Security Tool

Ardamax Keylogger 4.2

โดย

นายพัชรพล	อวยชัย	553020011-4
นางสาวภัททิรา	สกุลวรวิทย์	553020012-2
นางสาวประภาพันธ์	คงแก้ว	553020033-4
นายวรุตฆ์	เติมไพบูลย์	553020034-2
นางสาวศิรินภา	สิงห์โคตร	553020308-1
นายธนกฤต	อินทะพงษ์	5530207320-8

ผู้สอน

ผศ.ดร. จักรชัย โสอินทร์

เอกสารฉบับนี้เป็นส่วนหนึ่งของวิชา

322 376 Information and Communication Technology Security

ภาคเรียน 1 ปีการศึกษา 2557

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

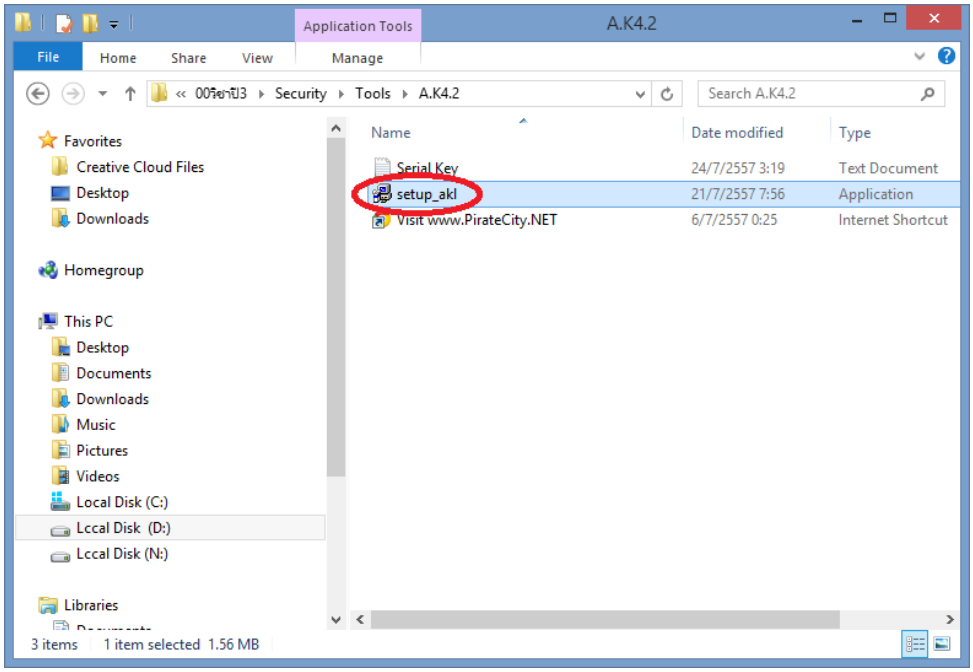
มหาวิทยาลัยขอนแก่น

Ardamax Keylogger 4.2

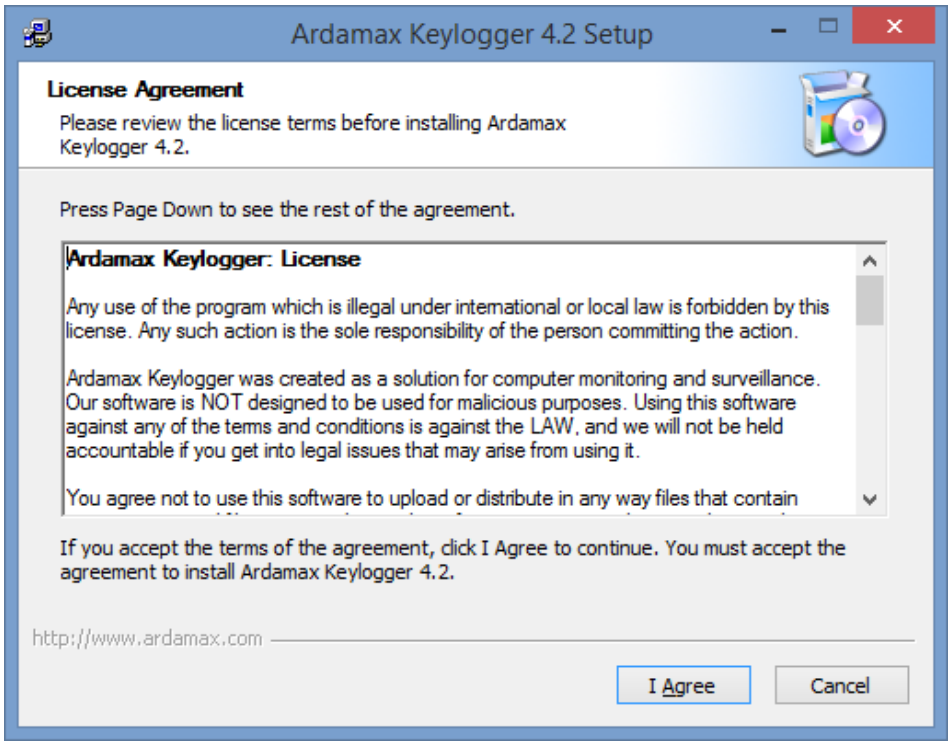
เป็นโปรแกรมที่จะตรวจสอบและบันทึกกิจกรรมทั้งหมดที่ได้ทำกับระบบคอมพิวเตอร์ของ และถือว่าเป็นสายลับที่มองไม่เห็นในการช่วยตรวจสอบและป้องกันคอมพิวเตอร์ของคุณแม้ในขณะที่ไม่ได้ใช้งาน Ardamax Keylogger สังเคราะห์และแจ้งให้ทราบกิจกรรมทั้งหมดที่ได้ทำกับคอมพิวเตอร์เช่นการพิมพ์การเข้าถึงเว็บไซต์การแลกเปลี่ยน E-mail, การสนทนากับเพื่อน, รหัสผ่าน, ข้อความ, และโปรแกรมประยุกต์ที่ทำงานบนคอมพิวเตอร์ ฯลฯ การแจ้งเตือนนั้นสามารถปรับตั้งค่าเวลาที่ต้องการแจ้งเตือนได้(นาที/ครั้งส่ง)

การติดตั้ง Ardamax Keylogger4.2 มีขั้นตอนดังนี้

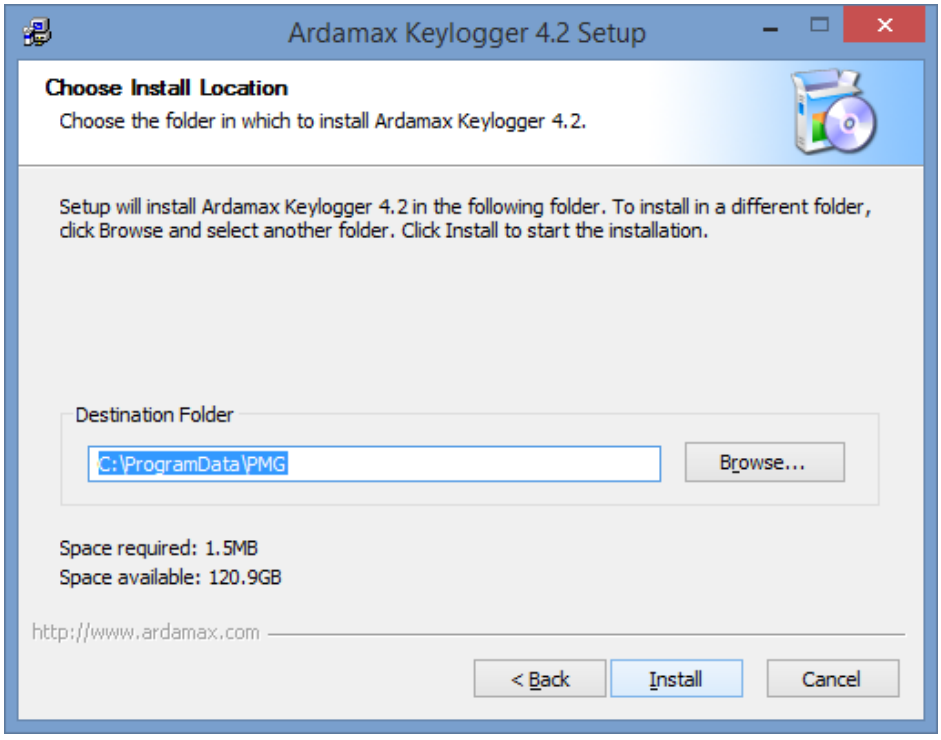
1. ขั้นตอนแรกเป็นการเริ่มติดตั้งโปรแกรม โดยดับเบิ้ลคลิก ที่ setup_aki.exe



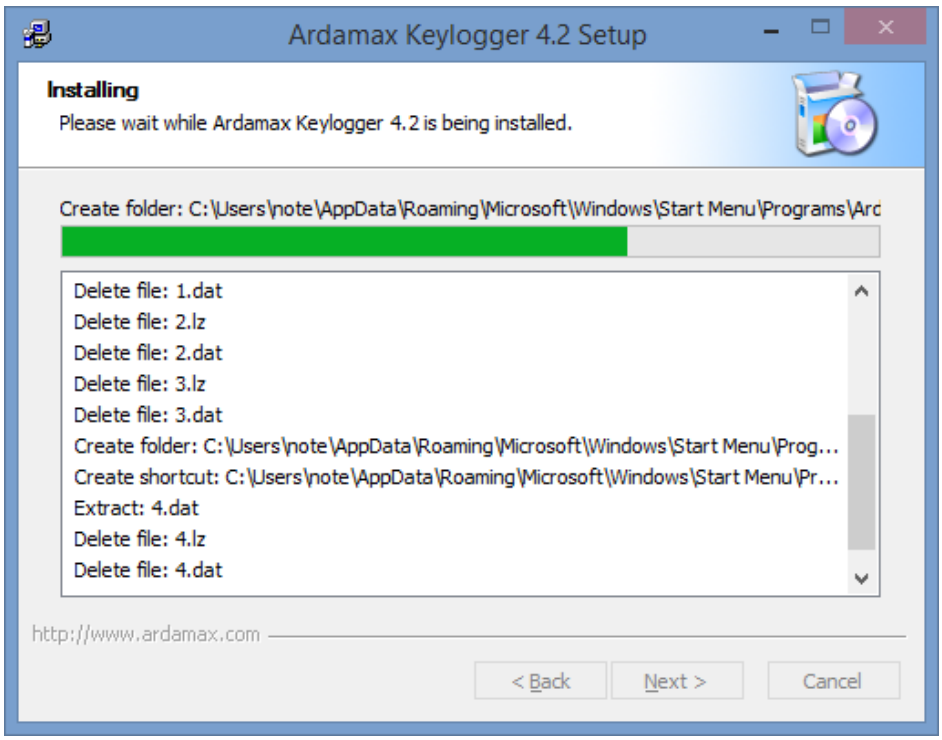
2. คลิก I Agree เพื่อยอมรับเงื่อนไขการใช้งาน



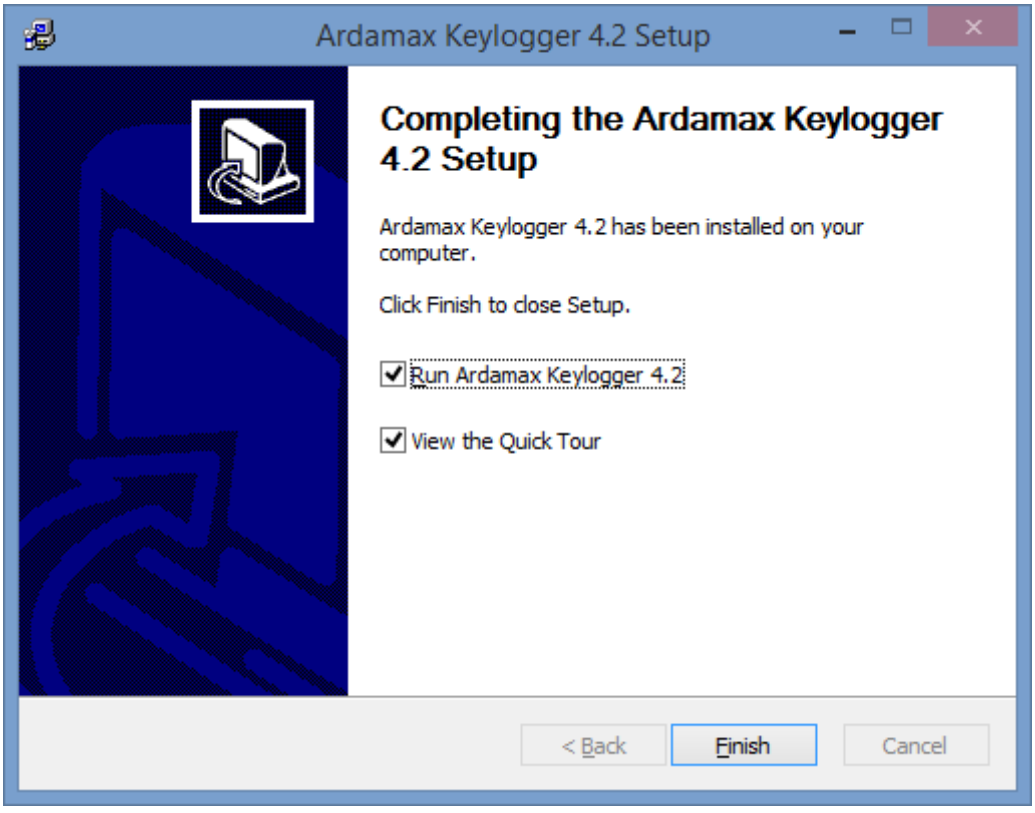
3. เลือก folder ที่ต้องการเก็บไฟล์ โดยเก็บไว้ที่ drive c:\ProgramData\PMG แล้วคลิก install เพื่อทำการติดตั้งโปรแกรม



4. หลังจากกด Install แล้วรอ การติดตั้ง

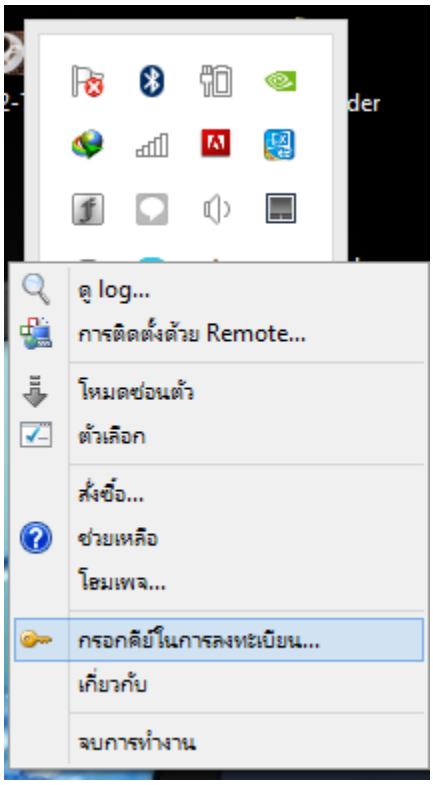


5. ติ๊กเลือก Run Ardamax Keylogger 4.2 และ View the Quick Tour c เมื่อเสร็จแล้วให้คลิกปุ่ม finish

