

Tugas Keamanan Jaringan Komputer

WARDIVING MENGGUNAKAN TOOLS WIGLE
DIKAWASAN JALAN LUNJUK JAYA PALEMBANG



Oleh :

Dyah Citra Soraya

09011281520107

SK8C

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019

WarDriving Menggunakan Tools “Wigle” Dikawasan Jalan Lunjuk Jaya Palembang

Dyah Citra Soraya (09011281520107)

1. Pendahuluan

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Komputer pada jaringan dapat terhubung melalui kabel, saluran telepon, gelombang radio, satelit, atau infra merah.

WirelessLAN merupakan sistem transmisi data yang didesain untuk menyediakan location independent network acces antar komputer dengan menggunakan gelombang radio. Wardriving memetakan populasi wireless access point yang bertujuan untuk memperoleh statistik yang digunakan untuk mengetahui permasalahan keamanan yang sedang terjadi pada jaringan (wireless network).

2. Tinjauan Pustaka

2.1 Wardriving

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

2.2 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 berbasis android lebih mudah dibawa daripada menggunakan 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.

2.3 Wireless Access Point

Wireless Access Point (WAP) dalam jaringan komputer, titik akses nirkabel adalah suatu peranti yang memungkinkan peranti nirkabel untuk terhubung ke dalam jaringan dengan menggunakan Wi-Fi, Bluetooth, atau standar lain. WAP biasanya tersambung ke suatu router (melalui kabel) sehingga dapat meneruskan data antara berbagai peranti nirkabel (seperti komputer atau pencetak) dengan jaringan berkabel pada suatu jaringan. Standar yang diterapkan untuk WAP ditetapkan oleh IEEE dan sebagian besar menggunakan IEEE 802.11. WAP terhubung pada jaringan, pada jarak jangkauan WAP siapapun dapat terhubung ke jaringan. Pada saat ini enkripsi merupakan keamanan standar yang harus dimiliki oleh setiap Access Point yang digunakan sebagai sistem keamanan yang akan menjamin keamanan user. Generasi enkripsi pertama yang diterapkan adalah Wired Equivalent Privacy (WEP), WEP sendiri telah banyak diuji karena memiliki banyak kelemahan sehingga sangat mudah untuk ditembus. generasi kedua dan ketiga adalah menggunakan Wi-Fi Protected Access (WPA), Beberapa WAP mendukung authentication menggunakan Remote Authentication Dial-In User Service (RADIUS) dan server authentication yang lain. dan digenerasi yang sama Wi-Fi Protected Access II (WPA2), keduanya memiliki algoritma yang kuat dan aman jika menggunakan password atau passphrase yang kuat (unik).

2.4 Global Position System

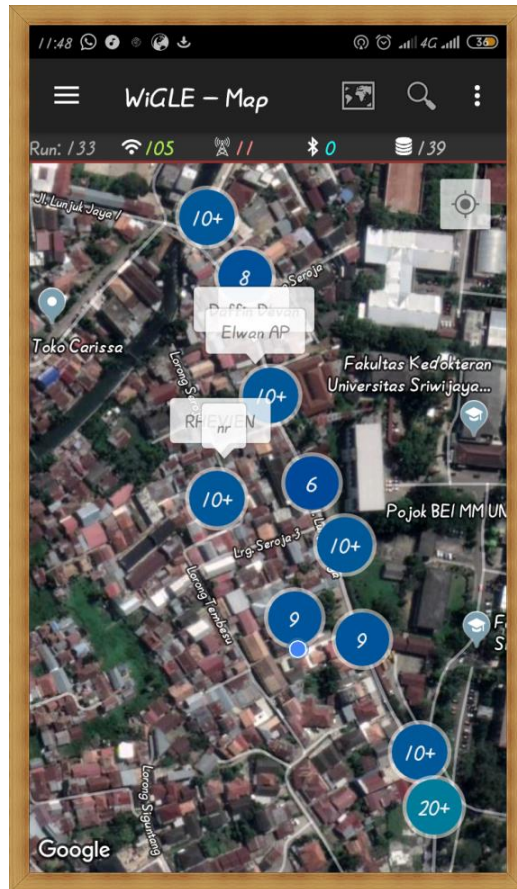
Global Position System (GPS) adalah sistem untuk menentukan letak di permukaan bumi dengan bantuan penyelarasan (synchronization) sinyal satelit. Sistem ini menggunakan 24 satelit yang mengirimkan sinyal gelombang mikro ke Bumi. Sinyal ini diterima oleh alat penerima di permukaan, dan digunakan untuk menentukan letak, kecepatan, arah, dan waktu. Sistem yang serupa dengan GPS antara lain GLONASS Rusia, Galileo Uni Eropa, IRNSS India.

