Hacker มาจากประเทศไหน รู้ไปทำไม? Where are you come from, Hacker? and Why?

ผู้ช่วยศาสตราจารย์ ดร.กิตติพงษ์ สุวรรณราช : เขียน

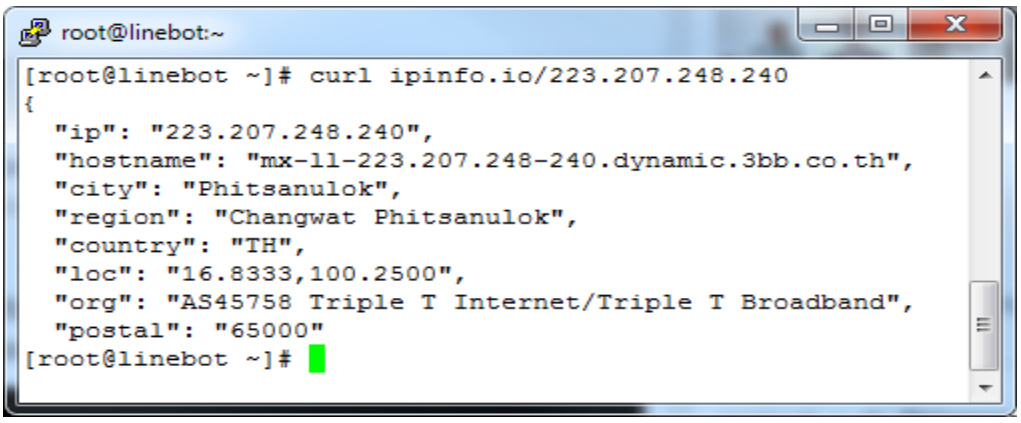
Asst. Prof. Dr. Kittipong Suwannaraj

ECA , MTCNA, MTCUME, MTCTCE, RHCT

kitti@psru.ac.th

การตรวจสอบแหล่งที่มาของ IP address เป็นเรื่องที่มีความสำคัญและจำเป็นในหลายๆ กรณี บางคนอาจจะมองว่า “แล้วจะรู้ไปทำไม รู้ไปก็เท่านั้น ทำอะไรไม่ได้อยู่ดี” จริงๆ แล้วข้อมูล IP address และแหล่งประเทศที่มาของ IP address ที่เรากำลังสนใจนั้นมีความสำคัญมากพอสมควรในการใช้เป็นข้อมูลในการป้องกันเซิร์ฟเวอร์ของเราได้เป็นอย่างดีครับ เพราะโดยทั่วไปแล้ว Hacker ก็จะใช้ IP address จากในประเทศในการทำการทดลอง Hack ก่อน ซึ่งอาจจะเป็น IP address ของคนอื่น หรือของตัวเองในการทดสอบแบบพื้นฐาน ดังนั้นถ้าเรารู้ว่า IP address นั้นอยู่ในประเทศใด เราก็สามารถนำข้อมูลนั้นมาเขียนเป็น Rule เพื่อให้ Firewall ทำการป้องกันโดยใช้เทคนิคที่เรียกว่า IP Geolocation ก็สามารถทำได้ง่าย หรือกล่าวอีกทางหนึ่งที่เราเรียกกันว่า “เป็นการปิดกั้น IP address ทั้งหมดที่มาจากประเทศนั้นๆ เลยก็ว่าได้” ด้วยเทคนิคนี้เองทำให้เราไม่ต้องไปสร้าง Firewall rule จำนวนมากมาย ตามที่ Hacker เปลี่ยนแปลงแหล่งที่มาใหม่