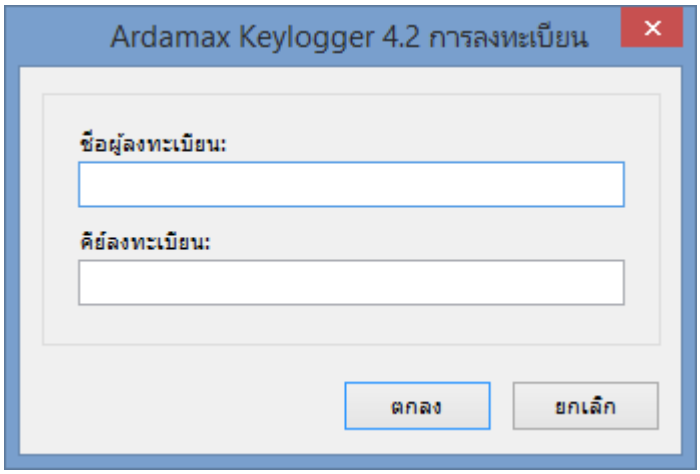


6. จะสังเกตเห็นไอคอน ตรงแถบ Task bar ด้านล่าง

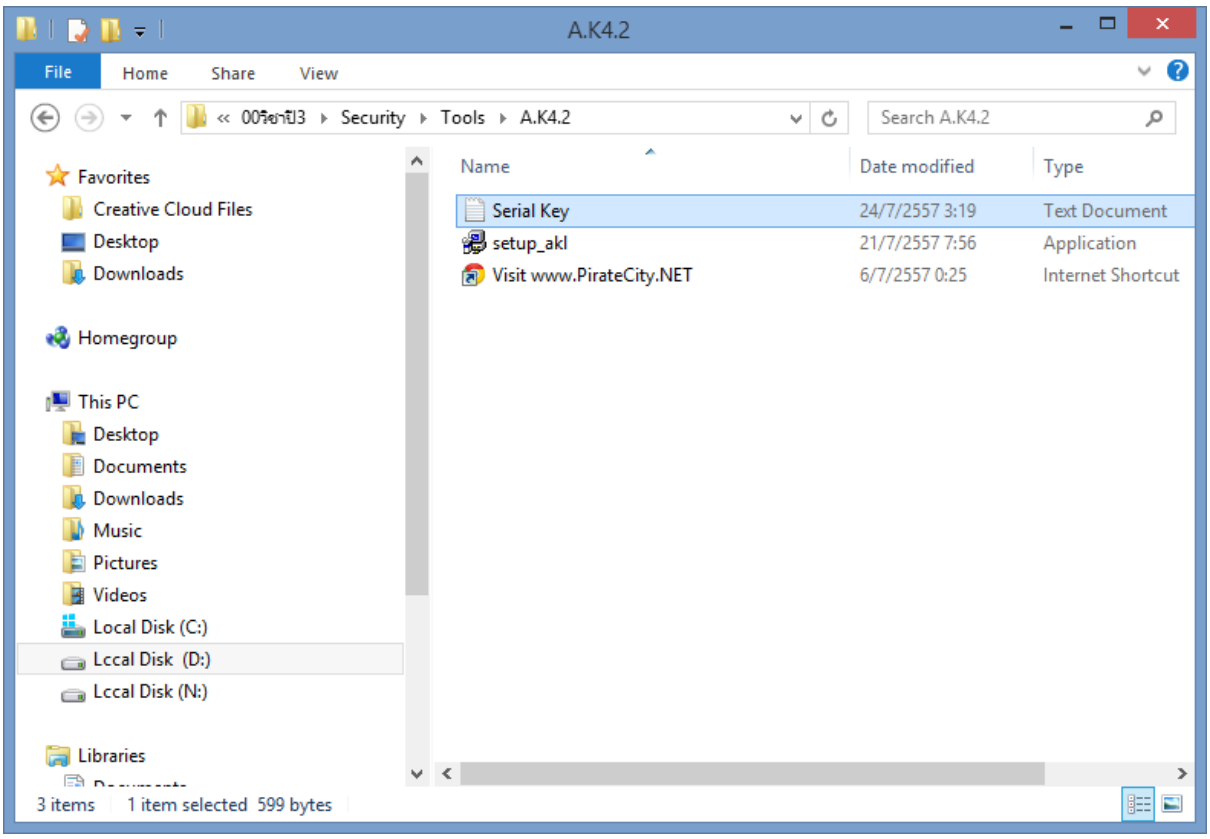
7. คลิกขวาที่ ไอคอน แล้วเลือก "กรอกคีย์ในการลงทะเบียน"



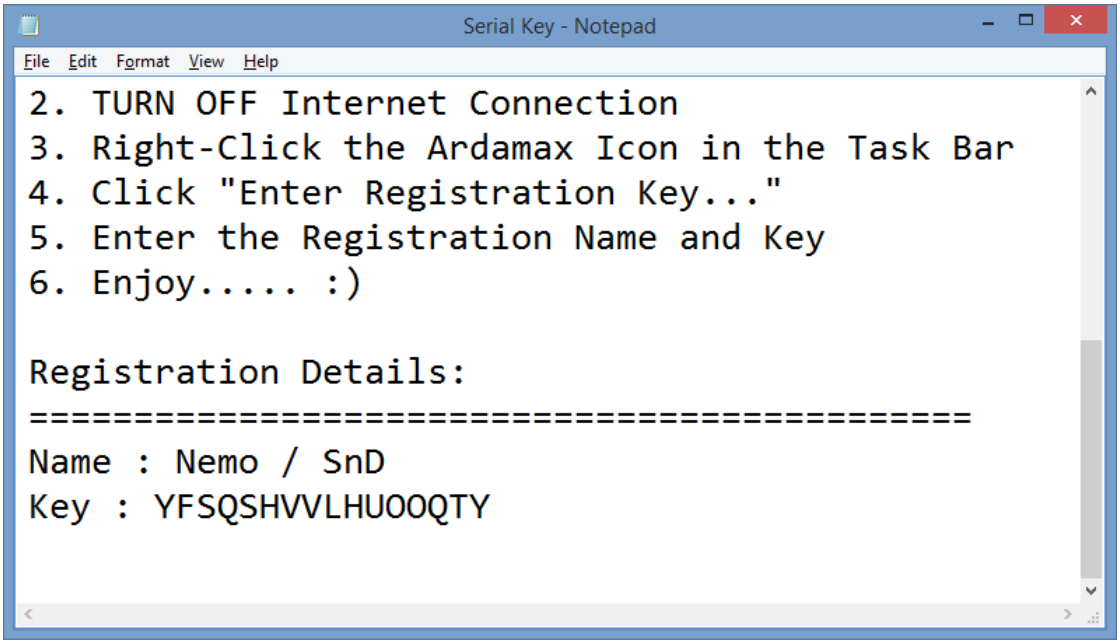
8. จากนั้น จะแสดงหน้าการลงทะเบียน เพื่อให้กรอกชื่อ และคีย์ที่ลงทะเบียน ลงในช่องที่กำหนด สำหรับคีย์ที่ใช้ลงทะเบียนนั้น ให้ดูในข้อที่ 11



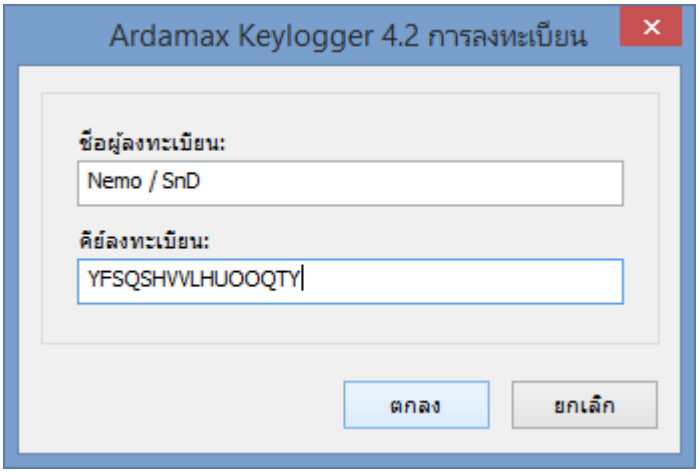
9. ให้เปิดไฟล์ Serial Key.txt ขึ้นมาเพื่อ เอา Name และ Key มาใส่



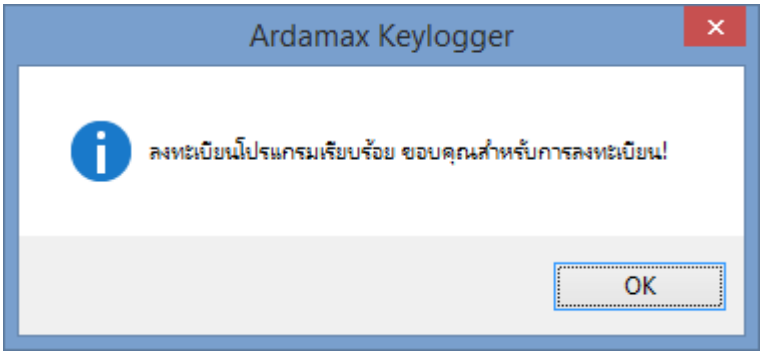
10. นำ Name และ Key ไปใส่เพื่อใช้ลงทะเบียนเข้าใช้โปรแกรม



11. ให้กรอกข้อมูล ของ ผู้ลงทะเบียน และ คีย์ลงทะเบียนให้ครบ

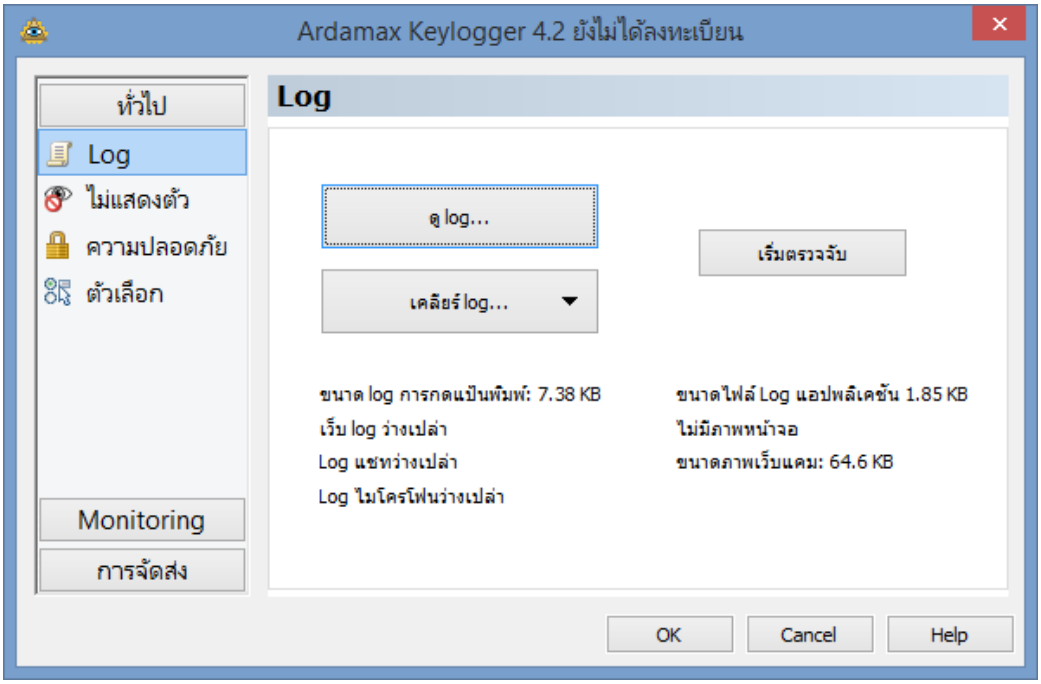


12. เสร็จสิ้นขั้นตอนการติดตั้งโปรแกรม

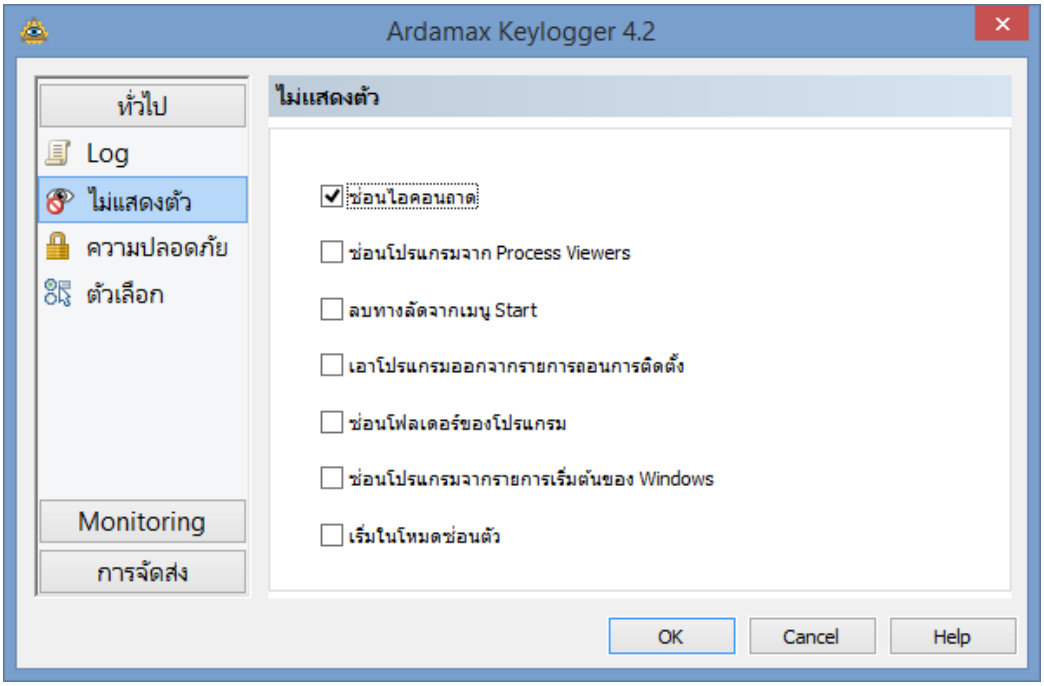


สำหรับการตั้งค่าการใช้งานมีขั้นตอนดังนี้

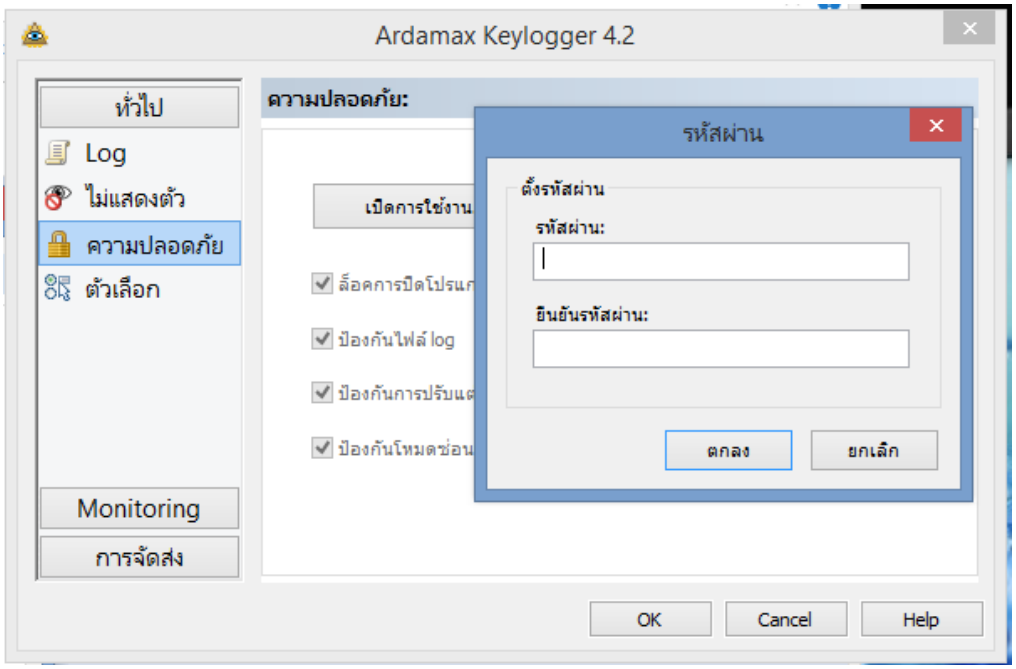
1. เข้าเริ่มเข้าสู้หน้าการตั้งค่า โดยเริ่มจากการตั้งทั่วไป ไปที่แถบทางซ้าย เลือกการตั้งค่า " Log "



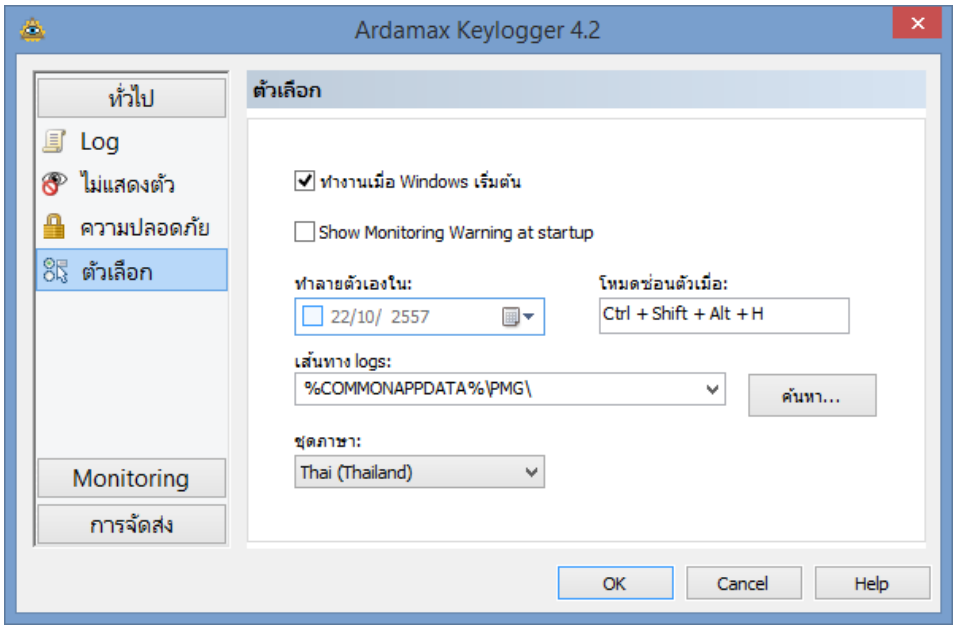
2. ไปที่แถบเมนูเลือก ไม่แสดงตัว ซึ่งขั้นตอนนี้เป็นการตั้งค่าการซ่อนตัวของโปรแกรม



