บริษัท บีเฟิร์สเน็ตเวิร์กคอนซัลติ้ง จำกัด

293/172 ซ.รามอินทรา119 ถ.รามอินทรา แขวงมีนบุรี เขตมีนบุรี กทม.10510, โทร: 02-070-2070

ตัวอย่างการเก็บข้อมูลการจราจรทางคอมพิวเตอร์

ข้อกำหนดในพรบ.คอมฯปี 2560 ที่เกี่ยวข้องกับผู้ให้บริการ ที่เป็นบริษัทฯ ทั่วไป ซึ่งให้บริการอินเตอร์เน็ตสำหรับพนักงานและต้องจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์นั้นที่สำคัญคือ มาตรา 17 ซึ่งมีข้อความดังนี้

การสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น”

มาตรา ๑๗ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

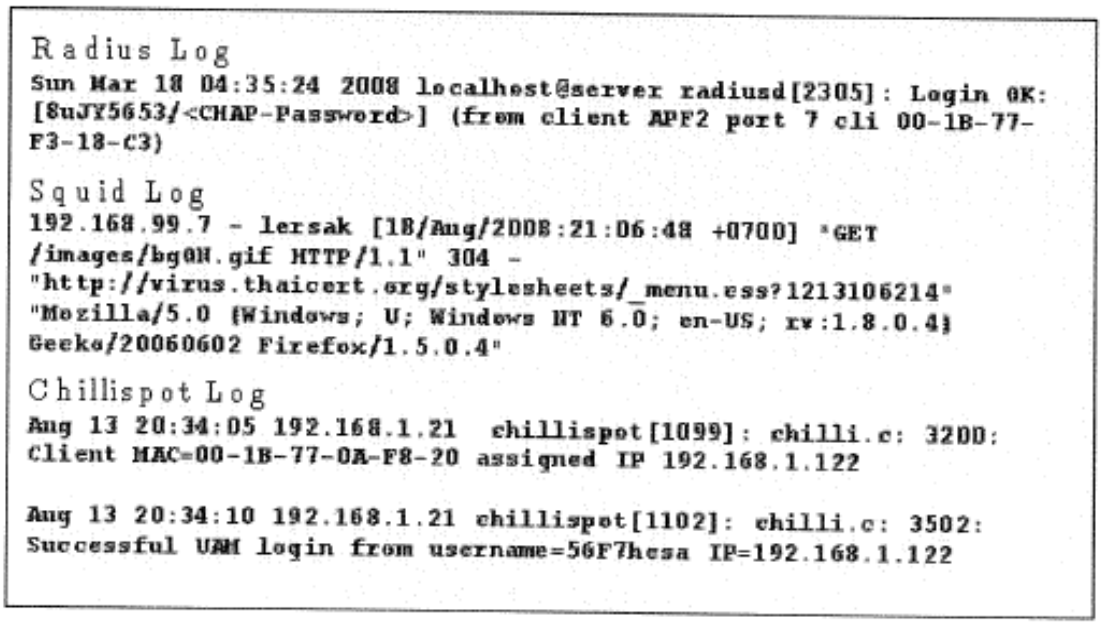
“มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้”

จะเห็นได้ว่าในพรบ.คอมฯ ปี 2550 หรือแม้แต่ปี 2560 เองนั้นไม่ได้ระบุไว้เลยว่าการเก็บข้อมูลการจราจรทางคอมพิวเตอร์ให้ครอบคลุมและครบถ้วนตามพรบ.นั้นต้องเก็บอะไรบ้าง จึงทำให้เกิดความไม่แน่ใจและสงสัยว่าอะไรคือข้อมูลที่ต้องเก็บบ้าง ดังนั้นทาง Nectec จึงได้ออกเอกสารมาตัวหนึ่งเพื่อให้เป็นเอกสารเพื่อช่วยเหลือผู้ประกอบการในการปฏิบัติตามพรบ. ตามเอกสารหมายเลข มศอ. 4003.1-2560 (NTS 4003.1-2560) ซึ่งจะพูดถึงหลักการในการเก็บข้อมูล และจำแนกประเภทของข้อมูลการจราจรทางคอมพิวเตอร์ออกเป็นส่วนต่างๆ ทั้งการเชื่อมต่อเข้าสู่ระบบเครือข่าย ผู้ให้บริการอีเมล ผู้ให้บริการเว็บ ผู้ให้บริการไฟล์แชร์ ผู้ให้บริการเครือข่ายขนาดใหญ่(Usenet) และการโต้ตอบกันบนเครือข่าย

