

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

ผู้ช่วยศาสตราจารย์ ดร.กิตติพงษ์ สุวรรณราช : เขียน

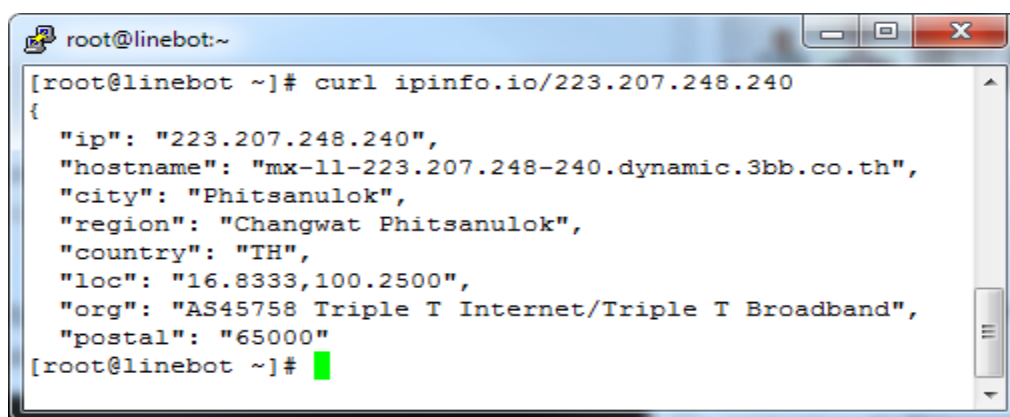
Asst. Prof. Dr. Kittipong Suwannaraj

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 ที่เรากำลังสนใจนั้น มีความสำคัญมากพอสมควรในการใช้เป็นข้อมูลในการป้องกันเซิร์ฟเวอร์ของเราได้เป็นอย่างดีครับ เพราะโดยทั่วไปแล้ว Hacker ก็จะใช้ IP address จากในประเทศในการทำการทดลอง Hack ก่อน ซึ่งอาจจะเป็น IP address ของคนอื่น หรือของตัวเองในการทดสอบแบบพื้นฐาน ดังนั้นถ้าเรารู้ว่า IP address นั้นอยู่ในประเทศใด เราก็สามารถนำข้อมูลนั้นมาเขียนเป็น Rule เพื่อให้ Firewall ทำการป้องกันโดยใช้เทคนิคที่เรียกว่า IP Geolocation ก็สามารทำได้ง่าย 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



```

root@linebot:~
[root@linebot ~]# curl ipinfo.io/223.207.248.240
{
  "ip": "223.207.248.240",
  "hostname": "mx-11-223.207.248-240.dynamic.3bb.co.th",
  "city": "Phitsanulok",
  "region": "Changwat Phitsanulok",
  "country": "TH",
  "loc": "16.8333,100.2500",
  "org": "AS45758 Triple T Internet/Triple T Broadband",
  "postal": "65000"
}
[root@linebot ~]#

```

รูปที่ 1 การใช้คำสั่ง curl ในการเรียกใช้ ipinfo.io เพื่อตรวจสอบแหล่งที่มาของ IP address

แต่หากเราไม่ได้ใช้งานระบบปฏิบัติการ Linux ก็สามารถใช้บริการตรวจสอบ IP Geolocation ผ่านทาง Web Services ได้

จาก www.iplocation.net

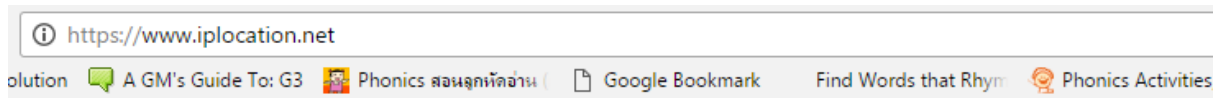
Hacker มาจากประเทศไหน รู้ไปทำไม? **Where are you come from, Hacker? and Why?**

The screenshot shows the website iplocation.net. The browser address bar displays "https://www.iplocation.net". The page title is "Where is Geolocation of an IP Address?". Below the title, there is a Google+1 button with 3,266 votes. The main content area shows the geolocation for IP **223.207.248.240**, with a button to "Hide IP with VPN". Below this is the "IP Location Finder" section, which includes a search input field containing "IPv4, IPv6 or Domain Name" and a red "IP Lookup" button. The text below the button reads: "Here are the results from a few Geolocation providers. Accuracy of geolocation data may vary from a provider to provider. Test drive yourself, and decide on the provider that you like." At the bottom of the screenshot, there is a link: "Do you have a problem with IP location lookup? Report a problem."

