Tugas Keamana Jaringan Komputer

WarDriving Menggunakan Tools “Wiggle & Google Earth”

Pada Daerah Gang Buntu Indralaya

Disusun Oleh:

Aditiya Gunanta

09011181520001

Universitas Sriwijaya

Fakultas Ilmu Komputer

Jurusan Sistem Komputer

2019

Pendahuluan

Wi-Fi , Wireless Ethernet dan Wireless LAN merupakan hal yg sudah lumrah saat ini , karena kini hamper setiap orang membutuh kan internet, oleh karna itu , Saat ini kini telah banyak di buat Access Point (AP) atau lebih sering di kenal dengan sebutan “HotSpot” dengan tujuan terjangkaunya sarana internet yang lebih memadai . Wi-Fi , Wireless Ethernet dan Wireless LAN memiliki jaringan standar milik IEEE 802.11. sebagai standar yang biasa digunakan instansi yang ada Di Indonesia 802.11b adalah jaringan standar yang memliki frekuensi 2.4GHz dengan kecepatan transfer data sebesar 11Mbps. Karna bersifat tanpa kabel (Wireless) , jangkauan dari pada system ini lebih jauh ketimbang system Wired. Keamanannya pun lebih tinggi karna teknologi ini menggunakan gelombang elektromagnetik . namun , setinggi apapun keamanan suatu system akan tetap memiliki celah. Wardriving adalah salah satu perilaku atau kegiatan yang sekarang biasa dilakukan untuk masuk kedalam jaringan internet yang disediakan melalui Wireless Ethernet. Selain merugikan , ini akan menjadi maslah serius dikemudian hari , karna semakin banyak tools yang bisa digunakan sebagai penyokong dari Wardriving.

Tinjauan Pustaka

WarDriving

Wardriving adalah tindakan mencari Wi-Fi jaringan nirkabel oleh seseorangdalam kendaraan yang bergerak , menggunakan komputer portable , smartphone atau personal digital assistant (PDA). Istilah ini mulai berkembang karna teknologi yang semakin hari semakin cepat kemajuannya. Banyak programmer yang berlomba lomba membuat tools baru untuk membobol jaringan yang bersifat Wireless

Wigle

Wigle adalah salah satu dari sekian banyak tools yang digunakan untuk menjalankan maksud dari Wardriving yaitu untuk Hacking Wireless . Wigle berbasis android walaupun wigle sendiri juga tersedia dalam versi PC , namun smartphone berbasi android lebih mudah dibawa dari pada menggunaka laptop atau notebook, itulah mengapa Wigle lebih mudah digunakan pada smartphone. NetStumbler juga merupakan salah satu tools yang bisa digunakan untuk Wardriving , kelemahan dari NetStumbler adalah kita perlu menambah Hardware yaitu GPS yang bisa dihubungkan menggunakan kabel connector Db9 yang ada dibelakan CPU PC, namun tentu saja itu akan memakan biaya lebih untuk pengaplikasiannya.

