ให้คลิก Finish เพื่อจบการติดตั้งโปรแกรม WinPcap



รูปที่ 9 License Agreement

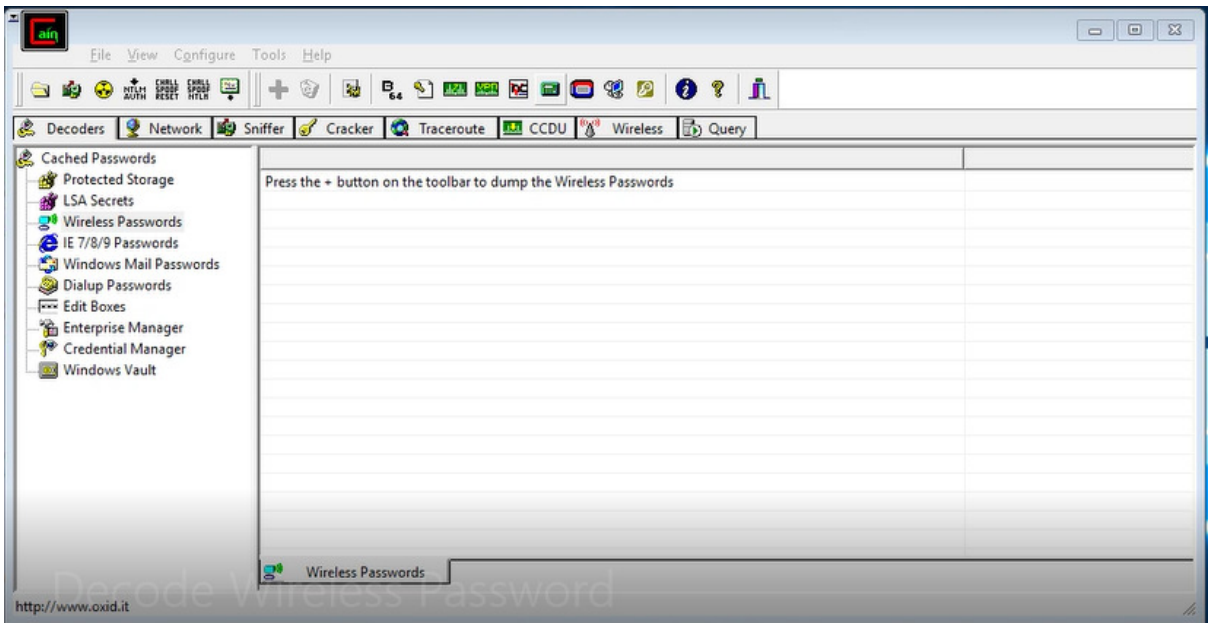


รูปที่ 10 Install Completed

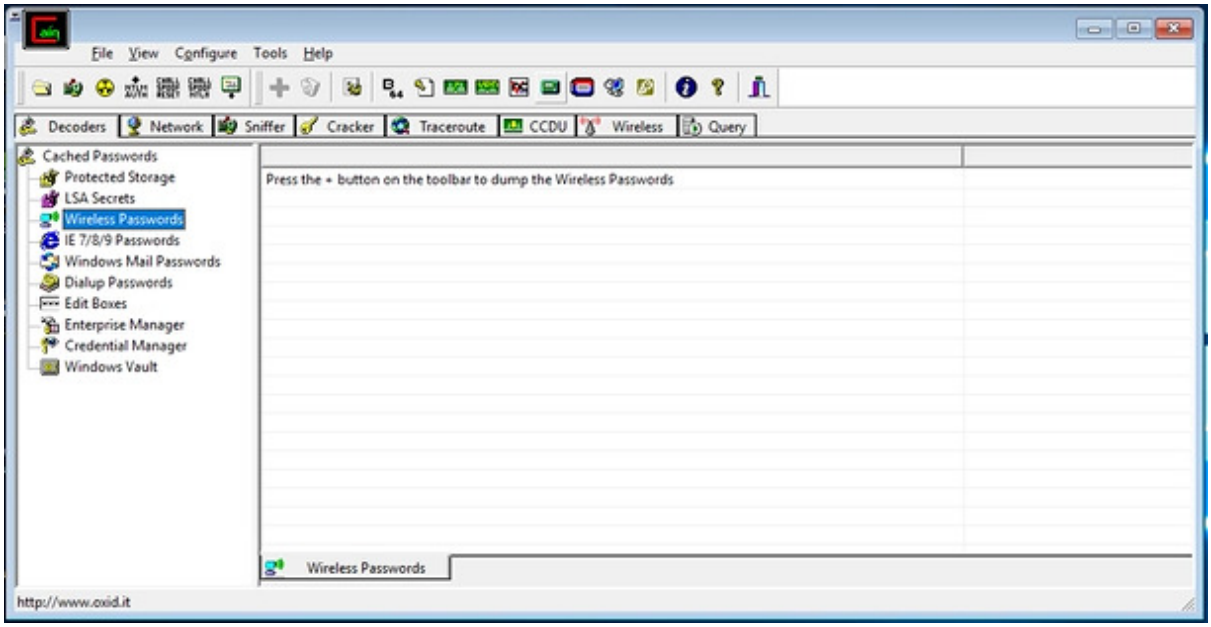
ขั้นตอนวิธีการใช้โปรแกรม

ขั้นตอนการใช้เมนู Decode Wireless Password

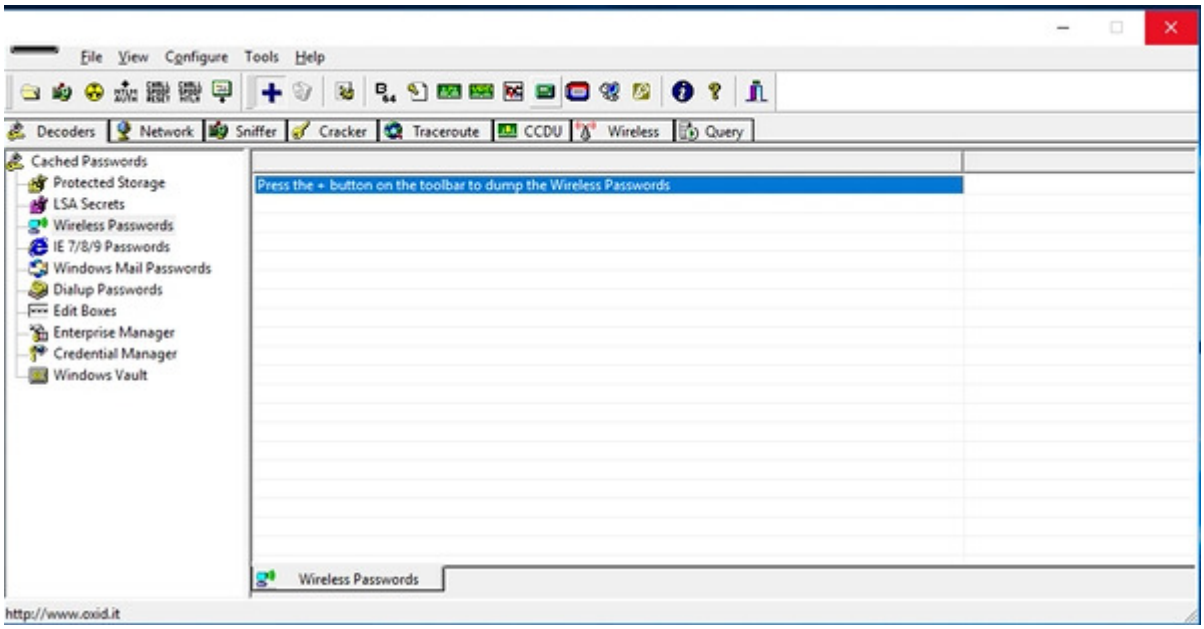
1. เปิดโปรแกรม Cain & Abel โดยดับเบิลคลิกที่ไอคอนของโปรแกรม ซึ่งจะได้หน้าต่างโปรแกรม



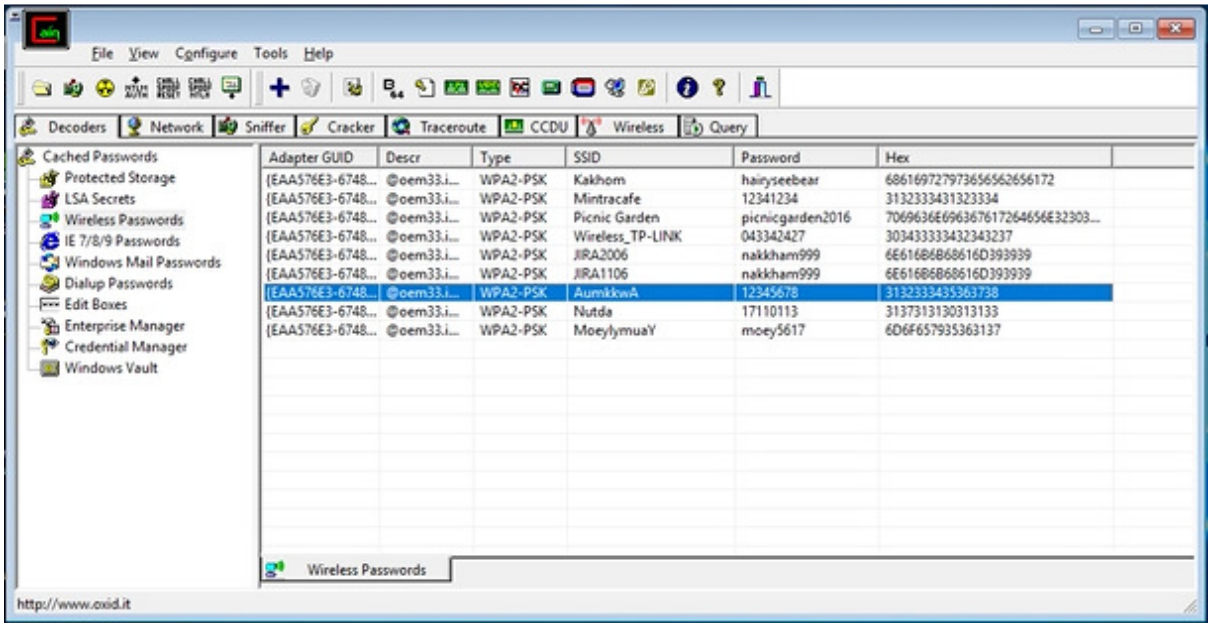
2.เลือกไปที่เมนู Wireless Password แทบซ้ายมือ