3. Metode Penelitian

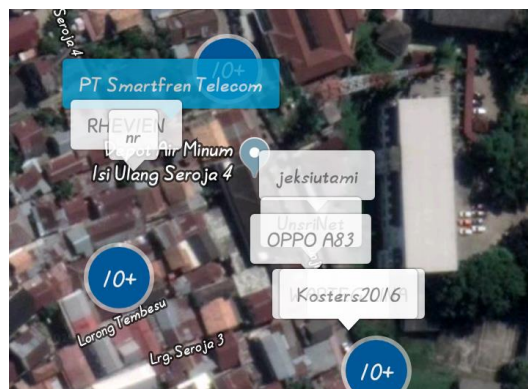
Pada penelitian ini penulis menggunakan Android sebagai device yang digunakan. Untuk melakukan scanning Wi-Fi, tools yang diinstal di android adalah Wigle. Scanning dilakukan dengan caramengaktifkan aplikasi Wigle dan melakukan perjalanan disepanjang jalan lunjuk jaya Palembang. Sehingga didapatlah hasil yang diinginkan.

4. Hasil dan Analisa Penelitian

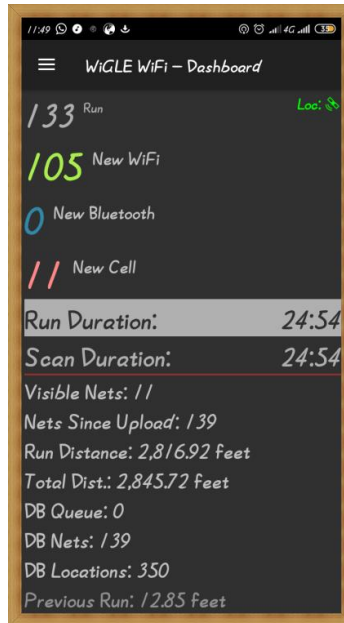
Berkut ini adalah seluruh Wi-Fi yang terdeteksi di sepanjang jalan lunjuk jaya, Palembang, setelah dilakukan proses scanning :



Ketika di zoom akan tampil nama Wi-Fi



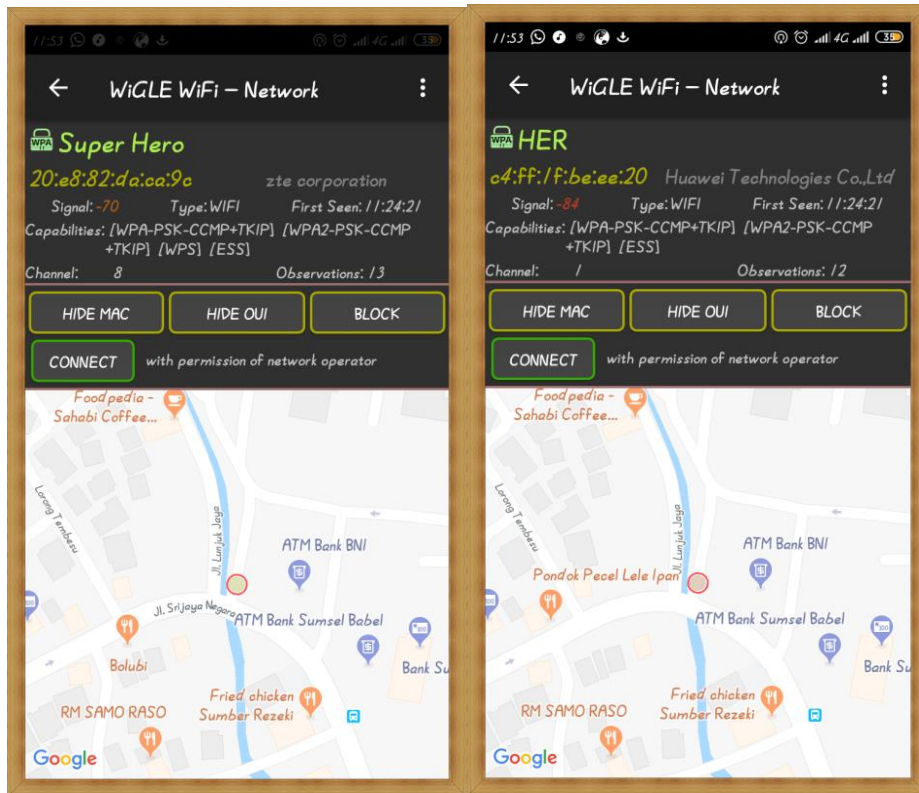
Pada dashboard akan muncul tampilan berupa jumlah WiFi yang baru. Pada percobaan kali ini terdapat 133 Wi-Fi yang sedang berjalan, 105 Wi-Fi baru yang terdeteksi, dan 11 *new call*, dengan durasi dan scan perjalanan berlangsung selama 24 menit 54 detik. Jumlah net yang tersedia yaitu 11, jumlah net 139, serta jarak yang ditempuh yaitu sejauh 2,8416.92 kaki.



