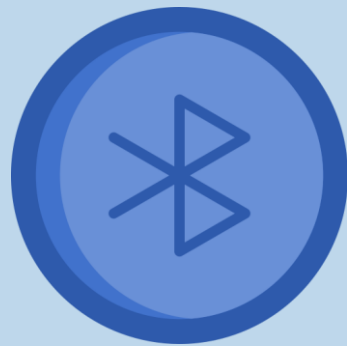


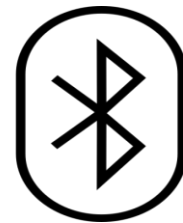


# Bluetooth

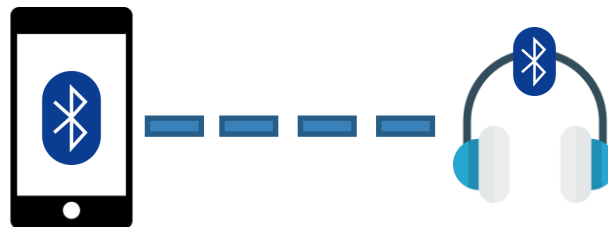


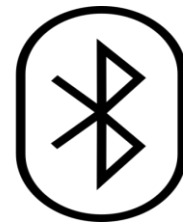
## Vulnerability

# Bluetooth ???



คือ เทคโนโลยีในการรับส่งข้อมูลระหว่าง Device 2 ตัว

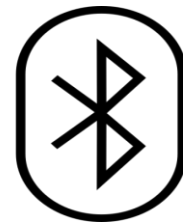




# Bluetooth

**Bluetooth** จะใช้สัญญาณวิทยุความถี่สูง 2.4 GHz. ซึ่งแต่ละประเทศความถี่นั้นจะต่างกันไป อย่างในแถบยุโรปและอเมริกา จะใช้ช่วง 2.400 ถึง 2.4835 GHz. แบ่งออกเป็น 79 ช่องสัญญาณ และจะใช้ช่องสัญญาณที่แบ่งนี้ เพื่อส่งข้อมูลสลับช่องไปมา 1,600 ครั้งต่อ 1 วินาที ส่วนที่ญี่ปุ่นจะใช้ความถี่ 2.402 ถึง 2.480 GHz. แบ่งออกเป็น 23 ช่อง ระยะทำการของ Bluetooth จะอยู่ที่ 5-10 เมตร





# การพัฒนาของ BLUETOOTH



## Version 1.0 และ 1.0B - 1.1-1.2

Device address (BD-ADDR)  
ในการส่งข้อมูลผ่านการ  
Connecting (การส่งข้อมูลแบบนี้  
ยังมีปัญหาอยู่)

## Version 2.0+EDR

เพิ่ม Enhanced Data  
Rate(EDR) เพื่อให้การเคลื่อนย้าย  
ข้อมูลทำได้เร็วขึ้น อัตราความเร็วของ  
EDR อยู่ 3 เมกกะบิตต่อวินาที

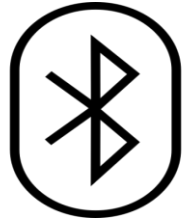
## Version 3.0 + HS

เวอร์ชันนี้ถูกปรับปรุงโดย  
Bluetooth SIG มีการรองรับการ  
ขนส่งข้อมูลด้วยความเร็วสูงสุด  
24 เมกกะบิตต่อวินาที

## Version V4.0 - 4.2

Protocols ที่ใช้พลังงานต่ำและนำ  
เทคโนโลยี ultra-low power  
Bluetooth เข้ามาใช้ ยกตัวอย่างกรณี  
ที่มีการใช้เทคโนโลยีนี้ เช่น การแสดง  
แสดงหมายเลขผู้โทรศัพท์