สำหรับในส่วนของบริษัทฯ ทั่วไปเราควรมุ่งไปที่การจัดเก็บข้อมูลสำหรับการเข้าสู่ระบบเครือข่ายและการโต้ตอบกันบนเครือข่าย ซึ่งมีสาระสำคัญที่ต้องจัดเก็บดังนี้

ข.๑ ประเภท "ข้อมูลจราจรทางคอมพิวเตอร์ จากการต่อเชื่อมเข้าถึงระบบเครือข่าย"
รายการข้อมูลที่ต้องจัดเก็บ

- ข้อมูลจราจรทางคอมพิวเตอร์ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย (access logs)
- ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (date and time of connection of client to server)
- ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (user ID)
- ข้อมูลหมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดโดยระบบผู้ให้บริการ (assigned IP address)
- ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (calling line identification)



Radius Log

```
Sun Mar 18 04:35:24 2008 localhost@server radiusd[2305]: Login OK:
[8uJY5653/<CHAP-Password>] (from client APF2 port 7 cli 00-1B-77-
F3-18-C3)
```

Squid Log

```
192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET
/images/bg0N.gif HTTP/1.1" 304 -
"http://virus.thaicert.org/stylesheets/_menu.css?1213106214"
"Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.0.4)
Geeko/20060602 Firefox/1.5.0.4"
```

Chillispot Log

```
Aug 13 20:34:05 192.168.1.21  chillispot[1099]: chilli.c: 3200:
Client MAC=00-1B-77-0A-F8-20 assigned IP 192.168.1.122

Aug 13 20:34:10 192.168.1.21 chillispot[1102]: chilli.c: 3502:
Successful UAM login from username=56F7hesa IP=192.168.1.122
```

รูปที่ ข.๑ ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์ จากการต่อเชื่อมเข้าถึงระบบเครือข่าย

ข.๖ ข้อมูลจราจรทางคอมพิวเตอร์ จากการโต้ตอบกันบนเครือข่ายคอมพิวเตอร์

รายการข้อมูลที่ต้องจัดเก็บ

- ข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (date and time of connection of client to server)
- ข้อมูลชื่อเครื่องบนเครือข่าย (client hostname and/or IP address) ข้อมูลหมายเลขพอร์ตในการใช้งาน (protocol process ID)
- หมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (destination hostname and/or IP address)

หมายเหตุ ตัวอย่างการโต้ตอบกันบนเครือข่ายคอมพิวเตอร์ เช่น Internet Relay Chat (IRC) หรือ instance messaging (IM)

```
1205326745.661 1912 192.168.42.165 TCP_MISS/200 8460 CONNECT
login.live.com:443/ - DIRECT/login.live.com - CMF:40 DCF:20 ERR:0
DEFAULT_CASE-DefaultGroup
```

รูปที่ ข.๖ ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์ จากการโต้ตอบกันบนเครือข่ายคอมพิวเตอร์

ซึ่งสรุปสาระสำคัญได้ว่าเราจะต้องจัดเก็บข้อมูลที่สามารถบอกได้ว่า ใคร เข้ามาในระบบเมื่อไหร่ เครื่องไหน IP อะไร ออกไปที่ไหน เวลาเท่าไหร่

ซึ่งจากระบบ Instant Hotspot และ Instant Kiosk ที่บริษัทฯให้บริการนั้นสามารถตอบโจทย์นี้ได้ดังตัวอย่างต่อไปนี้

สมมุติเรามีโจทย์ที่จะต้องหาว่าใครเป็นคนเข้าเว็บ www.sanook.com ในเวลา 15:47:48 ของวันที่ 16 เดือนสิงหาคม 2562 และเรามีการใช้งานระบบ Instant Kiosk ซึ่งผู้เข้าใช้เว็บต้องขอ username โดยการใช้บัตรประชาชน ดังนั้นในระบบเราจะมีข้อมูลดังนี้

