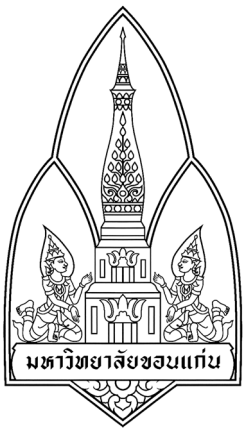


โปรแกรม Charles

โดย

1. นางสาวศิริลักษณ์ ดีกุดต้ม รหัสนักศึกษา 573020439-8
2. นายศุภกิตติ์ บุตรจันทร์ รหัสนักศึกษา 573020440-3
3. นายภูวกร บูรณ์เจริญ รหัสนักศึกษา 573021157-3
4. นางสาวสโรชา แตมสำราญ รหัสนักศึกษา 573021168-8
5. นางสาวสายสุดา ขันณะราย์ รหัสนักศึกษา 573021169-6
6. นางสาวสุวีณา บุดดาศรี รหัสนักศึกษา 573021174-3

อาจารย์ที่ปรึกษา: รศ.ดร.จักรชัย โสอินทร์

รายงานนี้เป็นส่วนหนึ่งของการศึกษาวิชา 322376 ความมั่นคงเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคเรียน 1 ปีการศึกษา 2559

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

มหาวิทยาลัยขอนแก่น

รายงานการเสนอโปรแกรม Charles

ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

ชื่อ นางสาวศิริลักษณ์ ดีกุดต้ม รหัสนักศึกษา 573020439-8

นายศุภกิตติ์ บุตรจันทร์ รหัสนักศึกษา 573020440-3

นายภูวกร บูรณ์เจริญ รหัสนักศึกษา 573021157-3

นางสาวสโรชา แตมสำราญ รหัสนักศึกษา 573021168-8

นางสาวสายสุดา ขันณะราย์ รหัสนักศึกษา 573021169-6

นางสาวสุวีณา บุดดาศรี รหัสนักศึกษา 573021174-3

นักศึกษาระดับปริญญาตรี หลักสูตรวิทยาศาสตร์บัณฑิต สาขาเทคโนโลยีสารสนเทศและการสื่อสาร

อาจารย์ที่ปรึกษาโครงงาน ผศ.ดร.จักรชัย โสอินทร์

1. ชื่อหัวข้อโครงงาน

ชื่อโปรแกรม : Charles

2. หลักการและเหตุผล

ในปัจจุบันการรักษาข้อมูลให้มีความปลอดภัยนั้นเป็นไปได้ยาก เพราะมีโปรแกรมมากมายที่ใช้ในการเจาะข้อมูล ไม่ว่าจะเป็นข้อมูลทางธุรกิจ ข้อมูลขององค์กร หรือแม้แต่ข้อมูลส่วนตัวของแต่ละบุคคล ซึ่งถ้า Hacker ได้เข้าถึงข้อมูลต่างๆเหล่านั้นแล้วอาจจะทำให้ข้อมูลที่สำคัญเหล่านั้นถูกเปิดเผยและถูกขโมยไปทำธุรกรรมต่างๆ ได้

จากปัญหาที่กล่าวข้างต้นทางคณะผู้จัดทำจึงได้ศึกษาการทำงานของ โปรแกรม Charles ซึ่งเป็นโปรแกรมที่สามารถตรวจเช็คการใช้งานต่างๆ ภายในระบบเน็ตเวิร์คได้อย่างละเอียด ไม่ว่าจะข้อมูลเป็นในส่วนของ โฮสต์ (Host) พอร์ต (Port) เลขไอพีของโดเมน (DNS) รวมถึงข้อมูลไฟล์ต่างๆ ที่ได้มีการรับส่งข้อมูลกันภายในเครือข่ายได้อย่างมีประสิทธิภาพ พร้อมกับฟังก์ชั่นการค้นหาข้อมูลอย่างละเอียด ซึ่งโปรแกรมนี้เหล่าบรรดา Hacker จะใช้ในการเจาะเข้าสู่ระบบ ซึ่งผู้ดูและระบบจะต้องเรียนรู้ถึงวิธีการเจาะระบบและการป้องกัน เพื่อเพิ่มความปลอดภัยให้มากยิ่งขึ้น

3. วัตถุประสงค์ของโครงงาน

3.1 เพื่อศึกษาการ แฮค FTP ไฟล์ รวมถึงดูข้อมูลไฟล์ต่างๆ ที่ได้มีการรับส่งข้อมูลกันภายในเครือข่าย โดยใช้โปรแกรม Charles

3.2 เพื่อศึกษาการทำงานของโปรแกรม Charles

4. ทฤษฎีและผลงานวิจัยที่เกี่ยวข้อง

4.1 Network Monitoring

Network Monitoring คือ การเฝ้า ดูแลและการบริการระบบเครือข่าย ในโลกของเรานี้คอมพิวเตอร์ต่างๆ มีการเชื่อมโยงกันสำหรับโอนถ่ายข้อมูลซึ่งกันและกันที่เรียกว่า อินเตอร์เน็ต ที่ถือได้ว่าเป็นเครือข่ายที่ใหญ่ที่สุดและลดระดับของระบบไปเรื่อยๆ จนถึงระบบเครือข่ายภายในบ้านหรือภายในบริษัท ในทุกวันนี้เราใช้เครือข่ายกันทุกคนไม่ว่าจะเป็น IPTV, CCTV, Mobile, Website, Cloud Computing เป็นต้น หากเราไม่มีระบบ Network Monitoring ที่จะคอยตรวจสอบสภาพเครือข่ายให้มีความเสถียร ปลอดภัย ดังนั้นหน่วยงานหรือองค์กรต่างๆ จะมีการใช้ ระบบจัดการเครือข่าย(Network Monitoring and Management Software) เพื่อคอยตรวจสอบระบบเครือข่ายของตนเอง

