

WARDRIVING SINYAL WIFI DI RSUD KABUPATEN OI

Agung Fitrianda

Email : agung.fitrianda@gmail.com

Abstrak

Pada dasarnya, proses wardriving ini merupakan kegiatan untuk mencari sumber hotspot dari access point sebanyak mungkin untuk mendapatkan informasi dari kumpulan access point yang berada disekitar gedung target, pada percobaan kali ini, gedung target yang telah ditentukan adalah gedung RSUD KABUPATEN OI, dimana di lokasi daerah tersebut terdapat banyak gedung – gedung lain yang berpotensi memiliki jaringan wi-fi, maka proses wardriving dimulai dari mengelilingi lokasi gedung target dengan menggunakan sepeda motor dan disaat bersamaan aplikasi wardriving pada smartphone melakukan scanning secara real time untuk mendapatkan kumpulan jaringan wi-fi yang terdapat di sekitar lokasi gedung target sehingga dalam beberapa saat akan didapatkan kumpulan dari wireless network pada gedung target beserta informasi dan lokasi dari access point yang telah terdeteksi oleh aplikasi pada smartphone android yang kita miliki, pada proses wardriving ini tools yang digunakan adalah aplikasi WiGle wifi pada smartphone android yang bisa diinstal melalui google play. Setelah melakukan scanning maka database hasil proses scanning wi-fi dapat disimpan dalam bentuk file yang memiliki format .kml, file ini selanjutnya digunakan untuk diekspor ke aplikasi Google Earth yang sudah terinstall pada computer, setelah file .kml diekspor ke aplikasi Google Earth, maka Google Earth akan memetakan lokasi access point yang telah terdeteksi oleh aplikasi WiGle wifi dan kita bisa melihat identitas dari masing – masing access point disekitar gedung target tersebut.

Keyword : wardriving, WiGle wifi, WPA-PSK, Google Earth, GPS

1. Pendahuluan

Dalam sebuah gedung, sering kali kita menjumpai banyak koneksi wireless network yang berada dalam gedung tersebut ketika kita mengaktifkan fasilitas wifi pada smartphone, baik hotspot yang berasal dari operator selular, wireless network yang berasal dari wireless router yang dipasang oleh sebuah toko dalam gedung tersebut, maupun wireless network yang berasal dari smartphone pribadi (wifi tethering) ataupun wireless modem, patut diketahui bahwa jaringan itu sendiri memiliki standar yang sudah ditetapkan dalam sebuah organisasi yang kita kenal dengan IEEE yaitu jenis IEEE 802.11. Dalam segi keamanan jaringan, wireless network memiliki range (jangkauan) internet yang cukup luas sampai cukup bagi pihak luar (orang asing) dapat terhubung ke internet selagi berada pada daerah jangkauan hotspot wireless network tersebut. dalam hal ini, disinilah proses wardriving dapat dilakukan, yaitu usaha untuk mendapatkan kumpulan dari wireless network yang terdapat dalam gedung tersebut dan masuk kedalam network dari salah satu access point tersebut untuk mendapatkan informasi dari salah satu access point yang bisa kita masuki seperti BSSID, frekuensi sinyal dan lain - lain, bahkan kita bisa memetakan lokasi sekitar gedung tersebut yang dimana lokasi access point berada dengan bantuan wardriving tools yang bisa kita install pada desktop maupun smartphone yang kita miliki, dan google earth yang bisa diinstall lewat desktop. Cukup dengan berjalan – jalan atau berkendara mengelilingi lokasi gedung target dan free wi-fi bisa kita dapatkan.