3.คลิกไปที่พื้นที่ว่างด้านขวาแล้วคลิกที่ ปุ่ม add to list

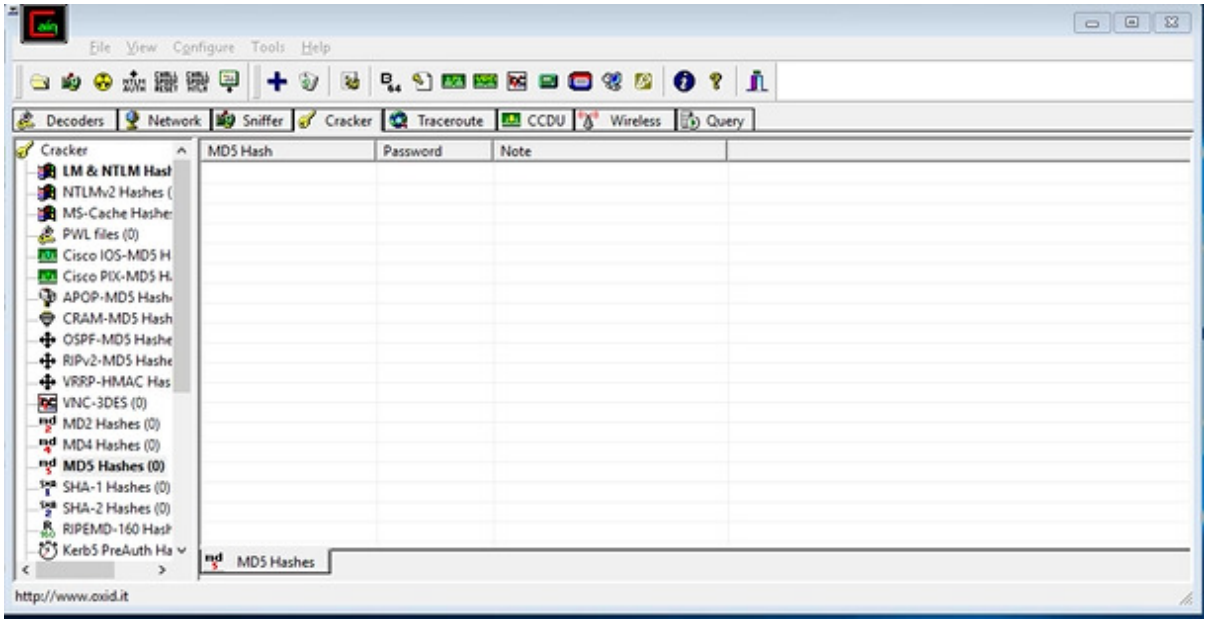


4.หน้าจอจะแสดง SSID และ Password ของWi-Fi ที่เครื่องนี้เคยเข้าใช้

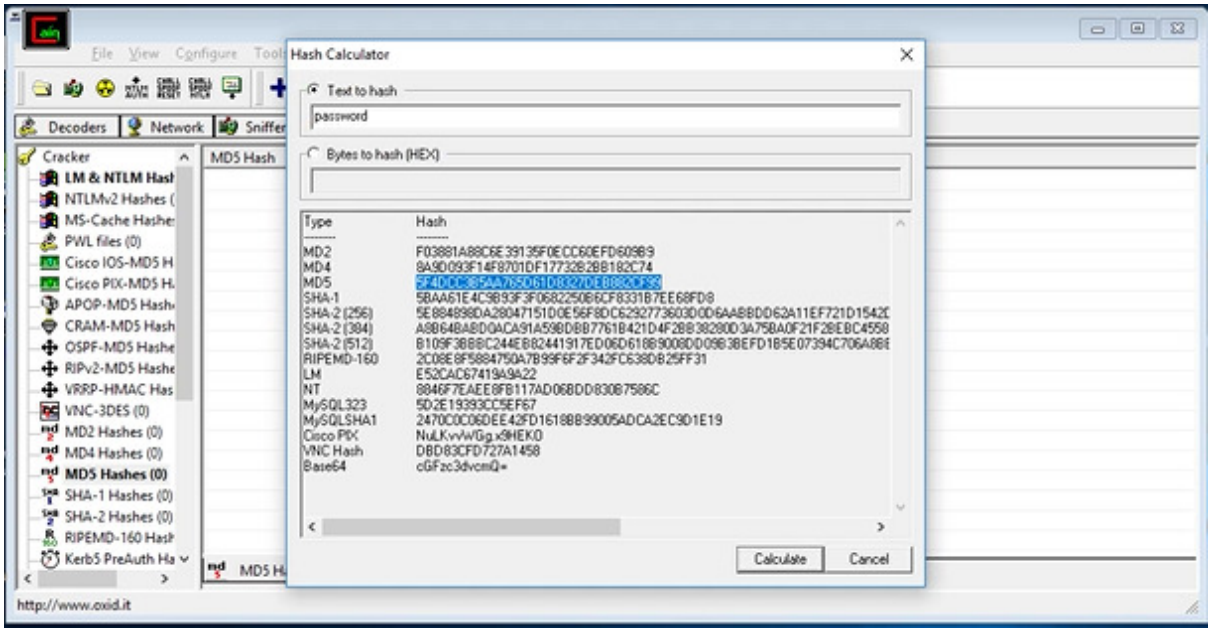


ขั้นตอนการใช้เมนู Crack Dictionary

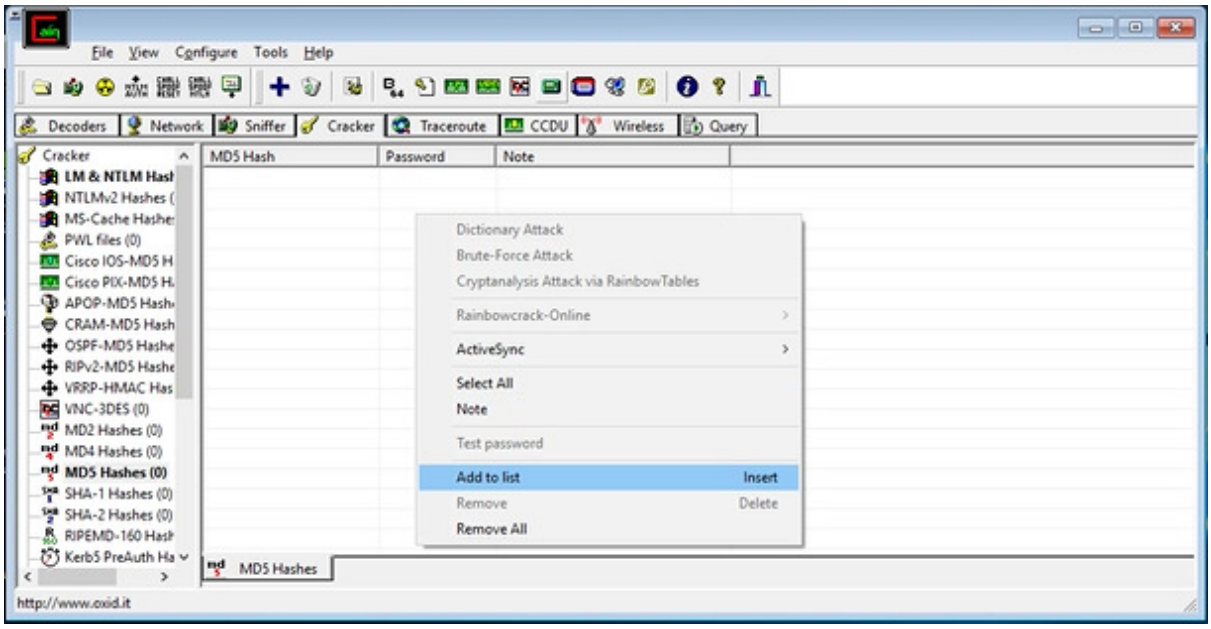
1.คลิกไปที่ Cracker เมนูบนแทบด้านบน จากนั้นคลิกไปที่ Hash Calculator 



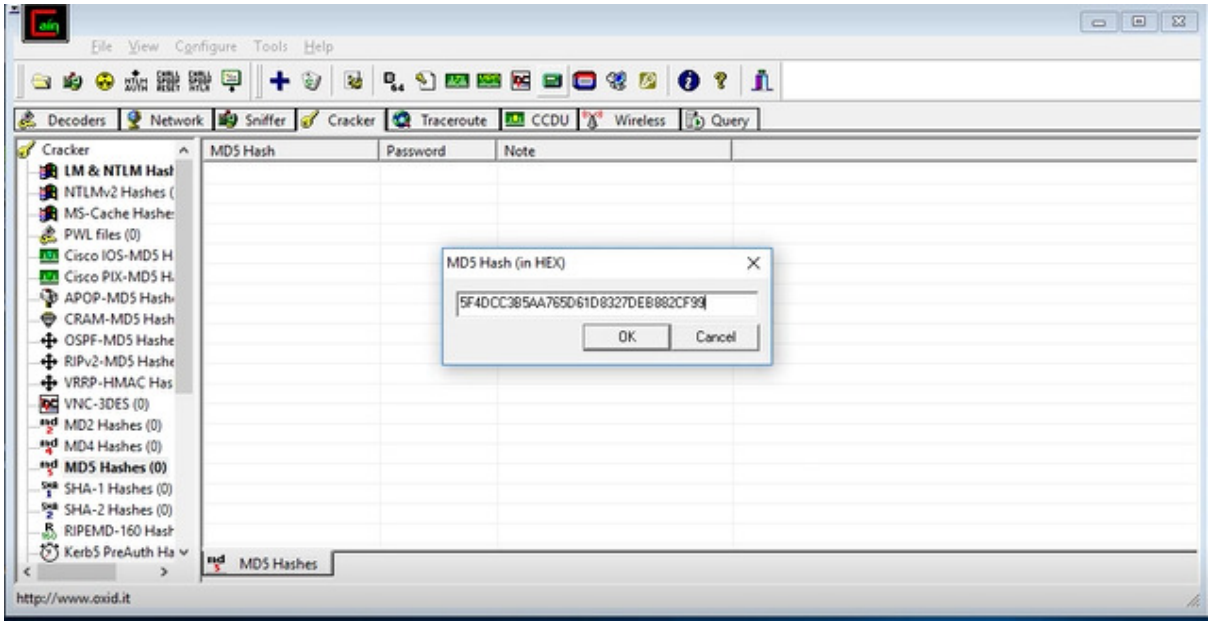
2.ใส่รหัสแบบง่ายๆ จากนั้นจะถอดรหัสออกมา Copy Hash ของ Type MD5 แล้วกด Calculate