ความสามารถและคุณสมบัติของโปรแกรม Network Monitoring

– ผู้ดูแลระบบ (Network Engineer) สามารถดูแลและตรวจสอบการทำงานระบบเน็ตเวิร์กและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับเน็ตเวิร์กทำงานตามปกติหรือมีข้อผิดพลาดใดๆเกิดขึ้น

– Network Monitoring สามารถใช้ในการวิเคราะห์และตัดสินใจแก้ปัญหาหรือเปลี่ยนอุปกรณ์ที่มีปัญหาบ่อย ๆ

– สามารถรู้ได้ทันทีว่าอุปกรณ์และส่วนงานใดบนระบบเน็ตเวิร์กมีปัญหา ช่วยลดเวลาในการแก้ปัญหาลดการสูญเสียโอกาสทางธุรกิจ

– ช่วยให้มองเห็นภาพรวมการทำงานและประสิทธิภาพการทำงานของระบบเน็ตเวิร์กและเหตุการณ์ต่าง ๆ ได้อย่างง่าย

– ช่วยตรวจสอบSecurity ต่าง ๆ เพื่อให้มั่นใจว่าระบบรักษาความปลอดภัยต่าง ๆ

– Network Monitoring บางโปรแกรมสามารถช่วยตรวจสอบการทำงานของ Program Application และ Service ต่าง ๆ ที่ทำงานอยู่บน Server

4.2. NetworkMiner

เป็นโปรแกรมที่ใช้สำหรับดูปริมาณการรับส่งของข้อมูลในระบบเน็ตเวิร์ค (Network Traffics) ที่ถูกพัฒนาโดยบริษัท NETRESEC ที่ตั้งอยู่ในเมือง เอ็นเชอพิงก์ (Enkoping) ของประเทศสวีเดน (Sweden) โปรแกรมสามารถดูข้อมูล และตรวจเช็คการใช้งานต่างๆ ภายในระบบเน็ตเวิร์คได้อย่างละเอียด ไม่ว่าจะข้อมูลเป็นในส่วนของ โฮสต์ (Host) พอร์ต (Port) เลขไอพีของโดเมน (DNS) รวมถึงข้อมูลไฟล์ต่างๆ ที่ได้มีการรับส่งข้อมูลกันภายในเครือข่ายได้อย่างมีประสิทธิภาพ พร้อมกับฟังก์ชั่นการค้นหาข้อมูลอย่างละเอียด ทั้งนี้ยังมีระบบ Live Sniffing แบบเรียลไทม์ซึ่งเป็นเทคโนโลยีที่ใช้ในการดักจับและวิเคราะห์การรับส่งข้อมูลภายในระบบเครือข่ายคอมพิวเตอร์ได้ตลอดเวลา พร้อมทั้งสามารถสร้างข้อมูลออกมาได้ในรูปแบบของไฟล์ PCAP ที่นิยมนำมาใช้ในการวิเคราะห์และตรวจสอบลักษณะของเครือข่ายข้อมูล และสามารถนำมาใช้วิเคราะห์ระบบเครือข่ายในขณะที่อยู่ในโหมดออฟไลน์ได้อีกด้วย

ความสามารถและคุณสมบัติของโปรแกรม NetworkMiner

- สามารถสร้างและวิเคราะห์ข้อมูลในรูปแบบของไฟล์ PCAP ได้

- มีฟังก์ชั่น Live Sniffing Buffer Usage สามารถดูปริมาณการใช้งาน รับส่งข้อมูลทั้งหมดได้แบบเรียลไทม์

- สามารถดูค่าของพอร์ตต่างๆ ได้อย่างละเอียด

- สามารถใช้ได้กับเครื่องคอมพิวเตอร์ที่มีการ์ดแลน (Network Card) หลายอันได้ และ ดูมอนิเตอร์แยกเฉพาะได้เช่นกัน

- มีฟังก์ชั่น File ที่สามารถดูรายละเอียดของไฟล์แต่ละรายการได้อย่างละเอียด

- มีฟังก์ชั่น Image ให้สามารถดูการรับส่งข้อมูลของไฟล์ที่อยู่ในประเภทของรูปภาพได้

- สามารถใช้งานได้ในขณะอยู่ในโหมดออฟไลน์

4.3 โปรแกรม Driodsheep ปีการศึกษา 2014

ผู้จัดทำ : นายณัฐพันธ์ กันเสนา พร้อมคณะ

ที่มา : http://csperson.kku.ac.th/chakchai/images/322376_2014/g11_droidsheep.jpg

6. ประโยชน์ที่คาดว่าจะได้รับ

6.1 ได้ทราบถึงหลักการทำงานของโปรแกรม Charles

6.2 ช่วยให้เป็นแนวทางในการป้องกันและรับมือในการโดนแฮคข้อมูลจากโปรแกรม Charles

6.3 ได้ทราบถึงช่องโหว่ของแอพพลิเคชั่นต่างๆที่ไม่มีความปลอดภัยในการเข้าถึงข้อมูล และจะได้นำความรู้นี้ไปช่วยในการป้องกันการเจาะเข้าสู่ข้อมูลได้