2. Tujuan Pustaka

2.1 Wardriving

Wardriving adalah tindakan mencari jaringan nirkabel Wi-Fi dengan seseorang dalam kendaraan yang bergerak, menggunakan komputer portabel, smartphone atau personal digital assistant (PDA). Seseorang berkeliling ke berbagai tempat dalam

usahanya mencari, mengeksplorasi, bahkan mungkin juga mengeksploitasi jaringan wireless yang ditemukannya. Kemudian orang yang melakukan kegiatan tersebut disebut sebagai "Wardriver", dalam upayanya itu dia melakukan pengumpulan data, membuat pemetaan area-area yang ada jaringan wirelessnya, dan menganalisa sistem securitynya. Kata Wardriving ini ada kaitannya bahwa sang wardriver menggunakan kendaraan bermotor untuk beraktivitas berkeliling ke berbagai tempat. Tujuannya berbagai macam mulai dari hanya sekedar ingin tahu, melakukan riset, hobi, menyadap untuk mendapatkan informasi rahasia, bahkan ada yang bertujuan untuk meyakinkan para pengguna dan pabrikan perangkat wireless untuk memperbaiki sistem keamanan mereka.

2.2 Wigle wifi

Wigle wifi adalah salah satu aplikasi yang tersedia untuk perangkat android pada smartphone yang digunakan untuk melakukan wardriving dengan perangkat mobile android. Tools ini sudah terhubung dengan GPS yang ada pada smartphone dan dengan file yang sudah kita save pada smartphone kita, kita dapat memetakannya pada map yang tersedia dengan mengekport file mapping wardriving yang ada pada smartphone. Aplikasi Wigle ini dapat mengeluarkan output dari hasil scanning kedalam bentuk csv ataupun Kml untuk menyimpan database yang digunakan oleh data terdapat pada aplikasi tersebut yang akan digunakan ketika kita ingin melakukan mapping hotspot wi-fi

2.3 WPA PSK

WPA-PSK (Wi-Fi Protected Access – Pre Shared Key) adalah pengamanan jaringan nirkabel dengan menggunakan metoda WPA-PSK jika tidak ada autentikasi server yang digunakan. Dengan demikian access point dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server. Cara mengkonfigurasikannya juga cukup sederhana. Perlu diketahui bahwa tidak semua access point akan mempunyai fasilitas yang sama dan tidak semua access point menggunakan cara yang sama dalam mendapatkan Shared-Key yang akan dibagikan ke client. Pada access point Dlink DWL-2000AP, pemberian Shared-Key dilakukan secara manual tanpa mengetahui algoritma apa yang digunakan. Keadaan ini berbanding terbalik dengan akses point Linksys WRT54G, dimana administrator dapat memilih dari dua algoritma WPA yang disediakan, yang terdiri dari algoritma TKIP atau algoritma AES. Setelah Shared-Key didapat, maka client yang akan bergabung dengan access point cukup memasukkan angka/kode yang diijinkan dan dikenal oleh access point. Prinsip kerja yang digunakan WPA-PSK sangat mirip dengan pengamanan jaringan nirkabel dengan menggunakan metoda Shared-Key.

2.4 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. Tersedia dalam tiga lisensi berbeda: Google Earth, sebuah versi gratis dengan kemampuan terbatas; Google Earth Plus, yang memiliki fitur tambahan; dan Google Earth Pro, yang digunakan untuk penggunaan komersial.

2.5 GPS

Global Positioning 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.

Sistem ini dikembangkan oleh Departemen Pertahanan Amerika Serikat, dengan nama lengkapnya adalah NAVSTAR GPS (kesalahan umum adalah bahwa NAVSTAR adalah sebuah singkatan, ini adalah salah, NAVSTAR adalah nama yang diberikan oleh John Walsh, seorang penentu kebijakan penting dalam program GPS). Kumpulan satelit ini diurus oleh 50th Space Wing Angkatan Udara Amerika Serikat. Biaya perawatan sistem ini sekitar US\$750 juta per tahun, termasuk penggantian satelit lama, serta riset dan pengembangan.