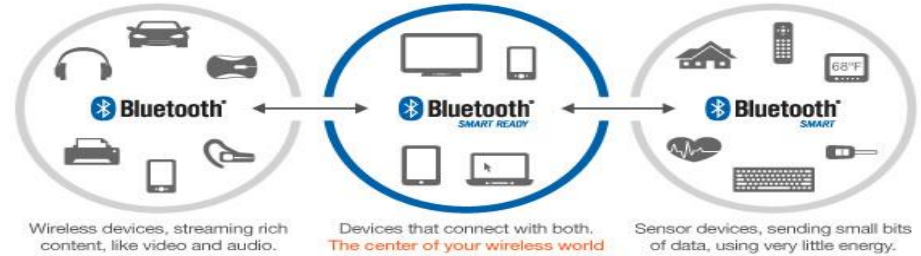
# BLUETOOTH



BLUETOOTH 2.0,  
3.0, 4.0, มีการเปลี่ยนแปลง  
ในระดับ HARDWARE



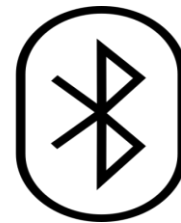
BLUETOOTH 4.0, 4.1,  
4.2, มีการเปลี่ยนแปลงในระดับ  
FEATURE



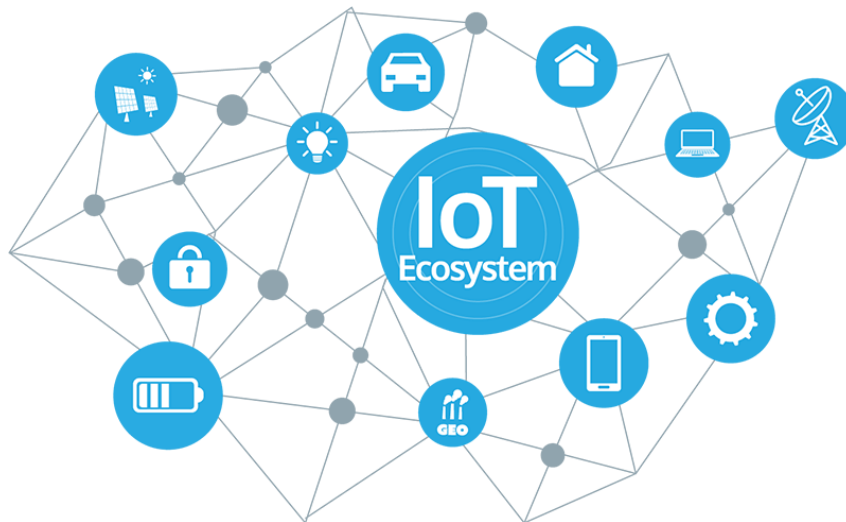
EDR กับ HS เหมือนกัน  
คือมีการเพิ่มความเร็วรับส่ง  
ข้อมูล

HS = HIGHSPEED

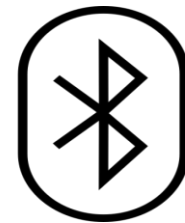
EDR = ENHANCED DATA RATES



**เทคโนโลยีBluetooth** นี้ก็ได้ถูกพัฒนามาจนเป็น “Bluetooth 5” ซึ่งว่ากันว่า  
ทรงประสิทธิภาพมากที่สุดเท่าที่เคยมีเทคโนโลยีนี้มา อีกทั้งหลักใหญ่ใจความของมัน  
ยังให้ความสำคัญเน้นหนักไปที่เรื่องของ Internet of Things (IoT),  
สมาร์ทโฮม (Smart Home) และการฟังเพลงแบบไร้สาย (Wireless Audio)



# BLUETOOTH 5.0



BLUETOOTH 5.0

5 มีแบนด์วิดธ์สูงสุดที่ 2Mbps ในทางปฏิบัติหมายความว่ามันเร็วพอและไวใจได้มากพอที่จะใช้ระบบไร้สายทำการอัปเดตเฟิร์มแวร์หรือใช้อัปโหลดข้อมูลสำคัญ Bluetooth