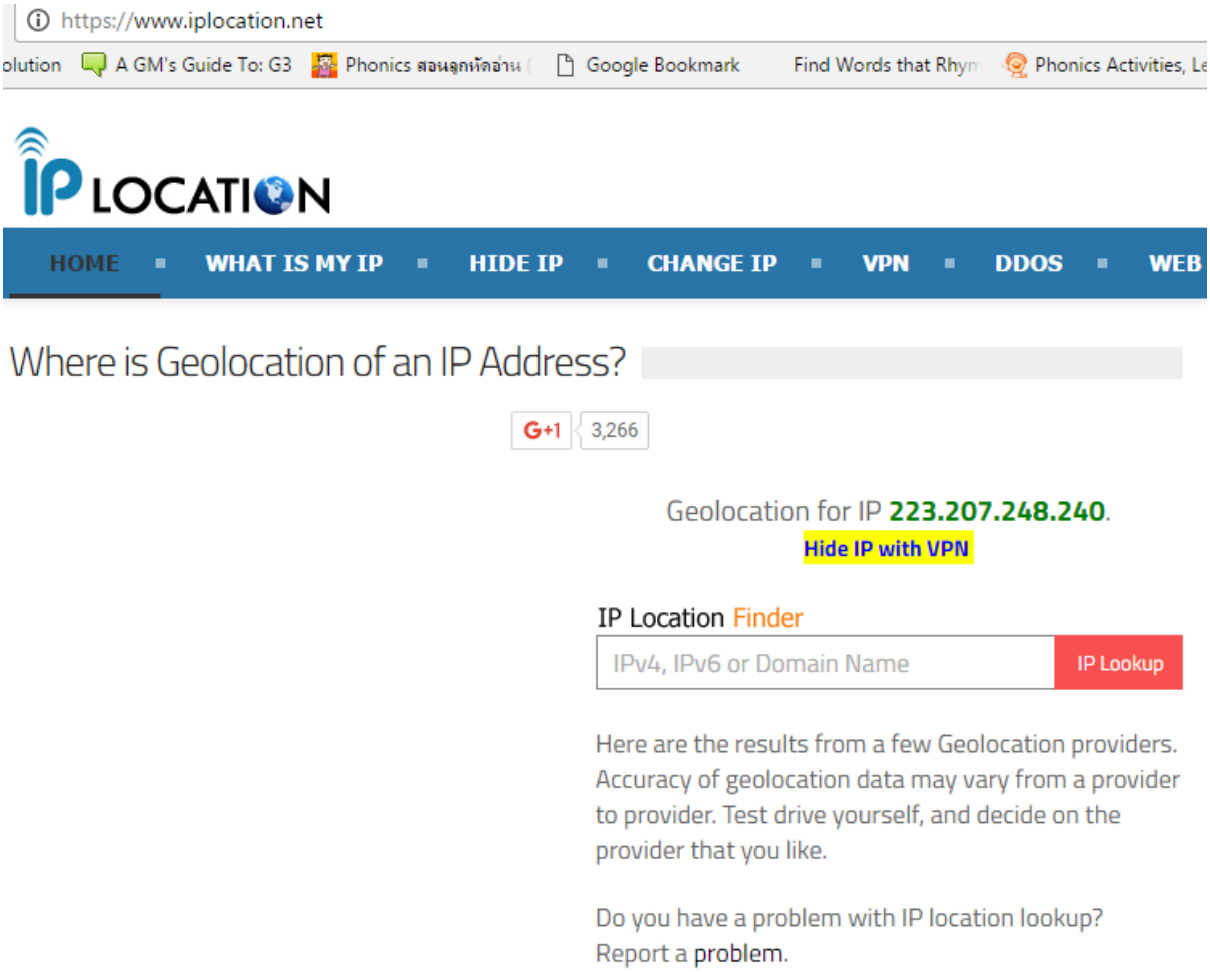
IP Geolocation นั้นเป็นเทคนิคที่จะทำการตรวจสอบว่า IP address ที่เรากำลังสนใจนั้น เป็น IP address ที่ได้รับจัดสรรของประเทศใด แล้วจัดสรรให้ผู้บริการรายใด ในบางกรณีบอกรายละเอียดลึกไปถึง Location แหล่งที่ตั้งที่เป็นค่าพิกัด GPS เลยทีเดียว (แต่ส่วนใหญ่แล้วไม่มีการ Update ให้เป็นปัจจุบัน) ตัวอย่างเช่น คำสั่งใน Linux



รูปที่ 1 การใช้คำสั่ง curl ในการเรียกใช้ ipinfo.io เพื่อตรวจสอบแหล่งที่มาของ IP address

แต่หากเราไม่ได้ใช้งานระบบปฏิบัติการ Linux ก็สามารถใช้บริการตรวจสอบ IP Geolocation ผ่านทาง Web Services ได้จาก www.iplocation.net