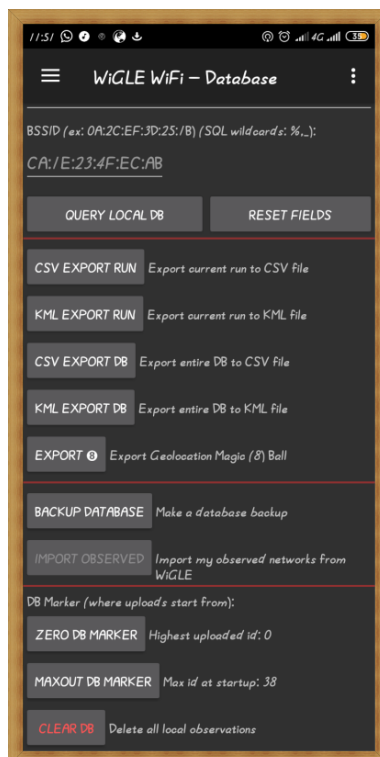
Halaman list seperti pada gambar menampi Wi-Fi yang sedang berjalan dan sedang tidak berjalan. Warna merah berarti Wi-Fi tersebut dilindungi oleh password dengan metode autentikasi (WPA / WiFi Protected Access, WPA2, WPS, atau ESS). Sedangkan yang berwarna hijau berarti menggunakan metode autentikasi radius. Jaringan yang paling aman adalah yang kunci dengan WPA/WPA2.



Berikut ini adalah tampilan informasi detail ketika salah satu Wi-Fi di klik. Berisi nama, sinyal, tipe jaringann, MAC, dan lain-lain seperti pada gambar.



Tampilan database berisi keseluruhan *scanning*.



5. Kesimpulan

Berdasarkan percobaan yang telah dilakukan maka didapatkan kesimpulan sebagai berikut ini :

1. Wifly sebagai Tools yang digunakan pada smartphone bisa menggantikan fungsi wifi searching yang ada pada smartphone tersebut, namun perbedaannya adalah pada saat penggunaannya, wi-fi searching pada smartphone digunakan untuk menghubungkan smartphone ke Access Point (AP) yang ada disekitar smartphone tersebut , sementara Wifly difungsikan untuk mengetahui ada atau tidaknya Access Point (AP) di sekitar smartphone tersebut.
2. Pengamanan dapat dilakukan dengan menggunakan teknologi password terbaru dengan enkripsi WPA2 agar password sulit dibobol, menggunakan password yang kuat dengan penggabungan alfabet, numerik, huruf kapital dan huruf kecil, mematikan fitur WPS pada wireless router karena WPS berfungsi sebagai alternatif untuk mengakses WiFi tanpa menggunakan password, serta mengaktifkan fitur macaddress filter untuk menentukan daftar perangkat yang dapat mengakses WiFi.
3. Pengamanan sangat penting pada proses autentikasi pengguna yang dapat mengakses jaringan WiFi untuk menghindari pembajakan.

Daftar Pustaka

- [1] (Meytri, 2018) Meytri, D. I. (2018). Laporan Wardriving Menggunakan Aplikasi Wigle Wifi Service.
- [2] Rachmat, F. A. (n.d.). War Driving Menggunakan Tools “ Wigle ” dan Mapping Menggunakan “ GoogleEarth ” Dikawasan PemKab OI (Ogan Ilir),
I(912100101032), 1–6.