



เครื่องมือที่ศึกษา : Cain & Abel

รายวิชา 322376 ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร

จัดทำโดย

Group 4 Section 1.

สมาชิก

นางสาวสุริตา เฟื่องฟู 553020014-8

นางสาวกชกร รักกุศล 553020296-2

นางสาวชนิกรรดา เอกวงค์ษา 553020299-6

นางสาวนลัทพร โอษฐ์วิเศษ 553020302-3

นางสาวลลิตา คำโมง 553020307-3

นายภูวดล ทาจันทร์ 553020741-7

เสนอ

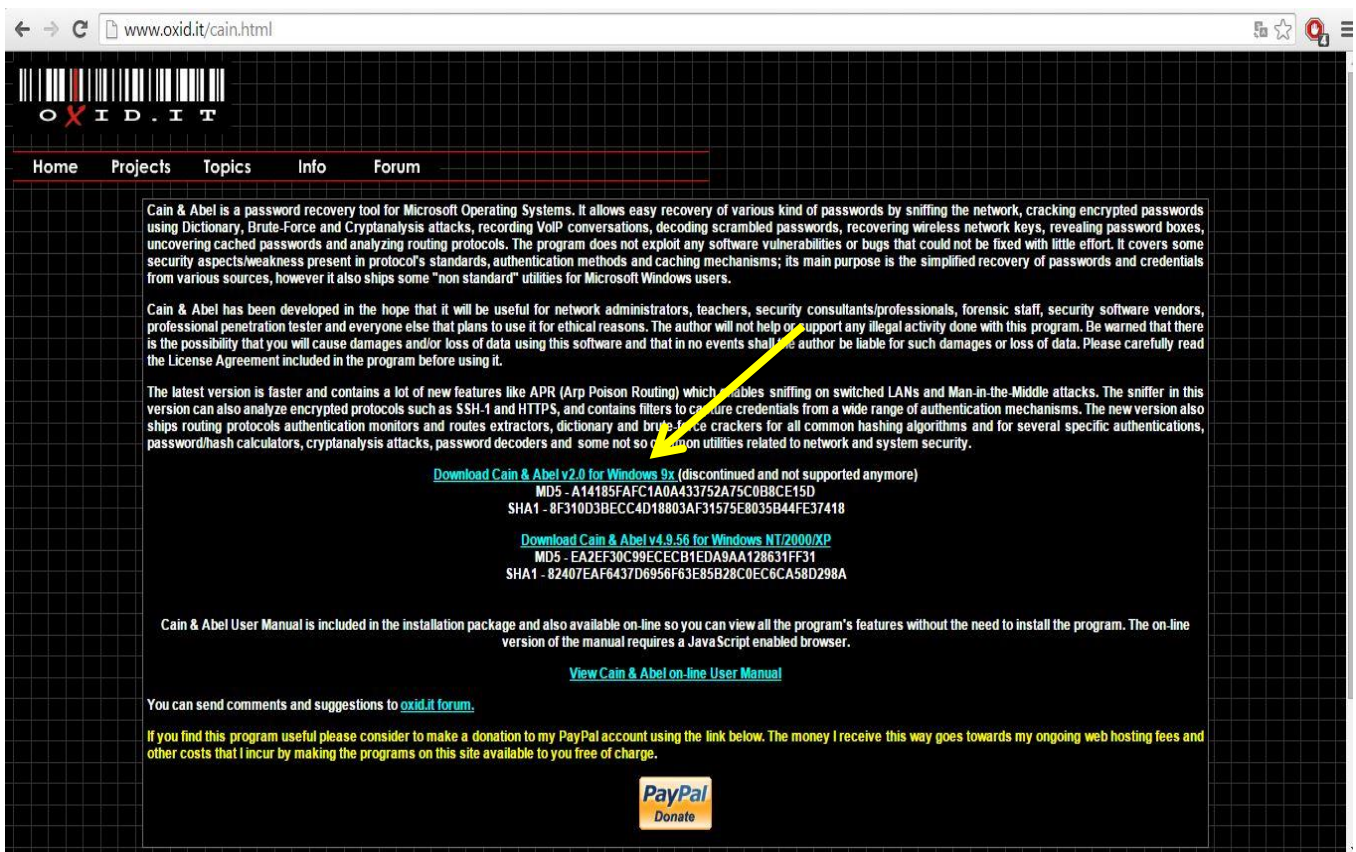
ผศ.ดร จักรชัย โสอินทร์

# โปรแกรม Cain & Abel

Cain & Abel เป็นเครื่องมือสำหรับใช้ในการกักตุนรหัสผ่าน สำหรับเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการวินโดวส์ และสามารถทำการถอดรหัสผ่านได้หลากหลายรูปแบบ เช่น ทำการดักข้อมูลรหัสผ่านจากเครือข่าย, การแคร็กรหัสผ่านโดยใช้ Dictionary ,การแคร็กรหัสผ่านแบบ Brute-Force, และการแคร็กรหัสผ่านแบบ Cryptanalysis attacks นอกจากนี้ยังสามารถทำการบันทึกการสนทนาแบบ VoIP, ทำการถอดรหัส scrambled passwords, ทำการแสดงรหัสผ่านใน password boxes, ทำการค้นหารหัสผ่านต่างๆ ที่เก็บอยู่ใน cache ได้อีกด้วย

## 1. ดาวน์โหลดโปรแกรม Cain & Abel

(สามารถดาวน์โหลดได้ที่ [www.oxid.it/cain.html](http://www.oxid.it/cain.html))



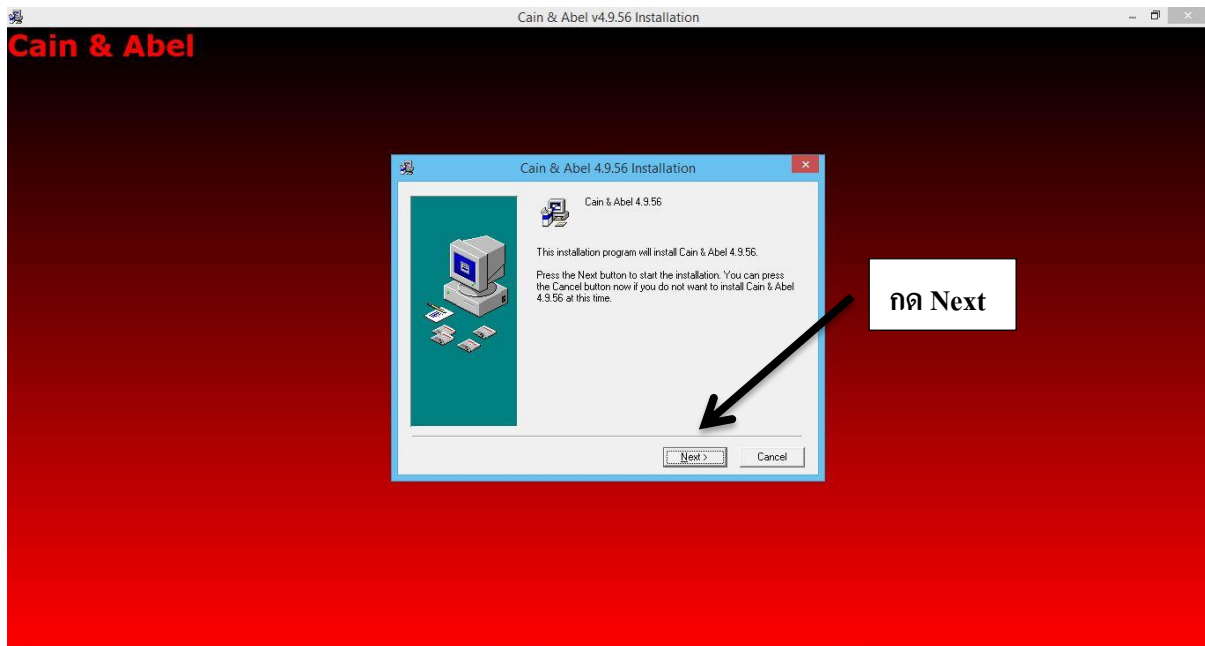
The screenshot shows the website [www.oxid.it/cain.html](http://www.oxid.it/cain.html). The page features a navigation menu with links for Home, Projects, Topics, Info, and Forum. The main content area contains a detailed description of the software, its capabilities, and a license agreement. Two download links are highlighted with a yellow arrow:

- [Download Cain & Abel v2.0 for Windows 9x](#) (discontinued and not supported anymore)  
MD5 - A14185F AFC1A0A433752A75C0B8CE15D  
SHA1 - 8F310D3BECC4D18803AF31575E8035B44FE37418
- [Download Cain & Abel v4.9.56 for Windows NT/2000/XP](#)  
MD5 - EA2EF30C99ECCB1EDA9AA128631FF31  
SHA1 - 82407EAF6437D6956F63E85B28C0EC6CA58D298A

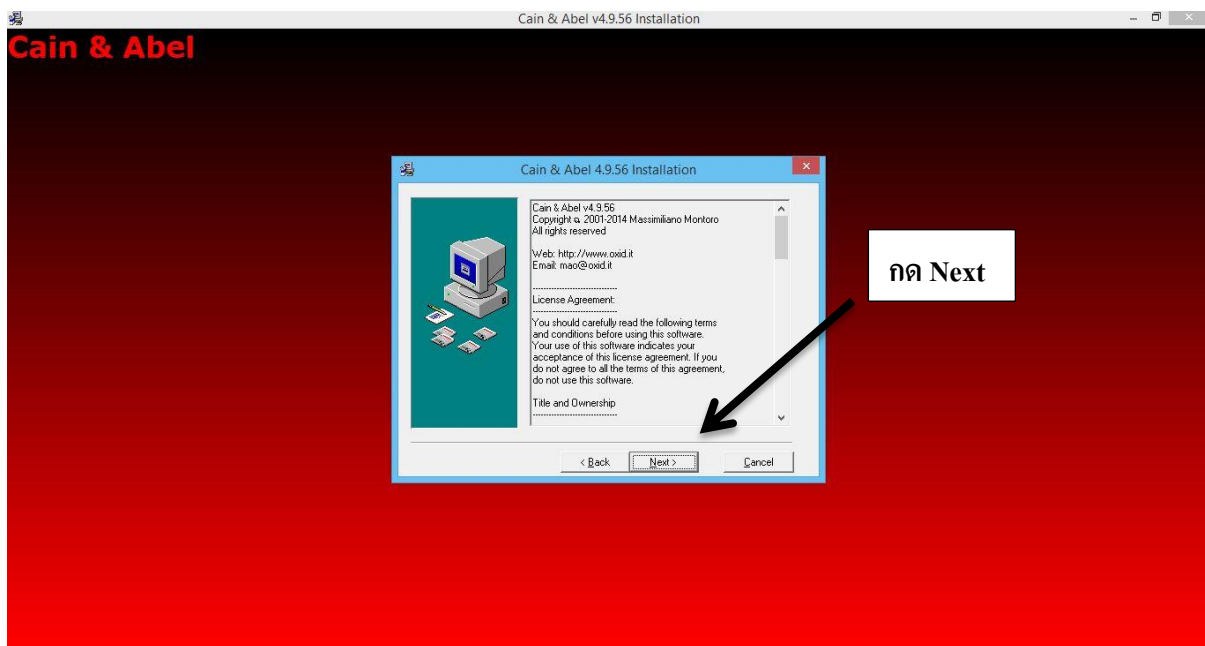
Below the download links, there is a link to the [Cain & Abel User Manual](#) and a [PayPal Donate](#) button.

รูปที่ 1 เว็บไซต์สำหรับดาวน์โหลดโปรแกรม Cain & Abel

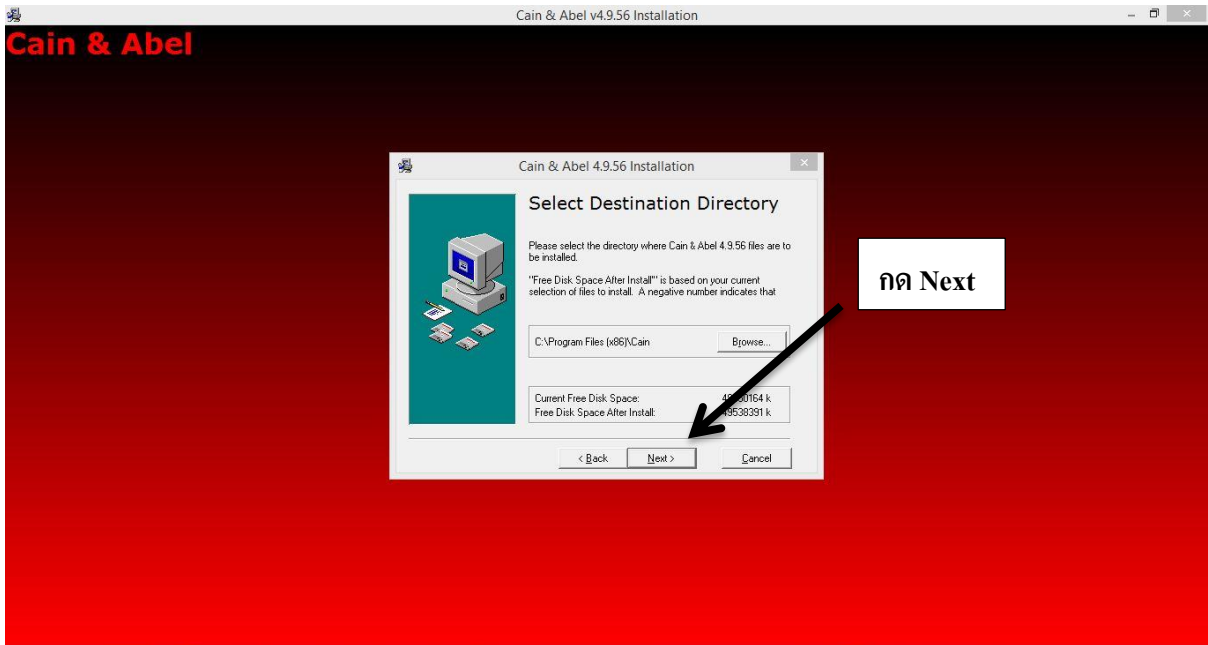
## 2. ติดตั้งโปรแกรม (คลิกปุ่มดังรูปลูกศร)



