

# PEMETAAN WIRELESS ACCESS POINT USING GPS SMARTPHONE ANDROID MENGGUNAKAN METODE WARDRIVING

Dikka Pratama<sup>1</sup>, Merry Agustina, MM, M.Kom<sup>2</sup>, Hadi Syaputra, S.Kom<sup>3</sup>

<sup>1</sup>Mahasiswa Teknik Informatika, <sup>2,3</sup> Dosen Fakultas Ilmu Komputer Universitas Bina Darma  
Jl.A.Yani No.12 Plaju, Palembang 30624

Email: [pratama\\_dikka@yahoo.co.id](mailto:pratama_dikka@yahoo.co.id)<sup>1</sup>, [merry\\_agustina@mail.binadarma.ac.id](mailto:merry_agustina@mail.binadarma.ac.id)<sup>2</sup>,  
[hadi\\_syaputra@mail.binadarma.ac.id](mailto:hadi_syaputra@mail.binadarma.ac.id)<sup>3</sup>

**Abstrak.** Perkembangan jaringan *teknologi nirkabel* saat ini berkembang dengan pesat dan hampir dapat ditemui disetiap tempat seperti kafe, perguruan tinggi, perkantoran, supermarket, ataupun perumahan daerah. Pengguna dengan mudah membuat koneksi ke *jaringan internet* dengan *jaringan nirkabel* tanpa bantuan kabel karena data akan disiarkan melalui *frekuensi* radio. Perkembangan jaringan computer ditempat umum terkadang memberikan layanan khusus, terutama *jaringan nirkabel gratis (free hotspot)*. *Jaringan nirkabel (wireless)* yang bersifat broadcast membuat komunikasi data yang terjadi cenderung tidak aman dan memang pengguna menyampingkan *issue security* pada *IEEE 802.11* sehingga banyak *intruders* yang memfokuskan serangannya pada *protocol* satu ini. Sebut saja *wardriving* atau *cracking WPA/WEP/WPA2*, *MitM (Man in the Middle Attack)* bahkan membuat *dumppy access point* yang digabung dengan *client-side exploit* dan *MitM pada protocol https*.

**Kata kunci :** *wireless, wardriving security, hacking, Palembang*

**Abstract.** The development of wireless network technology is currently growing rapidly and can be found almost every place such as cafes, colleges, offices, supermarkets, or even residential areas. Users can easily create a connection to the internet network with a wireless network without wires because the data will be broadcast via radio frequency. The development of computer network in public places sometimes provide special services, especially the free wireless network (free hotspot). Wireless network (LAN) that is broadcast makes data communications than occur tend to be insecure and indeed users generally exclude the issue of security on the IEEE 802.11 so many intruders are focusing their attacks on one's protocol. Call in wardriving or cracking WPA/WEP/WPA2 MitM (Man in the Middle Attack) even made a dumppy access point combined with client-side exploits and MitM the https protocol.

**Password:** wireless, wardriving security, security, hacking, Palembang.

## 1. PENDAHULUAN

### 1.1 Latar Belakang

Pemanfaatan jaringan nirkabel wireless yang bersifat broadcast membuat komunikasi data cenderung tidak aman, dan memang masih banyak pengguna yang menyampingkan issue security IEEE 802.11, sehingga banyak intruders yang memfokuskan serangan protokol satu ini. Sebut saja wardriving atau cracking WPA/WEP/WPA2.

Dari permasalahan pada jaringan wireless dan padatnya channel wireless di kota besar sehingga mendorong peneliti untuk melakukan pemetaan lokasi access point di wilayah kota Palembang dan menjelaskan metode atau cara yang akan digunakan intruders baik yang bersifat public atau pun bersifat pribadi.

### 1.2 Tujuan

Adapun tujuan yang ingin dicapai adalah untuk memetakan wireless access point yang terdapat di kota Palembang sehingga dapat diketahui wireless access point apa saja yang ada di kota Palembang

### 1.3 Batasan Masalah

Batasan masalah dalam penelitian ini, adalah Pemetaan Wireless Access Point Using Gps Smartphone Android Dengan Menggunakan Metode Wardriving di daerah-daerah Kota Palembang

## 2. Tinjauan Pustaka

### 2.1 Wireless Dan Sejarahnya

*Wireless* adalah *transfer* informasi antara dua atau lebih titik yang tidak terhubung secara fisik. Jarak bisa pendek, seperti beberapa meter untuk *remote control* televisi, atau sejauh ribuan atau bahkan jutaan kilometer untuk ruang-dalam *komunikasi radio*.