7. หลักการทำงานของโปรแกรม

7.1 เครื่องที่เป็นตัวดักจับ ทำการเปิดโปรแกรม Charles ขึ้นมาพร้อมกับตรวจสอบเลข IP ของเครื่องว่าเป็นเท่าไหร่

7.1 สลับมาที่เครื่องที่ต้องการให้เป็นตัวตรวจสอบข้อมูลให้ทำการ Set Proxy ตามเลขไอพีและเลขพอตของเครื่องที่เปิดโปรแกรม Charles ไว้ (เครื่องที่เป็นตัวดักจับ)

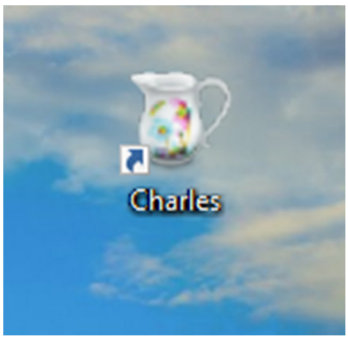
7.1 เครื่องที่เป็นตัวไว้ทดสอบก็เริ่มเข้าสู่เว็บไซต์ต่างๆที่ตนต้องการ ส่วนเครื่องที่เป็นตัวดักจับให้เริ่มจับข้อมูลได้ได้

7.1 ในการดักจับข้อมูล จะดักจับข้อมูลจำพวก รูปภาพ ไฟล์เอกสาร เช่น ไฟล์ word และ ไฟล์ pdf เป็นต้น

ขั้นตอนการติดตั้งโปรแกรม

1. ดาวน์โหลดโปรแกรม Charles จากลิ้ง https://www.charlesproxy.com/download/latest-release/ จากนั้นทำการแตกไฟล์พร้อมติดตั้งลงในคอมพิวเตอร์

2. หลังจากการติดตั้งเสร็จจะได้โปรแกรม Charles ที่มีรูปสัญลักษณ์โปรแกรม ดังรูป



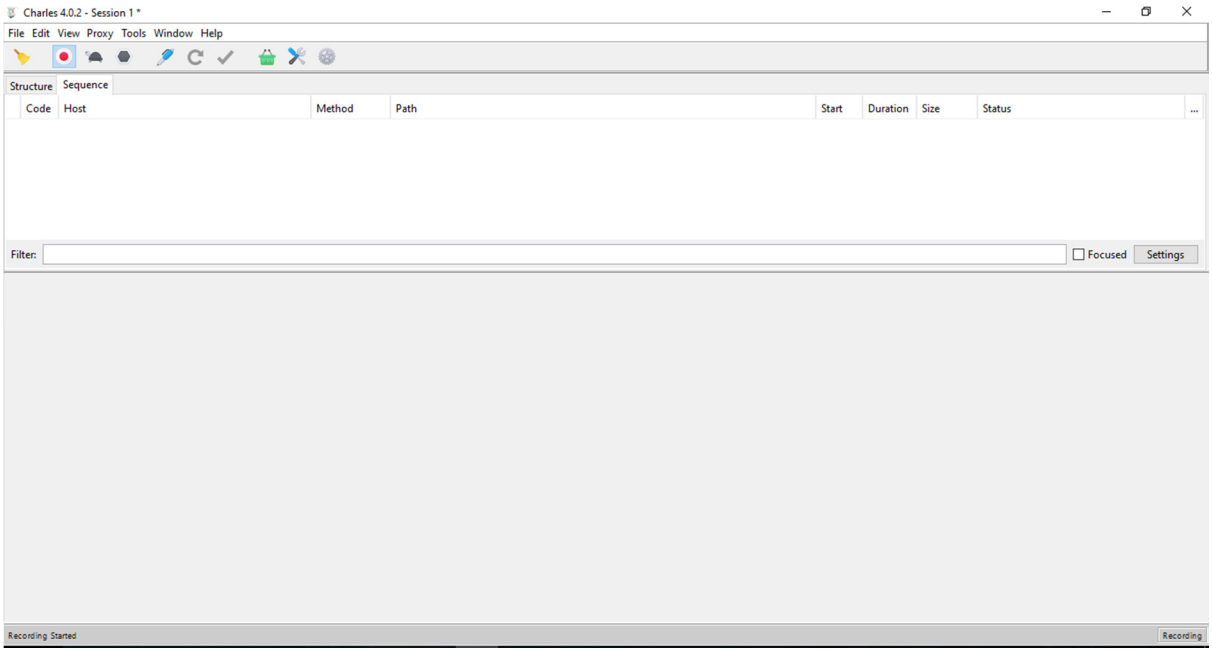
3. ขั้นตอนการใช้งานโปรแกรม

ในขั้นตอนการใช้โปรแกรม Charles จะใช้คอมพิวเตอร์ 2 เครื่อง โดยที่เครื่องที่ 1 จะใช้สำหรับเป็นตัวที่เครื่องซึ่งใช้เป็นเครื่องเข้าสู่เว็บไซต์ต่างๆ ส่วนคอมพิวเตอร์อีกเครื่องจะมีไว้สำหรับดักจับข้อมูลอีกเครื่องที่กำลังใช้งานอยู่