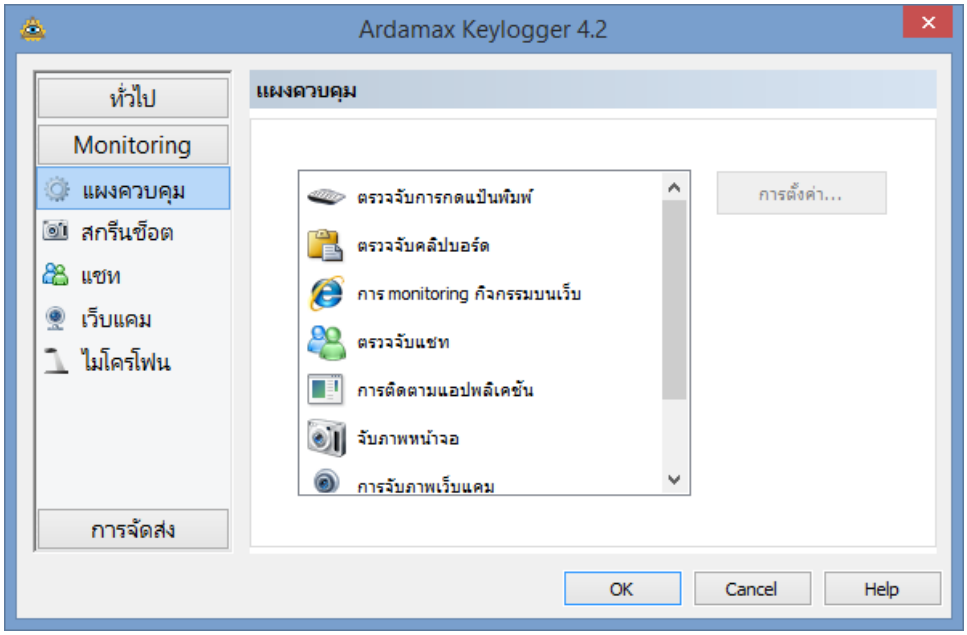
3. ไปที่แถบด้านข้างเลือก " ความปลอดภัย " เพื่อกำหนด รหัสผ่าน ในการเข้าใช้โปรแกรม จากนั้นกำหนดรหัสผ่านที่ต้องการ แล้ว กดตกลง



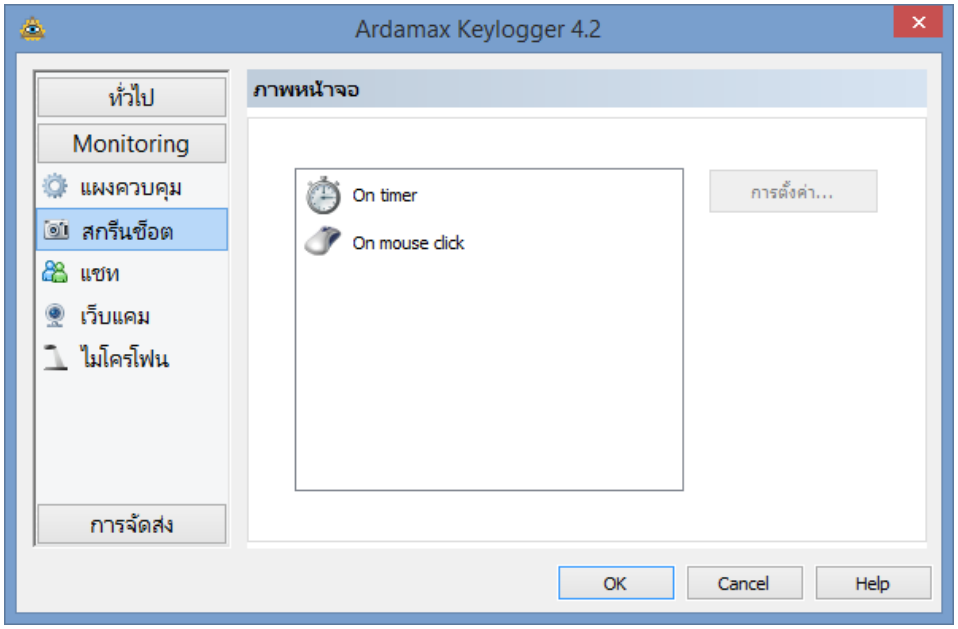
4. ขั้นตอนนี้เป็นการกำหนดตัวเลือกการทำงานของระบบ โดย double click ที่ "ตัวเลือก" จากแถบด้านข้าง แล้วตั้งค่าตามที่ต้องการ



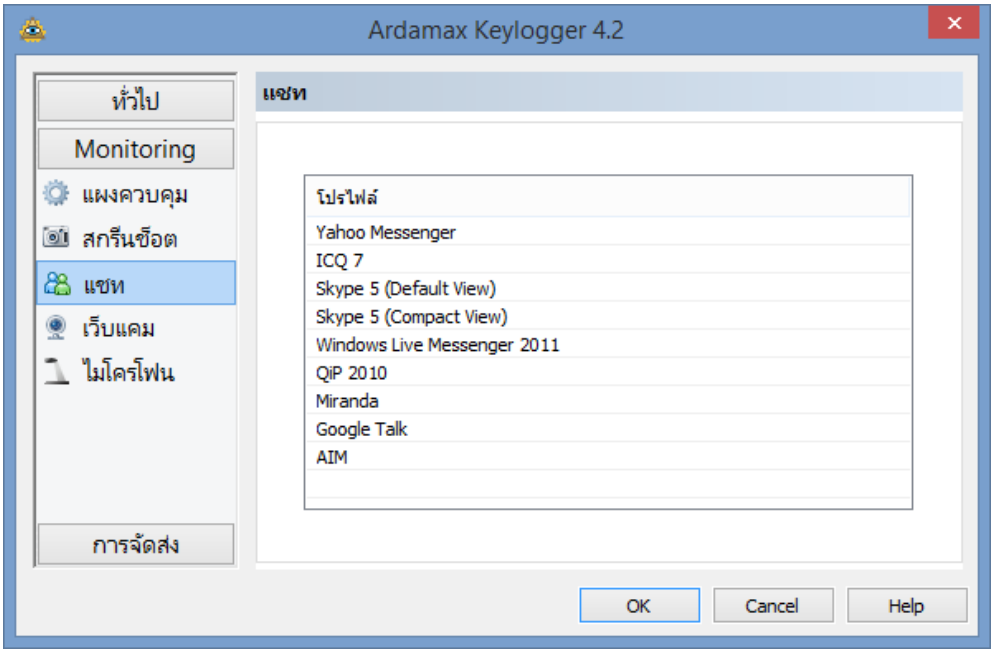
5. เลือกการตั้งค่า Monitoring เริ่มจากการตั้งค่าที่ "แผงควบคุม" เป็นการตั้งค่าการคุมควบส่วนต่างๆของโปรแกรมได้



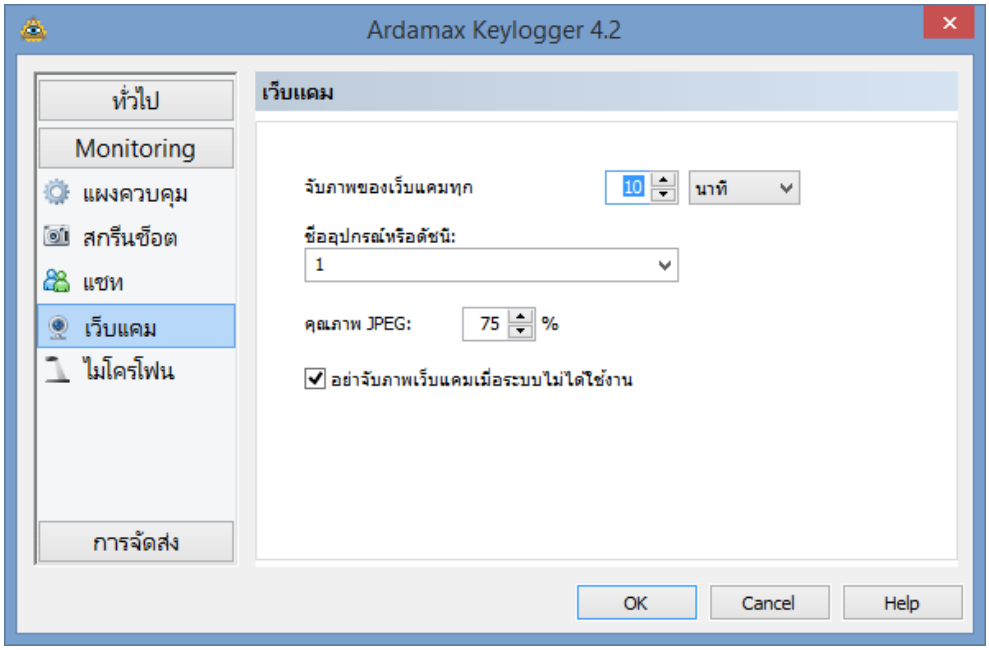
6. เลือกการตั้งค่า "สกรีนช็อต" เป็นการตั้งค่า กำหมดเวลา และการใช้เมาส์



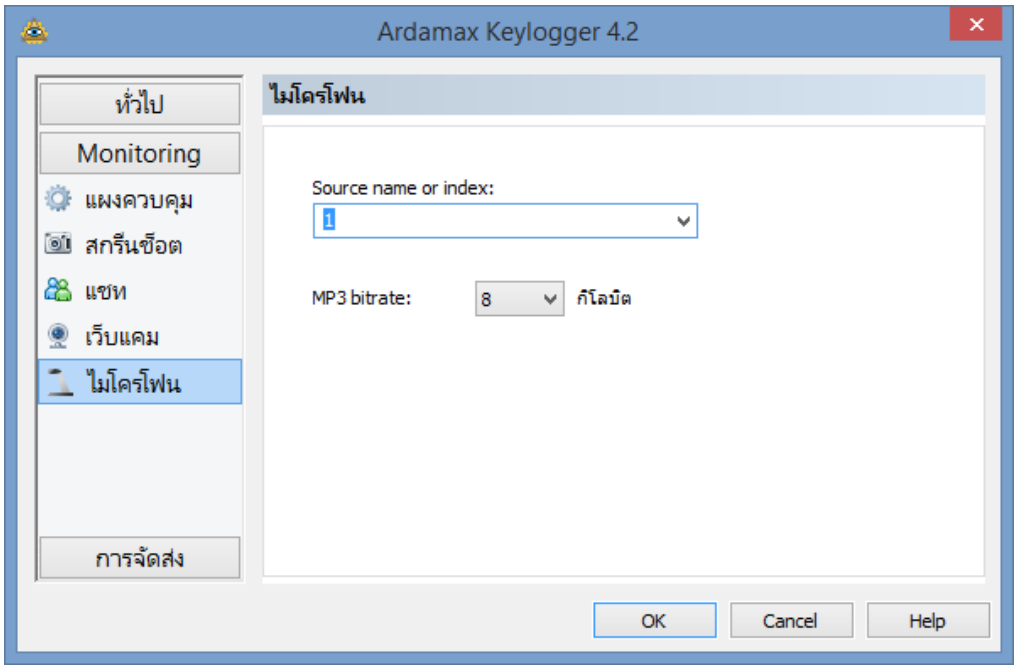
7. เลือกคลิกที่ไอคอน "แชท" ตรงแถบด้านซ้ายของหน้าต่าง จะแสดงรายละเอียดของโปรแกรมต่างๆ ที่เกี่ยวข้องกับการแชท ผ่านข้อความ



8. เลือกการตั้งค่า " เว็บแคม " เป็นการตั้งค่าเวลาที่จับความเคลื่อนไหวของการใช้งานคอมพิวเตอร์

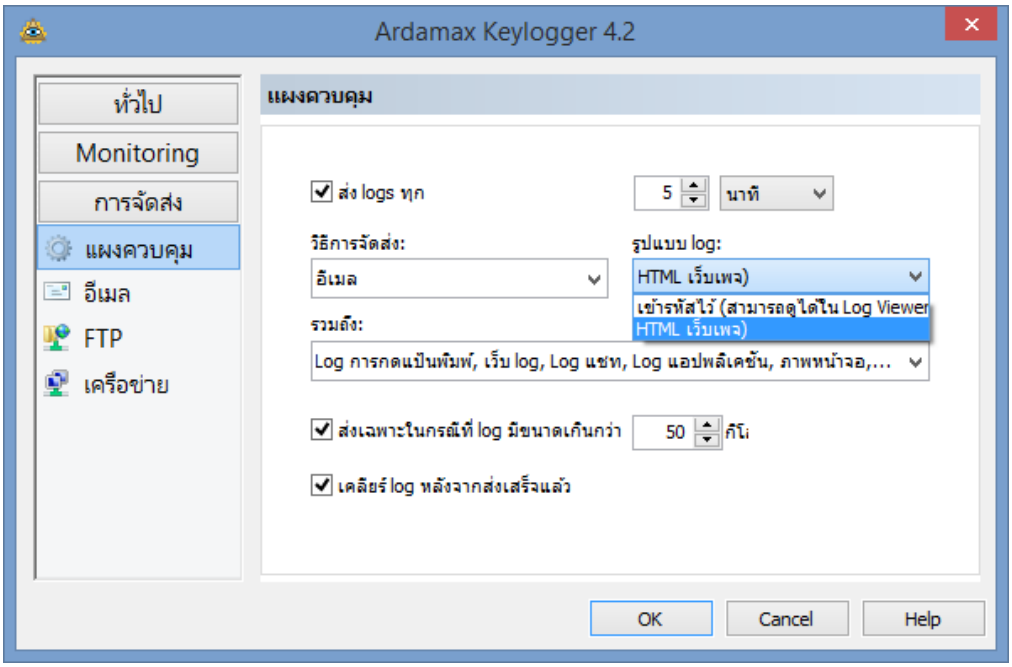


9. เลือกการตั้งค่าไมโครโฟน ในการบันทึกเสียง

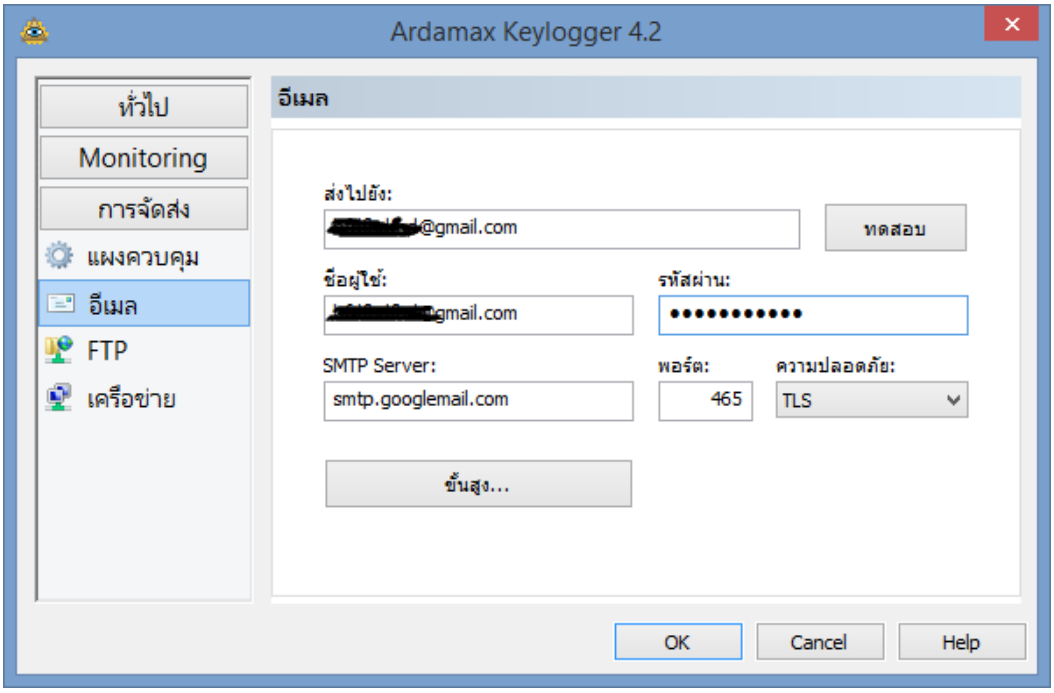


การจัดส่ง คือการส่งไฟล์ข้อมูลทุกอย่างไปยังที่อยู่ตามที่เราเลือกไว้โดยมีการตั้งค่าดังนี้