*Wireless* pertama pada tahun 1970-an, didahului oleh IBM dengan rancangan teknologi RI, dan perusahaan HP, dengan ISM band yaitu 902-908 Mhz, 2400+2483 dan 5725-5850 Mhz, pada tahun 1990 teknik *spektrum* tersebar (SS) pada pita ISM, terlisensi *frekuensi* 18-19 Ghz, pada tahun 1997 *IEEE* membuat *standar WLAN* dengan kode 802.11 dapat bekerja pada *frekuensi* 2.4 Ghz kecepatan 2 Mbps, pada juli 1999 *IEEE* kembali mengeluarkan kode 802.11b dengan kecepatan 11 Mbps dan pada waktu hampir bersamaan *IEEE* juga mengeluarkan 802.11a menggunakan *frekuensi* 5 Ghz, dan kecepatan data hingga 54Mbps. Tahun 2002 *IEEE* menggabungkan kelebihan 802.11b dan 802.11a yakni 802.11g bekerja pada *frekuensi* 2.4 Ghz hingga 54Mbps. Yang terakhir tahun 2006 *IEEE* mengeluarkan teknologi 802.11n dikembangkan dengan menggabungkan 802.11b dan 802.11g sehingga menghasilkan peningkatan *throughput* dengan kecepatan 108Mbps (James, 2009).

## 2.2 Wardriving

*Wardriving* merupakan aktifitas bergerak di sekitar area tertentu, melakukan pemetaan *access point* untuk tujuan *statistik*. Kemudian *statistik* ini digunakan untuk meningkatkan kesadaran akan masalah keamanan yang terkait dengan *wireless* (Joshua, 2007).

## 2.3 Pemetaan

Pemetaan adalah pengelompokan suatu kumpulan wilayah yang berkaitan dengan beberapa letak *geografis* wilayah yang meliputi dataran tinggi, pegunungan, sumber daya dan potensi penduduk yang berpengaruh terhadap sosial kultural yang memiliki ciri khas khusus dalam penggunaan skala yang tepat. (Soekidjo, 1994). Pengertian lain tentang pemetaan yaitu sebuah tahapan yang harus dilakukan dalam pembuatan peta. Langkah awal yang dilakukan dalam pembuatan data, dilanjutkan dengan pengolahan data, dan penyajian dalam bentuk peta (Juhadi dan Liesnoor, 2001).

Jadi, dari dua *definisi* diatas dan disesuaikan dengan penelitian ini maka pemetaan merupakan proses pengumpulan data untuk dijadikan sebagai langkah awal dalam pembuatan peta, dengan menggambarkan penyebaran kondisi alamiah tertentu secara meruang, memindahkan keadaan sesungguhnya kedalam peta dasar, yang dinyatakan dengan penggunaan skala peta.

## 3. Metodologi Penelitian

### 3.1 Variable Penelitian

Metode penelitian yang digunakan adalah metode penelitian tindakan (*action research*), adapun tahapan-tahapan nya sebagai berikut (Madya, 2006:9):

1. Variable Bebas (independen)
2. Variable terikat (dependen)
3. Variable Kontrol

### 3.2 Metode Pengumpulan data

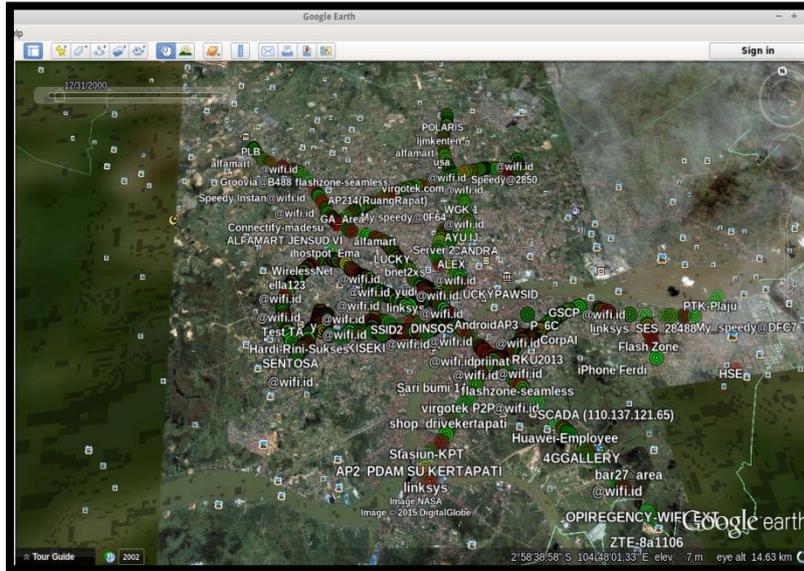
Adapun teknik yang digunakan dalam pengumpulan data:

1. Observasi  
metode ini mengumpulkan data dengan cara terjun langsung ke area-area yang terdapat wireless
2. Metode Studi Keputusan  
yaitu dengan cara mengumpulkan data-data yang dilakukan dengan membaca, mempelajari buku-buku dan jurnal-jurnal yang berkaitan dengan permasalahan yang akan menunjang materi yang akan diteliti

## 4. Hasil dan Pembahasan

### 4.1 Hasil

Hasil dari Pemetaan wireless access point using gps smartphone android menggunakan metode Wardriving