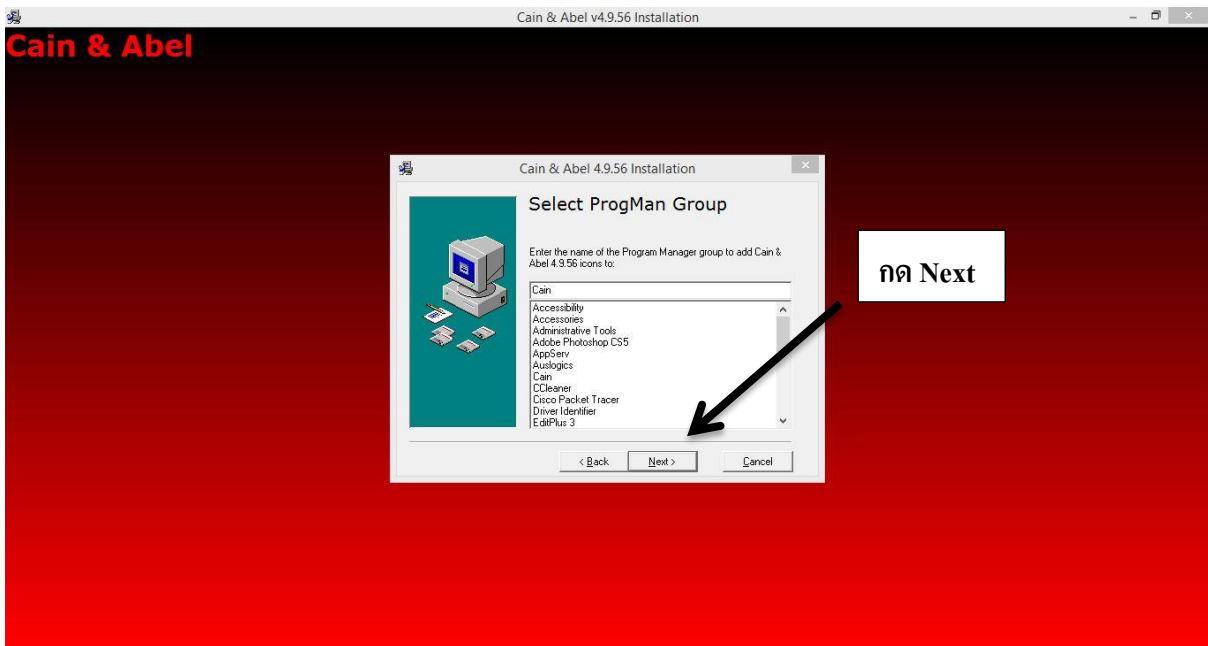
รูปที่ 2 การติดตั้ง โปรแกรม



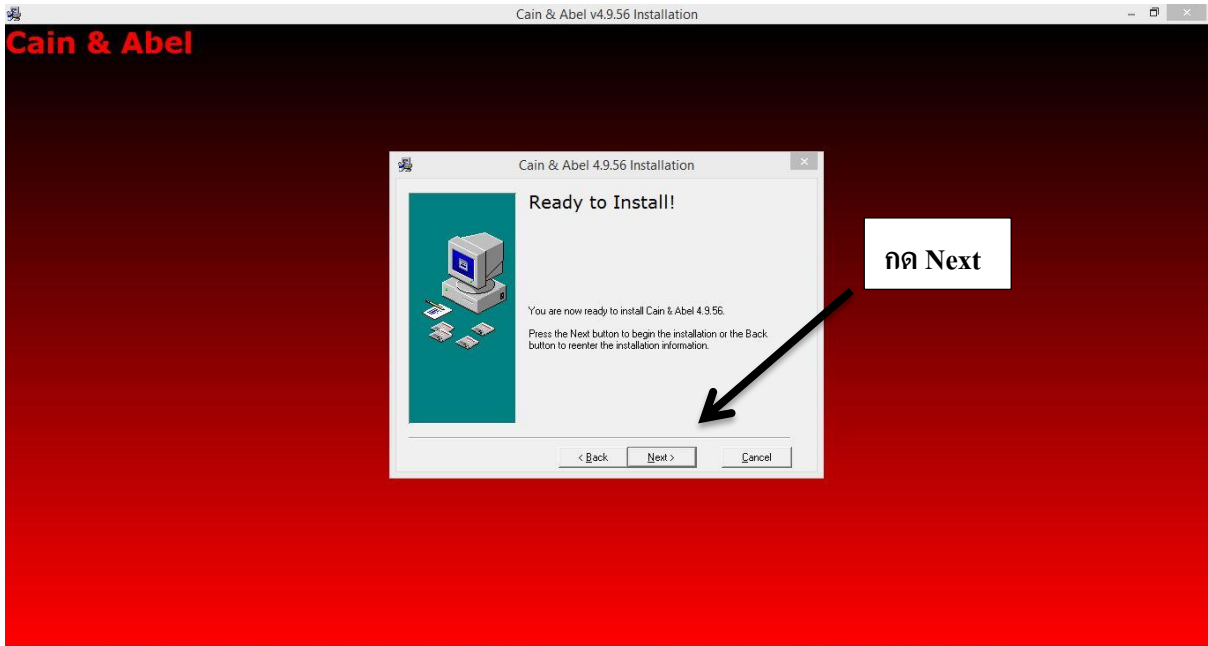
รูปที่ 3 การติดตั้ง โปรแกรม



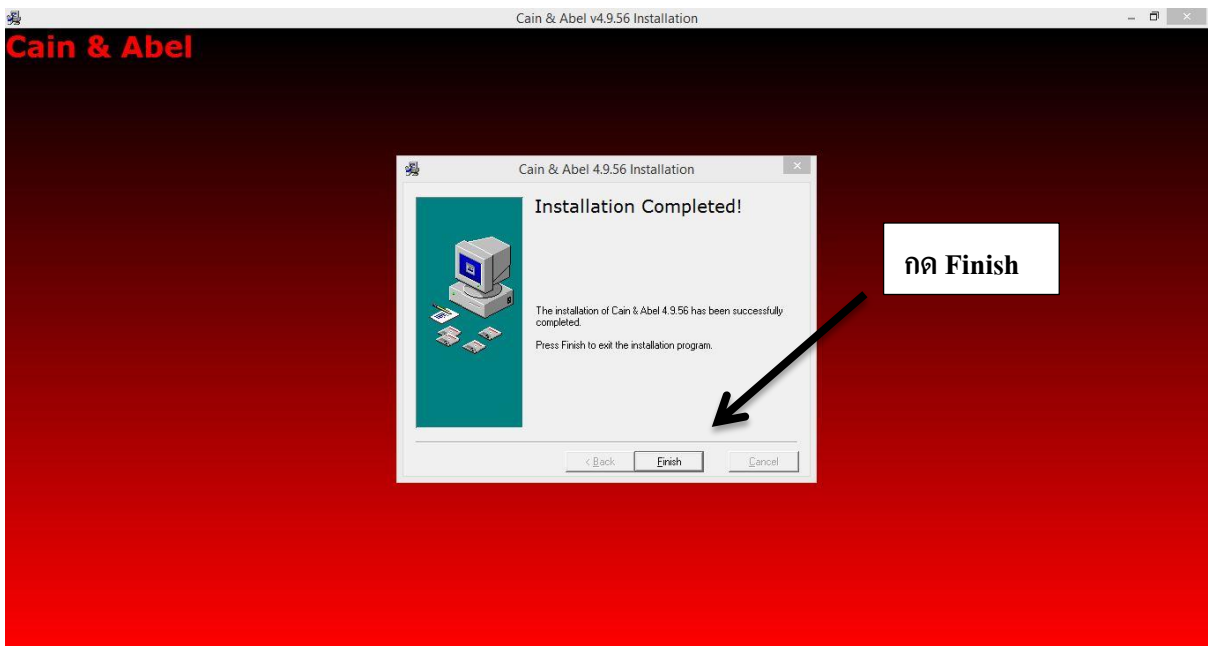
รูปที่ 4 การติดตั้ง โปรแกรม



รูปที่ 5 การติดตั้ง โปรแกรม