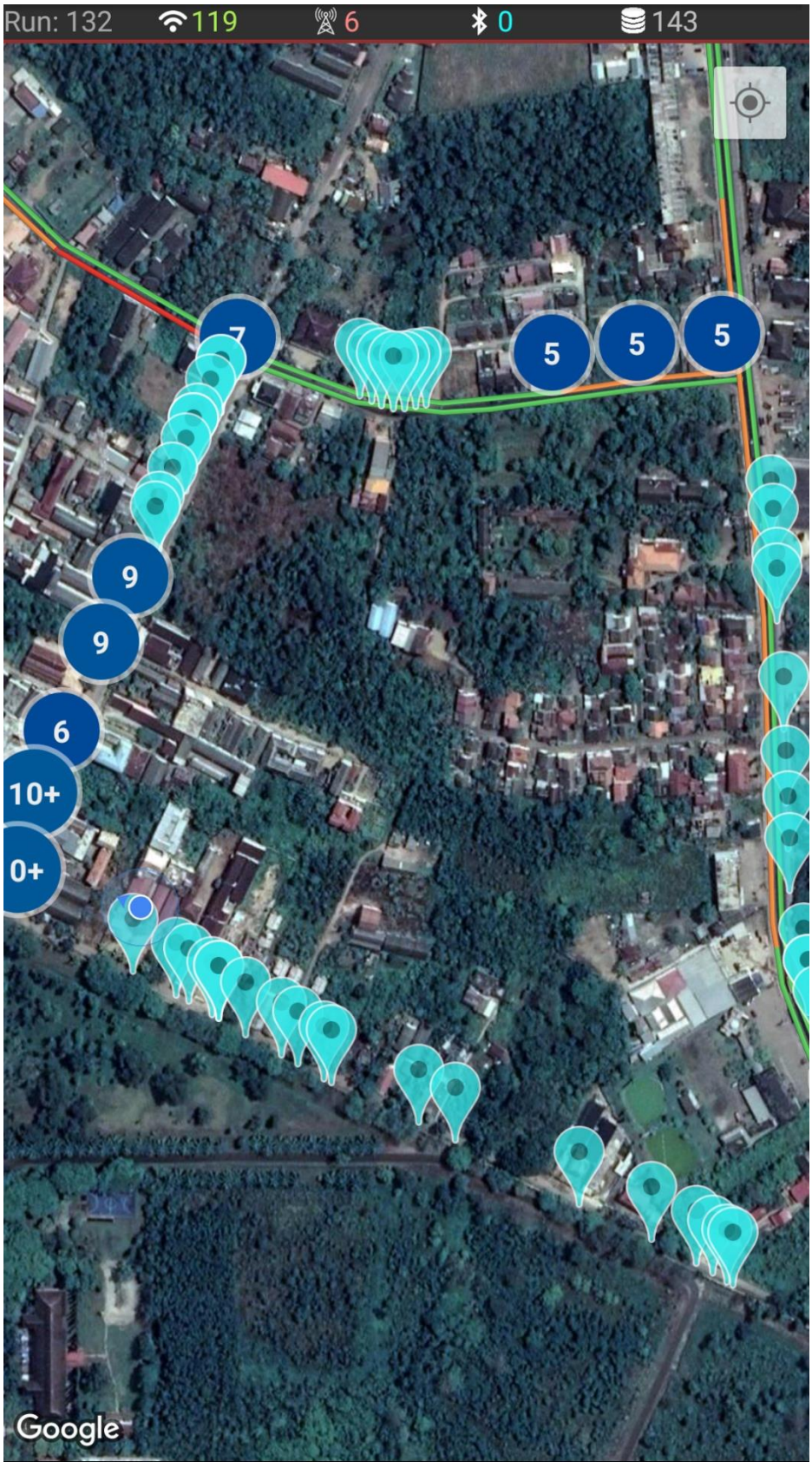
Google Earth

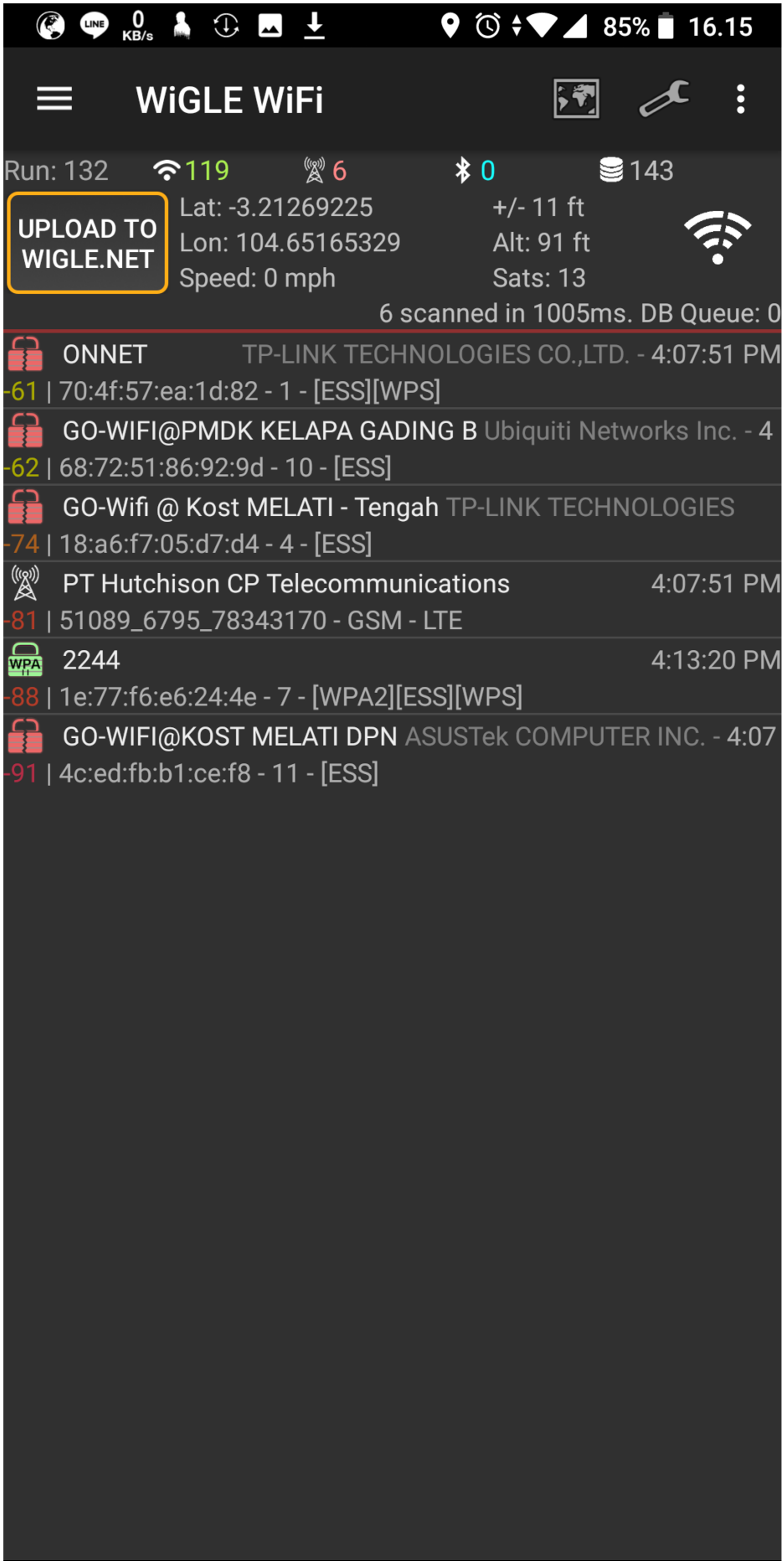
Google Earth merupakan sebuah program globe virtual yang sebenarnya disebut Earth Viewer dan dibuat oleh Keyhole, Inc.. Program ini memetakan bumi dari superimposisi gambar yang dikumpulkan dari pemetaan satelit, fotografi udara dan globe GIS 3D