Gambar 1 Pemetaan wireless access point

Gambar 1 diatas adalah hasil dari Pemetaan wireless access point using gps smartphone android menggunakan metode Wardriving di Kota Palembang, dapat dilihat bahwa terdapat banyak access point yang digunakan diberbagai daerah di kota Palembang

### 4.2 Pembahasan

#### 4.2.1 Persiapan wardriving

- Tentunya harus memiliki *smartphone android* yang terdapat GPS
- *Install BlueNMEA* yang bisa *download di playstore* dan pastikan *smartphone android* terkoneksi dengan internet
- *Install Android Debug Bridge*  
*Sudo add-apt-repository ppa:nilarimogard/webupd8*  
*Sudo apt-get update*  
*Sudo apt-get install android-tools-adb android-tools-fastboot*
- *Install Kismet, Giskismet, Sqlite dan Google Earth*

#### 4.2.2 Start Wardriving

- Pertama-tama *connect android* ke laptop terlebih dahulu dan pastikan

- android sudah dalam kondisi *diroot*.
- Lalu buka *aplikasi BlueNMEA diandroid* kemudian jalankan di terminal laptop dan jalankan perintah berikut ini :  
*adb devices*  
*adb forward tcp:4352 tcp:4352*
  - Kemudian *koneksikan GPSnya* dengan menjalankan perintah berikut:  
*Gpsd -N -n -D 5 tcp://127.0.0.1:4352*  
Cek *BlueNMEA*, apabila "*Status Provider : OK*" Berarti *gps* nya sudah *terkoneksi*, apabila masih *waiting* berarti harap menunggu sebentar.
  - *Aktifkan mode interface mon0* dengan menjalankan perintah berikut :  
*Airmon-ng start wlan0*
  - Jalankan *kismet* dan *kismet\_client*
  - Jika diminta untuk memasukan *interface*, masukan "*mon0*"
  - Jalankan perintah berikut  
*Kismet*
  - Kemudian bukar terminal baru kemudian jalankan perintah berikut:  
*Kismet\_client*
  - Hasilnya Akan seperti gambar dibawah ini apabila *GPS* nya sudah *terkoneksi*.
  - Jika sudah, baru lah berjalan-jalan mengelilingi daerah mana saja yang terdapat *wifi* untuk dipetakan, kalo sudah mengelilingi daerah yang terdapat *wireless* tutup semua *kismet* apabila sudah mengelilingi daerah yang terdapat *wireless*
  - *Filter hasil scanning* tersebut dengan menggunakan *giskismet*.  
*giskismet -x nama\_log\_kismet.netxml*  
*giskismet -q "SELECT \* FROM WIRELESS" -o wardrive.kml*
  - Apabila sudah selesai buka file *wardrive.kml* dengan *google earth*.

## 5 Kesimpulan

Kesimpulan dari penelitian *Wireless Access Point Using Gps SmarthPhone Android* Dengan Menggunakan *Metode Wardriving*

1. Wilayah kota Palembang yang memiliki jaringan wireless yang paling padat yakni wilayah kampus, Perkantoran, Rumah Sakit, Supermarket, minimarket.
2. Untuk Enkripsi Jaringan Wireless di Kota Palembang cukup baik karena Masyarakat umum sudah menyadari tingkat keamanan jaringan wireless sangatlah penting.
3. Interferensi Channel pada wilayah Kota Palembang bisa dikatakan cukup tinggi karena 49,5% masih terjadi interferensi ini menunjukkan bahwa user belum mengetahui channel yang tepat agar terhindar dari interferensi sehingga performance wireless akan menjadi lebih baik.
4. Untuk mengurangi resiko keamanan jaringan wireless user bisa mensetting access point, mengganti password default, dan mengganti enkripsi yang lebih baik yakni wpa/wpa2

## References

1. Chandra. 2008 Penelitian tindakan (*action research*)  
<https://chandrax.wordpress.com/2008/07/05/action-research-penelitian-tindakan/>
2. Ismayudi. 2014 “ Analisis Keamanan jaringan WIFI SMPN 1 Sembawa”  
<http://eprints.binadarma.ac.id/164/> diakses pada tanggal 20  
january 2014
3. Juhadi dan Liesnoor, 2001. Pengertian Pemetaan  
PengetahuanPintar.blogspot.com.Sejarah Wireless  
<http://pengetahuanpintars.blogspot.com/2011/12/sejarah-wireless-dan-pengertiannya.html>
4. Reza Jalaluddin Al-Haroh. 2012 “Wardriving dan Penetrasi wifi lanjut di wilayah kota Yogyakarta”  
[http://repository.amikom.ac.id/files/publikasi\\_08.11.2153.pdf](http://repository.amikom.ac.id/files/publikasi_08.11.2153.pdf)
5. Tedi Wahyono. 2012 “Analisis Pemetaan Jaringan *HotsPot* Di Perpustakaan Daerah (PUSDA) Provinsi Sumatera Selatan”  
<http://eprints.binadarma.ac.id/424/>
6. (Soekidjo,1994). Pengertian Pemetaan
7. Wright Joshua 2007. Wardriving dan Penetration Testing.