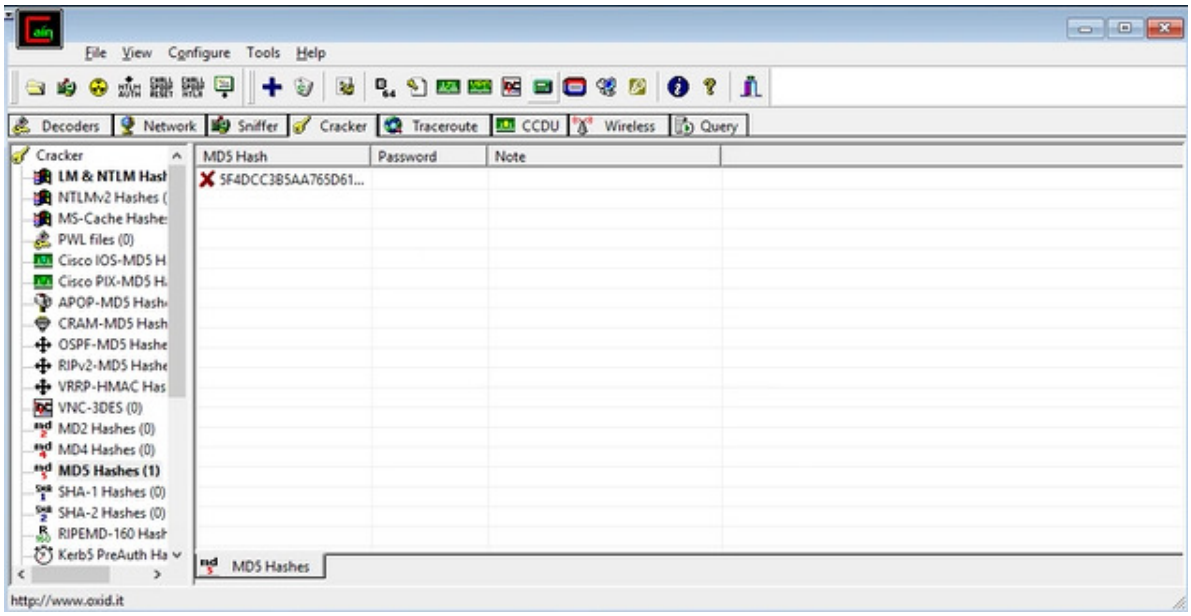
3.จากนั้นคลิกขวาตรงพื้นที่ว่าง และเลือก Add to list