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 ที่เป็นปัจจุบันให้เรา กับ ดั่งภาพที่ปรากฏ

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



Geolocation data from [IP2Location](#) (Product: DB6, updated on 2016-10-1)

IP Address	Country	Region	City
223.207.248.240	Thailand	Sukhothai	Thung Saliam
ISP	Organization	Latitude	Longitude
Triple T Internet PCL	Not Available	17.321060180664	99.560920715332

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
223.207.248.240	Thailand	Changwat Phitsanulok	Phitsanulok
ISP	Organization	Latitude	Longitude
Triple T Internet/Triple T Broadband	Triple T Internet PCL	16.8333	100.2500

Geolocation data from [EurekAPI](#) (Product: API, real-time)

IP Address	Country	Region	City
223.207.248.240	Thailand	Phitsanulok	Phitsanulok
ISP	Organization	Latitude	Longitude
3BB Broadband	3BB Broadband	16.8333	100.25

รูปที่ 3 ผลลัพธ์การตรวจสอบ IP address จาก iplocation.net

โดยผลลัพธ์ที่แสดงออกมานั้นก็จะให้รายละเอียดจากการสืบค้นจากผู้บริการ 3 รายคือ IP2location , ipinfo.io และ EurekAPI ซึ่งก็เป็นข้อมูลสนับสนุนให้กับเราในการจะนำเอาข้อมูลนี้ไปวิเคราะห์หรือทำงานต่อไป ขอบขอบคุณครับ

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 เพียงเท่านั้นระบบก็จะทำการค้นหาให้โดยอัตโนมัติ ดังภาพที่ปรากฏด้านล่างนี้

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

ipcheck.psu.ac.th/index.php

สงเสด็จผู้สวรรคตาลัย น้อมรำลึกถึงพระมหากรุณาธิคุณ และร่วมถวายความอาลัย
พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช
 ด้วยเกล้า ด้วยกระหม่อม
 นำพระพุทธเจ้า คณะผู้บริหาร คณาจารย์ บุคลากรและนักศึกษา มหาวิทยาลัยราชภัฏพิบูลสงคราม

ระบบตรวจสอบแหล่งที่มาของหมายเลขไอพีแอสเดรส (รองรับ IPv4 และ IPv6)
 IP Check system (Support IPv4 and IPv6)
 มหาวิทยาลัยราชภัฏพิบูลสงคราม


ตรวจสอบหมายเลขไอพีแอสเดรส | เกี่ยวกับระบบ | ทีมพัฒนาระบบ

กรอกหมายเลขไอพีแอสเดรสที่ก่นต้องการเช็คลงช่องด้านล่างแล้วคลิกที่ปุ่ม **เช็คไอพีที่ก่นต้องการ**


1.0.206.136

เช็คไอพีที่ก่นต้องการ

ผลลัพธ์หมายเลขไอพีที่ก่นกำลังค้นหา (Your Searching IP Address)

หมายเลขไอพีแอสเดรส :	1.0.206.136
รหัสประเทศ :	TH
ชื่อประเทศ :	ไทย
ธงชาติ :	

เราารู้ได้อย่างไรว่าหมายเลขไอพีแอสเดรสมาจากประเทศอะไร ?
 คำตอบคือ เว็บนี้เท่านั้นที่จะทำให้คุณรู้หมายเลขไอพีแอสเดรสมาจากประเทศอะไร



จัดทำโดย ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพิบูลสงคราม
 ชั้นที่ 1 อาคารศูนย์ภาษา และคอมพิวเตอร์ มหาวิทยาลัยราชภัฏพิบูลสงคราม 156 หมู่ 5 ต.พลาญชุมพล อ.เมือง จ.พิษณุโลก 65000
 โทรศัพท์ 0-5526-7200

สถิติการใช้งาน IP Check system: **43**

รูปที่ 4 เว็บไซต์ <http://ipcheck.psu.ac.th>

ท่านสามารถติดตามองค์ความรู้ใหม่ ๆ ได้จากทางเว็บไซต์ <http://thahinc.psu.ac.th> หรือทาง <http://itc.psu.ac.th> แล้วพบกันใหม่ในบทความใหม่ ๆ ครับ

แหล่งสืบค้นเพิ่มเติม :

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

บริการบน : linux , FreeBSD , Unix services , web Services

Article number : 201610220615