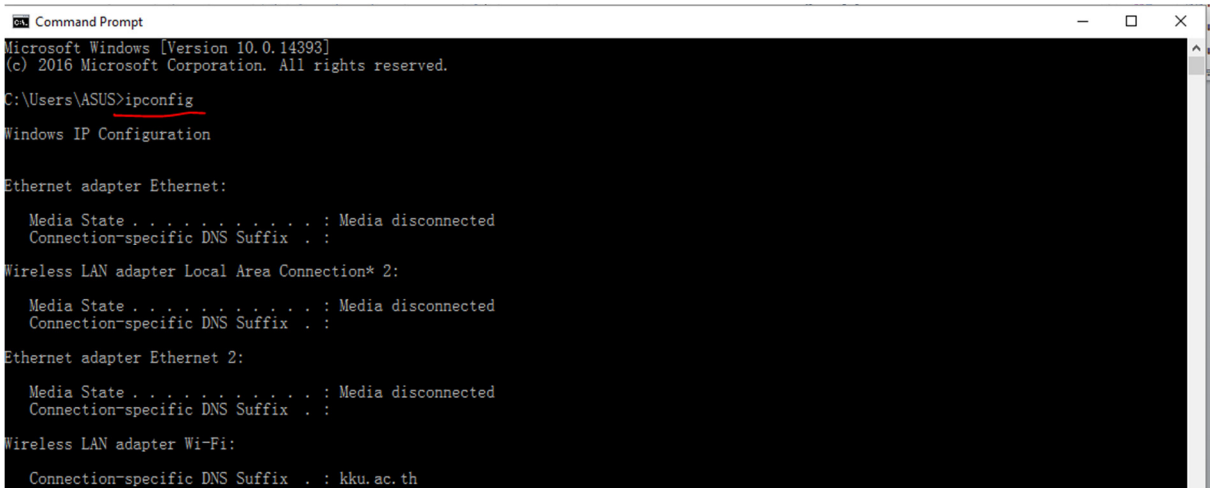
การกระทำกับเครื่องที่เป็นตัวที่ใช้ในการดูข้อมูล ส่วนอีกเครื่องจะเป็นเครื่องที่ใช้ในการเข้าดูข้อมูล