3. Metode Penelitian

Dalam Melakukan Penelitian tentang tindakan wardriving ini, peralatan – peralatan yang digunakan antara lain :

1. Laptop dengan sistem operasi windows 8.
2. Smartphone dengan sistem operasi Android.
3. Wardriving Tools : WiGLE Wifi
4. Mapping Wi-fi Tools : Google Earth

Pada percobaan kali ini, yang menjadi gedung target adalah gedung yang terdapat di RSUD KABUPATEN OI. Tindakan wardriving menggunakan kendaraan sepeda motor untuk berkeliling di sekitar lokasi gedung Rumah Sakit, dengan kecepatan lebih kurang 20KM/Jam, setelah itu mulai menghidupkan GPS pada smartphone android dan membuka aplikasi WiGLE wifi. Dalam perjalanan menuju lokasi gedung target, aplikasi pada smartphone telah mulai melakukan scanning wireless network dan setelah beberapa saat sudah terlihat kumpulan wireless network muncul pada layar smartphone, kemudian setelah mendapatkan kumpulan wireless network yang diinginkan, maka database diekspor dalam bentuk file dengan format .kml dimana file ini akan diimport kedalam aplikasi mapping tools google earth yang sudah terinstall di desktop sebelumnya untuk mendapatkan hasil mapping berupa lokasi wireless network yang ada pada gedung RSUD KABUPATEN OI dalam peta.

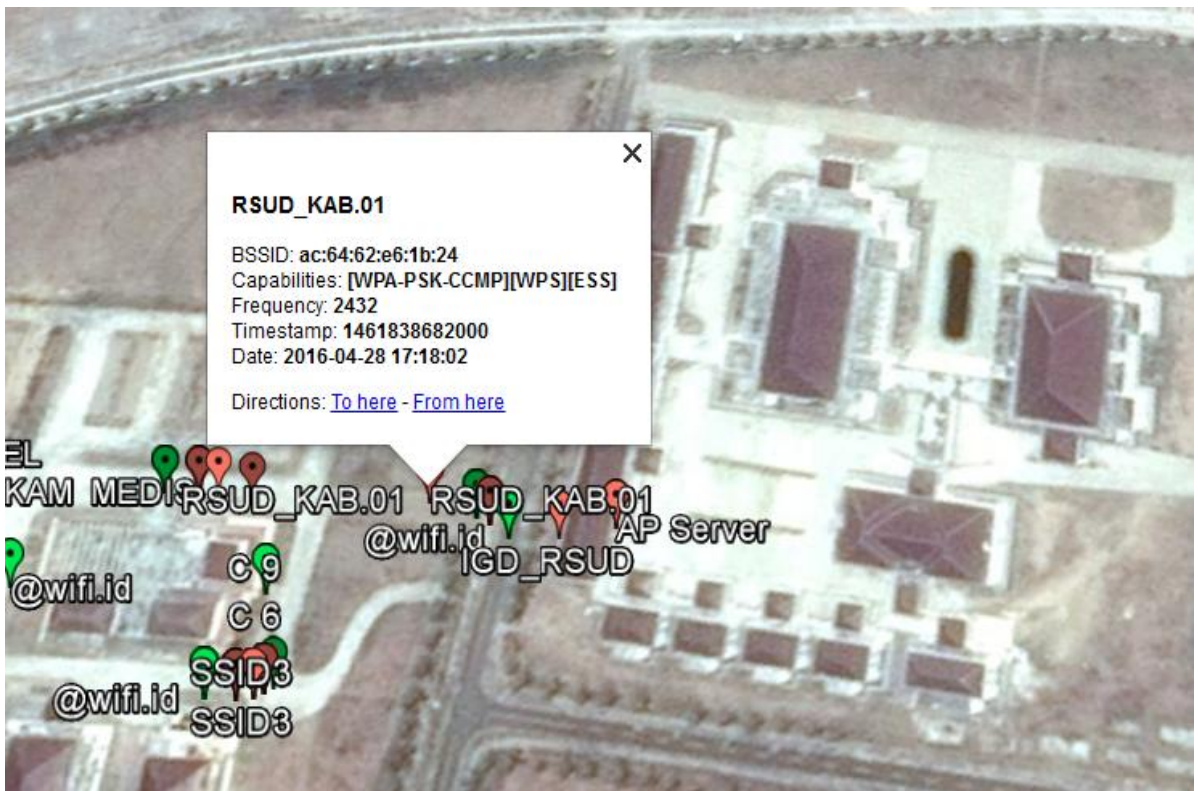
4. Hasil dan Analisa

4.1. Hasil

Hasil dari proses mapping wireless network dengan menggunakan aplikasi google earth adalah sebagai berikut :