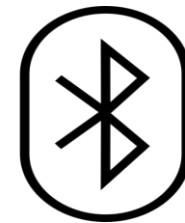
สามารถรับ-ส่งข้อมูลได้เร็วกว่า Bluetooth 4.2 LE (Low Energy) ถึง 2 เท่า เชื่อมต่อได้ในระยะห่างไกลกว่าถึง 4 เท่า และสามารถส่งผ่านปริมาณข้อมูลในหนึ่งช่วงเวลาได้มากกว่าถึง 8 เท่า มีระยะห่างในการเชื่อมต่อระหว่างอุปกรณ์เพิ่มขึ้นเป็น 800 ฟุต (ประมาณ 240 เมตร)



Bluetooth Vulnerability



# ข้อดีและข้อเสียBLUETOOTH



## ข้อดี

1. เพิ่มความสะดวกสบายในการใช้อุปกรณ์อิเล็กทรอนิกส์ต่างๆ
2. สามารถโอนถ่ายข้อมูลต่างๆได้ง่ายและรวดเร็วขึ้น
3. ประหยัดค่าใช้จ่ายในการส่งข้อมูลหรือรูปภาพต่างๆ
4. การใช้อุปกรณ์จะช่วยให้ประหยัดเวลาในการตั้งอุปกรณ์ต่างๆ และสามารถเคลื่อนย้ายอุปกรณ์ได้ง่าย
5. ลดความกังวลในการใช้โทรศัพท์ เนื่องจากถ้าผู้ใช้เลือกใช้ Smalltalk แบบมีสายต่อก็ต้องคอยกังวลว่า
6. เมื่อเปรียบเทียบกับการใช้อินเทอร์เน็ตแล้ว การใช้ Bluetooth มีข้อดีกว่า เนื่องจากการรับส่งข้อมูลแบบอินเทอร์เน็ตต้องใช้แสงเป็นสื่อในการติดต่อและผู้ส่งกับผู้รับ

## ข้อเสีย

1. ความง่ายตายในการโอนถ่ายข้อมูลอาจทำให้เกิดอาชญากรรมเพิ่มมากขึ้นได้ถ้าบุคคลเหล่านั้นนำข้อมูลไปใช้งานในแบบที่ไม่เหมาะสม
2. ถ้ามีการเปิดบลูทูธทิ้งไว้นานอาจมีกลุ่มบุคคลที่ไม่ประสงค์ดีปล่อยตัวไวรัสมาที่อุปกรณ์อิเล็กทรอนิกส์ของเราได้ ซึ่งก่อให้เกิดความเสียหายต่อทรัพย์สินและข้อมูลต่างๆได้
3. การใช้ Booth Headset และโทรศัพท์มือถืออย่างเพลิดเพลินและความสะดวกสบาย อาจทำให้ผู้ใช้ขาดความระมัดระวังได้
4. การส่งข้อมูลทาง Bluetooth อาจทำให้เกิดการดักฟังหรือการลักลอบขโมยข้อมูลต่างๆได้ถึงแม้ว่าจะทำได้ยากก็ตาม