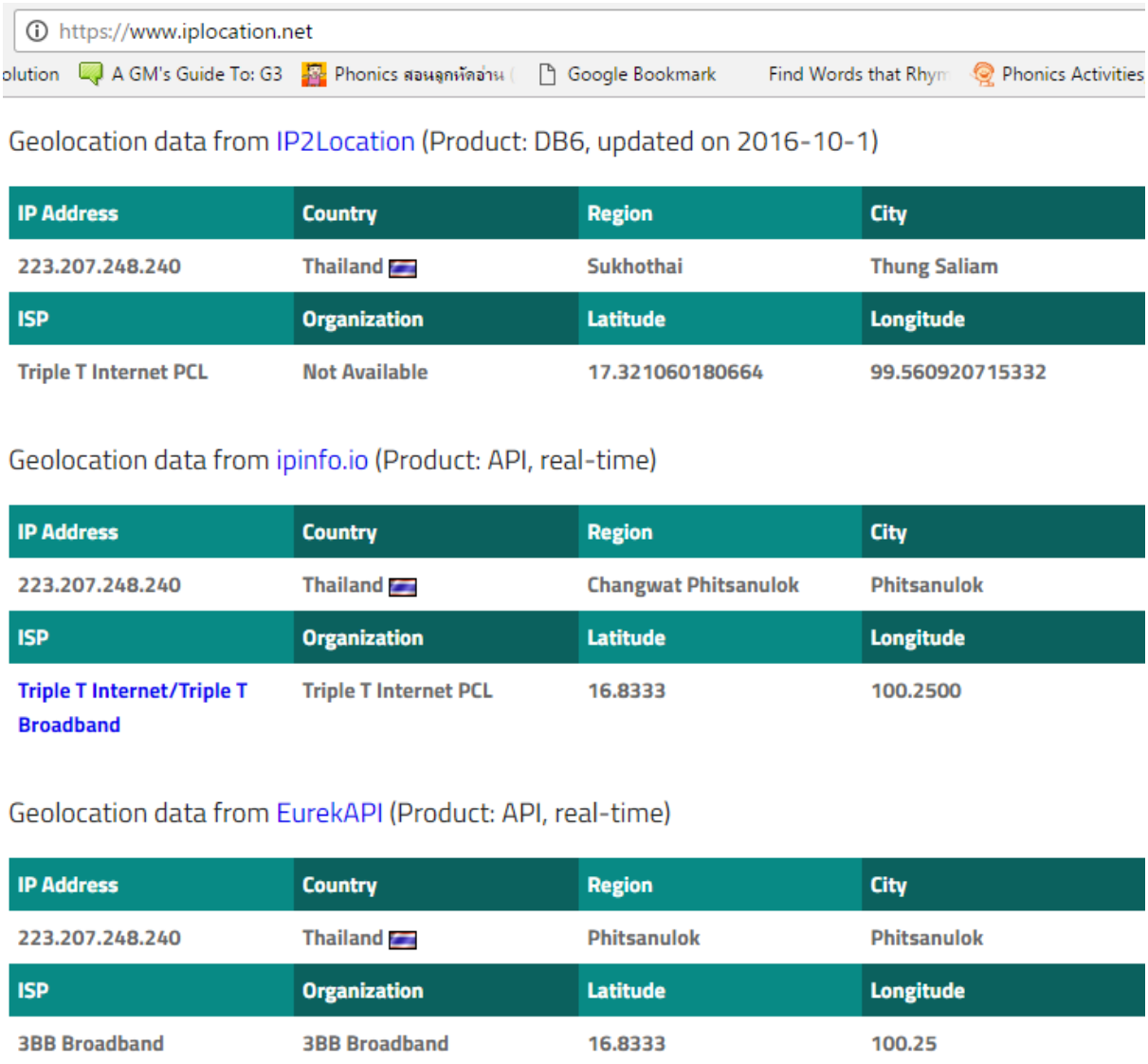
Hacker มาจากประเทศไหน รู้ไปทำไม? Where are you come from, Hacker? and Why?



รูปที่ 2 เว็บไซต์ iplocation.net ตรวจสอบแหล่งที่มาของ IP address

รูปที่ปรากฏจะเป็นหน้าแรกของเว็บ iplocation.net เราสามารถใส่หมายเลข IP address ที่ต้องการหาข้อมูลได้ในช่อง IP location Finder ซึ่งจะรองรับทั้ง IPv4 , IPv6 และ Domain Name จากนั้นก็ให้กดปุ่ม IP Lookup ได้เลย ระบบจะค้นหาข้อมูล IP address ในฐานข้อมูล IP location ที่เป็นปัจจุบันให้เรากับ ดังภาพที่ปรากฏ

Hacker มาจากประเทศไหน รู้ไปทำไม? Where are you come from, Hacker? and Why?



รูปที่ 3 ผลลัพธ์การตรวจสอบ IP address จาก iplocation.net

โดยผลลัพธ์ที่แสดงออกมานั้นก็จะให้รายละเอียดจากการสืบค้นจากผู้บริการ 3 รายคือ IP2localtion , ipinfo.io และ EurekAPI ซึ่งก็เป็นข้อมูลสนับสนุนให้กับเราในการจะนำเอาข้อมูลนี้ไปวิเคราะห์หรือทำงานต่อไป ขอบคุณครับ

ปัจจุบัน เพื่อให้การติดตามแหล่งที่มาของ Hacker ทำได้สะดวกกับคนไทย และรวดเร็วมากยิ่งขึ้น ทางศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพิบูลสงคราม ได้พัฒนาระบบ IP Country Checker ขึ้นมาที่รองรับการทำงานได้ทั้งบน IPv4 และ IPv6 เพื่อตรวจสอบแหล่งที่มาของ IP address เพื่อนำมาใช้งานประโยชน์ต่อไป ซึ่งมีหลักการการทำงานง่าย ๆ เพียงท่านใส่หรือกรอก IP address ที่ต้องการตรวจสอบ เพียงเท่านี้ระบบก็จะทำการค้นหาให้โดยอัตโนมัติ ดังภาพที่ปรากฏด้านล่างนี้

Hacker มาจากประเทศไหน รู้ไปทำไม? Where are you come from, Hacker? and Why?

รูปที่ 4 เว็บไซต์ http://ipcheck.psru.ac.th

ท่านสามารถติดตามองค์ความรู้ใหม่ ๆ ได้จากทางเว็บไซต์ http://thahinc.psru.ac.th หรือทาง http://itc.psru.ac.th แล้วพบกันในบทความใหม่ ๆ ครับ

แหล่งสืบค้นเพิ่มเติม :

1. Website : ipinfo.io
2. Website : iplocation.net

บริการบน : linux , FreeBSD , Unix services , web Services

Article number : 201610220615