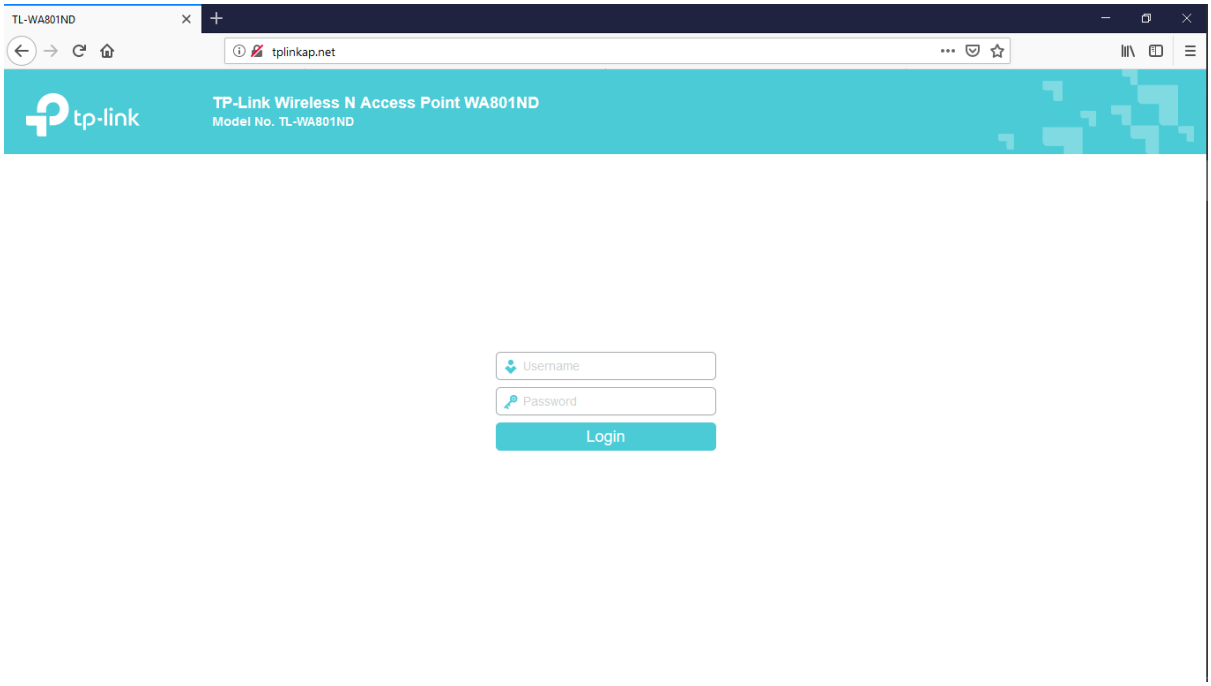
Metode Penelitian

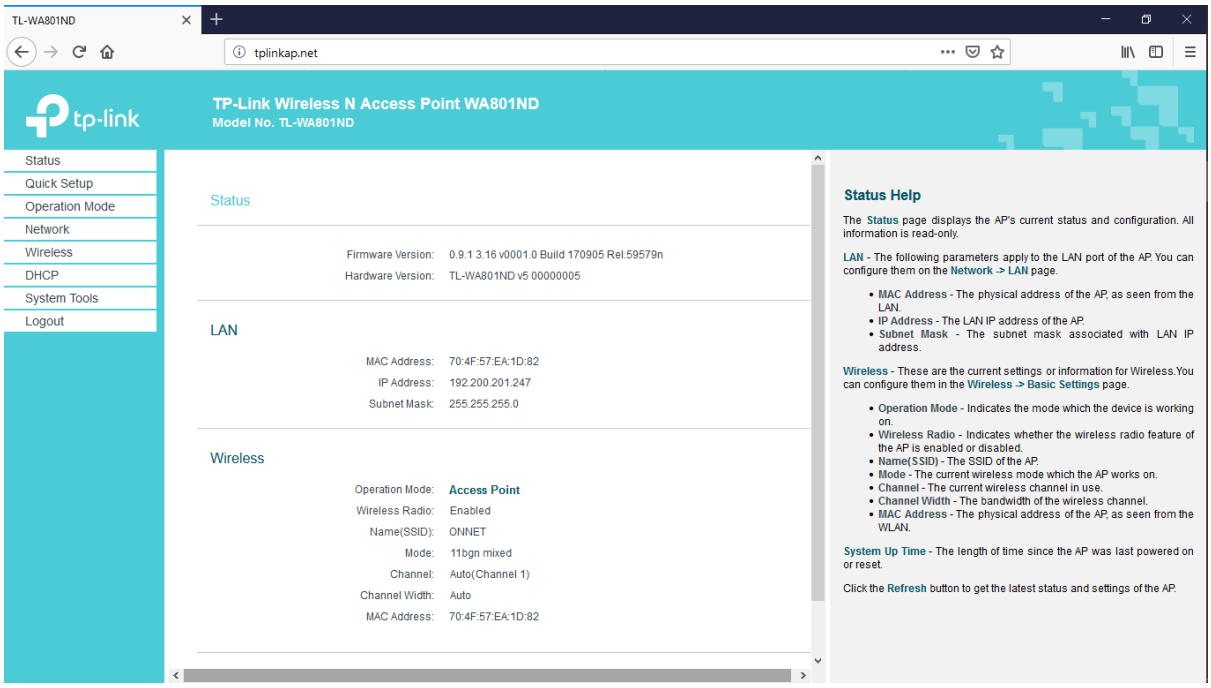
Pada penelitian kali ini , Saya menggunakan sebuah perangkat android dengan Operating System (OS) Android OREO (8.1). Saya telah menginstal aplikasi Wiggle pada perangkat saya untuk mulai melakukan WarDriving. Kendaraan yg di gunakan sebuah sepeda motor , Kecepatan dari sepeda motor ketika melakukan capture data adalah anatara 20-50 Km/H ,Lokasi yg saya gunakan untuk uji coba kali ini adalah Kawasan Gang Buntu Indralaya, Setelah melakukan capture data, hasil capture di export dengan fomat KML