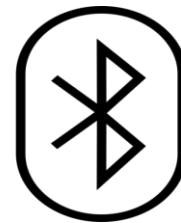






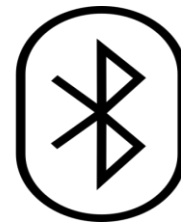
# Bluetooth

มีความเสี่ยงของการถูก  
โจรกรรมทางข้อมูล

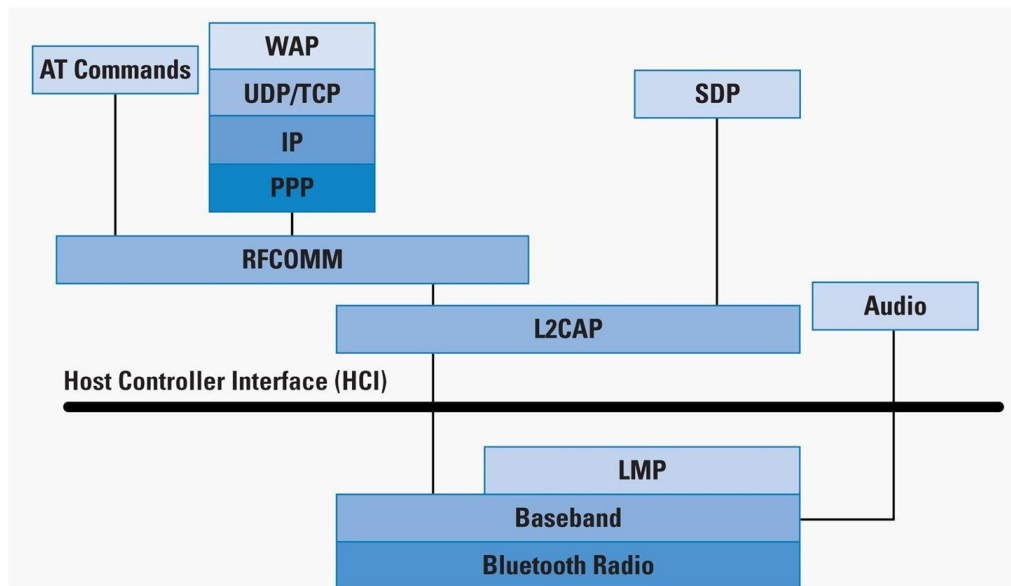


## ช่องโหว่ของบลูทูธ

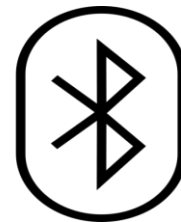
1. ไม่มีการรักษาความปลอดภัยที่ใช้งานอยู่
2. ความปลอดภัยระดับบริการ ผู้จัดการความปลอดภัยส่วนกลางจัดการการรับรองความถูกต้อง การกำหนดค่า และการอนุญาต อาจไม่สามารถเปิดใช้งานโดยผู้ใช้ ไม่มีความปลอดภัยระดับอุปกรณ์
3. ความปลอดภัยระดับอุปกรณ์ การรับรองความถูกต้องและการเข้ารหัสตามคีย์ลับ เปิดเสมอ บังคับใช้การรักษาความปลอดภัยสำหรับการเชื่อมต่อระดับต่ำ



- Bluetooth Core Protocols
- Baseband: LMP, L2CAP, SDP
- Cable Replacement Protocol: RFCOMM
- Telephony Control Protocol: TCS Binary, AT-commands
- Adopted Protocols: PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE



Bluetooth Protocol Stack



BlueBorne™

เตือนภัยช่องโหว่ชื่อ BlueBorne (บลูบอร์น) อาจจะถูกขโมยข้อมูล หรือถูกติดตั้งมัลแวร์ที่เปิดใช้งานบลูทูธ (Bluetooth) และอยู่ในรัศมีประมาณ 10 เมตร โดยที่ตัวอุปกรณ์ไม่จำเป็นต้องจับคู่ (Pair) กับอุปกรณ์ที่ใช้โจมตี รวมถึงไม่จำเป็นต้องเปิดโหมดค้นหอุปกรณ์ (Discovery mode) แต่อย่างใด

BlueBorne ส่งผลกระทบต่ออุปกรณ์บลูทูธทั่วโลก ไม่ว่าจะเป็นระบบปฏิบัติการ Android, Apple iOS, Microsoft หรือ Linux ตั้งแต่สมาร์ทโฟน แท็บเล็ต โน้ตบุ๊ก อุปกรณ์ IoT ไปจนถึงรถยนต์อัจฉริยะรวมแล้วกว่า 5,300 ล้านเครื่อง

 Bluetooth Vulnerability

ระวังภัย ช่องโหว่อันตราย

BlueBorne

ถูกแฮกเครื่อง ฟังมัลแวร์ได้ผ่าน Bluetooth

เวอร์ชัน 01  
13 ก.ย. 2560  
เวลา 10:40 น.