รูปที่ 6 การติดตั้ง โปรแกรม

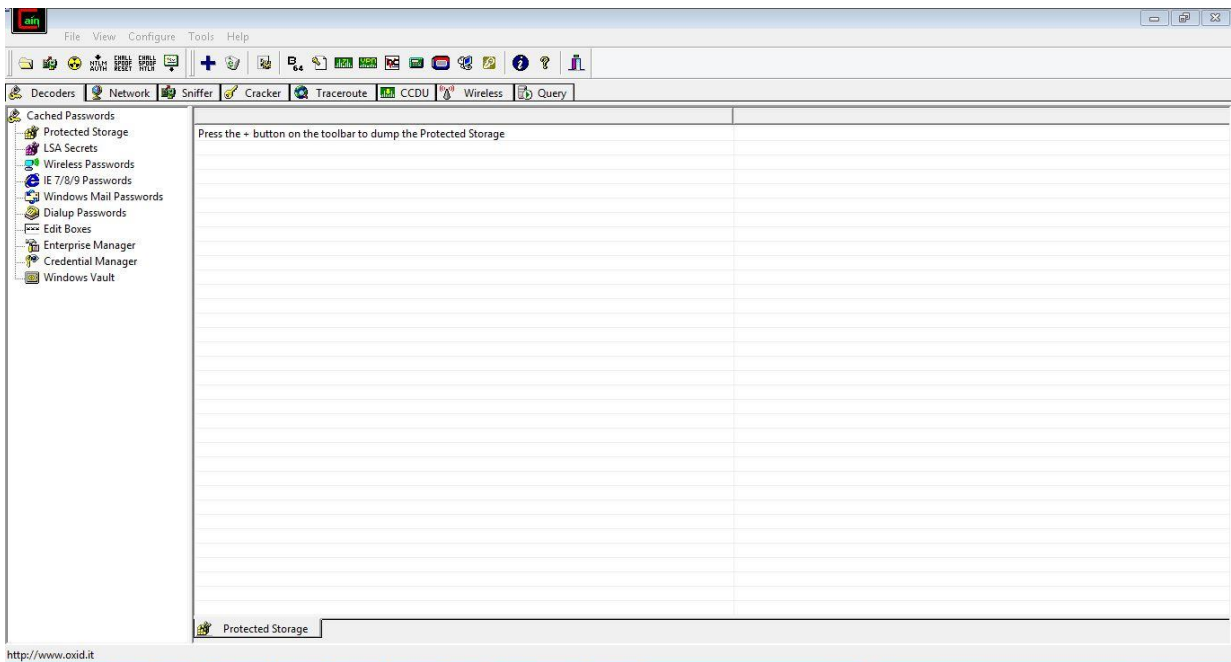


รูปที่ 7 การติดตั้ง โปรแกรม



รูปที่ 8 การติดตั้งโปรแกรม

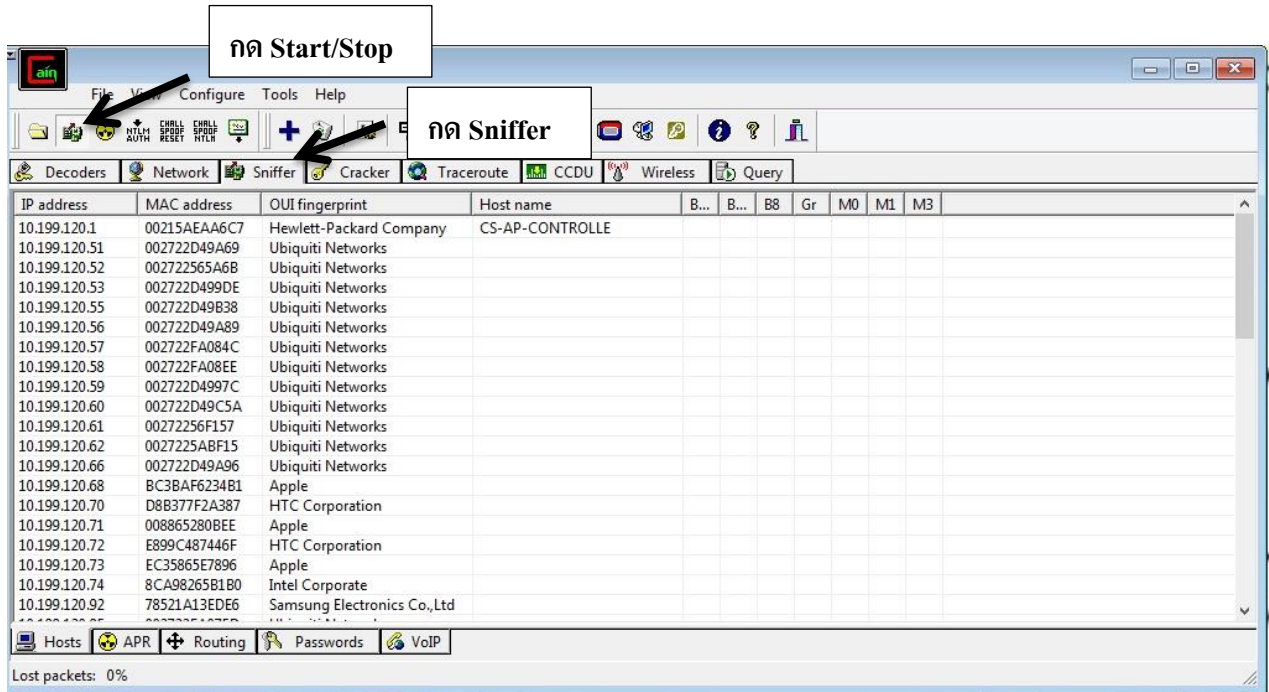
เมื่อติดตั้งโปรแกรมสำเร็จจะมีรูปภาพโปรแกรมดังรูปที่ 9