Hasil Penelitian




85% 16.15
WiGLE WiFi
Run: 132
119
6
0
143
UPLOAD TO WIGLE.NET
Lat: -3.21269225
Lon: 104.65165329
Speed: 0 mph
+/- 11 ft
Alt: 91 ft
Sats: 13
6 scanned in 1005ms. DB Queue: 0
ONNET TP-LINK TECHNOLOGIES CO.,LTD. - 4:07:51 PM
-61 | 70:4f:57:ea:1d:82 - 1 - [ESS][WPS]
GO-WIFI@PMDK KELAPA GADING B Ubiquiti Networks Inc. - 4
-62 | 68:72:51:86:92:9d - 10 - [ESS]
GO-Wifi @ Kost MELATI - Tengah TP-LINK TECHNOLOGIES
-74 | 18:a6:f7:05:d7:d4 - 4 - [ESS]
PT Hutchison CP Telecommunications 4:07:51 PM
-81 | 51089_6795_78343170 - GSM - LTE
2244 4:13:20 PM
-88 | 1e:77:f6:e6:24:4e - 7 - [WPA2][ESS][WPS]
GO-WIFI@KOST MELATI DPN ASUSTek COMPUTER INC. - 4:07
-91 | 4c:ed:fb:b1:ce:f8 - 11 - [ESS]


TL-WA801ND
tplinkap.net
tp-link
TP-Link Wireless N Access Point WA801ND
Model No. TL-WA801ND
Username
Password
Login