ภาพรวมช่องโหว่

ข้อผิดพลาดในซอฟต์แวร์ที่ใช้ควบคุมการเชื่อมต่อ Bluetooth เปิดรับข้อมูลอันตราย มาประมวลผลได้โดยไม่ต้อง Pair หรือ Connect กับอุปกรณ์ที่ใช้โจมตี

ผลกระทบ

อุปกรณ์ที่เปิด Bluetooth และอยู่ในรัศมีใกล้เคียงกับผู้โจมตี มีโอกาสถูกแฮกขโมยข้อมูลหรือถูกฟังมัลแวร์ได้

วิธีป้องกัน

หากยังไม่มีความจำเป็นต้องใช้งาน ควรปิด Bluetooth แล้วอัปเดตเฟิร์มแวร์ให้เรียบร้อยก่อนเปิดใช้งานใหม่

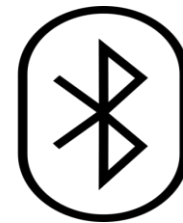
Android : อัปเดตเฟิร์มแวร์ประจำเดือนเมษายน 2560  
iOS : อัปเดตเฟิร์มแวร์ iOS 10 หรือใหม่กว่า  
Windows : อัปเดตเฟิร์มแวร์ประจำเดือนเมษายน 2560  
macOS : อัปเดตระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุด  
Linux : อัปเดตเฟิร์มแวร์ Bluetooth (ดูเพิ่มเติมที่เว็บไซต์การกระจาย (Distribution))

QR Code

สงวนลิขสิทธิ์  
www.thaicert.or.th

ศูนย์ประสานงานด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (ThaCERT)  
สำหรับงานพัฒนาความรู้ทางเทคนิคคอมพิวเตอร์ (องค์การมหาชน)  
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ThaCERT ETDA  
www.thaicert.or.th

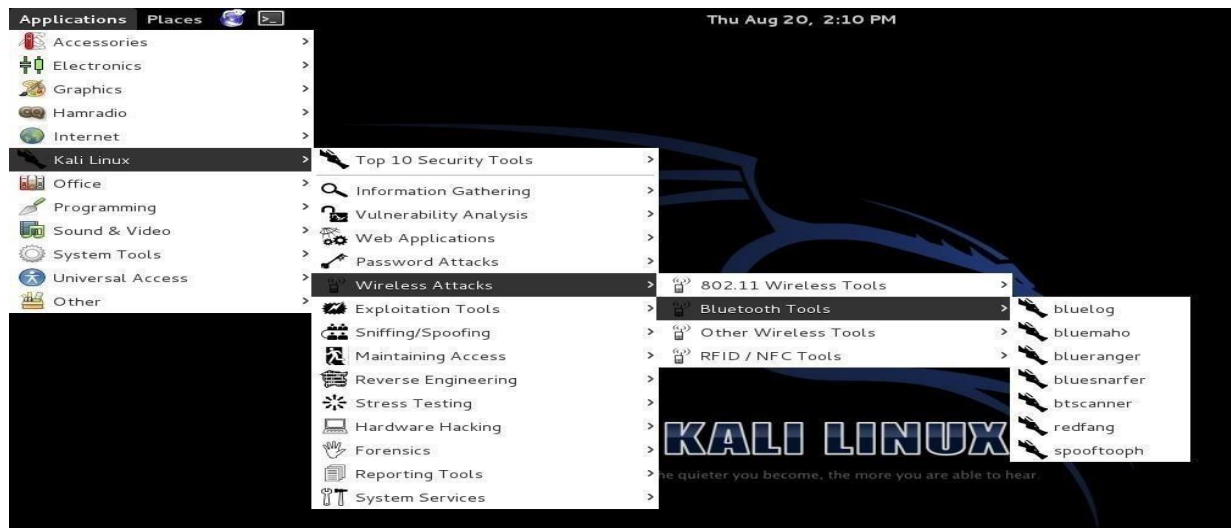
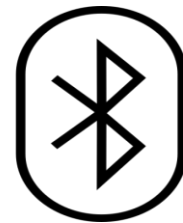