รูปที่ 9 รูปแบบโปรแกรม Cain & Abel

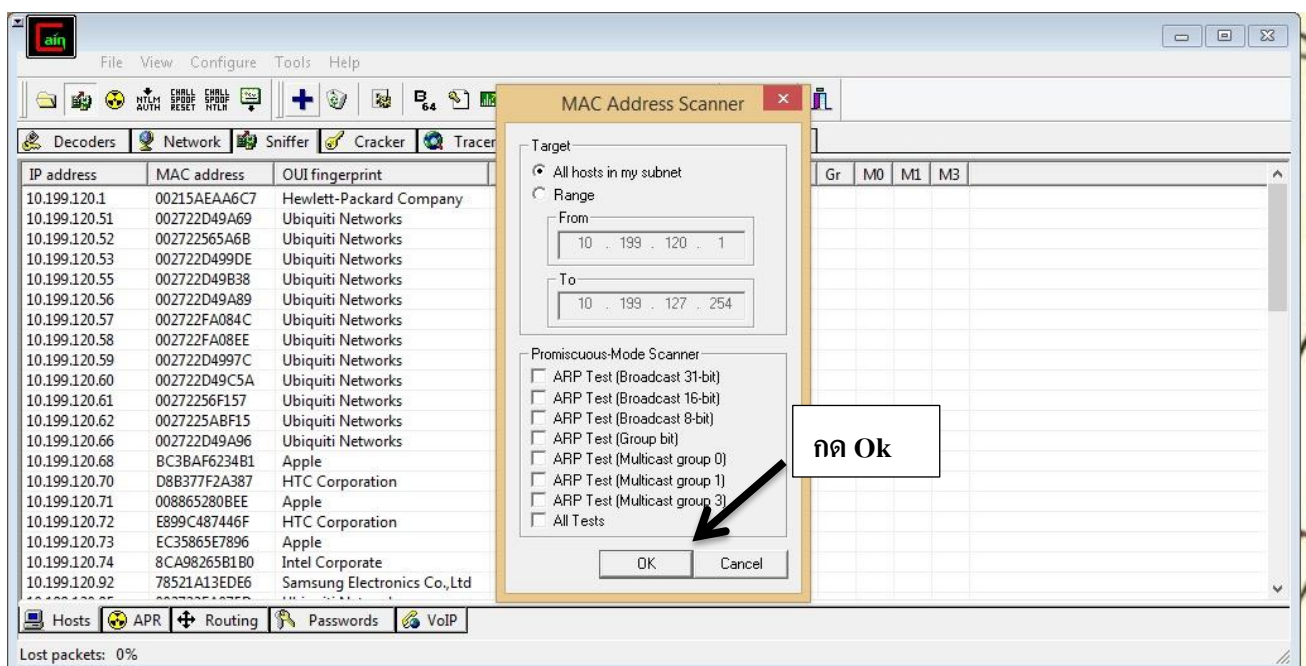
## การใช้งานโปรแกรมฟังก์ชัน sniffer

1. เข้าโปรแกรม Cain & Abel ที่เครื่องผู้บุกรุก เปิดแท็บ Sniffer แล้วเลือก Start/Stop Sniffer ที่แถบเมนูด้านบน



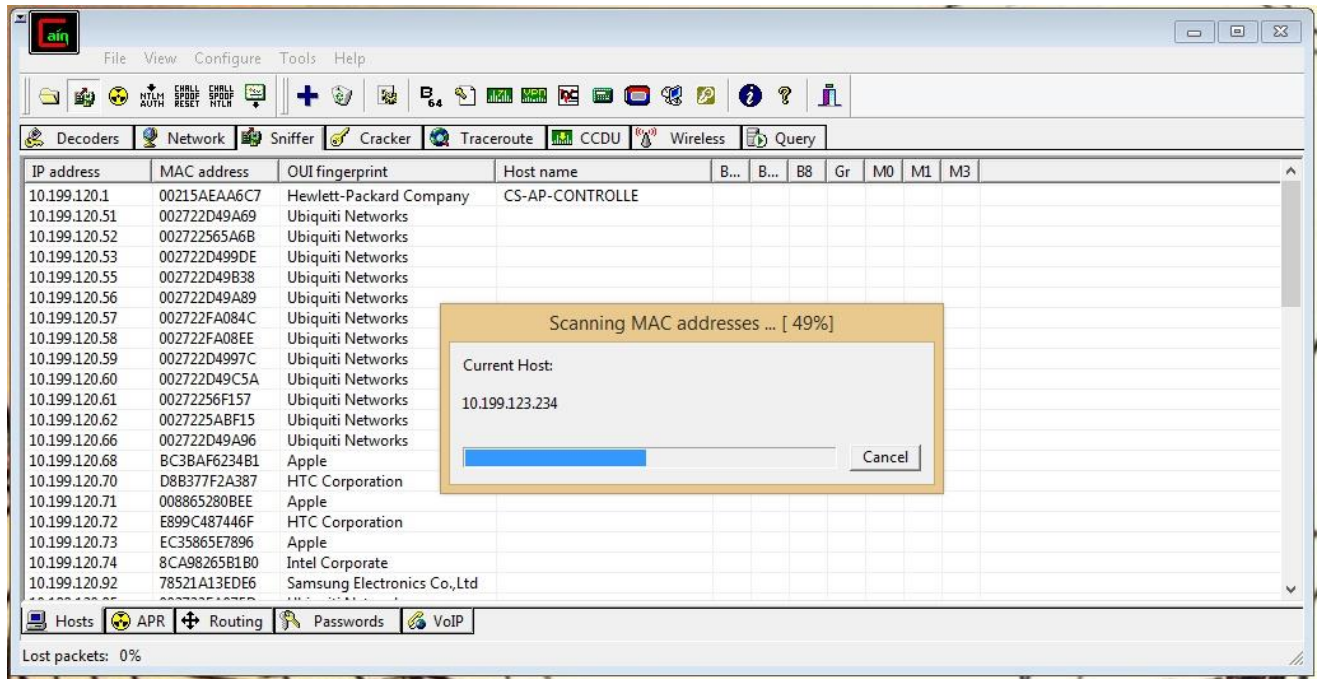
รูปที่ 10 โปรแกรมเมื่อเลือก sniffer และคลิกปุ่ม Start/Stop