3.1 เครื่องที่เป็นตัวดักจับข้อมูล ทำตามขั้นตอนดังนี้

3.1.1 ให้ดับเบิ้ลคลิกที่ตัวโปรแกรม จะได้หน้าจอของโปรแกรมดังนี้

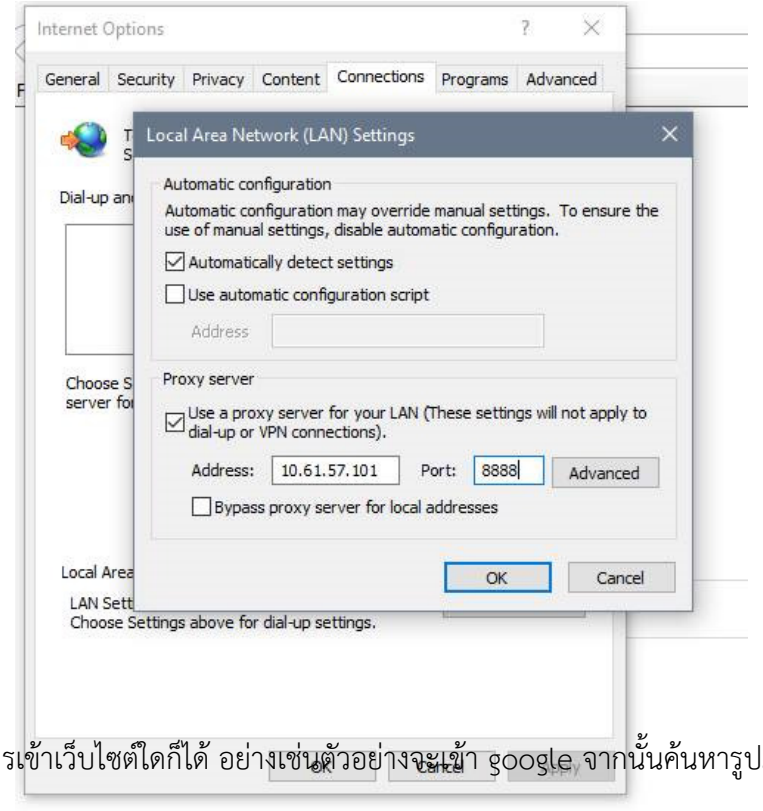


3.1.2 ทำการเช็ค IP ของเครื่องว่ามีเลข IP เท่าไหร่ โดยพิมพ์คำสั่ง ipconfig

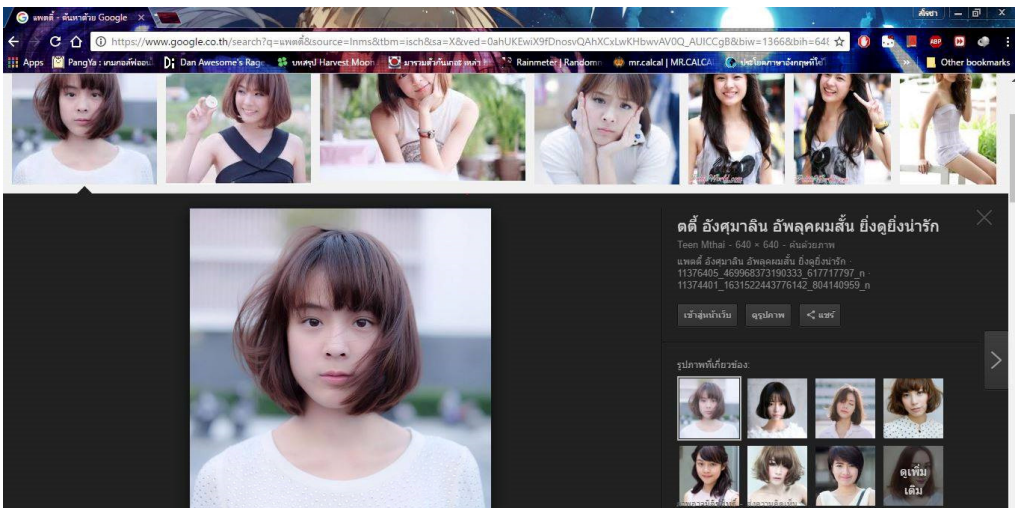


3.2 ณ เครื่องที่จะใช้เป็นตัวสำหรับเข้าเว็บไซต์ต่างๆ ทำตามขั้นตอนดังนี้

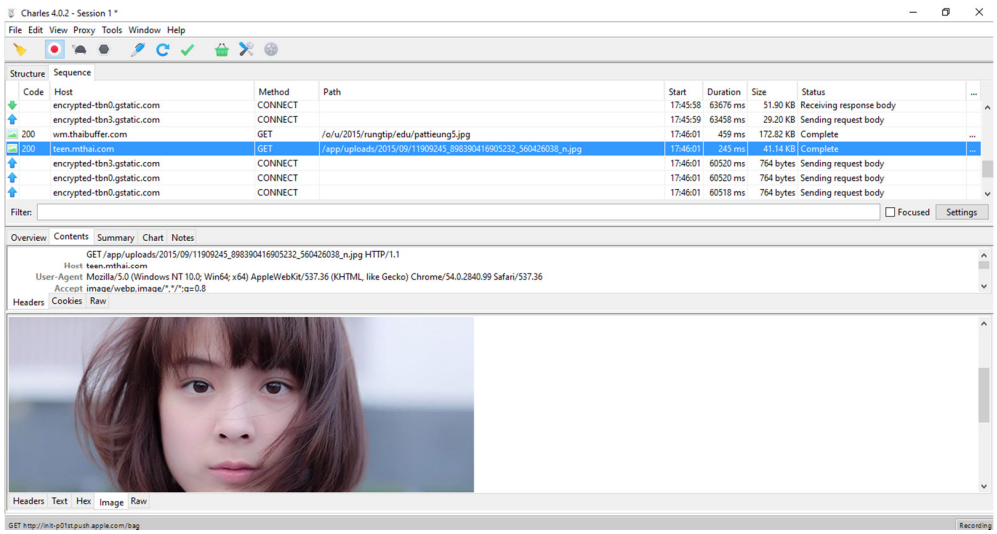
3.2.1 ให้ทำการ Set Proxy โดยช่อง Address ให้ใส่เลขไอพีเครื่องแม่(เครื่องที่ต้องการดูดข้อมูล) ส่วนช่อง Port ให้ใส่เลข Port ของโปรแกรม Charles ซึ่งก็คือ 8888 ดังรูป



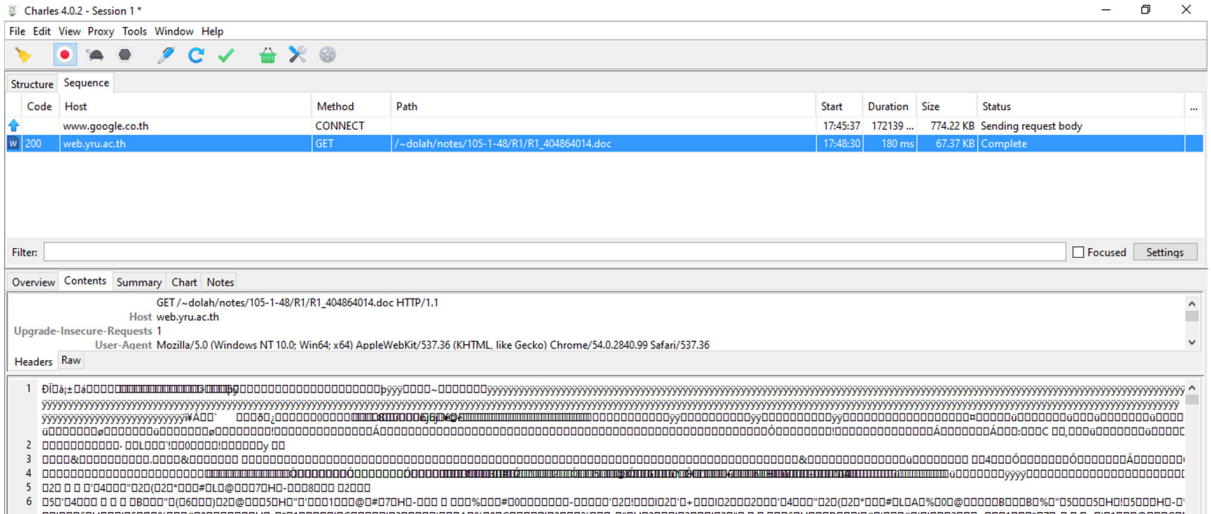
3.2.2 ทำการเข้าเว็บไซต์ใดก็ได้ อย่างเช่นตัวอย่างจะเข้า google จากนั้นค้นหารูปภาพต่างๆ ดังรูป



