**WARDRIVING DENGAN METODE SIGNAL SCANNING WIGLE DAN MAPPING MENGGUNAKAN GOOGLE EARTH**



Di susun :

Nama : Muhammad Riandi Kurniawan

Nim : 09030581822014

Kelas : TK3B

Dosen : Deris Stiawan, M.T.,PH.D.

**PROGRAM STUDI TEKNIK KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**PALEMBANG**

**2019/2020**

# KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa hingga saat ini masih memberikan kita nikmat iman dan kesehatan, sehingga penulis diberi kesempatan yang luar biasa ini yaitu kesempatan untuk menyelesaikan makalah ini dengan tepat waktu.

Makalah ini berisikan tentang informasi konsep analisa titik hotspot di sebagian daerah plaju dan opi. Dalam prinsip melihat keamanan jaringan menggunkan aplikasi WIGLE dengan Google Earth untuk mapping jaringan wifi, diharapkan makalah ini dapat memberikan pengetahuan kepada kita semua tentang pemahaman keamanan jaringan komputer terutama Wifi.

Selain itu penulis juga sadar bahwa pada makalah ini dapat ditemukan banyak sekali kekurangan serta jauh dari kesempurnaan oleh karena itu kritik dan saran dari semua pihak yang bersifat membangun selalu Penulis harapkan demi kesempurnaan makalah ini.

akhir kata, dalam rangka perbaikan selanjutnya, penulis akan terbuka terhadap saran dan masukan dari semua pihak karena penulis menyadari makalah yang telah disusun ini memiliki banyak sekali kekurangan.

Palembang 9 Desember 2019

# DAFTAR ISI

[**KATA PENGANTAR** II](#_Toc26867590)

[**DAFTAR ISI** III](#_Toc26867591)

[**BAB I** 1](#_Toc26867592)

[**PENDAHULUAN** 1](#_Toc26867593)

[1.1 Latar Belakang 1](#_Toc26867594)

[1.2 Rumusan Masalah 1](#_Toc26867595)

[**BAB II** 2](#_Toc26867596)

[**PEMBAHASAN** 2](#_Toc26867597)

[2. Landasan Teori 2](#_Toc26867598)

[2.1 Definisi Wardriving 2](#_Toc26867599)

[2.2 Sejarah Wardriving 2](#_Toc26867600)

[2.3 Wireless dan Sejarahnya 2](#_Toc26867601)

[2.4 Standar Jaringan Wireless 3](#_Toc26867602)

[2.5 Mekanisme Keamanan Wireless 4](#_Toc26867603)

[3. Metodologi Penelitian 5](#_Toc26867604)

[3.1 Penelitian Wardriving 5](#_Toc26867605)

[3.2 Persiapan dalam Wardriving 5](#_Toc26867606)

[3.3 Peralatan yang dibutuhkan 5](#_Toc26867607)

[3.4 Langkah-Langkah Wardriving 5](#_Toc26867608)

[3.5 Pemetaan dalam Wardriving 5](#_Toc26867609)

[4. Hasil dan Pembahasan 7](#_Toc26867610)

[4.1 Analisa Pemetaan pada Wardriving 7](#_Toc26867611)

[4.2 Analisa Channel Wireless 17](#_Toc26867612)

[**BAB III** 18](#_Toc26867613)

[**PENUTUP** 18](#_Toc26867614)

[Kesimpulan : 18](#_Toc26867615)

# BAB I

# PENDAHULUAN

Dalam komplek perumahan maupun di sekitar jalan, 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 wirelss network yang berasal dari smarthpone 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 maupun sekitar jalan tersebut dan masuk kedalam network dari salah satu access point tersebut untuk mendapatkan informasi dari salah satu access, frekuensi sinyal dan lain – lain.

### Latar Belakang

Wi-Fi , Wireless Ethernet dan Wireless LAN merupakan hal yang sangat diperlukan pada saat sekarang ini , sebab , kebutuhan setiap orang akan internet dewasa ini sangat tinggi . oleh karna itu , sekarang banyak sekali kita lihat Access Point (AP) yang dipasang di setiap sudut ruangan ataupun ditengah tengah ruangan 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)

### Rumusan Masalah

1. Bagaimana Pemetaan Acces Point Hotspot /Wifi saat Wardriving?
2. Apa meteologi yang digunakan ketika Wardriving?
3. Apa mekanisme Keamanan yang masih sering dipakai dalam Hostspot / Wifi ?

# BAB II

# PEMBAHASAN

## Landasan Teori

### Definisi 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).

### Sejarah Wardriving

Istilah wardriving berasal dari Wardialing, sebuah istilah yang pertama kali diperkenalkan ke public oleh Matthew Broderick, David Lightman di film wargames(1983). wardialing merupakan praktek menggunakan modem telephone yang terpasang ke computer untuk melakukan dial ke seluruh nomor secara berurutan (misal 555-111, 555112 dan seterusnya) untuk mencari komputer yang terhubung dengan modem yang menyertainya. Pada dasarnya wardriving menggunakan konsep yang sama, meskipun teknologi terus berkembang seperti saat ini. Seorang wardiving sering melakukan pemetaan route yang akan di lewati terlebih dahulu, untuk menemukan access point wireless di daerah tersebut. Setelah access points wireless ditemukan seorang wardriver menggunakan software dan website untuk memetakan hasilnya. Berdasarkan hasil tersebut, dilakukan analisis statistik. Statistik analis dapat dilakukan seper-area , seperdaerah ataupun keseluruhan dari wireless tersebut (Joshua, 2007).