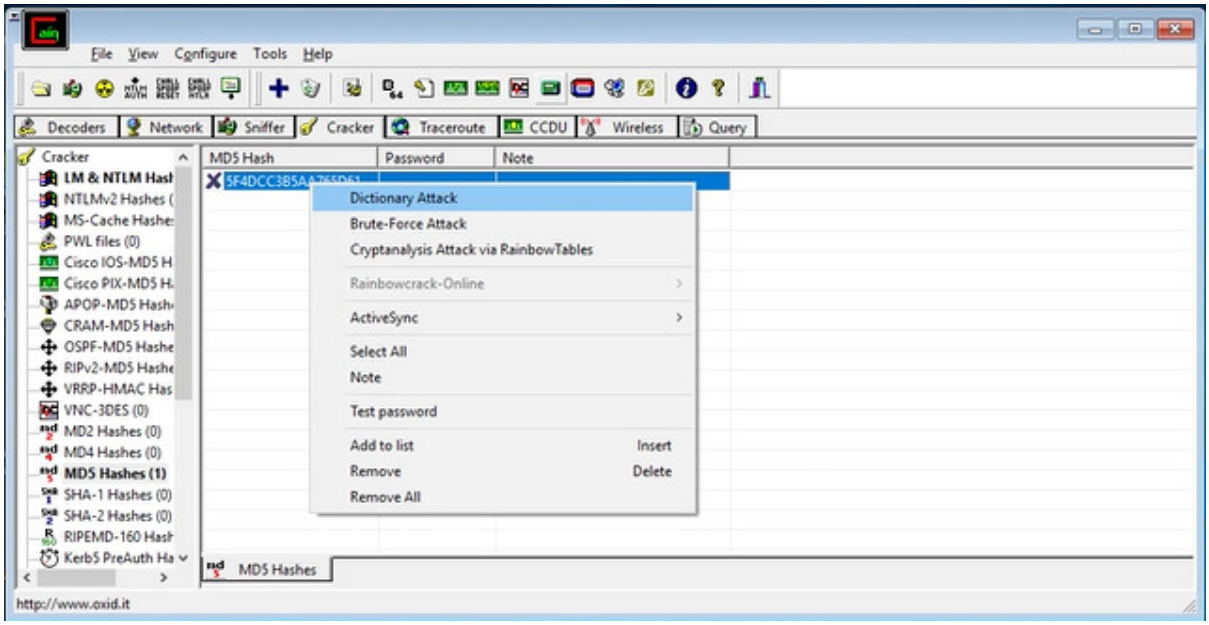
4.วางรหัสที่เรา Copy มา แล้วกด OK



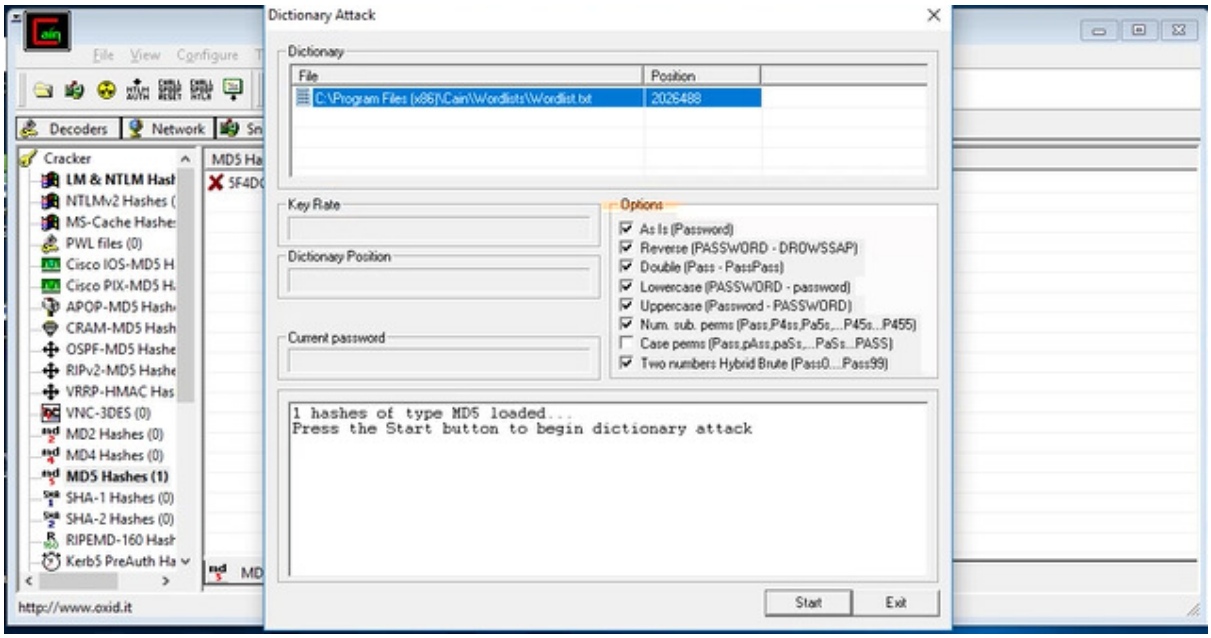
5.หน้าจอจะแสดง รหัสที่ช่องMD5 Hash



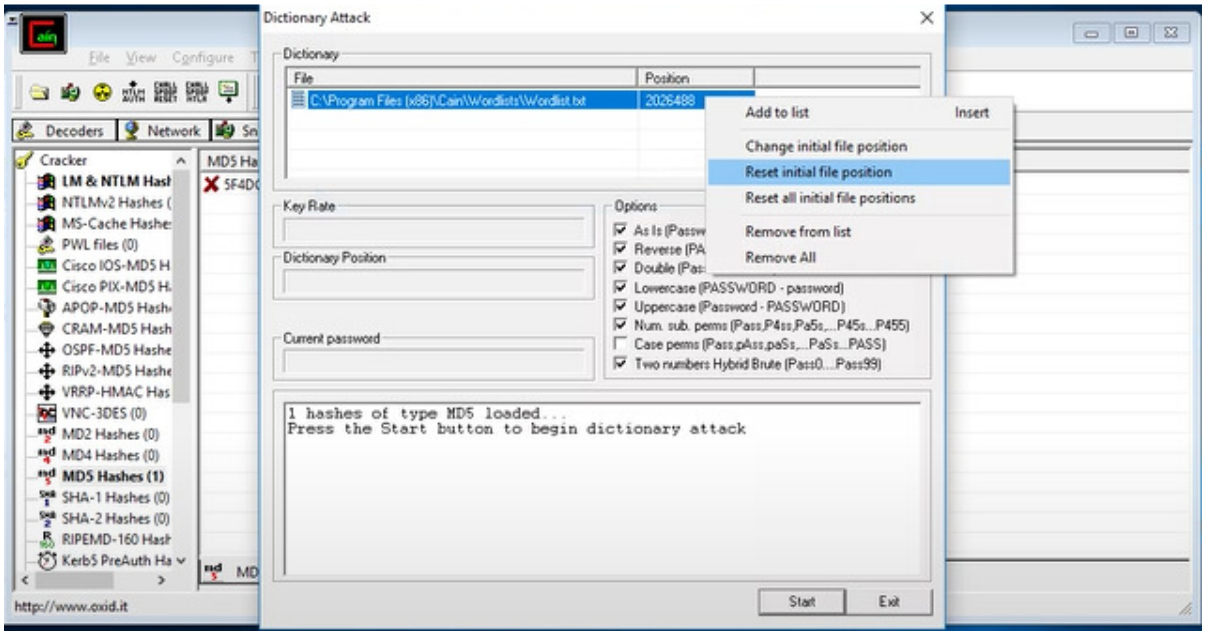
6.คลิกขวา แล้วเลือก Dictionary Attack



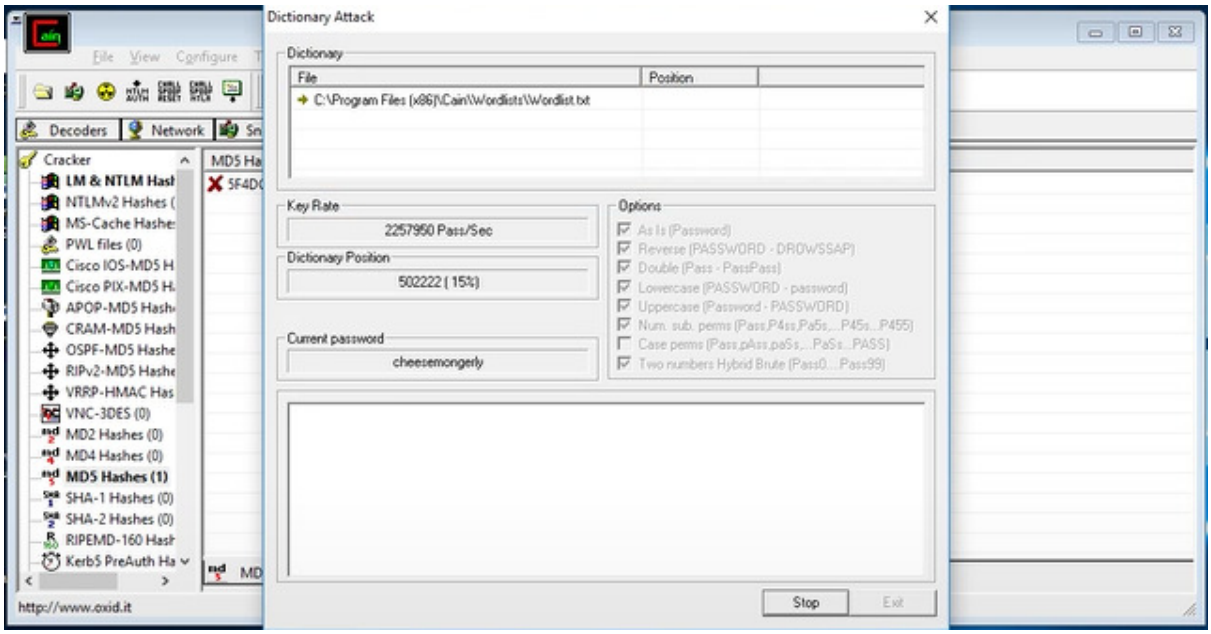
7.หน้าจอจะแสดงแบบนี้



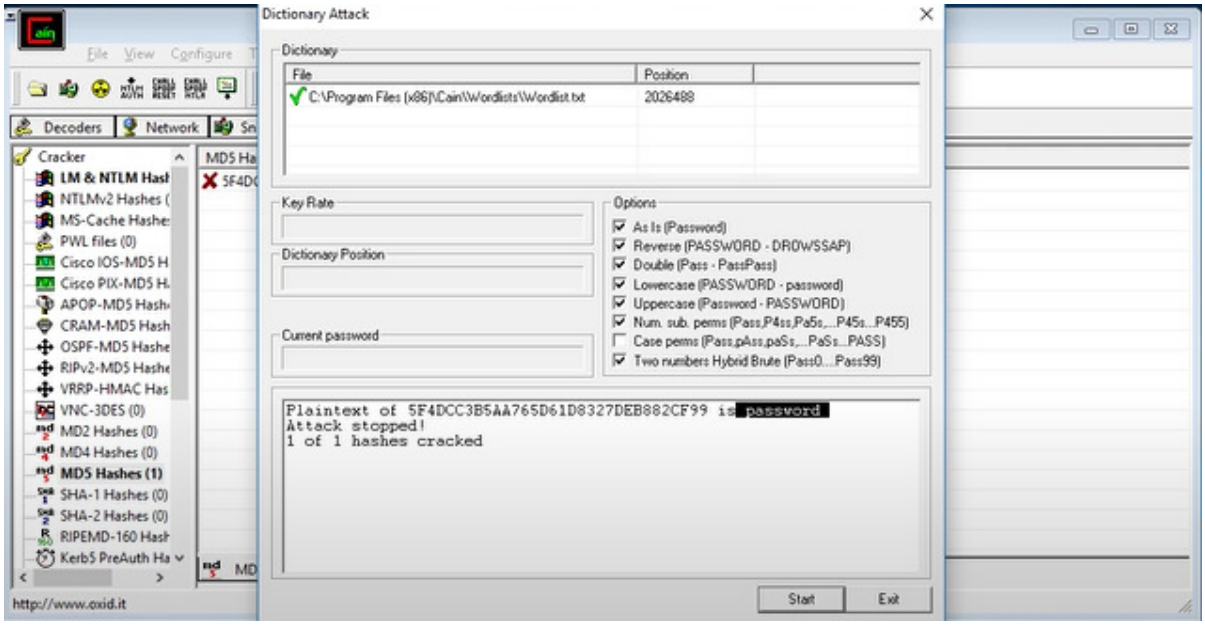
8.คลิกขวา แล้วเลือก Reset initial file position



9.จากนั้นกดปุ่ม Start

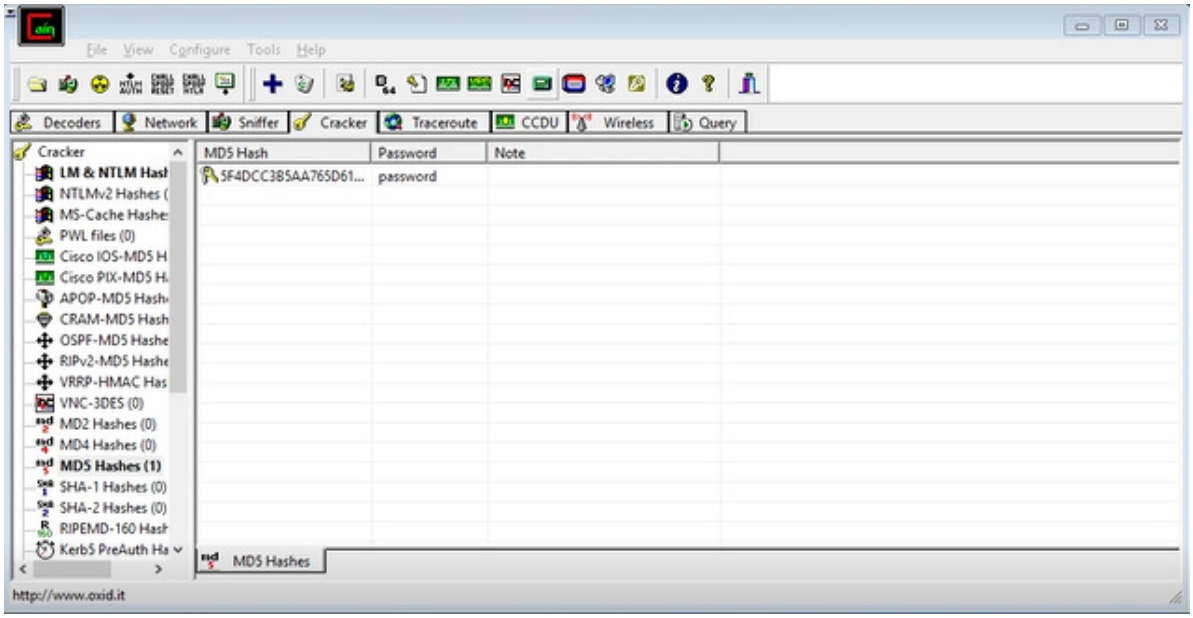


10.เมื่อโหลดเสร็จโปรแกรมจะถอดรหัสออกมาเป็นรหัสที่เราหรอก

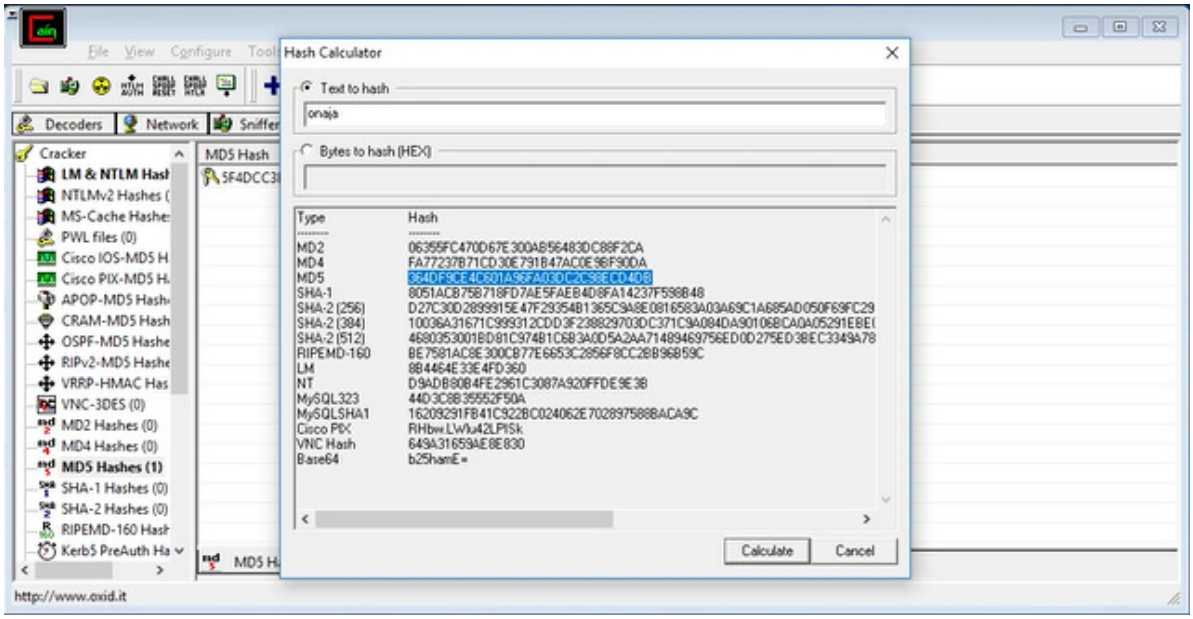


ขั้นตอนการใช้เมนู Crack Brute Foce

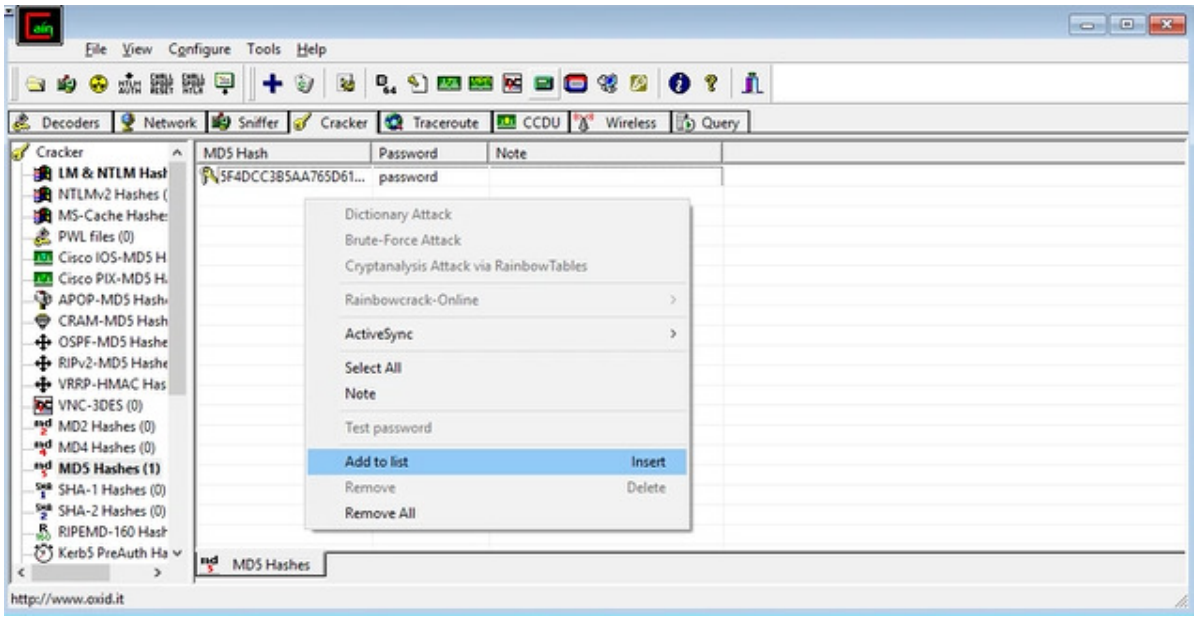
1.คลิกไปที่ Cracker เมนูบนแทบด้านบน จากนั้นคลิกไปที่ Hash Calculator 