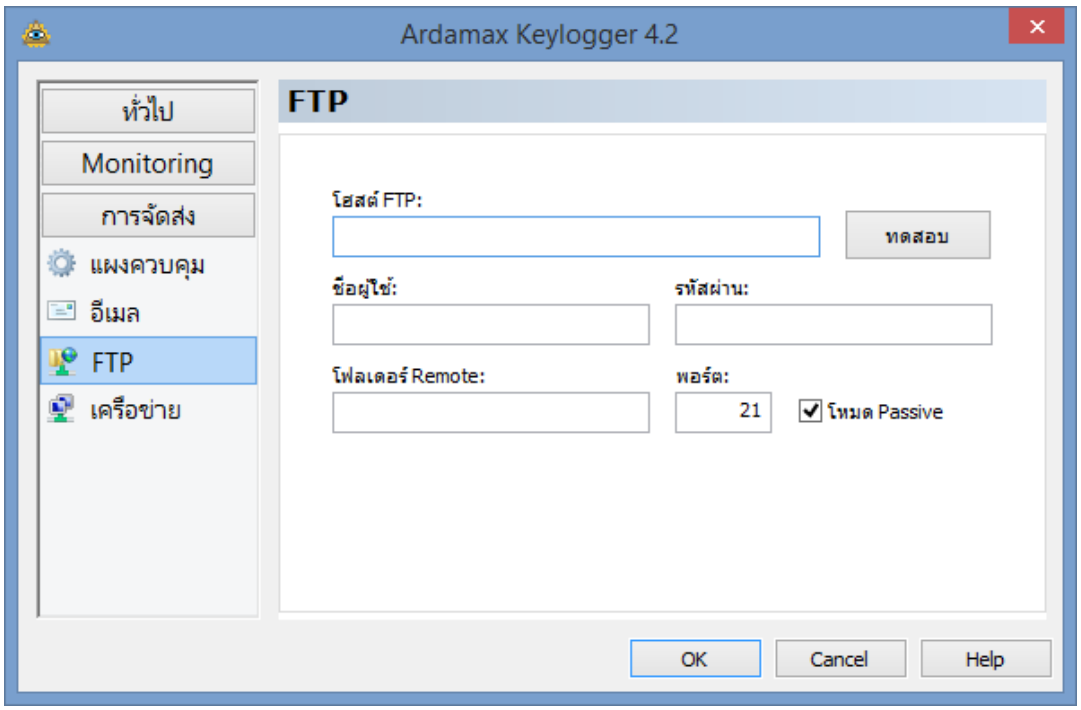
10. เลือกการตั้งค่าแผงควบคุม ขั้นตอนนี้เราสามารถตั้งค่าชนิดของไฟลีที่จะทำการส่งไปยังที่อยู่ที่เลือกไว้



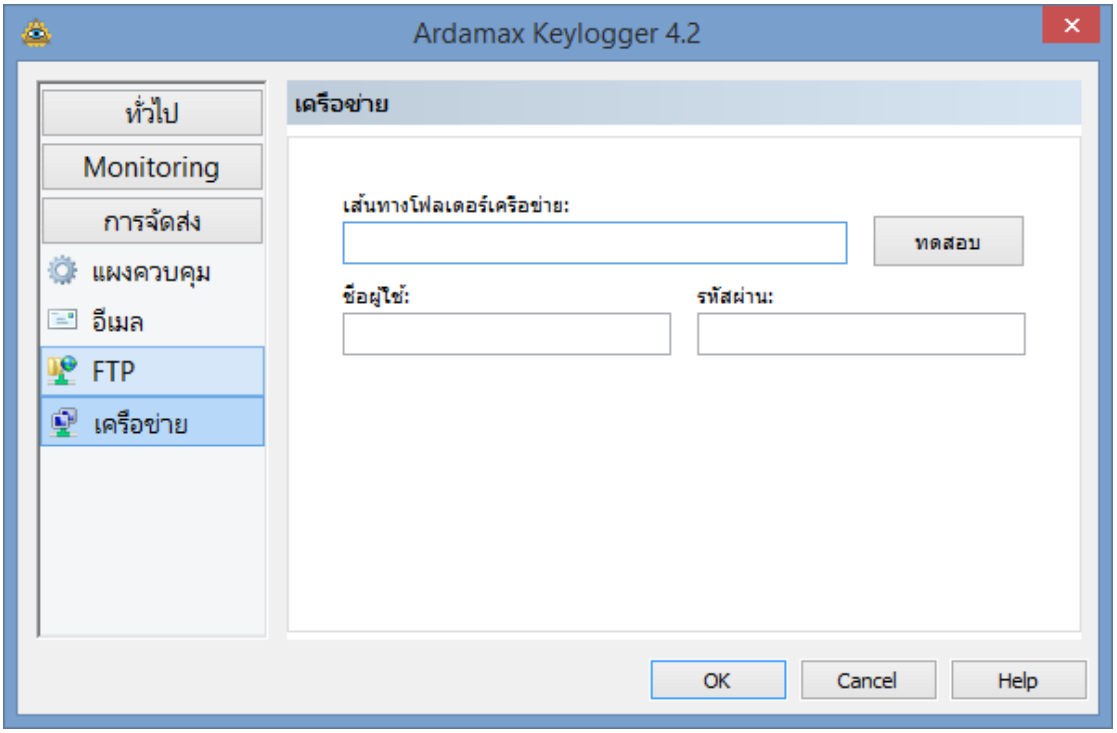
11. เลือกการตั้งค่า E-mail ขั้นตอนนี้เป็นการกำหนด E-mail ปลายทาง ที่ต้องการส่งข้อมูล



12. เลือกการตั้งค่า FTP

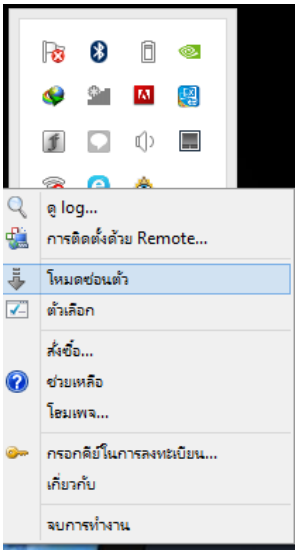


13. ตั้งค่าเครือข่าย

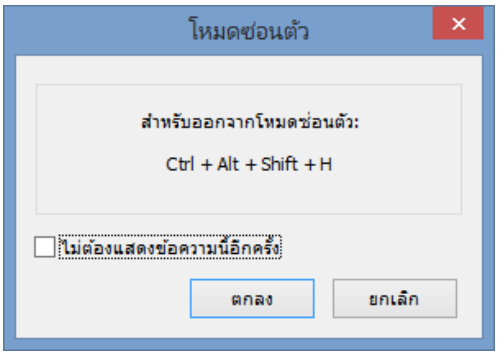


การตั้งค่าโหมดซ่อนตัว สารมารถซ่อนโปรแกรมไม่ให้แสดงได้ มีการตั้งค่าดังนี้

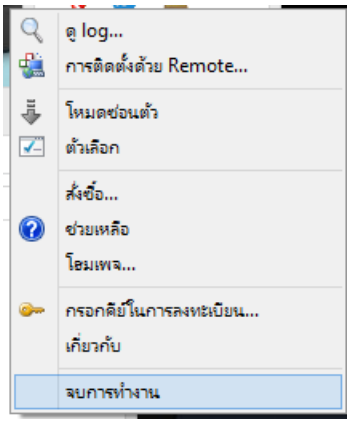
1. คลิกขวาที่ไอคอนโปแกรม ตรงแถบ Task bar ด้านล่าง เลือกโหมดการซ่อนตัว



2. หน้าต่างแสดง คีย์ลัด ในการออกจากโหมดซ่อนตัว

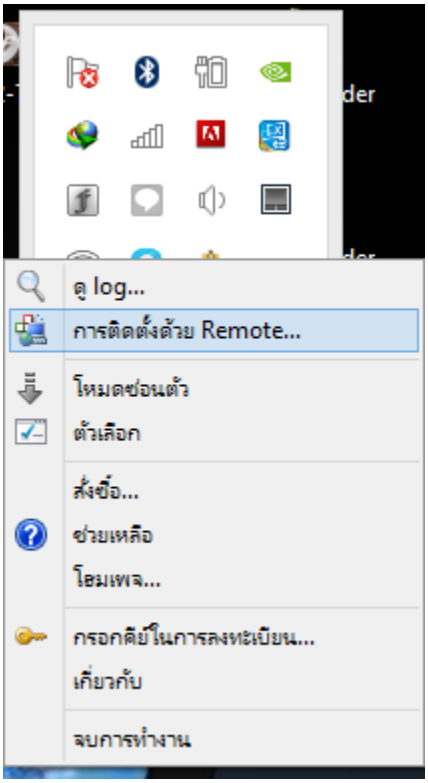


3. สามารถปิดโปรแกรมได้โดยการเลือกที่ จบการทำงาน

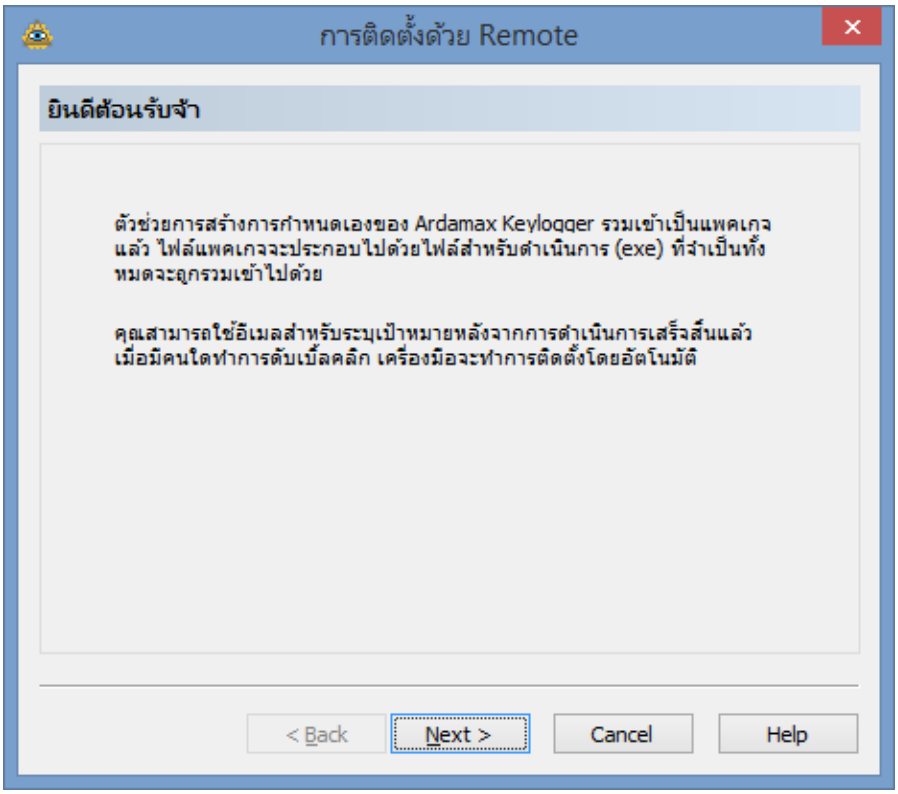


การตั้งค่าด้วย Remote คือการสร้างไฟล์ .exe ไปรันบนเครื่องเป้าหมาย มีการตั้งค่าดังนี้

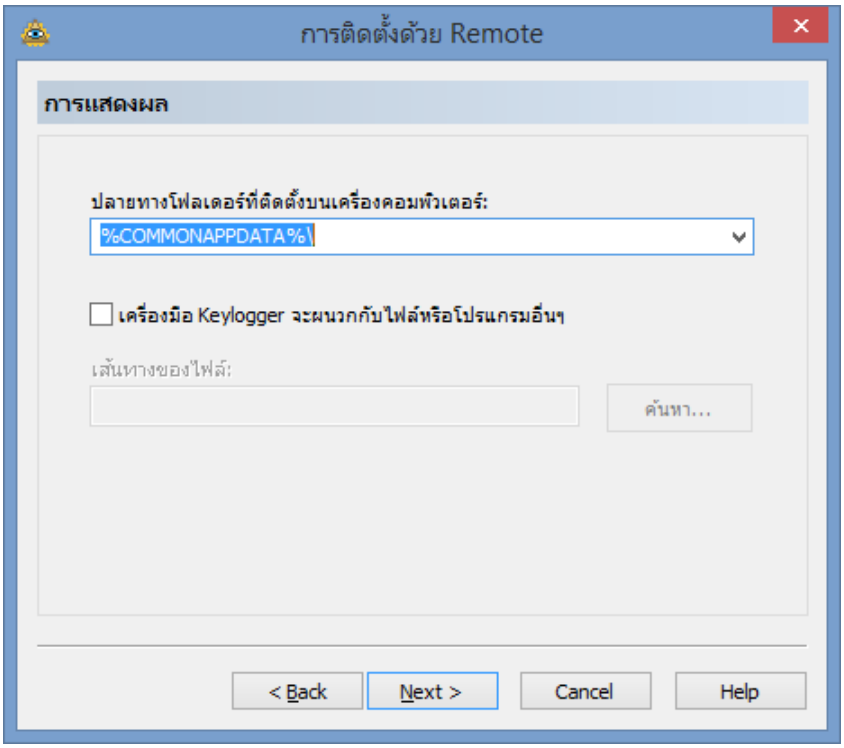
1. คลิกขวาที่ ไอคอน ของโปรแกรมเลือก "การติดตั้งด้วย Remote"



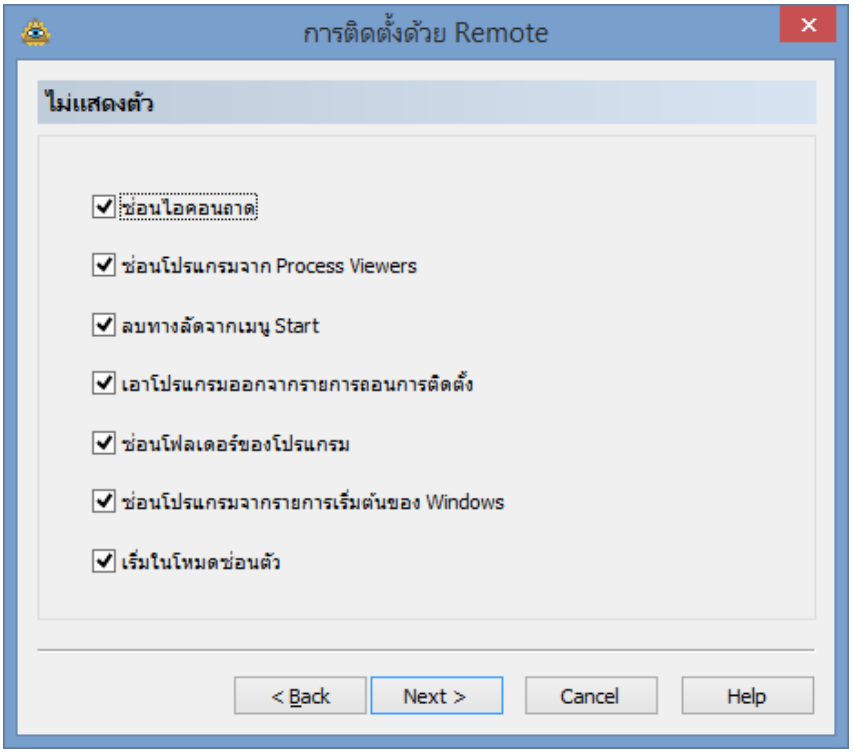
2. จะเห็นหน้าต่าง การติดตั้งด้วย Remote จากนั้น ให้ คลิกปุ่ม Next