Issue Date	ID	Full Name	User Name
20 Jun 2018, 03:13:54pm	1237931741676	Prof. Jeremie Haley Jr.	dyfkmc
20 Jun 2018, 02:41:55pm	9551472535646	Tanya Nolan	zonnci
20 Jun 2018, 02:24:49pm	8741295155681	Esperanza Bauch	uxptdf
20 Jun 2018, 01:03:15pm	2593429014990	Allison Dickens	rbnwxg
20 Jun 2018, 11:16:09am	5199800529593	Mr. Trystan Murazik	tldayc
20 Jun 2018, 10:53:44am	3442261337925	Prof. Virgil Kiehn Jr.	wrnzul

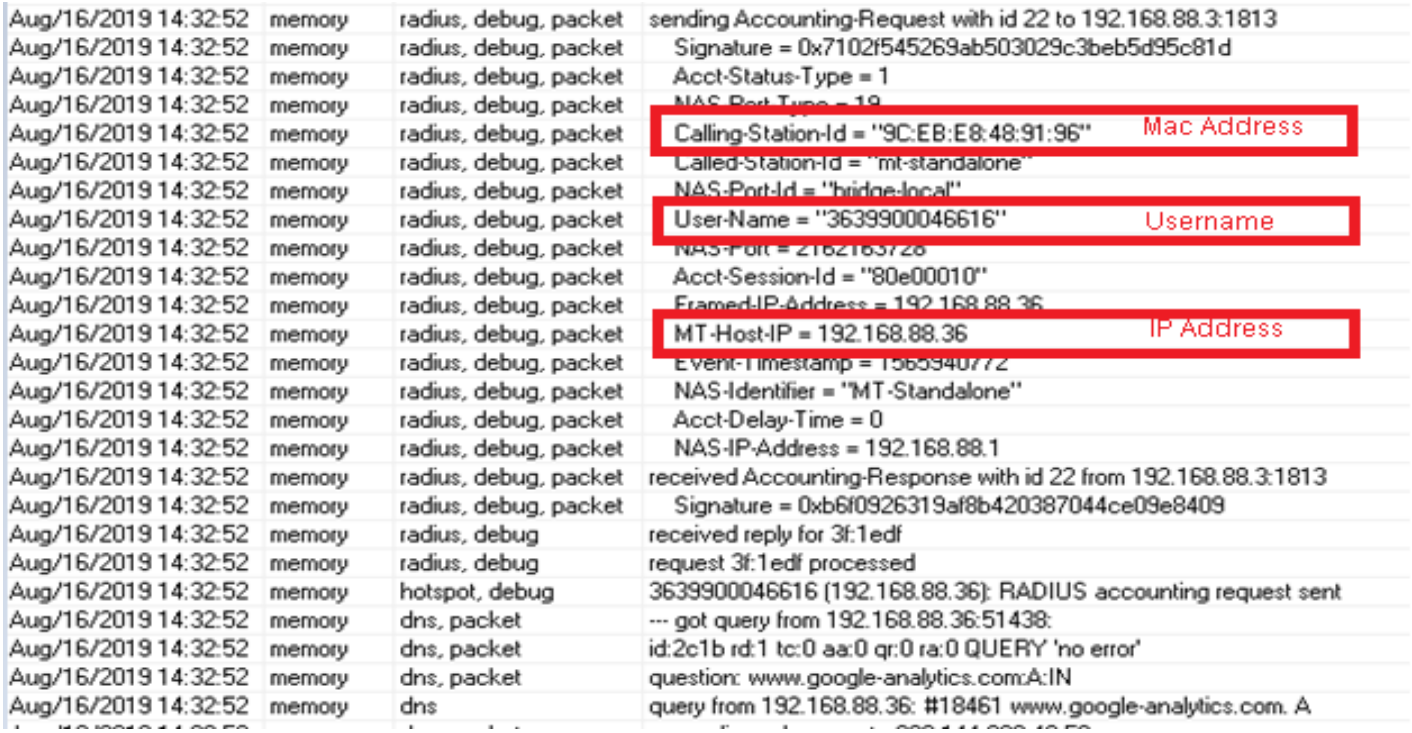
เมื่อผู้ใช้งานเสียบบัตรประชาชน เพื่อรับชื่อผู้ใช้ ตัว Controller จะจัดเก็บข้อมูลสาธารณะของบัตรประชาชนนั้น เช่นหมายเลขบัตรประชาชน ชื่อ และชื่อผู้ใช้ที่สร้างให้กับบัตรประชาชนใบนั้นตามภาพด้านบน

หมายเหตุ: รูปด้านบนเป็นรูปประกอบเพื่อบอกว่าระบบเก็บอะไรไปบ้างเท่านั้น จากนี้เป็นต้นไปในตัวอย่างจะสมมุติให้ผู้ใช้มีข้อมูลดังนี้

รหัสบัตรประชาชน : 1237931741676

ชื่อ : Prof. Jeremie Haley Jr.