**Kali** คือระบบปฏิบัติการลินุกซ์ (Linux) ตัวหนึ่งของคอมพิวเตอร์ เหมือนกับการที่มีมือถือเรามี iOS กับ Android คอมฯ เรายังมีระบบปฏิบัติการหลายตัวอย่าง MacOS, Windows และลินุกซ์ ซึ่งโดยปกติแล้วลินุกซ์มักจะถูกใช้ใน เครื่องเซิร์ฟเวอร์เช่นไวร์เลสเซิร์ฟเวอร์

แต่ Kali เป็นลินุกซ์ที่ออกแบบมาสำหรับ “งานด้านความปลอดภัยระบบไอที” โดยการที่ติดตั้งซอฟต์แวร์ต่าง ๆ ที่มักจะถูกใช้งานบ่อย ๆ ในการทำงานเอาไว้เรียบร้อยแล้ว หรือยังไม่ได้ติดตั้ง แต่ว่า สามารถติดตั้งได้โดยง่าย ผ่านระบบติดตั้งโปรแกรมที่มีให้เรียกว่า software repository ของ Kali โดยเฉพาะ

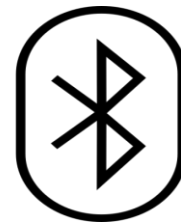


# ตัวอย่างของแถบเครื่องมือKali ในฟังก์ชันของBluetooth





## เครื่องมือของKali

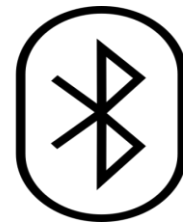


- 1.Blueelog: เครื่องมือสำรวจไซต์บลูทูธ มันสแกนพื้นที่เพื่อค้นหาอุปกรณ์ที่ค้นพบได้จำนวนมากในพื้นที่แล้ว มันก็ลงในไฟล์
- 2.Bluemaho: ชุดเครื่องมือที่ใช้ GUI สำหรับการทดสอบความปลอดภัยของอุปกรณ์ Bluetooth
- 3.Blueranger: สคริปต์ Python แบบง่ายที่ใช้ i2cap pings เพื่อค้นหาอุปกรณ์บลูทูธ และกำหนดระยะทางโดยประมาณ
- 4.Btscanner: เครื่องมือที่ใช้ GUI นี้สแกนหาอุปกรณ์ที่สามารถค้นพบได้ภายในระยะ
- 5.Redfang: เครื่องมือนี้ช่วยให้เราค้นหาอุปกรณ์บลูทูธ ที่ซ่อนอยู่





## เครื่องมือของKali



6.Spooftooth: นี่คือการปลอมแปลงบลูทูธ

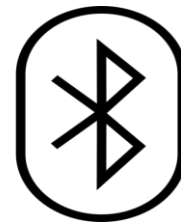
7.Bluesnarfing: การโจมตีนี้ใช้ข้อมูลจากอุปกรณ์ที่ใช้เทคโนโลยี Bluetooth ซึ่งอาจรวมถึงข้อความ SMS ข้อมูลปฏิทินรูปภาพสมุดโทรศัพท์และการแชท

8.Bluebugging: ผู้โจมตีสามารถควบคุมโทรศัพท์ของเป้าหมายได้ Bloover ได้รับการพัฒนาเป็นเครื่องมือ POC สำหรับจุดประสงค์นี้