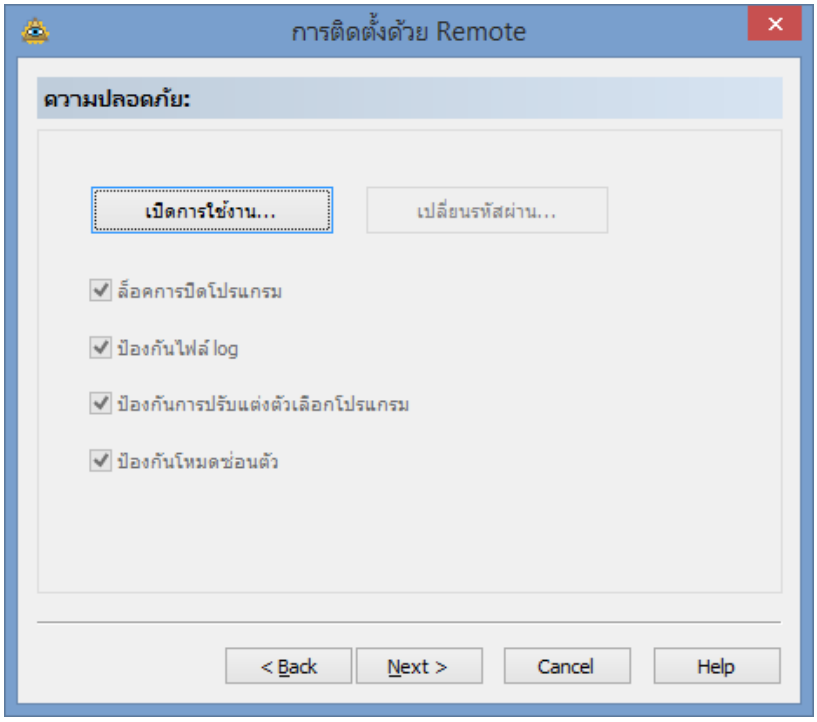
3. เลือกปลายทาง Folder ที่เก็บไฟล์ไว้บนเครื่องคอมพิวเตอร์ เสร็จแล้วกดปุ่ม Next



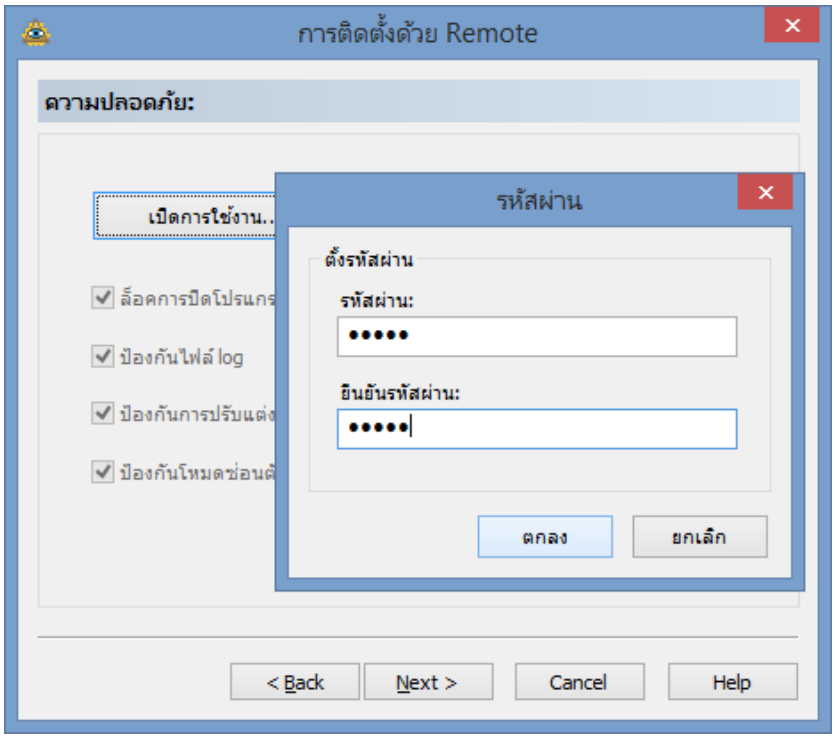
4. เลือกรูปแบบการแสดงตัว แล้วกด Next



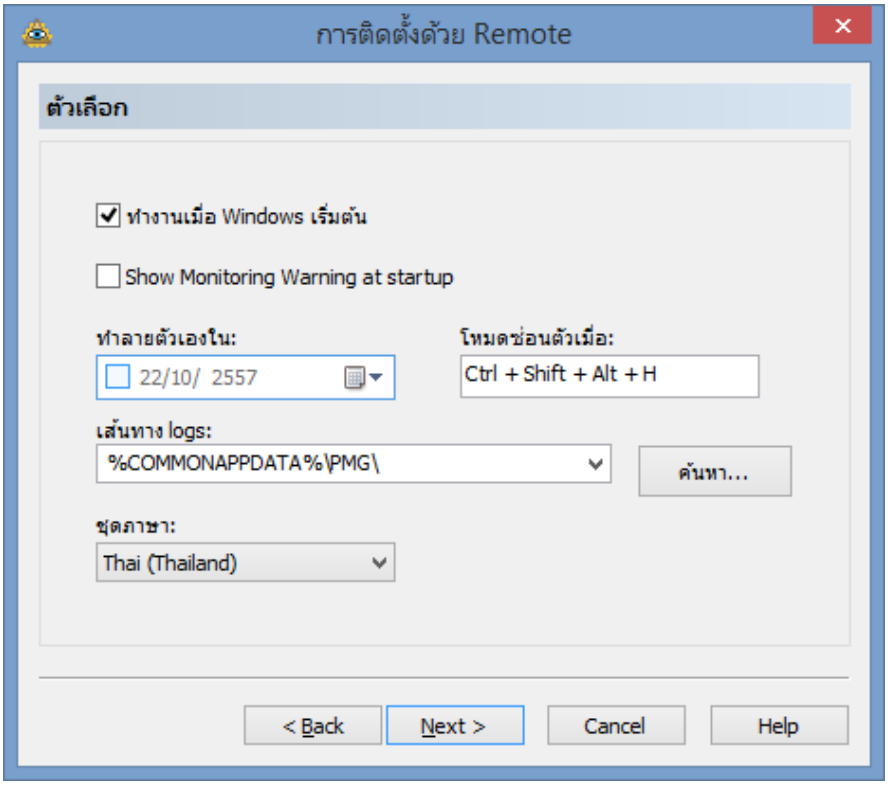
5. จากนั้นจะให้ตั้งค่าความปลอดภัยสามารถตั้ง Password ในการป้องการไม่ให้เข้าไปแก้ไขหรือดูข้อมูลต้นทางได้ จากนั้นคลิกที่เปิดการใช้งานแล้วกด Next



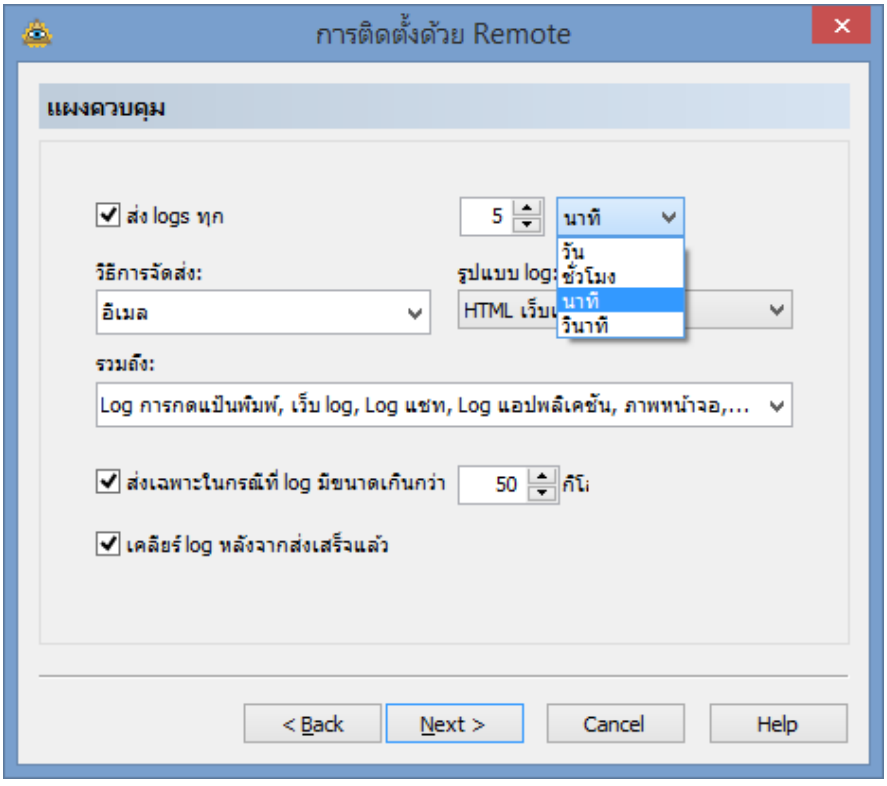
6. จากนั้นจะแสดง หน้าต่างให้กรอก รหัสผ่าน แล้วกด Next



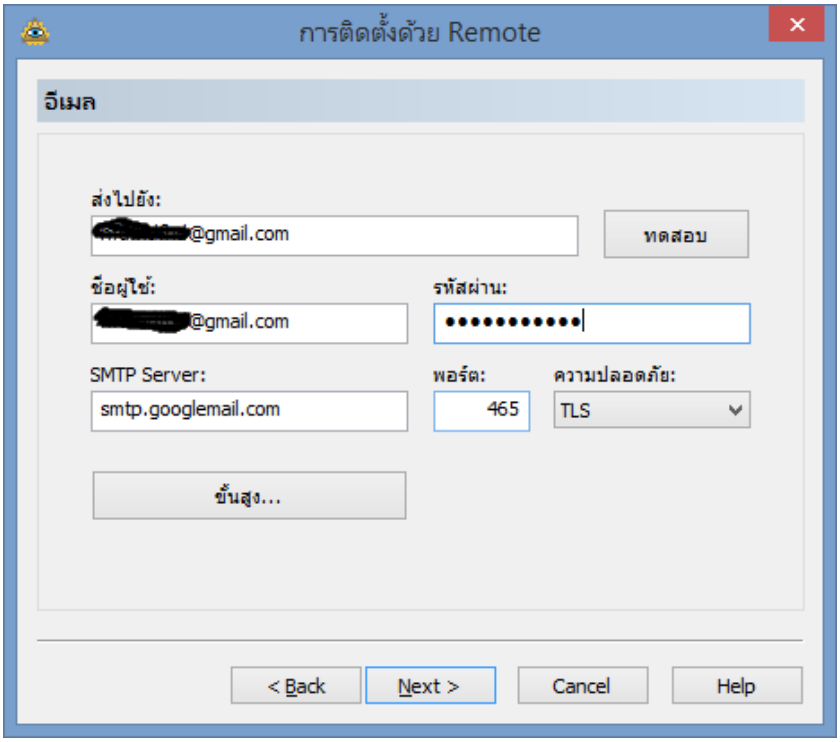
7. หน้าตัวเลือก เพื่อเลือก รูปแบบการทำงานของโปรแกรม จากนั้น กด Next



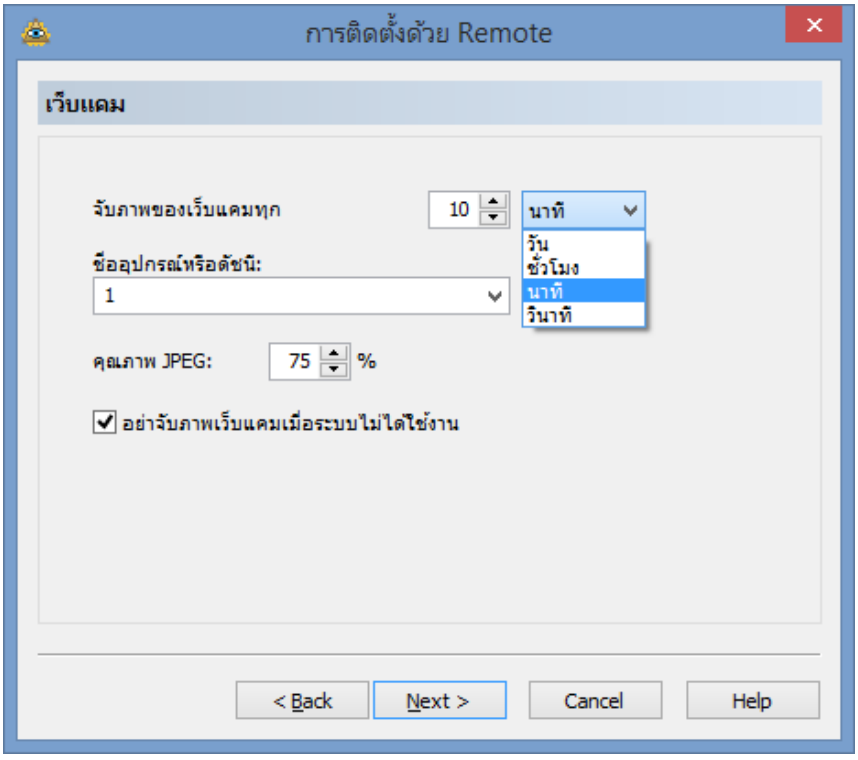
8. จะแสดงหน้า แผงควบคุมเพื่อ กำหนด การจัดส่ง ทั้งรูปแบบในการจัดส่ง เวลาในการจัดส่ง และขนาดไฟล์ที่จัดส่ง จากนั้น กด Next



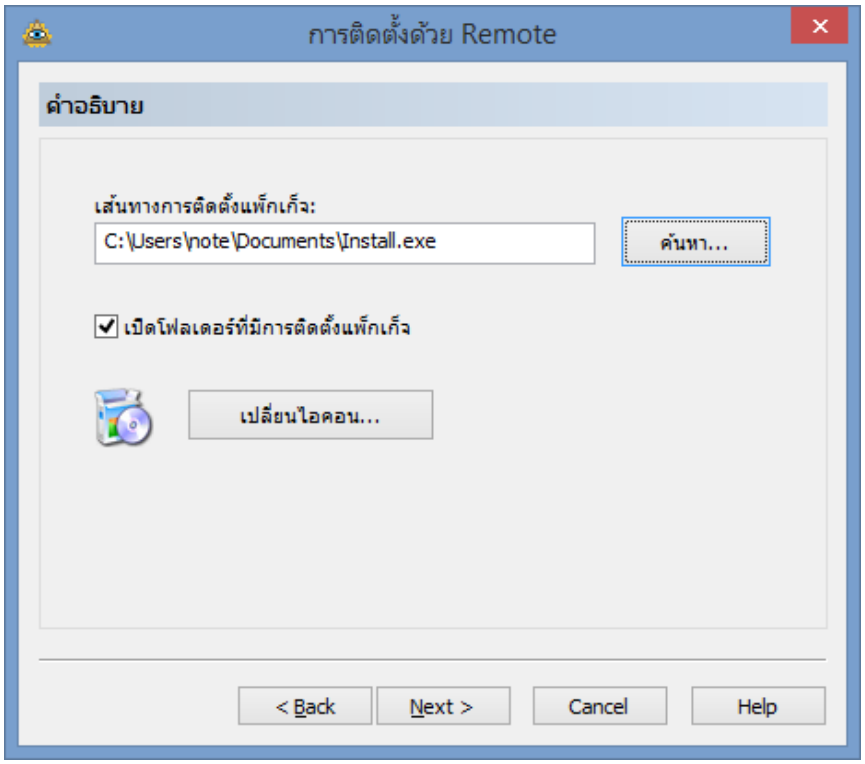
9. จากนั้นจะแสดงหน้า อีเมล หน้านี้จะเป็นการ กำหนด ปลายทางที่ต้องการส่งข้อมูล จากนั้นกด Next