Username: 3639900046616



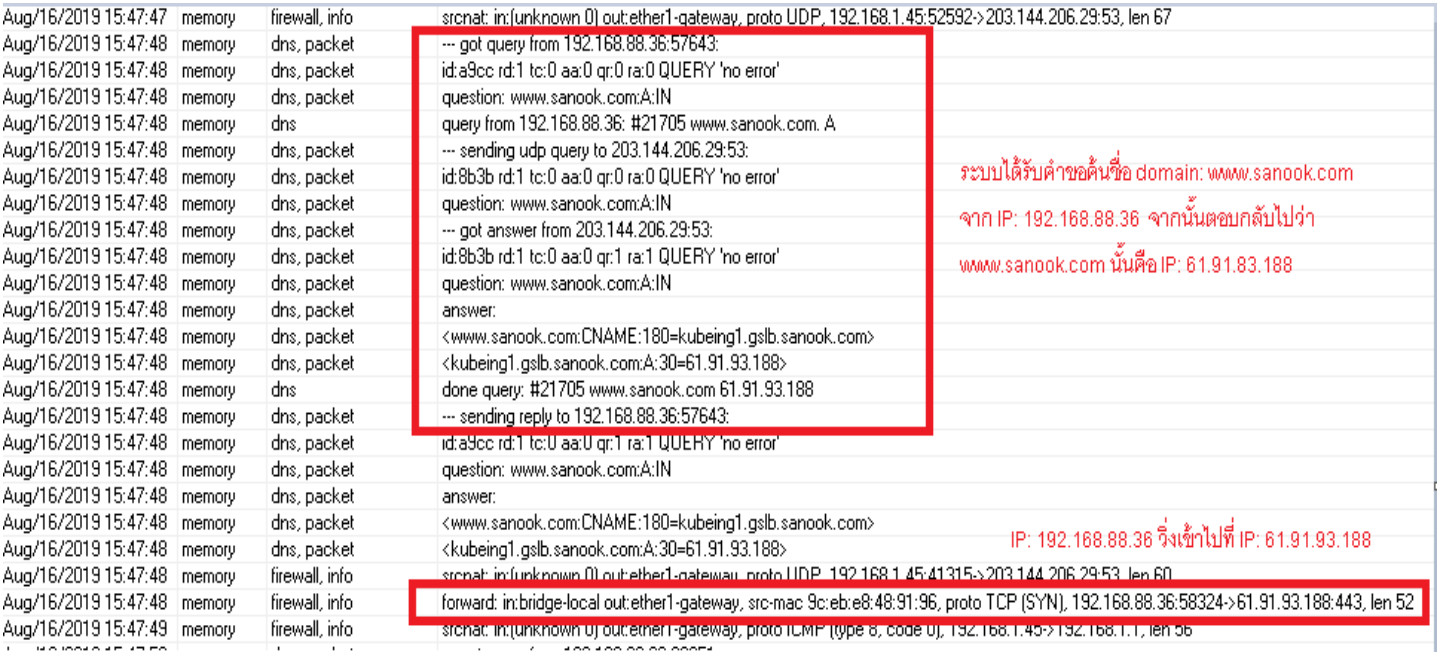
เมื่อผู้ใช้นำ username ที่ได้ไป login เพื่อใช้งาน WiFi ตัว Mikrotik จะส่ง Log ออกมาเพื่อบอกว่าผู้ใช้ชื่ออะไร Mac Address อะไร IP Address อะไร จากตัวอย่างคือ