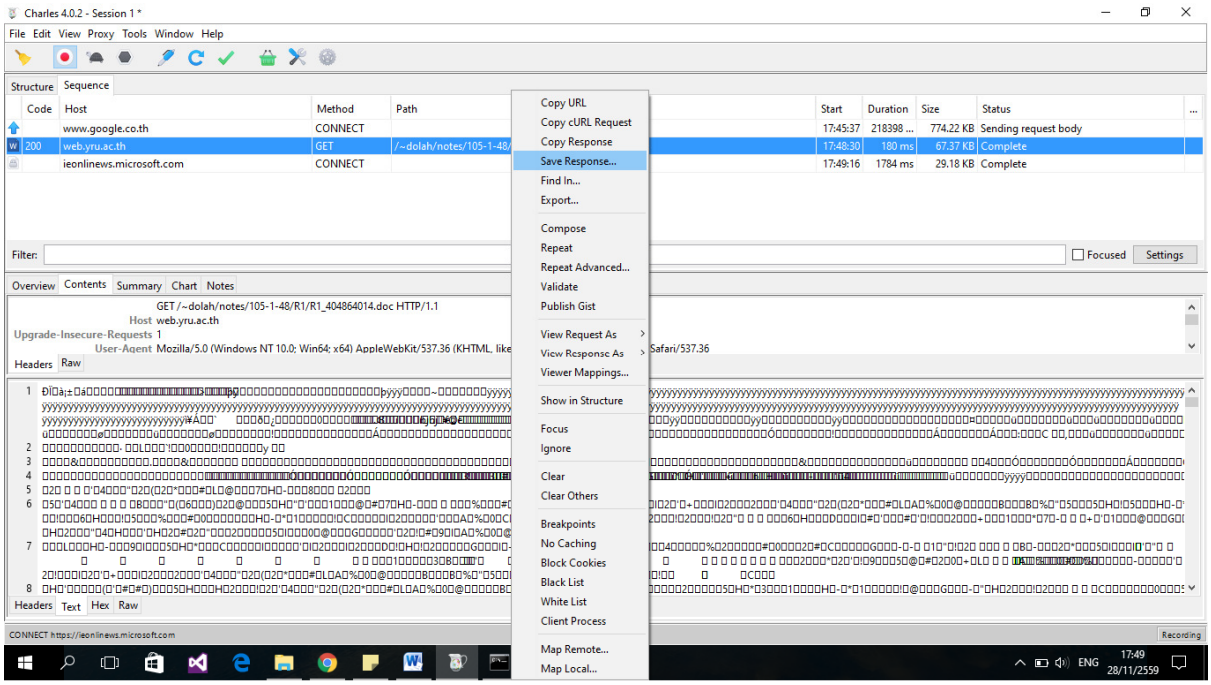
3.3 กลับมาที่เครื่องที่เป็นตัวดักจับข้อมูล จะปรากฏการเข้าใช้งานของเครื่องที่ใช้ในการเข้าเว็บไซต์ต่างๆ ซึ่งในรูปนี้จะเห็นเป็นรูปเดียวกันกับที่เครื่องก่อนหน้านี้จับภาพได้ ดังรูป



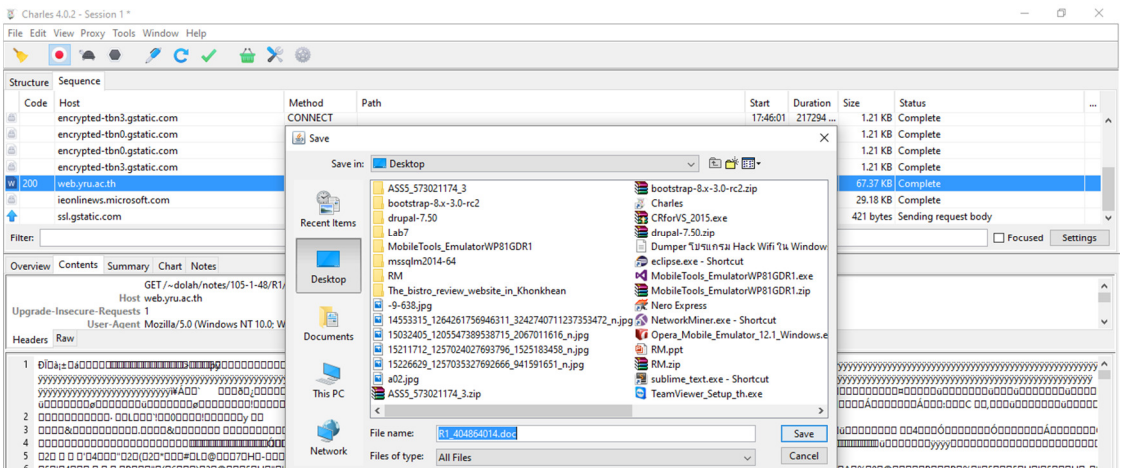
3.4 ต่อไปจะเป็นการดาวห์โหลดไฟล์ซึ่งในที่นี้จะป็นไฟล์ .doc