2. เลือก Add to list เพื่อค้นหาเครื่องเป้าหมายภายในเครือข่าย



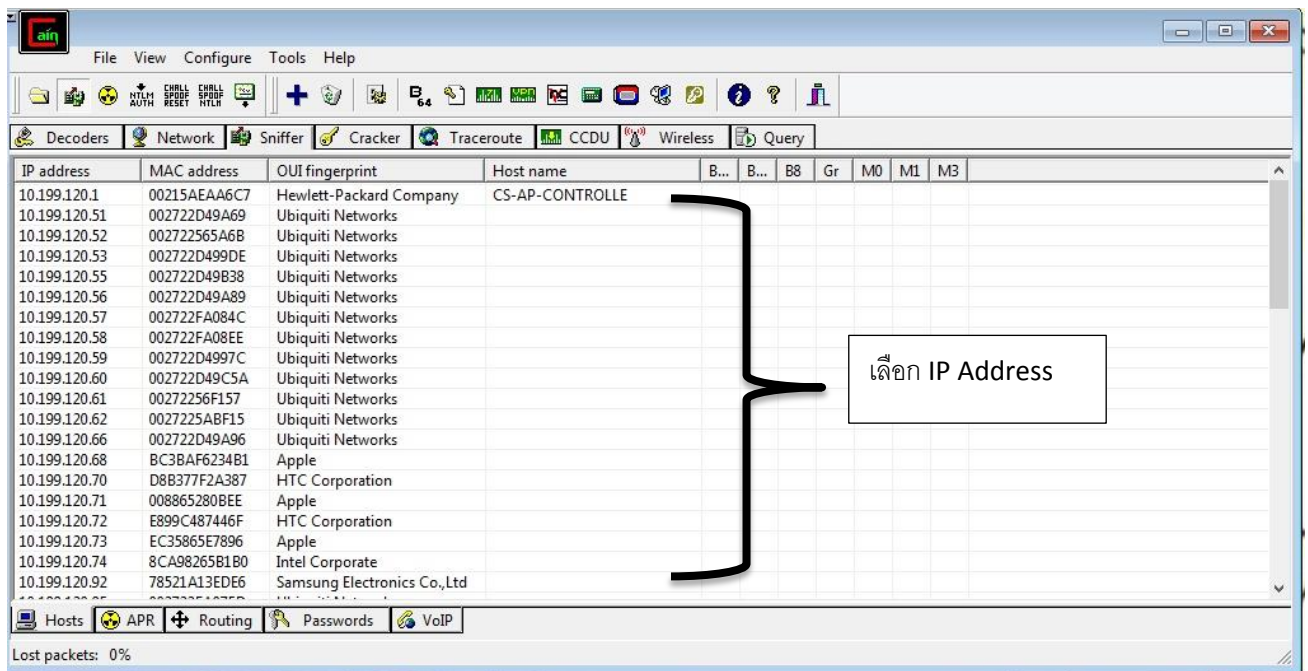
รูปที่ 11 การเลือกเป้าหมาย

### 3. รอทการ Scanning MAC addresses



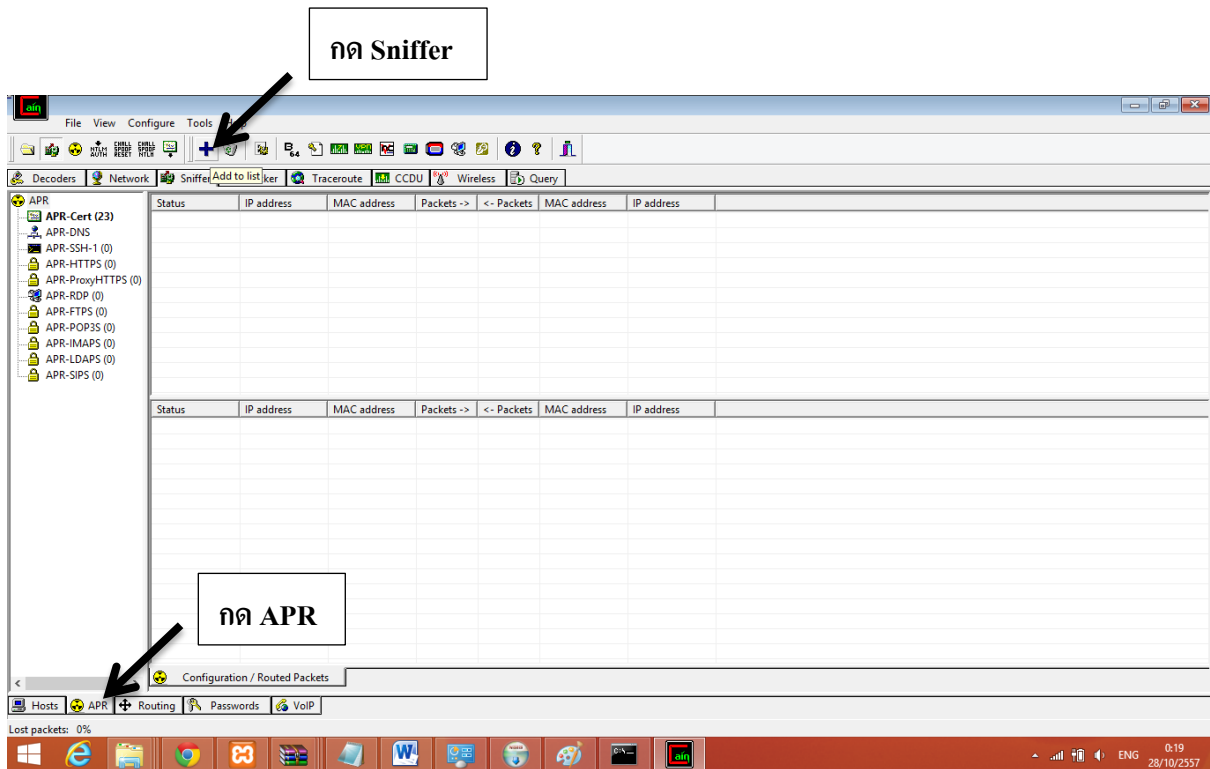
รูปที่ 12 Scanning MAC addresses

4. เลือก IP Address เป้าหมายที่ต้องการโจมตี จากนั้นไปที่แถบเมนูด้านล่าง เลือก ARP และ คลิกปุ่ม Add to list