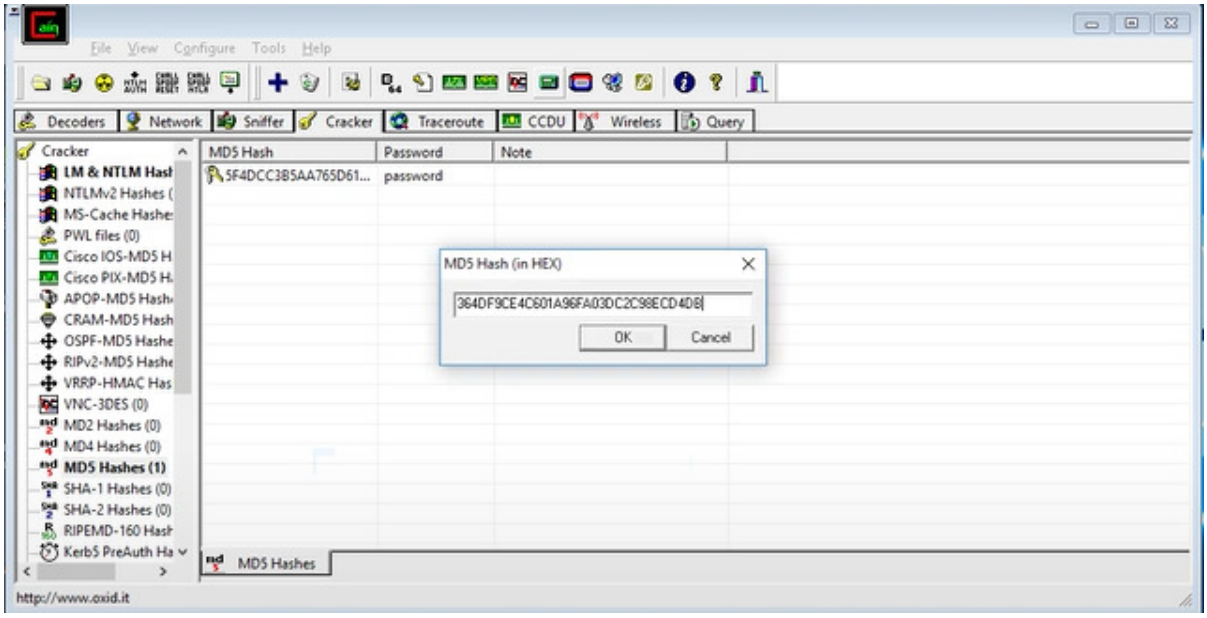
2.ใส่รหัสแบบง่ายๆ จากนั้นจะถอดรหัสออกมา Copy Hash ของ Type MD5 แล้วกด Calculate



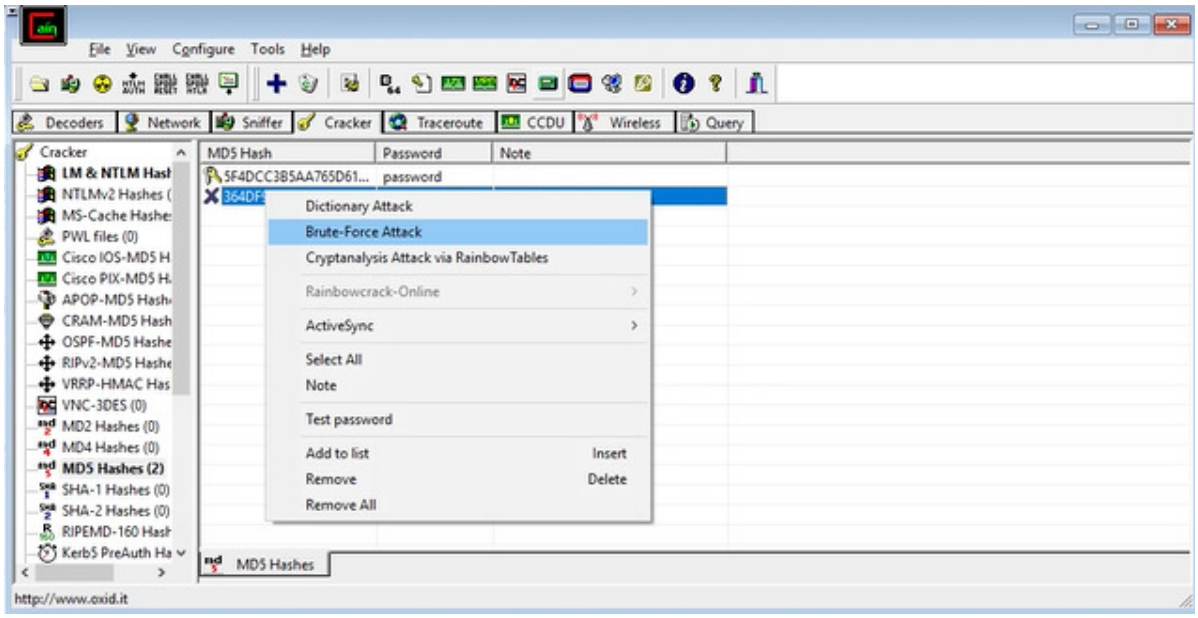
3.จากนั้นคลิกขวาตรงพื้นที่ว่าง และเลือก Add to list