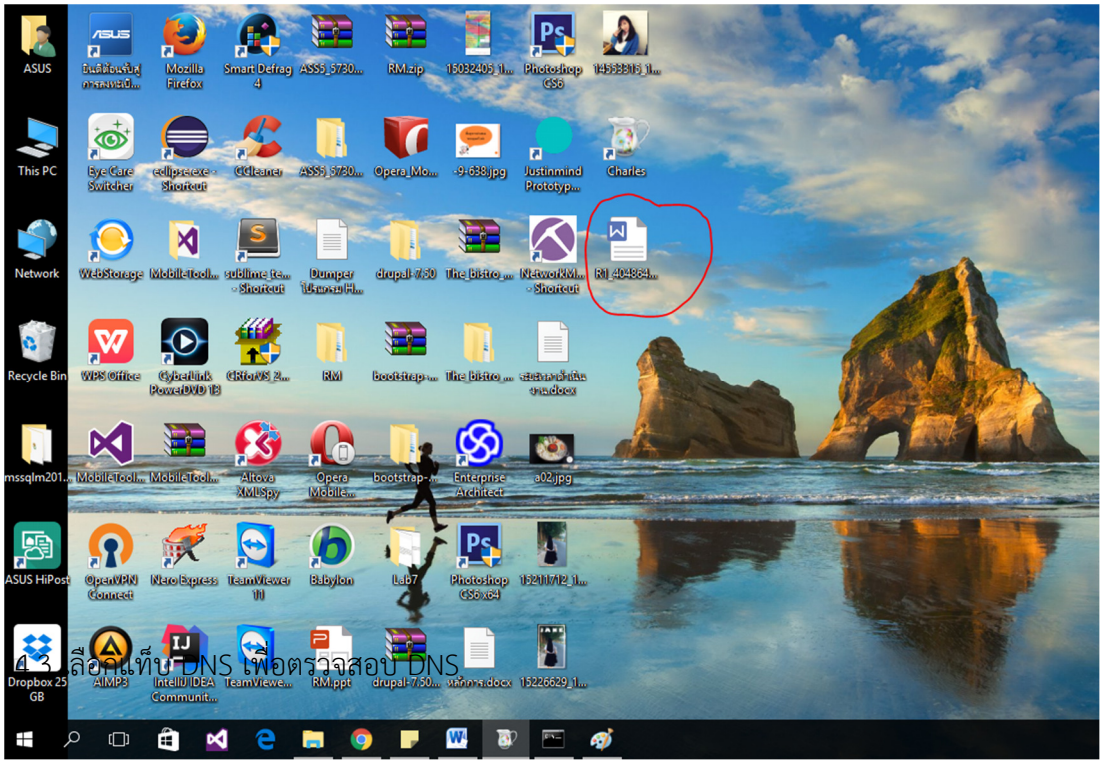
3.5 ทำการดาวน์โหลดไฟล์ไว้ที่เครื่อง



3.6 ณ เครื่องแม่จะได้ไฟล์ที่ต้องการซึ่งไฟล์นี้จะได้มาจากกรที่อีกเครื่องค้นหาข้อมูลไฟล์นี้ในเว็บไซต์อื่น แต่เครื่องแม่สามารถดักจับได้ ละสามารถทำการโหลดได้นั่นเอง



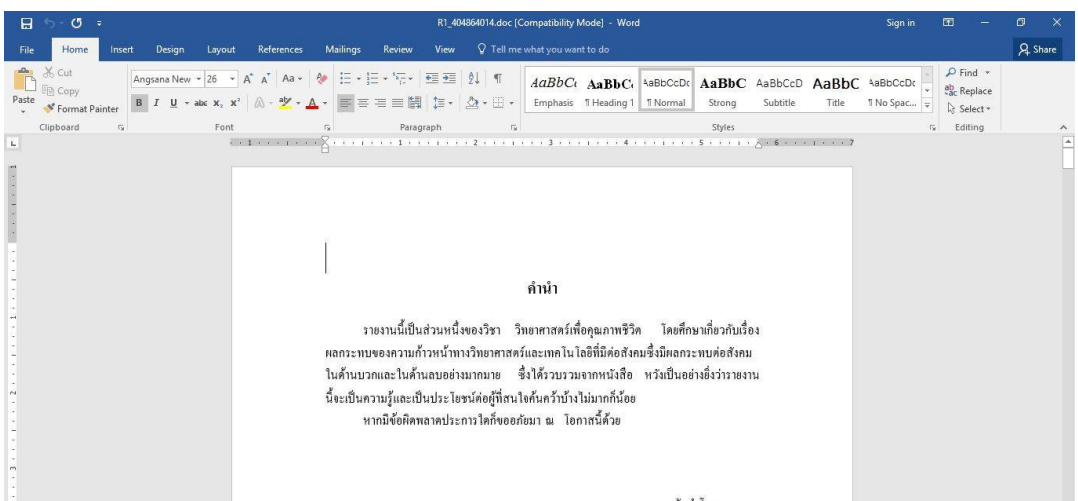
3.7 ไฟล์ .doc ที่ทำการโหลดจะมาขึ้นที่หน้าจอ desktop ของเครื่องตัวแม่