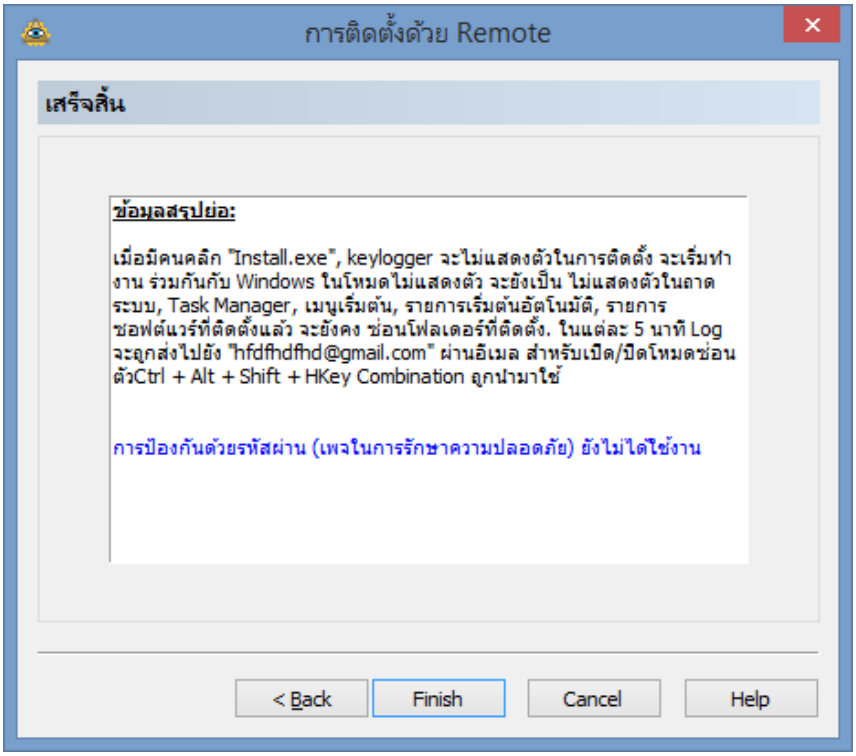
10. กำหนด เวลาในการจับภาพของ เว็บแคม



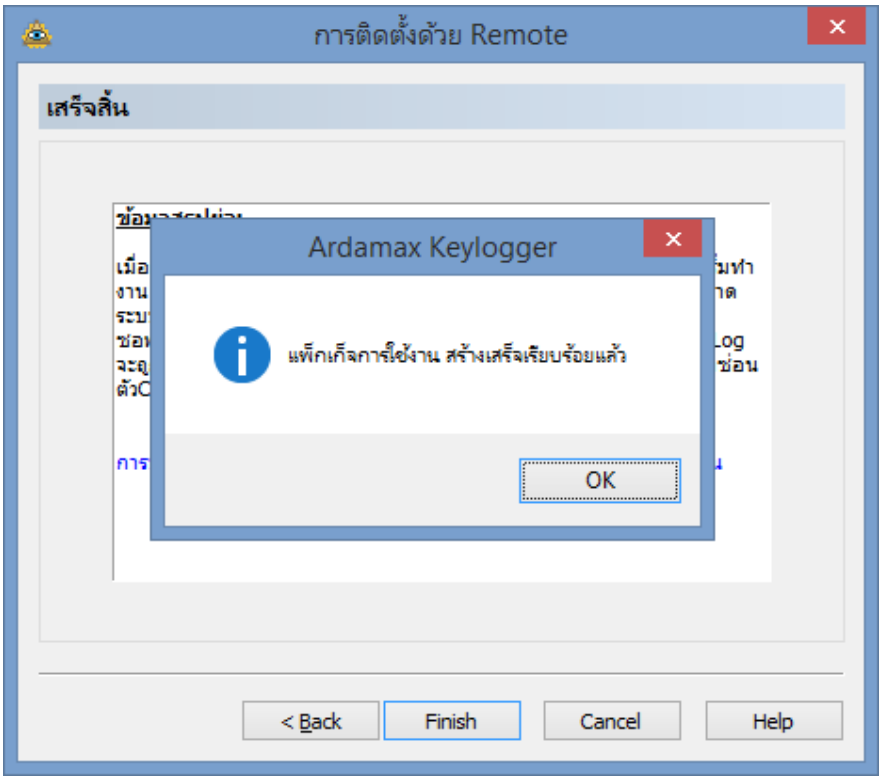
11. เลือกเส้นทางการติดตั้ง Packet



12. ติดตั้งเรียบร้อย จากนั้นกดปุ่ม finish



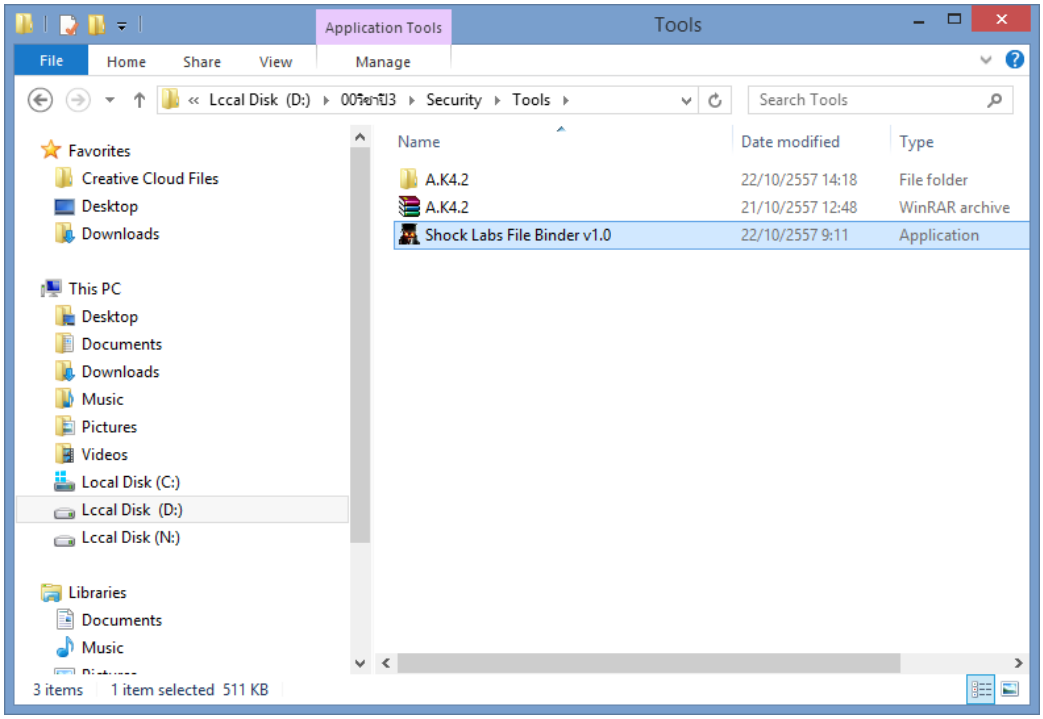
13. เสร็จสิ้นขั้นตอนการติดตังด้วย รีโมท จากนั้น กด OK



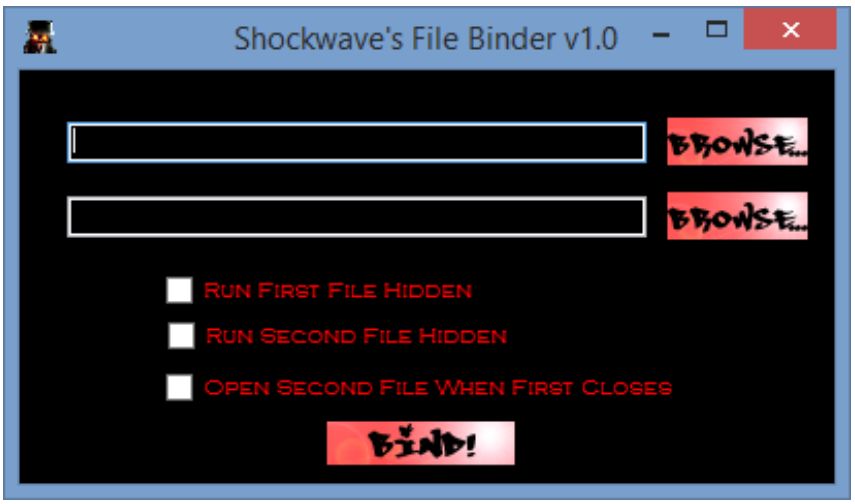
การแฝงไฟล์ สามารถแฝงไฟล์ไปกับไฟล์รูปภาพหรือไฟล์เพลงก็ได้

ในการแฝงไฟล์มีรูปแบบขั้นตอนดังนี้

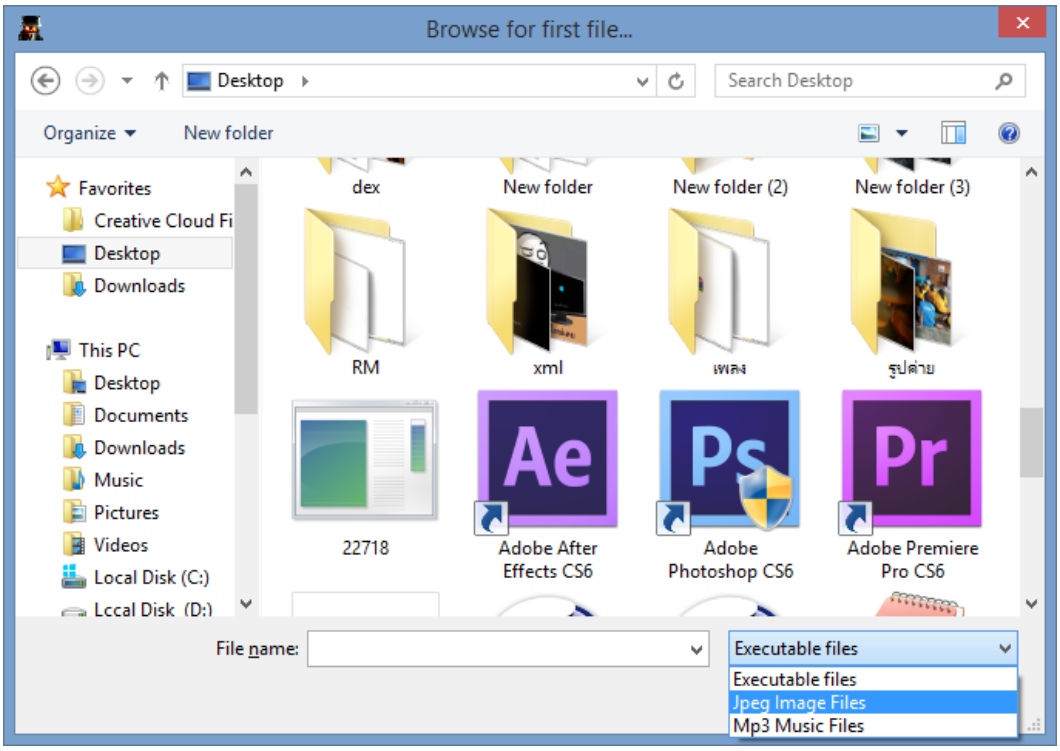
1. Double Click ที่ไอคอน Shock labFle Binder v1.0



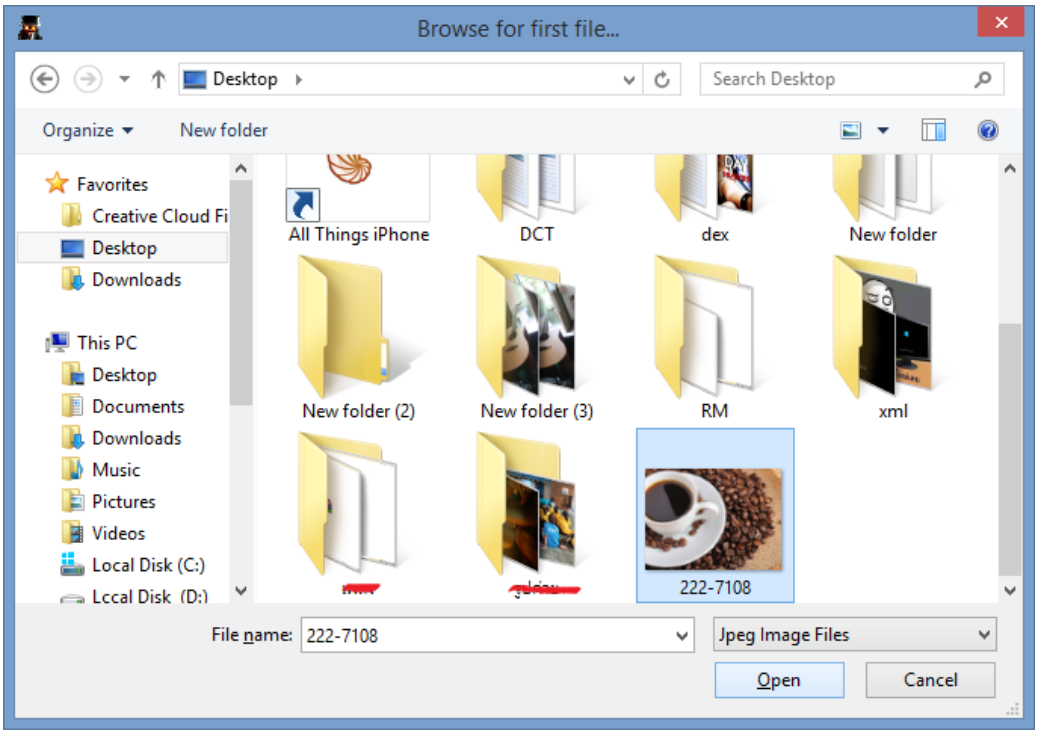
2. จะเห็นหน้าต่าง Shockwave's File Binder V1.0 .ให้เลือก Browser ในช่องด้านบนคือเลือกไฟล์ที่ต้องการจะแฝงโปรแกรมไป



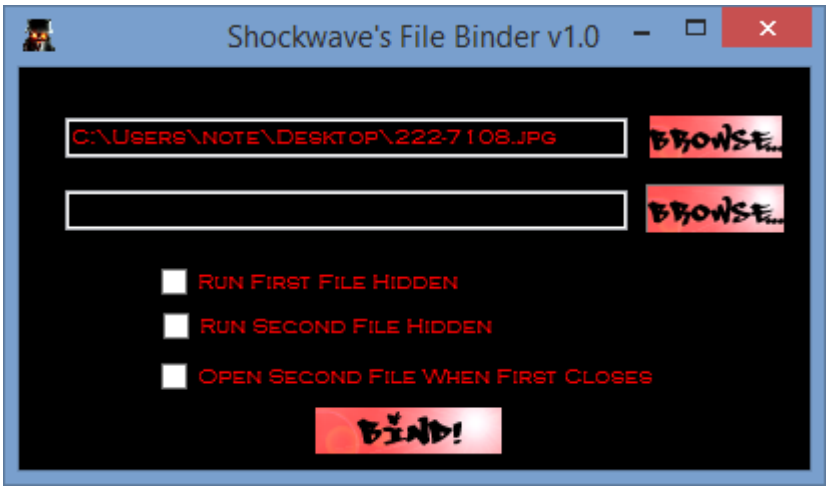
3. เลือกไฟล์ที่ต้องการ (ยกตัวอย่างเป็นไฟล์ Jpeg Image Files)



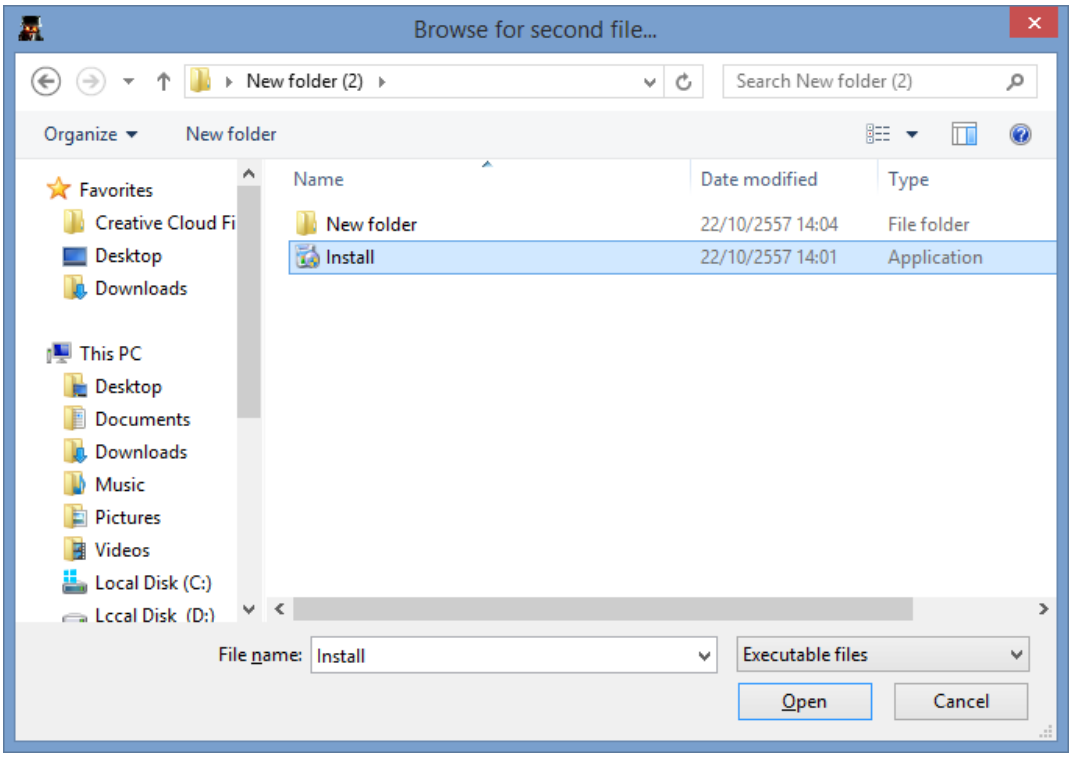
4. เลือกไฟล์ที่ต้องการแล้วกด Open



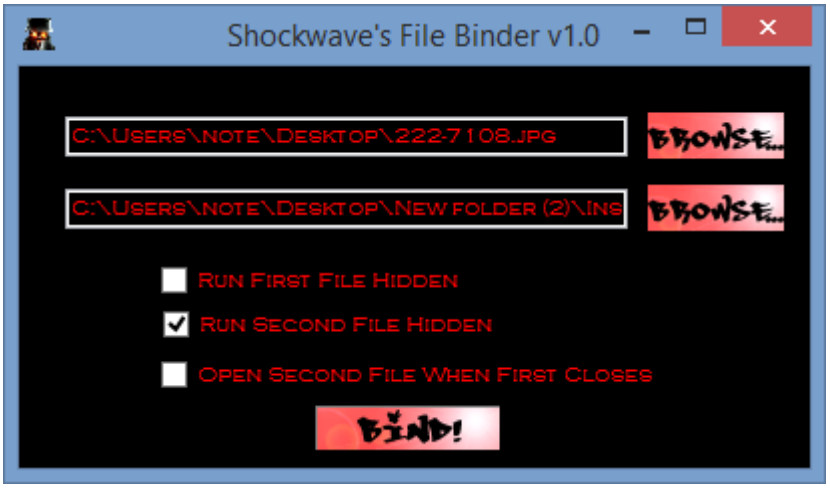
5. ต่อมาในช่องด้านล่างคือเลือกไฟล์ที่ได้ทำการสร้างขึ้นมาในขั้นตอนการ Remote