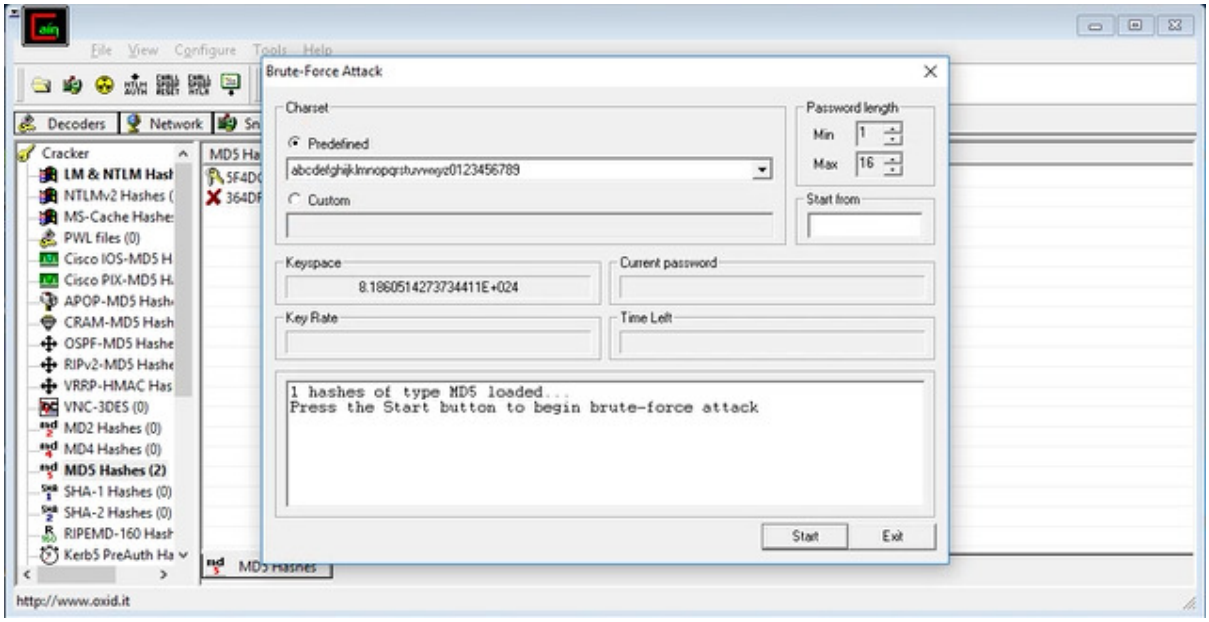
4.วางรหัสที่เรา Copy มา แล้วกด OK



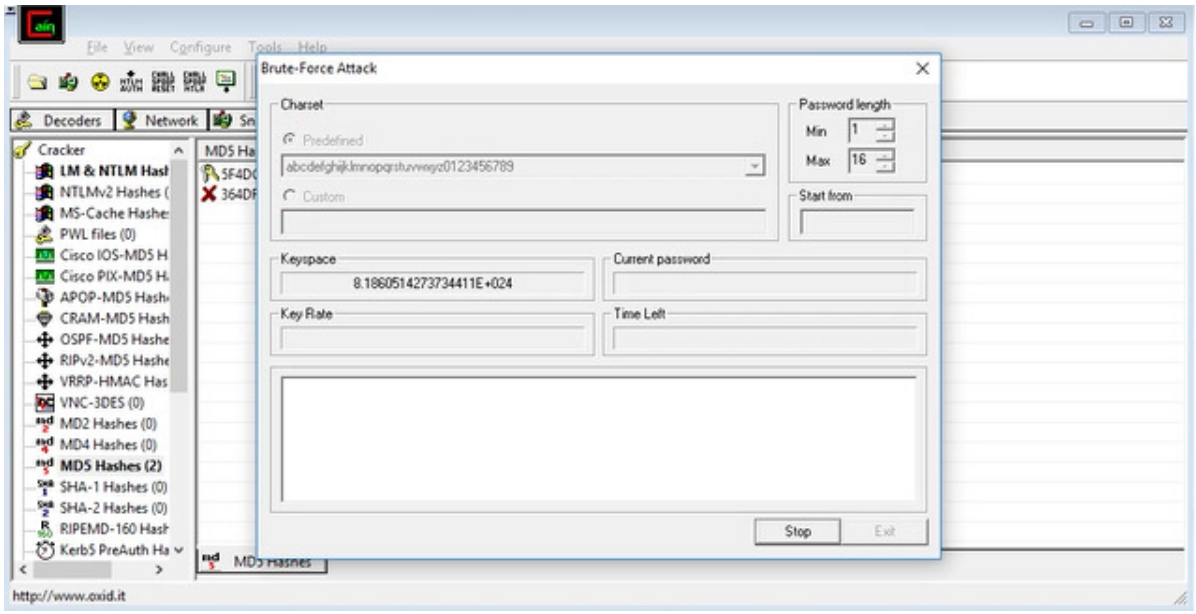
5.คลิกขวา แล้วเลือก Brute-Force Attack



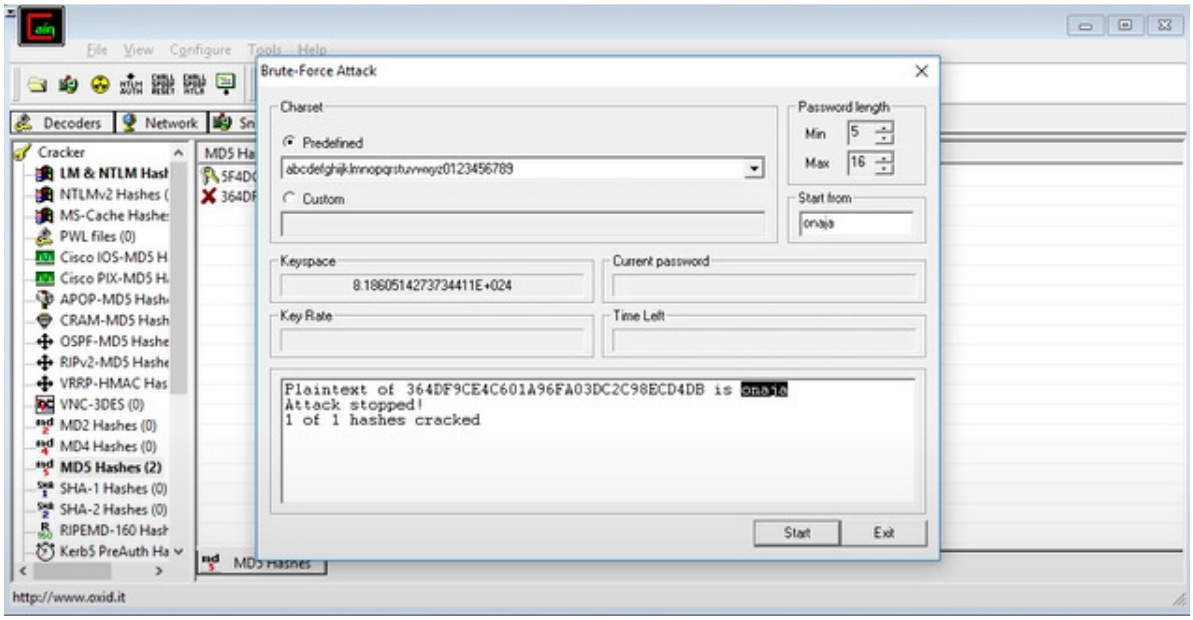
6.หน้าจอจะแสดงผลแบบนี้



7.จากนั้นกดปุ่ม Start

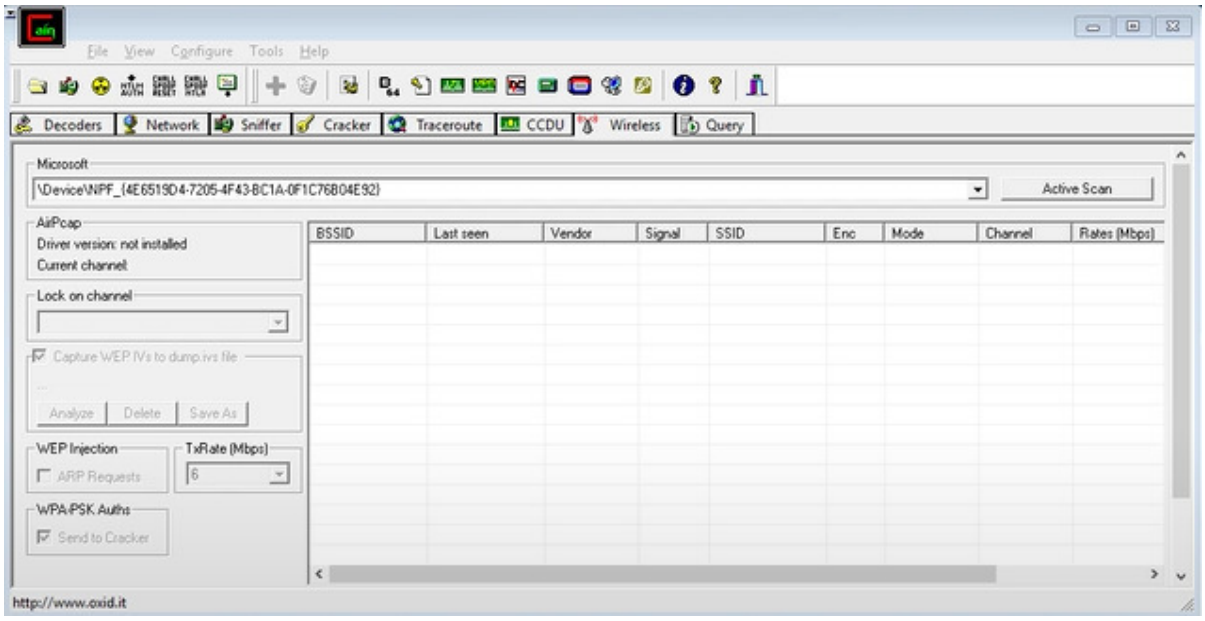


8.เมื่อโหลดเสร็จโปรแกรมจะถอดรหัสออกมาเป็นรหัสที่เราหรอก

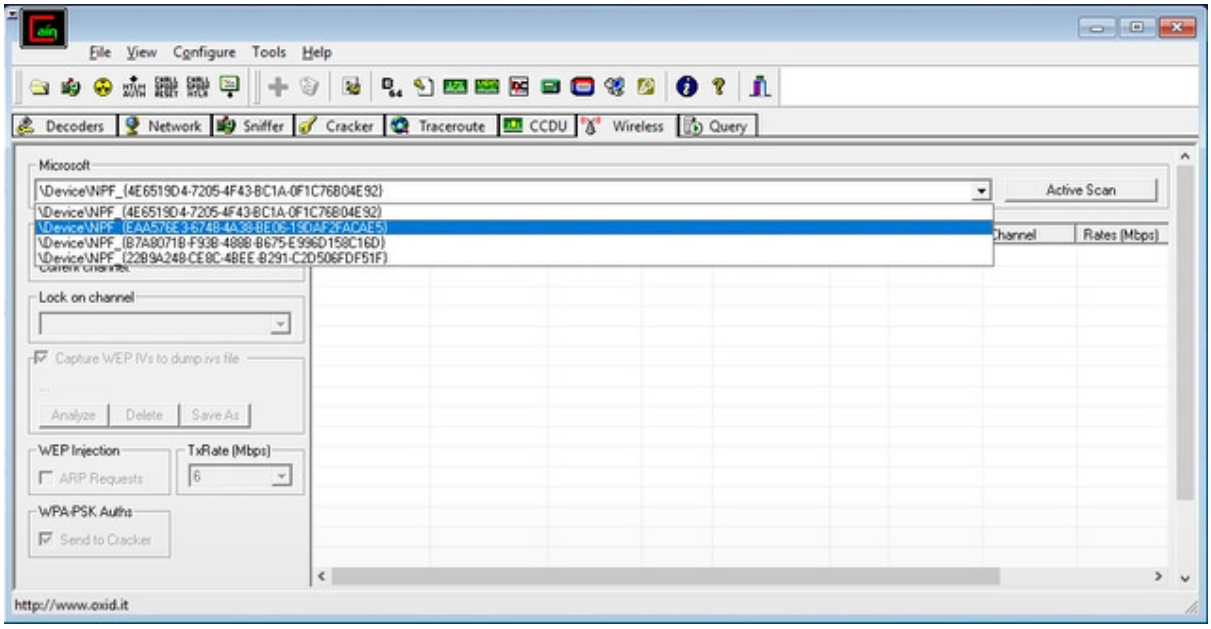


ขั้นตอนการใช้เมนู Wireless

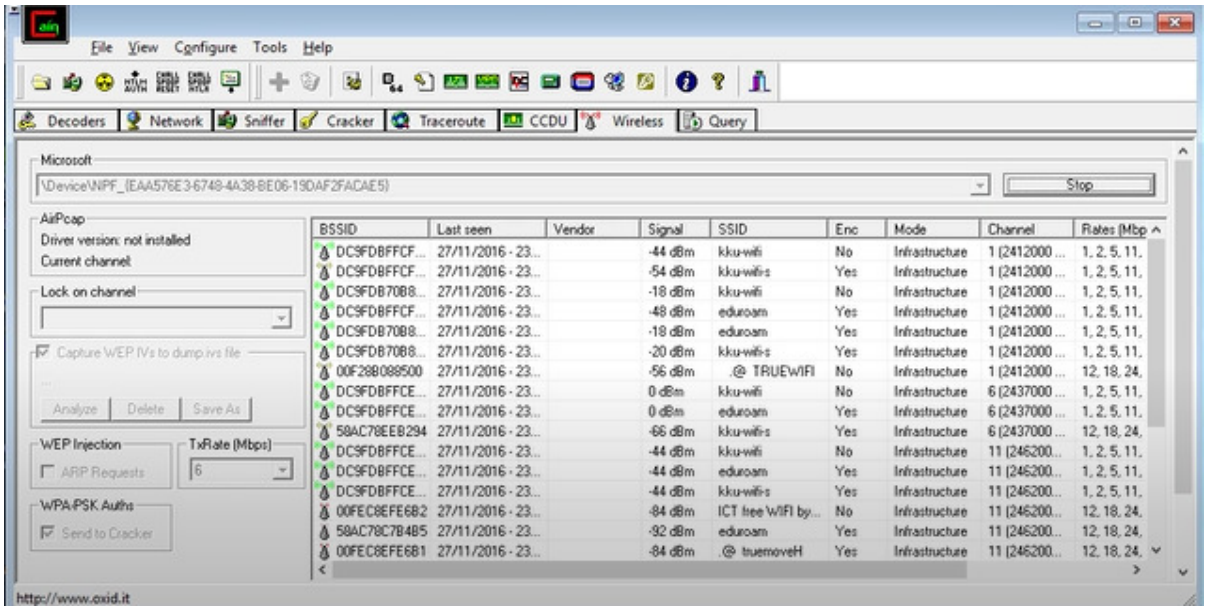