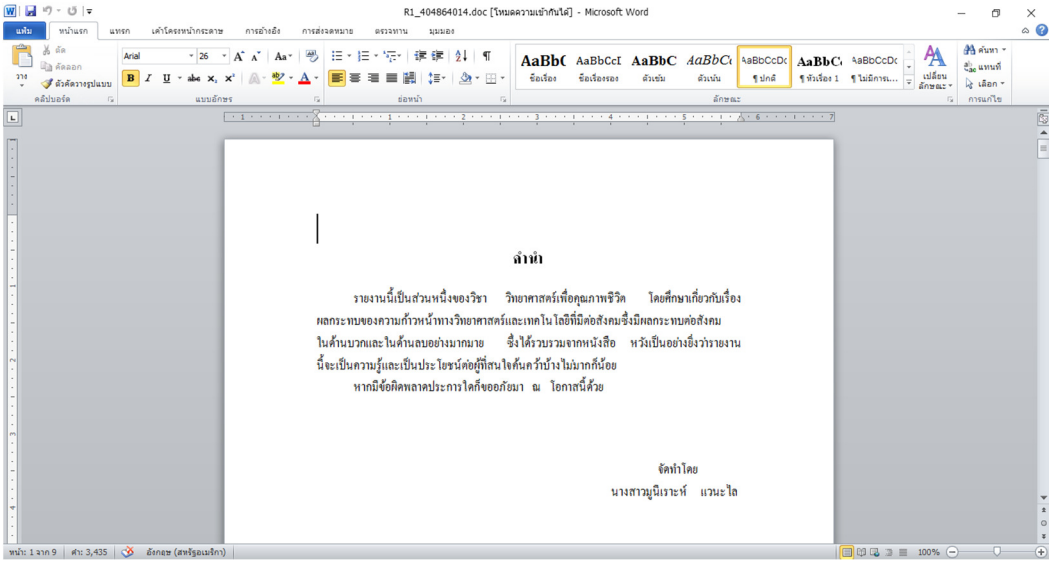
4.3 ล็อคแท็ป DNS เพื่อตรวจสอบ DNS

3.8 ที่เครื่องลูกที่ใช้ในการเข้าเว็บไซต์ต่างๆไฟล์ก็จะโหลดมาไว้ที่เครื่องเช่นกัน ดังรูป ซึ่งไฟล์2ตัวนี้จะเป็นตัวเดียวกัน และมีชื่อไฟล์เดียวกัน

3.9 เนื้อหาภายในไฟล์ที่เป็นเครื่องแม่



3.10 เนื้อหาภายในไฟล์ที่เป็นเครื่องลูก จะสังเกตว่าทั้ง2ไฟล์มีเนื้อหาเดียวกันเพราะเป็นไฟล์เดียวกันที่โหลดมาจากลิ้งเดียวกัน แต่เครื่องนึงโหลดจากเว็บไซต์โดยตรง แต่อีกเครื่องโหลดมาจากโปรแกรม Charles



อธิบายเพิ่มเติมเกี่ยวกับ Tool หลักๆที่มีอยู่ในโปรแกรม Charles

1. บล็อกเครื่องมือคุกกี้ Block Cookies

Block Cookies เป็นเครื่องมือที่ระงับการใช้คุกกี้ เพราะ Cookies เป็นข้อมูลการเข้าเว็บไซต์ต่างๆซึ่งถูกบันทึกและเก็บโดยเว็บบราวเซอร์

2. Rewrite

เครื่องมือ Rewrite ช่วยให้สามารถสร้างกฎที่ปรับเปลี่ยนการร้องขอและการตอบสนองที่ผ่านชาร์ลส์ได้ กฎระเบียบ เช่น การเพิ่มหรือเปลี่ยนส่วนหัวหรือค้นหาและแทนที่

3. Black list

ไม่อนุญาตให้ใส่ชื่อโดเมนที่ไม่ต้องการ เมื่อเว็บเบราว์เซอร์พยายามที่จะขอให้หน้าใด ๆ จากชื่อโดเมนขึ้น บัญชีดำก็จะถูกปิดกั้น

4. White list

เป็นรายการที่อนุญาตให้เข้าถึงหรือเปิดการใช้โดเมนที่ต้องการได้

5. DNS Spoofing

เครื่องมือการปลอมแปลง DNS การทำ DNS Spoofing หรือ DNS Cache Poisoning คือการเปลี่ยนข้อมูลของ DNS ให้วิ่งไปที่ IP Address ปลายทางที่อื่นที่ไม่ใช่ของจริง ซึ่งวิธีการโจมตีแบบนี้จะสังเกตเห็นความผิดปกติได้ยาก เนื่องจากใน Address Bar ของเบราว์เซอร์จะแสดง URL ที่ถูกต้อง แต่เว็บไซต์ปลายทางนั้นไม่ใช่เว็บไซต์ที่แท้จริง

5. ภาพรวมระบบ

6. เอกสารอ้างอิง

1 Thaoware. (2558). **NetworkMiner Download.** ค้นเมื่อ 18 พฤศจิกายน 2559, จาก http://software.thaiware.com/12384-NetworkMiner-Download.html

2. Matthew Buchanan. (2016). Charles. ค้นเมื่อ 26 พฤศจิกายน 2559, จาก https://www.charlesproxy.com/download/latest-release/

3. Matthew Buchanan. (2016). Charles. ค้นเมื่อ 26 พฤศจิกายน 2559, จาก https://www.charlesproxy.com/

4. Discuz!. (2013). ค้นเมื่อ 26 พฤศจิกายน 2559, จาก http://openkore.in/forum.php?mod=viewthread&tid=4796