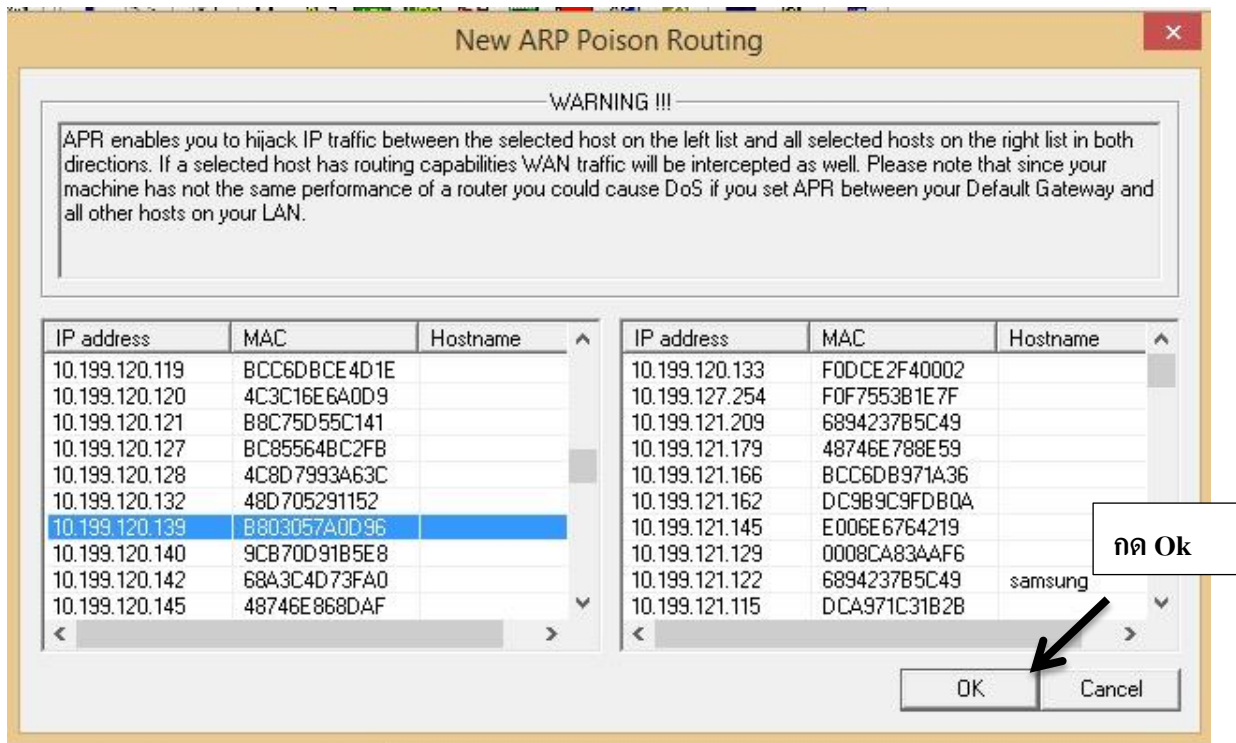
รูปที่ 13 การเลือก IP Address



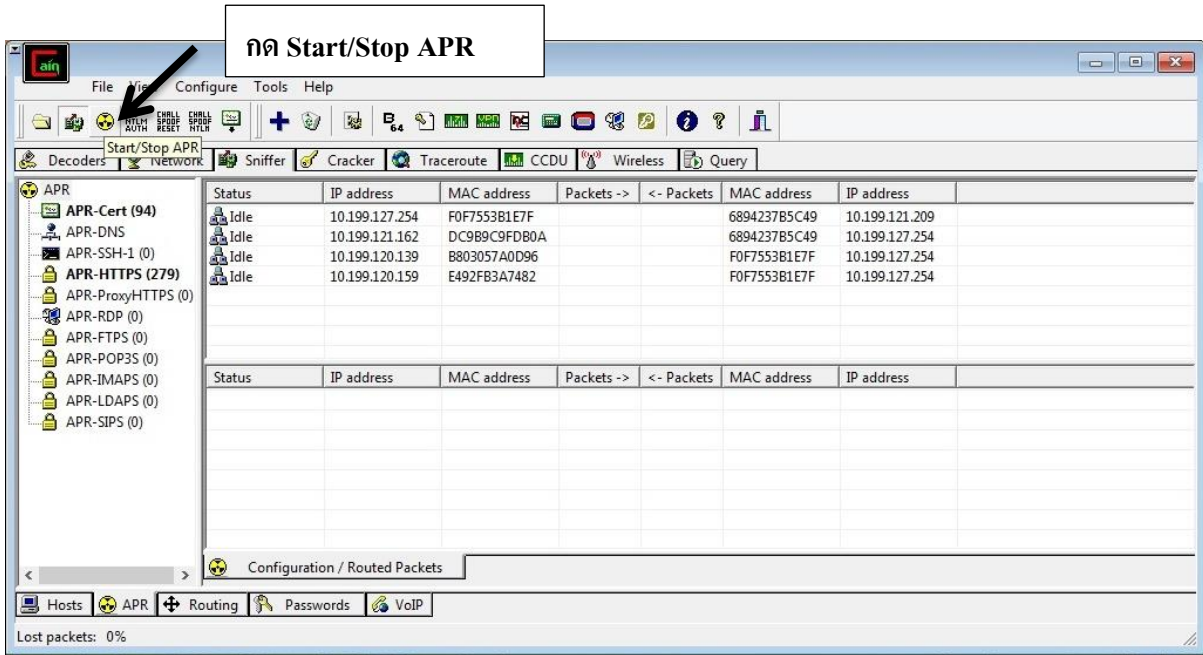


รูปที่ 14 หน้าของส่วน APR

5. เลือก IP Address (ขวา) และ Gateway เครื่องเหยื่อ (ซ้าย) หลังจากนั้นกดปุ่ม start/stop