1.คลิกไปที่ Wireless เมนูบนแทบด้านบน



2.จากนั้นเลือก Microsoft ไหนก็ได้ แล้วจากปุ่ม Active Scan

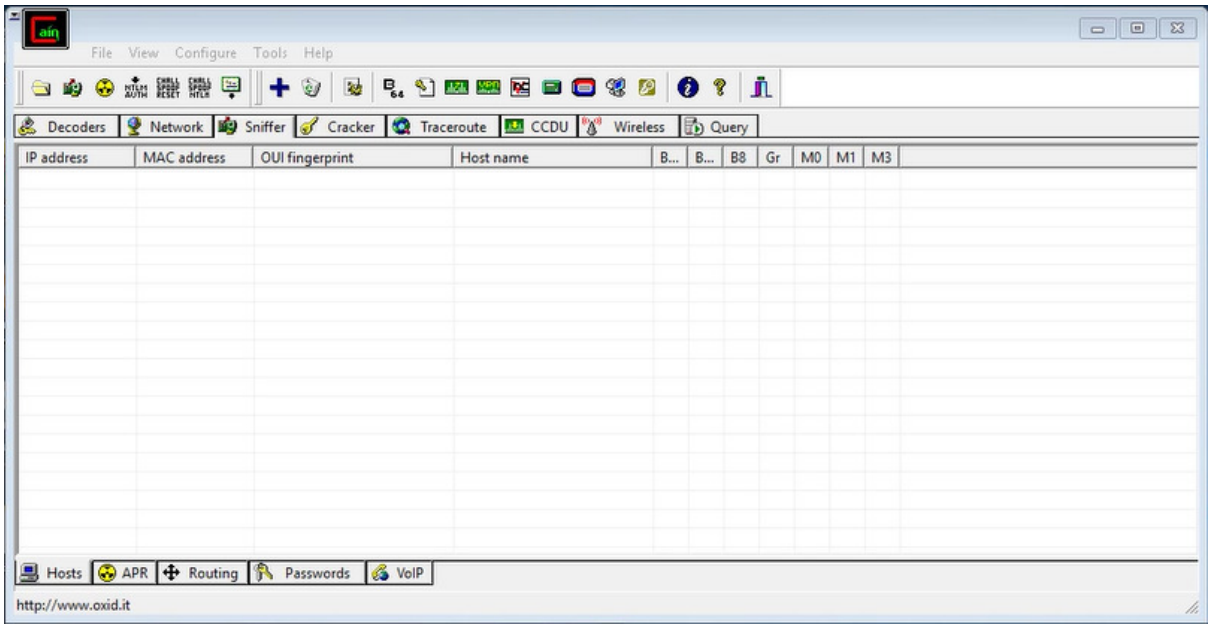


3.เมื่อกดปุ่ม Active Scan หน้าจอจะแสดงชื่อWi-Fi ที่ใช้งานอยู่ปัจจุบัน

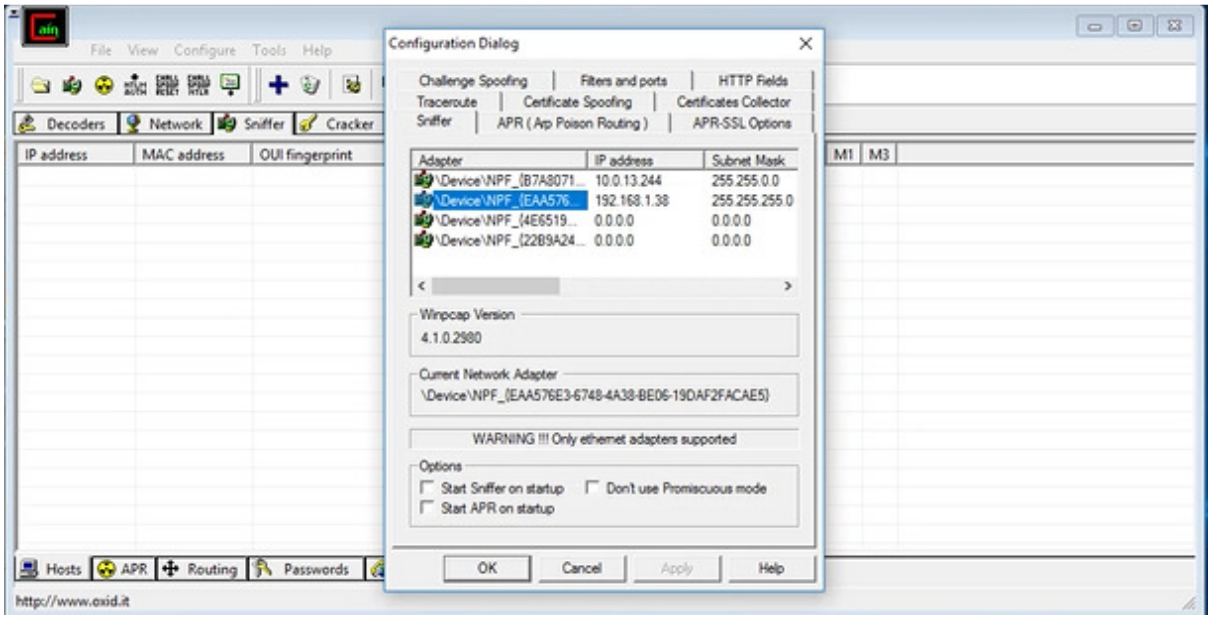


ขั้นตอนการใช้เมนู Sniffer

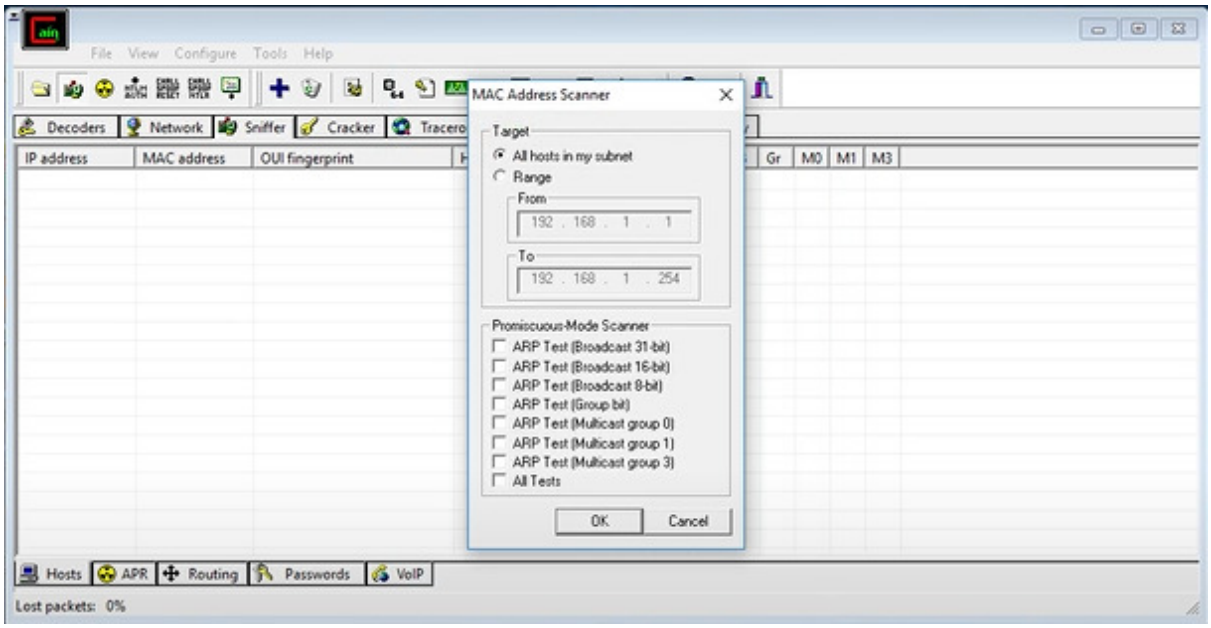
1.เลือกที่เมนู Sniffer



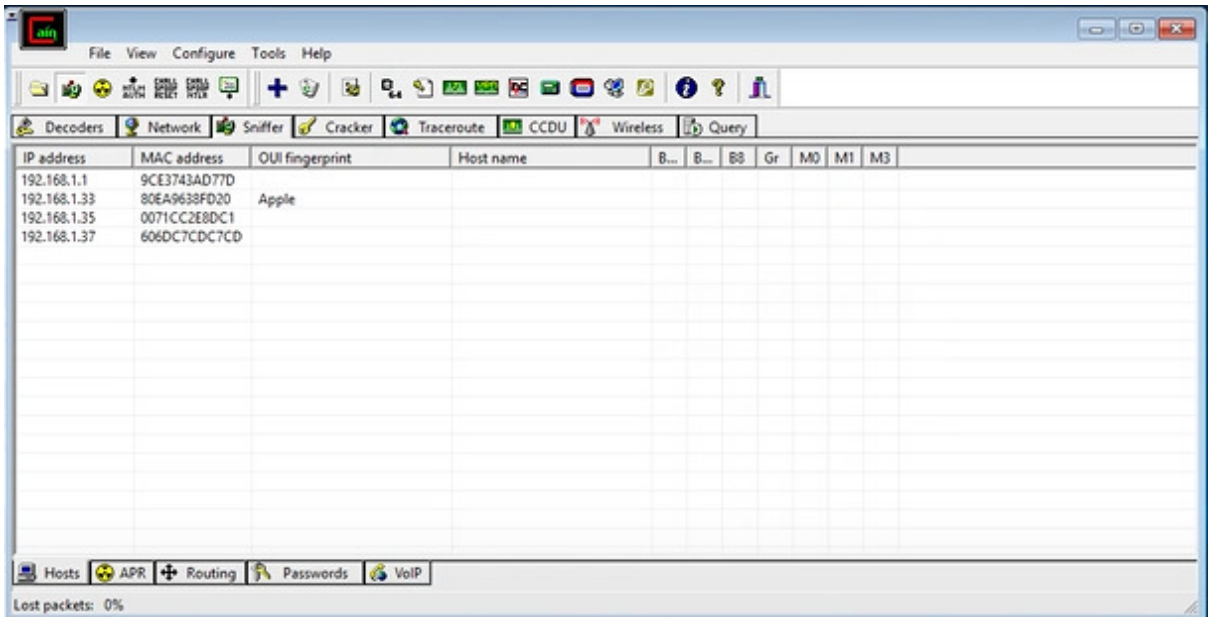
2.คลิกไปที่ Configure แทบด้านบน เลือก IP เครื่องเรา จากนั้นกด OK