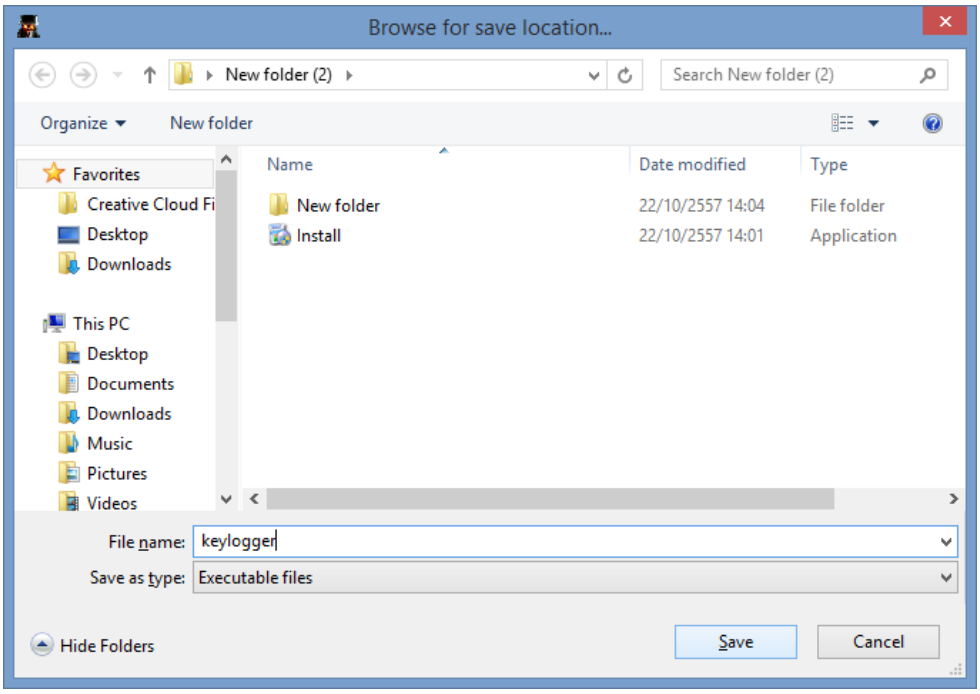
6. ไฟล์จะอยู่ในรูปแบบ Install.exe ที่ได้สร้างไว้แล้ว จากนั้นกด Open



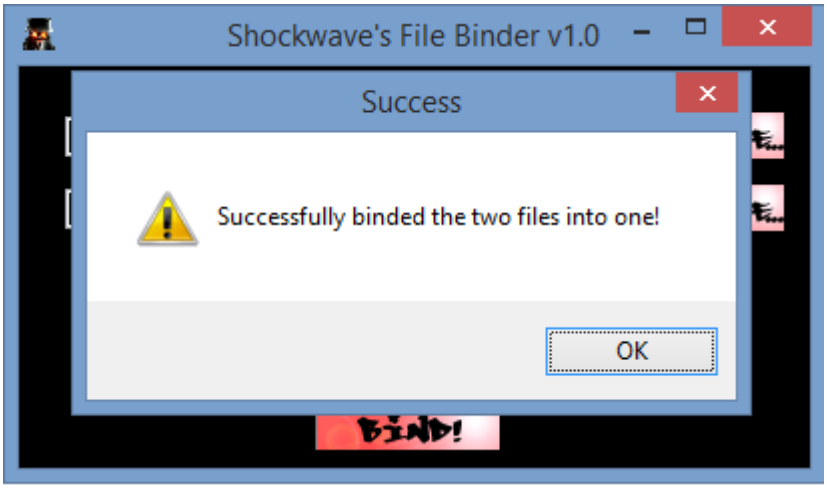
7. เลือกที่ “RUN SECOND FILE HIDDEN”



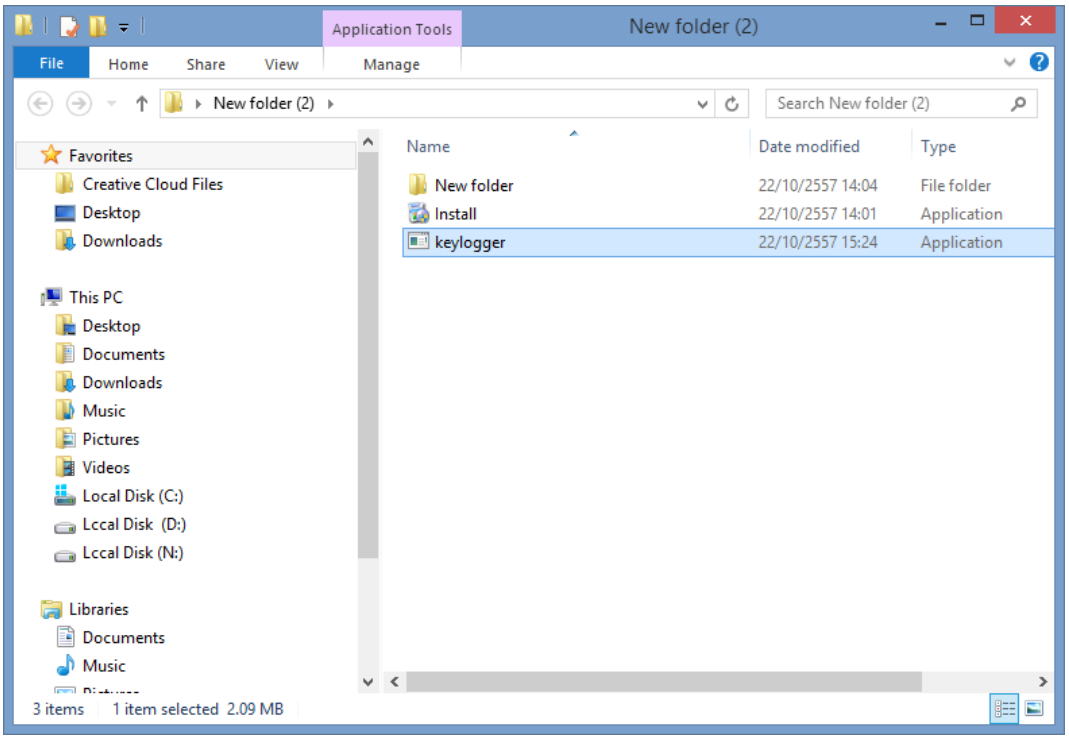
8. เลือกที่อยู่เก็บไฟล์ Save เป็น Executable files



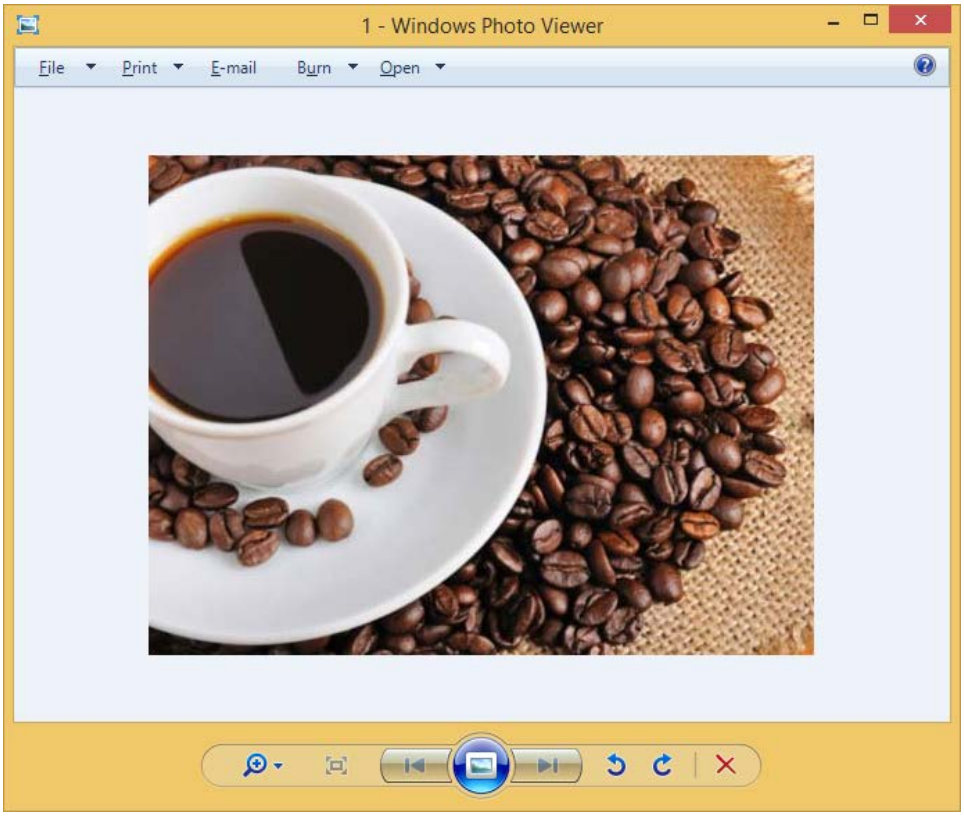
9. จากนั้นจะเห็นหน้าต่าง Success ให้กด Ok



10. จะได้ไฟล์สำหรับ ติดตั้งบนเครื่อง พร้อมตัว Install

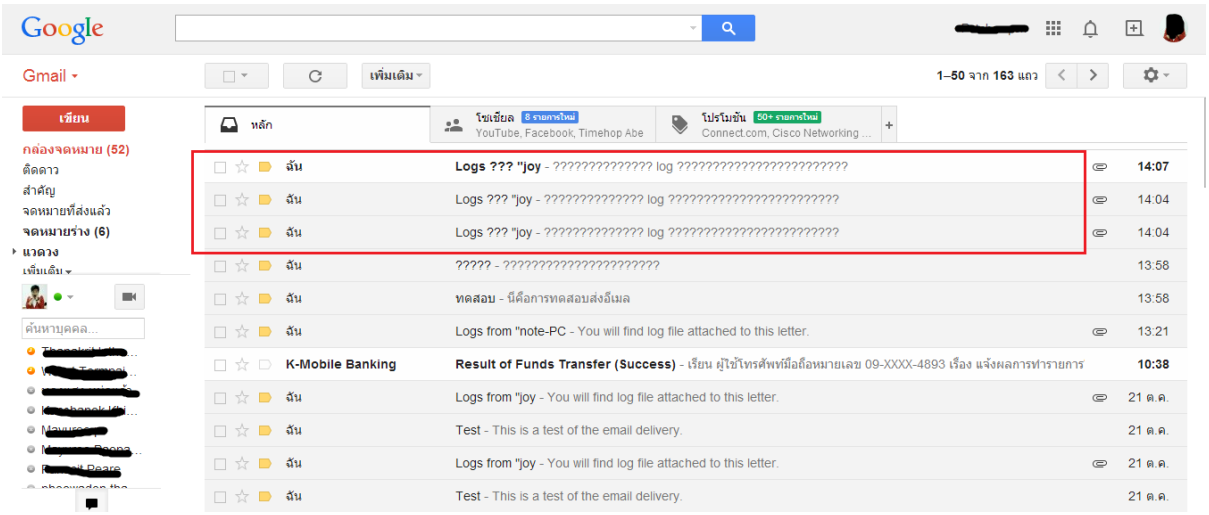


11. จะได้ไฟล์ตัวโปรแกรมจะอยู่ในรูปภาพนี้ ซึ่งเป็นการซ่อนโปแกรมไว้ หาก กดเปิดรูปนี้ขึ้นมาจะมีการ Install files ที่ซ่อนไว้ทันที โดยผู้ใช้ อาจไม่รู้ตัว

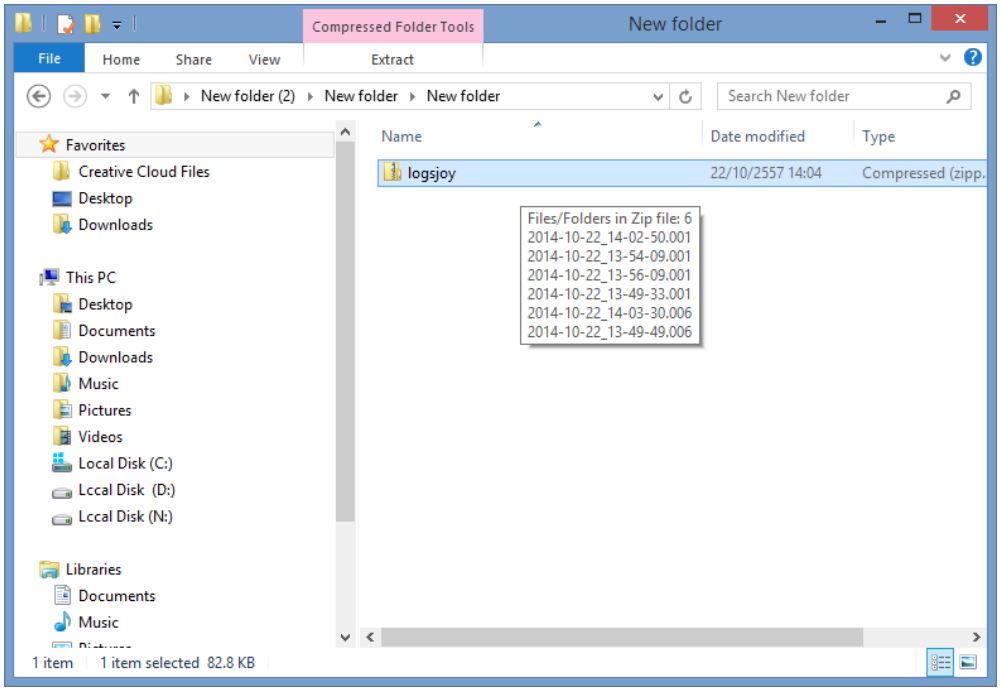


การส่งไฟล์ผ่านทาง E-mail

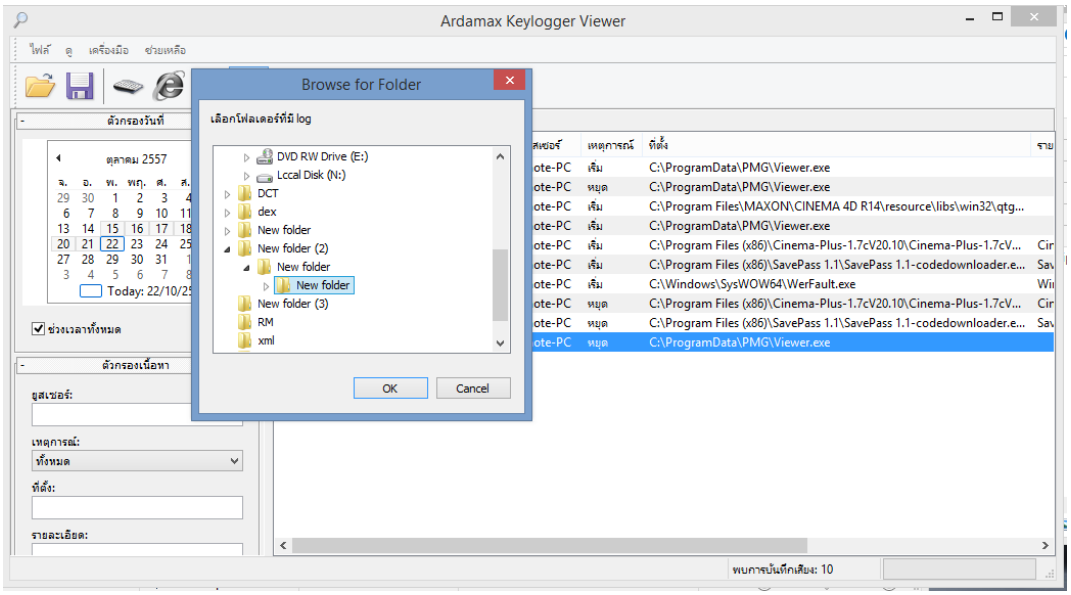
1. โปรแกรมจะส่งข้อมูลทั้งหมด ตามเวลาที่ตั้งไว้ผ่านมาทาง Mail แล้วทำการโหลดไฟล์นั้นมา