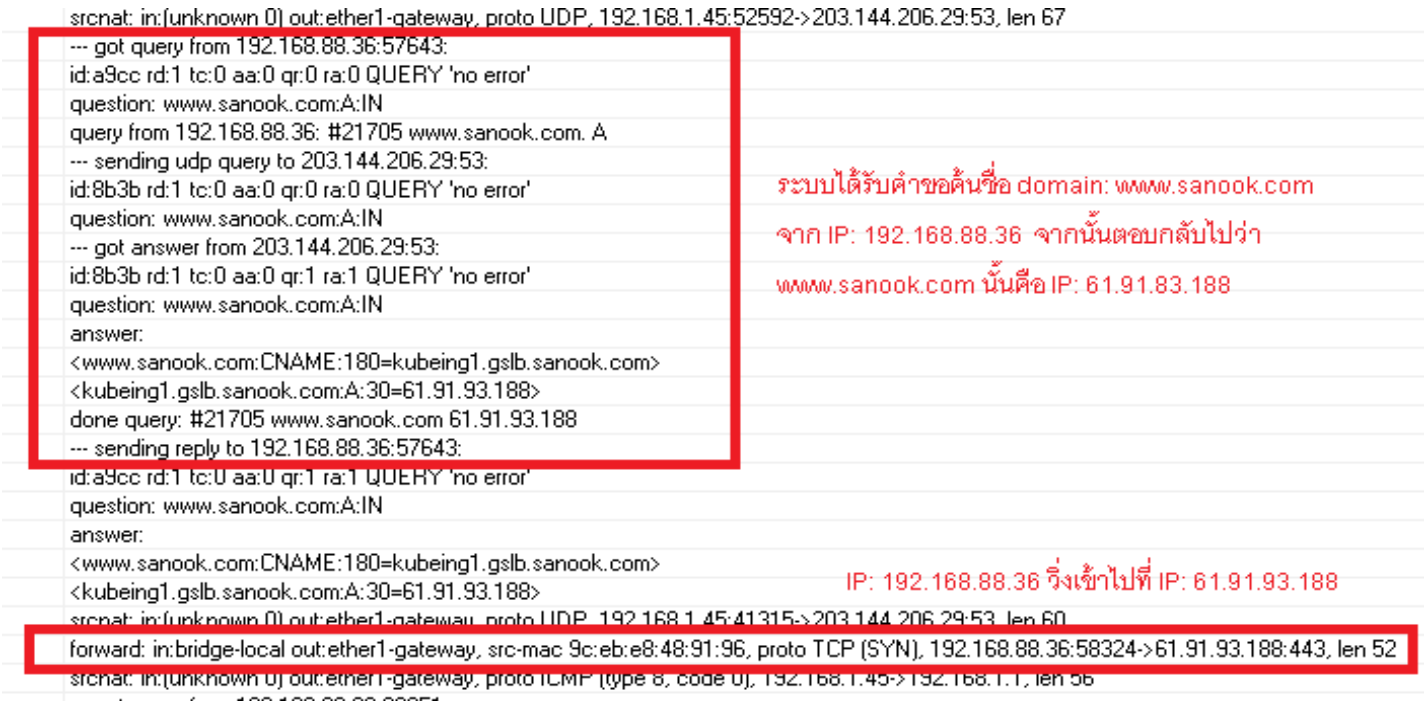
Username: 3639900046616

IP: 192.168.88.36

Mac: 9C:EB:E8:48:91:96

จากนั้นผู้ใช้นี้เข้าเว็บ www.sanook.com ทำให้เกิด Log ดังนี้





จากตัวอย่างจะเห็นได้ว่าระบบเก็บข้อมูลได้ครบถ้วนและสามารถตรวจสอบย้อนหลังไปได้ว่าใครเป็นผู้เข้าเว็บปลายทางดังนี้

- IP ต้นทางจาก Log คือ 192.168.88.36 วิ่งไปที่ IP ปลายทาง 61.91.93.188 ในเวลา 15:47:48 ของวันที่ 16 เดือนสิงหาคม 2562
- IP 61.91.93.188 คือเว็บ www.sanook.com , ซึ่ง IP 192.168.88.36 เป็นผู้ร้องขอให้ค้นชื่อนี้
- IP 192.168.88.36 แจกให้กับ username: 3639900046616
- Username: 3639900046616 คือผู้ใช้ชื่อ Prof. Jeremie Haley Jr. มีรหัสบัตรประชาชนหมายเลข 1237931741676