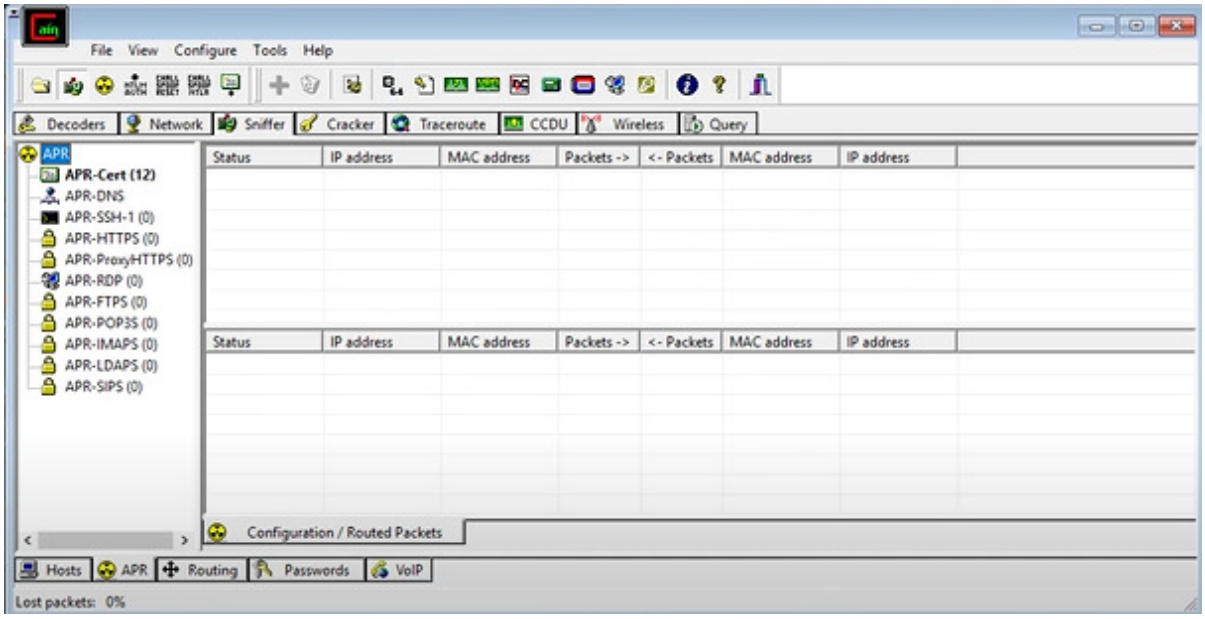
3.จากนั้นคลิกปุ่ม Start/Stop Sniffer และ ปุ่ม Add to list แล้วกด OK



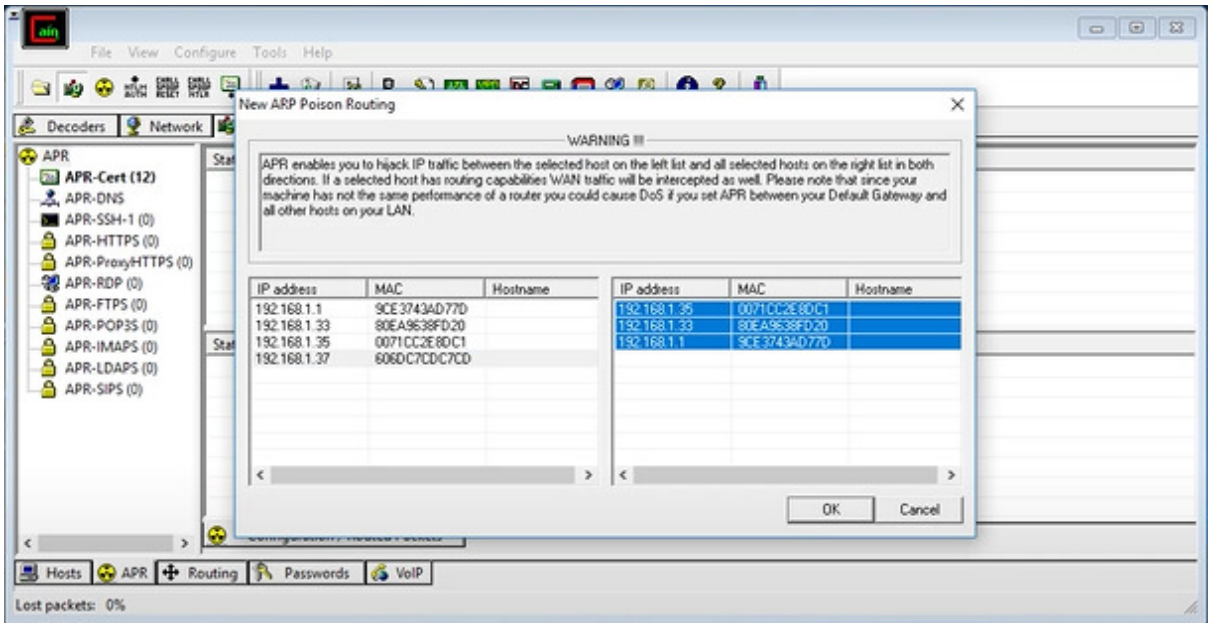
4.หน้าจอจะแสดง IP ที่ใช้งานอยู่



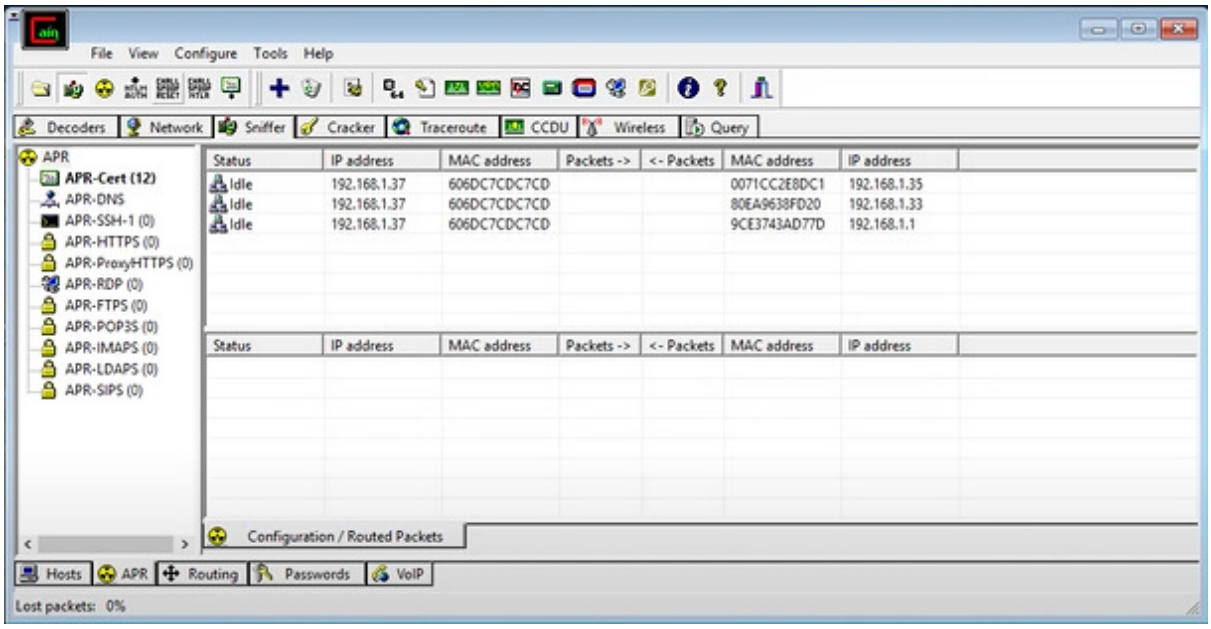
5.เลือก APR ที่แทบด้านล่าง



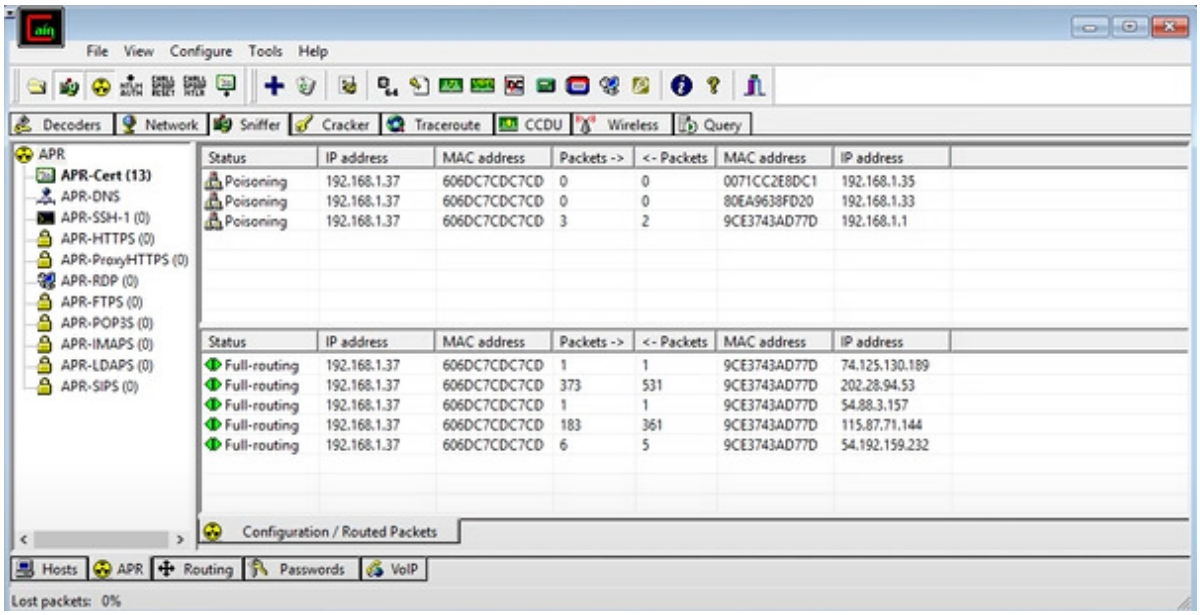
6.กดปุ่ม Add to list แล้วเลือก IP เครื่องที่จะดักจับด้านซ้าย แล้วเลือก IP เครื่องเราด้านขวา แล้วกด OK



7.หน้าจอจะแสดงจากทำงานของ IP เครื่องที่เราเลือก



8.กดปุ่ม Start/Stop APR จะแสดงการทำงานของเครื่องที่ดักจับ



9.จากนั้นเลือก Passwords แทบด้านล่าง จะแสดง Usernameและ Password ของเครื่องที่ดักจับ