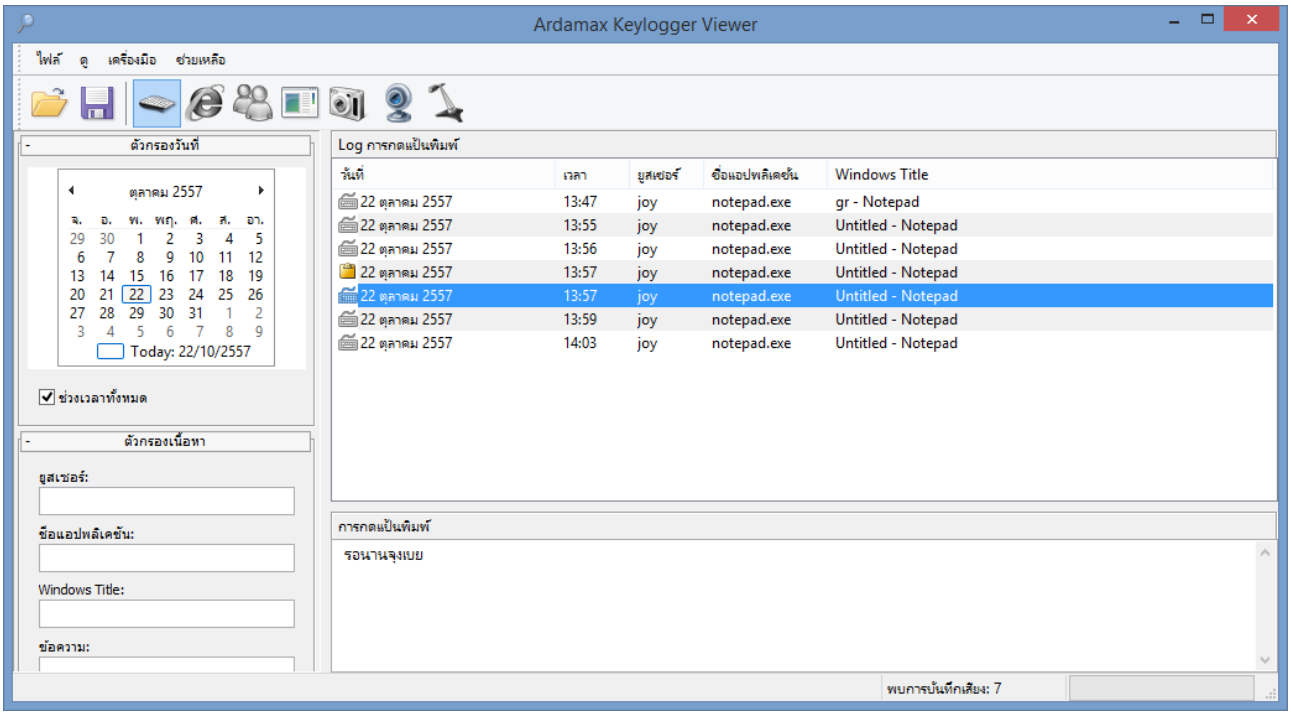
2. จากนั้นก็ทำการแตกไฟล์ที่โหลดมา



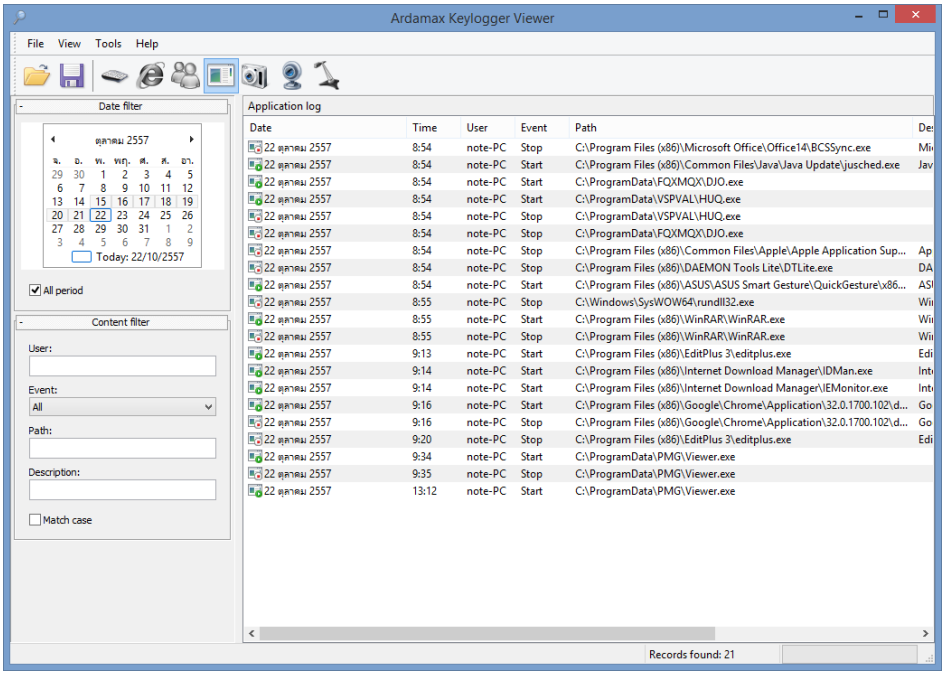
3. จากนั้นเลือกที่อยู่ที่ต้องการเก็บไฟล์



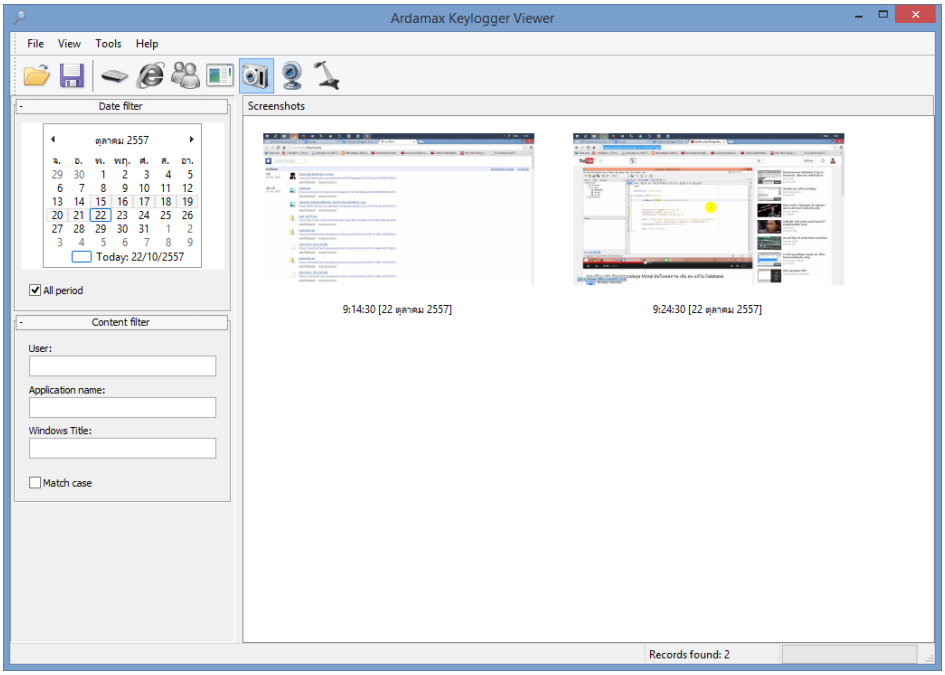
4. เลือกดูข้อมูลที่พิม์ลงไปบน keyboard จะเก็บทุกตัวที่พิมพ์ลงไป



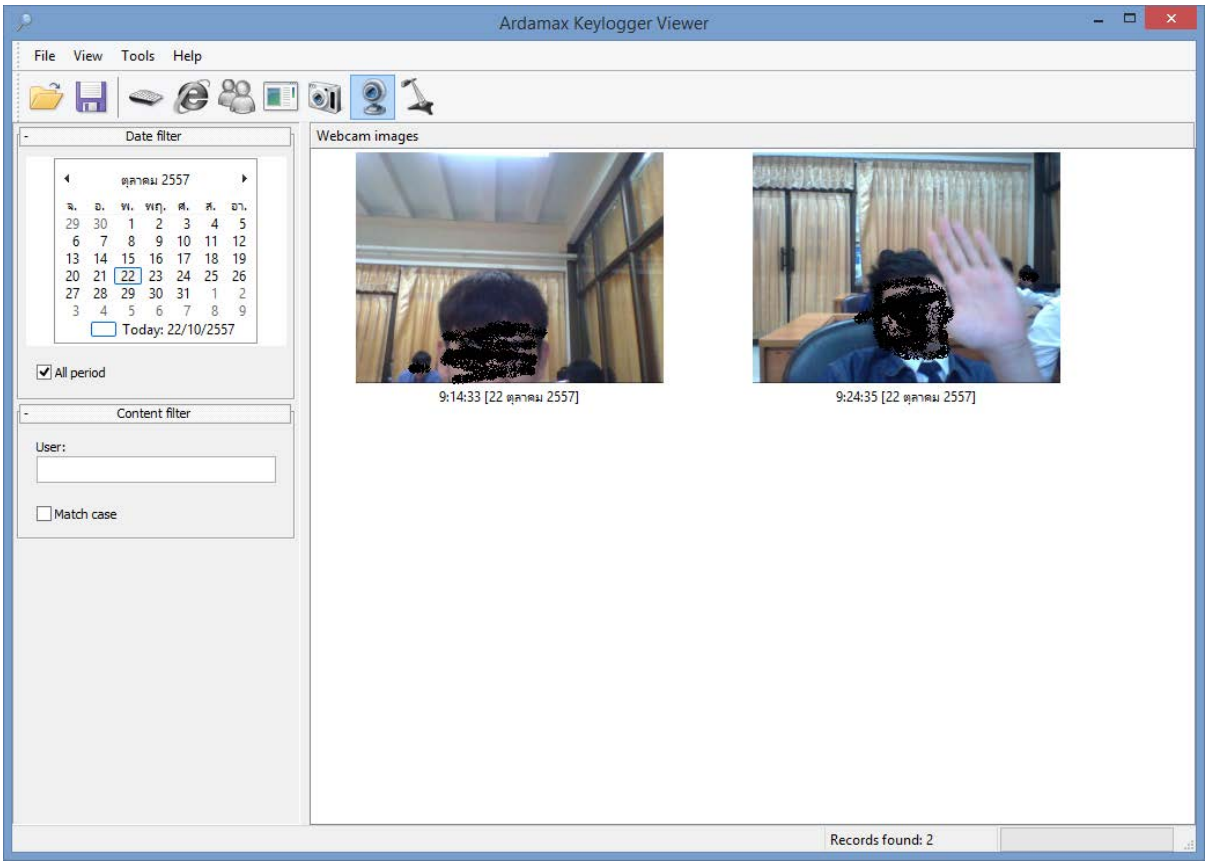
5. เลือกดูโปรแกรมที่ได้เข้าใช้งานในเครื่องนั้นได้ว่าเข้าใช้โปรแกรมอะไรบ้าง



6. ไฟล์รูปภาพการใช้งานบนหน้าจอ



7. ไฟล์จากกล้องเว็บแคม จะได้รู้ว่ามีใครใช้คอมพิวเตอร์เครื่องนั้นบ้าง



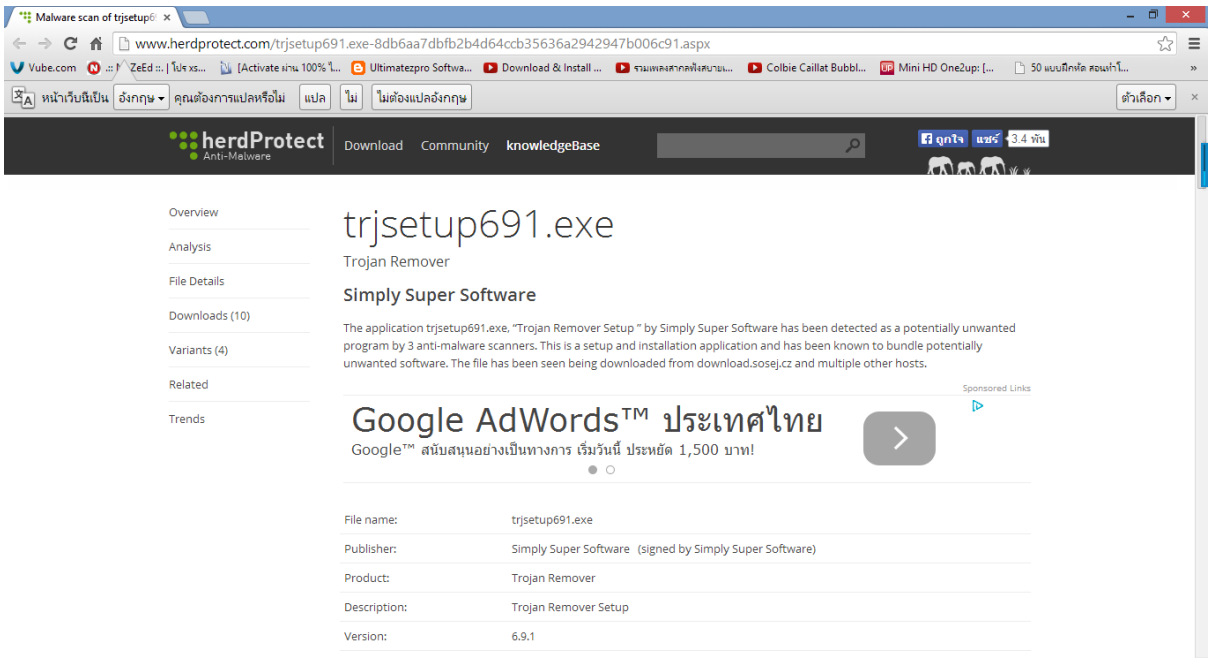
---------- จบการทำงาน ----------

วิธีการถอดการติดตั้งโปรแกรม

สามารถทำได้ดังนี้

วิธีที่ 1

สามารถดาวน์โหลดโปรแกรมสแกนไวรัสมาใช้ทำการสแกนหาเพื่อกำจัดออกได้และยังสามารถหาไฟล์แปลกปลอมเพื่อกำจัดได้อีกด้วย



สามารถดาวน์โหลดได้ตามลิ้งนี้

http://www.herdprotect.com/trjsetup691.exe-8db6aa7dbfb2b4d64ccb35636a2942947b006c91.aspx

หากยังหลงเหลืออยู่สามารถทำตามขั้นตอนนี้ได้

วิธีที่ 2

1.กดคีย์ลัด Alt+Ctrl+Shift+h เพื่อเปิดโหมดแสดงตัว

2.คลิกขวาที่โปรแกรมแล้วกด Exit

3.ไปที่ C:/PragramData/.... โดยชื่อFolder ของโปรแกรมนี้จะเป็นตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ทุกตัวจะมี 6 ตัวอักษรเป็นชื่อที่ไม่มีความหมาย

4.ลบทั้ง Folder เพียงเท่านี้คอมพิวเตอร์ของคุณก็จะปลอดภัยแล้ว