Gambar 1



Gambar 2

4.2 Analisa:

1. Gambar 1

Pada gambar 1 dapat kita ketahui bahwa lokasi sekitar RSUD KABUPATEN OI terdapat beberapa access point yang merupakan milik dari salah satu vendor yang terkenal di Indonesia, yaitu wifi.id yang merupakan wireless network berbayar milik perusahaan telekomunikasi selular (TELKOMSEL). Wireless network ini sengaja tanpa protect karena ketika kita terhubung ke wireless network wifi.id, maka kita akan dialihkan ke interface dari wifi.id yang merupakan salah satu dari sistem keamanan dari vendor tersebut. Kemudian kita dapat menemukan wireless network flashzone seamless yang juga merupakan wireless network milik perusahaan TELKOMSEL. Lalu kita dapat menjumpai access point dari server yang terkoneksi dengan database yang dimiliki oleh rumah sakit tersebut (AP server).

2. Gambar 2

Pada gambar 2, sebelumnya kita telah menentukan wi-fi yang akan dijadikan sampel untuk mendapatkan informasi tentang access point dari wireless network tersebut, pada gambar didapatkan informasi bahwa wireless network RSUD_KAB1 memiliki BSSID yaitu ac:64:62:e6:1b:24, frekuensi sinyal yang dimiliki adalah 2432, kapabilitas yang dimiliki network tersebut adalah [WPA-PSK-CCMP][WPS][ESS] dimana CCMP singkatan Kontra mode CBC-MAC Protocol. CCMP, juga dikenal sebagai AES CCMP, adalah mekanisme enkripsi yang telah menggantikan TKIP, dan itu adalah standar keamanan yang digunakan dengan jaringan nirkabel WPA2. Menurut spesifikasi, jaringan WPA2 harus menggunakan CCMP secara default (WPA2-CCMP), meskipun CCMP juga dapat digunakan pada jaringan WPA untuk meningkatkan keamanan (WPA-CCMP).

5. Kesimpulan

Dari Percobaan ini dapat ditarik kesimpulan sebagai berikut :

1. Dengan proses mapping access point, kita bisa mengetahui lokasi access point dengan cepat dan tepat.
2. Semakin luas daerah yang menjadi target untuk proses wardriving, maka semakin banyak potensial ditemukan access point yang menjadi sumber wi-fi.
3. Kekuatan sinyal dari suatu access point bergantung pada jarak (range), semakin jauh area cakupan lokasi akses dari suatu access point, maka semakin lemah sinyal yang diterima oleh pengguna access point tersebut dan sebaliknya.
4. Access point yang memiliki proteksi pada jaringannya, misalnya access point yang dilindungi oleh password SSID(WPA2 – PSK atau WPA PSK) masih rentan (vulnerable) dari ancaman dari pihak asing (attacker) dari ancaman attacker, apalagi access point yang tidak memiliki sistem proteksi pada jaringannya sama sekali.

DAFTAR PUSTAKA

1. <http://kodokngorekid.blogspot.co.id/2012/01/apakah-yang-dimaksud-dengan-wardriving.html>
2. https://id.wikipedia.org/wiki/Google_Earth
3. <https://sontang95.wordpress.com/2012/11/28/pengertian-wep-wpa-wpa-psk-dan-perbedaannya/>
4. https://id.wikipedia.org/wiki/Sistem_Pemosisi_Global
5. <https://www.acrylicwifi.com/en/blog/about-wpa-psk-tkip-ccmp-wi-fi-security-information/>