9.Bluejacking: ผู้โจมตีส่ง "นามบัตร" (ข้อความ) ซึ่งหากผู้ใช้อนุญาตให้เพิ่มในรายชื่อผู้ติดต่อผู้โจมตีสามารถส่งข้อความเพิ่มเติมได้

10.Bluesmack: การโจมตี DoS จากอุปกรณ์บลูทูธ

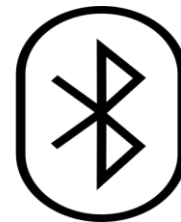




## ตัวอย่างการใช้งาน(Kali)ในการแฮกบลูทูธ

```
root@kali:~# hciconfig hci0 up
root@kali:~# hciconfig hci0
hci0:  Type: BR/EDR  Bus: USB
       BD Address: A0:02:DC:11:4F:85  ACL MTU: 310:10  SCO MTU: 64:8
       UP RUNNING PSCAN
       RX bytes:913 acl:0 sco:0 events:43 errors:0
       TX bytes:915 acl:0 sco:0 commands:43 errors:0
```

(การตั้งค่า)



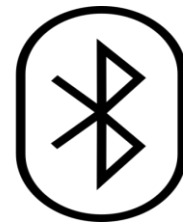
## ตัวอย่างการใช้งาน(Kali)ในการแฮกบลูทูธ

```
Applications ▾ Places ▾ Terminal ▾ Thu 2/2/14 root@kali: ~
File Edit View Search Terminal Help
pageparams [win:int] Get/Set page scan window and interval
pagesto [int] Get/Set page timeout
afmode [mode] Get/Set AFM mode
sigmode [mode] Get/Set Simple Pairing Mode
aclmtu <mtu> Set ACL MTU and number of packets
scoctu <mtu> Set SCO MTU and number of packets
delay <delay> Delay link key from the device
oobdata Get local OOB data
commands Display supported commands
features Display device features
version Display version information
revision Display revision information
block <bdaddr> Add a device to the blacklist
unblock <bdaddr> Remove a device from the blacklist
lerandaddr <bdaddr> Set LE Random Address
leadv [type] Enable LE advertising
0 Connectable undirected advertising (default)
3 Non connectable undirected advertising
nleadv Disable LE advertising
teststates Display the supported LE states
root@kali:~# hciconfig -a hci0 up
root@kali:~# hciconfig hci0
hci0: Type: Primary Bus: USB
BD Address: 3C:A0:67:AD:77:14 ACL MTU: 8192:328 SCO MTU: 64:328
UP RUNNING
RX bytes:1006 acl:0 sco:0 events:44 errors:0
TX bytes:672 acl:0 sco:0 commands:44 errors:0
root@kali:~# hcitool scan hci0
scan: too many arguments (maximal: 0)
Usage: scan [-length] [-numsp=N] [--lsc=lap] [--flush] [--class] [--info] [--oui] [--refresh]
root@kali:~# hcitool scan
Scanning...
11:11:12.C4:04 YET-M1
01:1F:0E:73:27 B31E
root@kali:~# l2ping
```

การค้นหาสัญญาณบลูทูธเพื่อทำการเชื่อมต่อ เมื่อทำการเชื่อมต่อสำเร็จก็สามารถทำการโจรกรรมข้อมูลหรือปล่อยมัลแวร์ทำลายโทรศัพท์ของเป้าหมายได้

```
Applications ▾ Places ▾ Sat Feb 23 14:00:43 root@kali: ~
File Edit View Search Terminal Help
Time Address Clk off Class Name
2014/02/01 10:40:03 E4:32:CB:71:90:52 0x0000 0x5a020c GT-S6310N
starting inquiry scan
Found device E4:32:CB:71:90:52
aborting scan
aborted
root@kali:~#
```

\*\*\*หมายเหตุบลูทูธตั้งแต่4.0+ขึ้นไปมีระบบป้องกันการโจรกรรมข้อมูลทำให้ถอดการเชื่อมต่อได้ยาก



ขอบคุณครับ