TL-WA801ND
tplinkap.net
tp-link
TP-Link Wireless N Access Point WA801ND
Model No. TL-WA801ND
Status
Quick Setup
Operation Mode
Network
Wireless
DHCP
System Tools
Logout
Status
Firmware Version: 0.9.1 3.16 v0001.0 Build 170905 Rel.59579n
Hardware Version: TL-WA801ND v5 00000005
LAN
MAC Address: 70:4F:57:EA:1D:82
IP Address: 192.200.201.247
Subnet Mask: 255.255.255.0
Wireless
Operation Mode: Access Point
Wireless Radio: Enabled
Name(SSID): ONNET
Mode: 11bgn mixed
Channel: Auto(Channel 1)
Channel Width: Auto
MAC Address: 70:4F:57:EA:1D:82
Status Help
The Status page displays the AP's current status and configuration. All information is read-only.
LAN - The following parameters apply to the LAN port of the AP. You can configure them on the Network -> LAN page.
MAC Address - The physical address of the AP, as seen from the LAN.
IP Address - The LAN IP address of the AP.
Subnet Mask - The subnet mask associated with LAN IP address.
Wireless - These are the current settings or information for Wireless. You can configure them in the Wireless -> Basic Settings page.
Operation Mode - Indicates the mode which the device is working on.
Wireless Radio - Indicates whether the wireless radio feature of the AP is enabled or disabled.
Name(SSID) - The SSID of the AP.
Mode - The current wireless mode which the AP works on.
Channel - The current wireless channel in use.
Channel Width - The bandwidth of the wireless channel.
MAC Address - The physical address of the AP, as seen from the WLAN.
System Up Time - The length of time since the AP was last powered on or reset.
Click the Refresh button to get the latest status and settings of the AP.

Analsia

Setelah melakukan WarDriving di daerah Gang Buntu Indralaya hasil nya bisa dilihat pada Gambar 1 , dapat dilihat pada mapping bahwasannya hasil scanning juga mengenai beberapa Access Point milik beberapa Provider terkenal yang ada Di Indonesia yang juga memiliki Hotspot dikawasan tersebut . hasil pada Gambar 1 merupakan hasil yang kami dapat setelah mengitari kawansan Gang Buntu Indralaya. Pada gambar 1 terlihat ada ikon berwarna merah dan hijau, ikon berwarna merah menyatakan bahwa Access Point (AP) tersebut dilindungi oleh password dengan metode autentikasi WEP/WPA PSK/WPA2-PSK, sementara ikon yang berwarna hijau menyatakan bahwa Access Point (AP) tersebut menggunakan metode autentikasi dengan servis RADIUS.

Pada Gambar kedua menampil kan beberapa Acces Point yg berada di sekitar User dan masuk dalah jangkauan Radius dari setiap Acces Point yg ada disana, lalu saya mencoba memilih salah satu Acces Point yg ada pada list tersebut saya memilih Acces Point teratas untuk mencoba masuk ke dalam system configurasi dari pada Accses Point tersebut.

Pada Gambar 3 dan 4 meninjukan bahwa pada Acces Point Tersebut menggunakan WEB service untuk mengkonfigurasi Acces Point tersebut tanpa menggunakan PUTTY, saya coba melakukan password guessing dan berhasil masuk ke dalam system konfigurasi yg di miliki oleh Acces Point Tersebut.

Kesimpulan

Dalam perkembangannya , keamanan jaringan wireless haruslah menjadi sesuatu yang diperhatikan, sebab , bahkan dengan menggunakan tools sederhana seperti wigle dan netstumbler saja , kemanan yang ada pada sebuah jaringan wireless akan sangat riskan semakin banyak upaya dari seorang hacker untuk membobol ataupun meretas sebuah jaringan wireless. Dalam penelitian kali ini didapatlah kesimpulan yang tentunya berdasarkan apa yang terjadi dilapangan

1. Wigle sebagai Tools yang digunakan pada smartprhone bisa menggantikan fungdi wifi searching yang ada pada smartphone tersebut, namun perbedaannya adalah pada saat penggunannya , wi-fi searching pada smartphone digunakan untuk menghubungkan smartphone ke Access Point (AP) yang ada disekitar smartphone tersebut , sementara Wigle difungsikan untuk mengetahui ada atau tidaknya Access Point (AP) di sekitar smartphone tersebut
2. Dalam mengaman kan konfigurasi Acces Point harus sangat di perhatikan karena, para pengguna awam sering kali tidak memperhatikan password default yg di berikan oleh setiap manufacture perangkat, karena jika password default tidak di rubah maka akan sangat mudah bagi para penyerang untuk memanfaat kan celah yg fatal ini untuk kepentingan mereka sendiri.