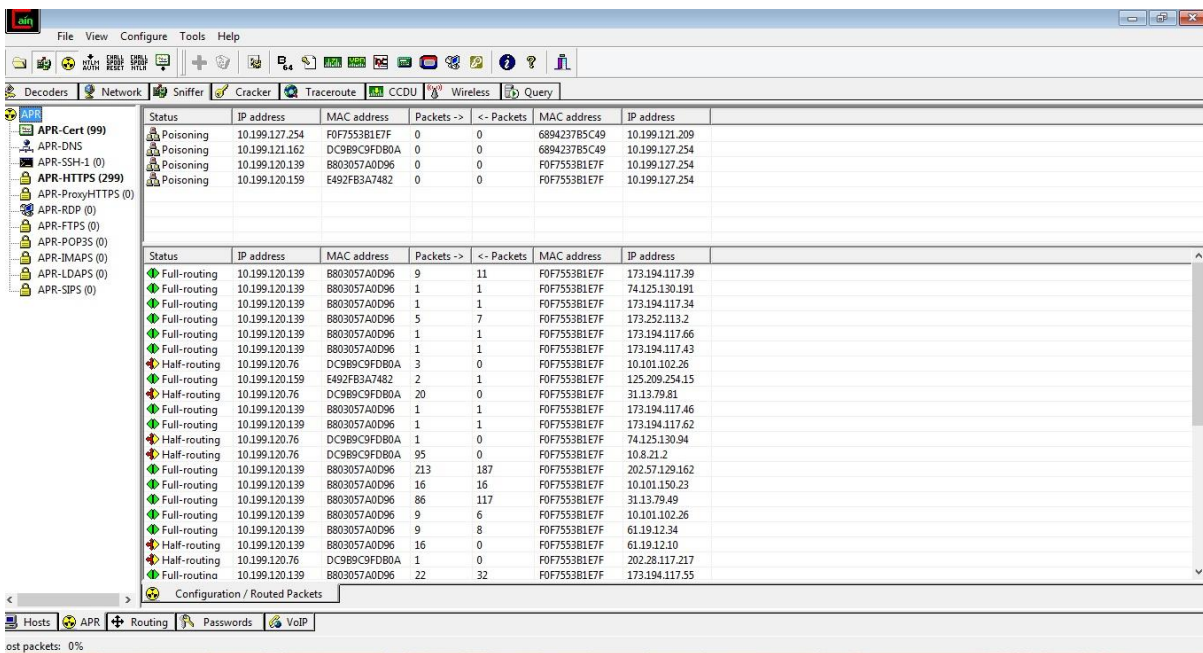


รูปที่ 15 เลือก IP Address (ขวา) และ Gateway



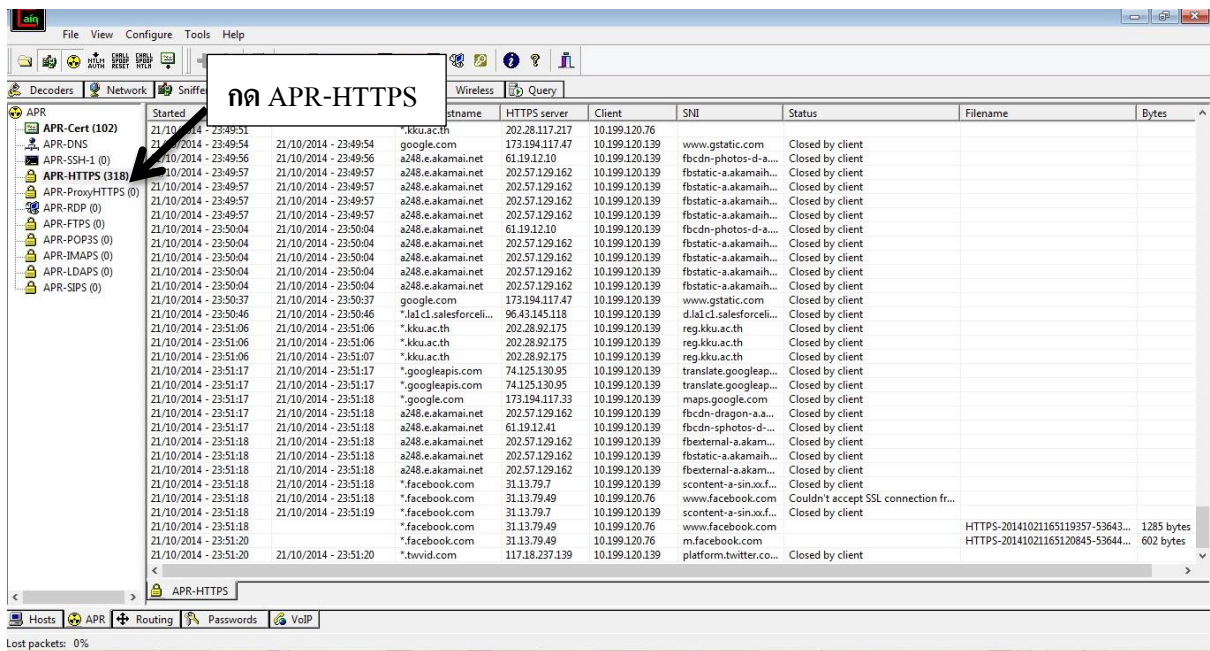
รูปที่ 16 หน้าต่าง APR เมื่อเลือก IP Address (ขวา) และ Gateway

6. จากนั้นให้เลือกเครื่องที่เราต้องการจะทำการบุกรุก แล้วกดที่ Start/Stop ARP สถานะของเครื่องที่เลือกจะเปลี่ยนจาก Idle เป็น Poisoning



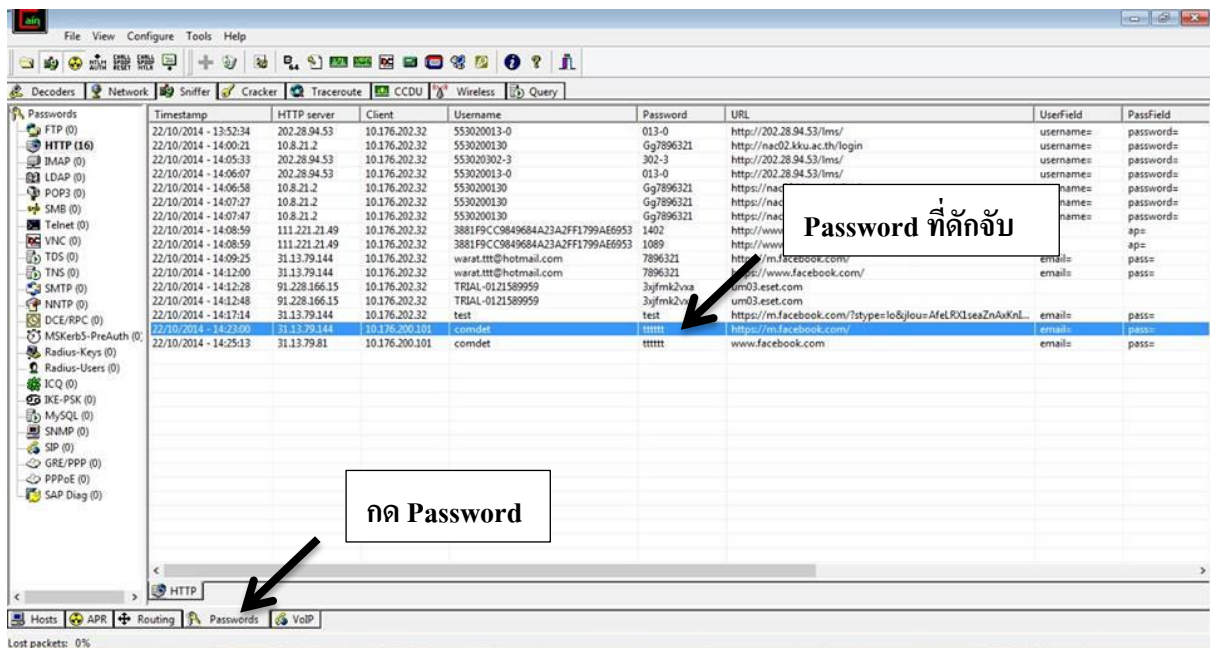
รูปที่ 17 Poisoning

7. กดแถบด้านซ้ายมือ APR-HTTPS เมื่อเหยือกดผ่านตัวโปรแกรมจะทำการดักจับข้อมูลแพ็คเกจ และถอดรหัสข้อมูล username และ password ของเหยื่อ



รูปที่ 18 การดักข้อมูล

8. กดแถบด้านล่าง Password



รูปที่ 19 ดักจับ Password