### 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 rancaranga teknologi RI, dan perusahaan HP, dengan ISM band yaitu 902-908 Mhz, 2400+2483 dan 5725-5850 Mhz, pada tahun 1990 dipasarkan dengan 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 terkhir tahun 2006 IEEE mengeluarkan teknologi 802.11n dikembangkan dengan menggabungkan 802.11b dan 802.11g sehingga menghasilakan peningkatan throughput dengan kecepatan 108Mbps (James, 2009).

### Standar Jaringan Wireless

-802.1

1a Selesai dirilis Oktober 1999. Standar wireless network dengan maksimum data transfer rate 54 Mbps dan bekerja pada frekuensi 5 GHz. Metode transmisi yang digunakan adalah Orthogonal Frequency Division Multiplexing (OFDM), yang mengizinkan pentransmisian data secara paralel di dalam sub-frekuensi (resisten terhadap interferensi dengan gelombang lain). Range maksimal untuk indoor hanya sekitar 15 meter/ ± 50 ft. Sedangkan outdoor ± 100 ft/30 meter. Standar 802.11a tidak kompatibel dengan 802.11 b,g

-802.11b Muncul di pasaran pada tahun 2000. Standar wireless network dengan maksimum data transfer rate 5.5 Mbps dan 11 Mbps bekerja pada frekuensi 2,4 GHz. Dikenal juga dengan IEEE 802.11 HR. Pada prakteknya, kecepatan maksimum yang dapat diraih mencapai 5.9 Mbps pada protokol TCP, dan 7.1 Mbps pada protokol UDP. Metode transmisi yang digunakannya adalah DSSS. memiliki range area yang lebih panjang (~150 feet/45 meters di dalam indoor dan ~300 feet/90 meter dalam outdoor)

-802.11g Dipublikasikan pada bulan Juni 2003 mampu mencapai kecepatan hingga 54 Mbps pada pita frekuensi 2,4 GHz, sama seperti halnya IEEE 802.11 biasa dan IEEE 802.11b. Standar wireless network yang hampir sama dengan 802.11b tetapi metode transmisi yang digunakan adalah OFDM (sama dengan 802.11a). Range area ~150 feet/45 meter untuk indoor dan ~300 feet/90 meter untuk outdoor.

-802.11n Baru sajadirilis 11 September 2009. Secara teoritis, dapat mencapai kecepatan 600 Mbps. Namun, setelah Wi-Fi Alliance menguji, hanya mencapai kecepatan maksimum 450 Mbps. Bekerja pada frekuensi 2,4 GHz dan 5 GHz. Sama seperti teknologi MIMO (multiple-input multiple-output), 802.11n bekerja dengan cara mengutilisasi banyak komponen pemancar dan penerima sinyal sehingga transmisi data dapat dilakukan paralel untuk meningkatkan nilai throughput (50-144 Mbps). Range maksimal untuk indoor 70 metersedangkanoutdoor bisa mencapai 250 meter. Wi-Fi 802.11n ini akan diaplikasikan di device router dan adapter (James, 2009).

### Mekanisme Keamanan Wireless

1. WEP WEP merupakan standart keamanan & enkripsi pertama yang digunakan pada wireless, WEP (Wired Equivalent Privacy) adalah suatu metoda pengamanan jaringan nirkabel, disebut juga dengan Shared Key Authentication. Shared Key Authentication adalah metoda otentikasi yang membutuhkan penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk authentikasi menuju access point, dan WEP mempunyai standar 802.11b.

2. WPA Menyikapi kelemahan yang dimiliki oleh WEP, telah dikembangkan sebuah teknik pengamanan baru yang disebut sebagai WPA (WiFI Protected Access). Teknik WPA adalah model kompatibel dengan spesifikasi standar draf IEEE 802.11i. Teknik ini mempunyai beberapa tujuan dalam desainnya, yaitu kokoh, interoperasi, mampu digunakan untuk menggantikan WEP, dapat diimplementasikan pada pengguna rumahan atau corporate, dan tersedia untuk publik secepat mungkin. WPA mempunyai mekanisme enkripsi yang lebih kuat. Namun, ada yang pesimistis karena alur komunikasi yang digunakan tidak aman, di mana teknik man- in-the-middle bisa digunakan untuk mengakali proses pengiriman data. Agar tujuan WPA tercapai, setidaknya dua pengembangan sekuriti utama dilakukan. Teknik WPA dibentuk untuk menyediakan pengembangan enkripsi data yang menjadi titik lemah WEP, serta menyediakan user authentication yang tampaknya hilang pada pengembangan konsep WEP.

3. WPA2 WPA2 adalah sertifikasi produk yang tersedia melalui Wi-Fi Alliance. WPA2 Sertifikasi hanya menyatakan bahwa peralatan nirkabel yang kompatibel dengan standar IEEE 802.11i. WPA2 sertifikasi produk yang secara resmi menggantikan wired equivalent privacy (WEP) dan fitur keamanan lain yang asli standar IEEE 802.11. WPA2 tujuan dari

sertifikasi adalah untuk mendukung wajib tambahan fitur keamanan standar IEEE 802.11i yang tidak sudah termasuk untuk produk-produk yang mendukung WPA.

## **Metodologi Penelitian**

### Penelitian Wardriving

Dalam Penelitian ini terdapat bahan digunakan serta tujuannya :

* Bahan yang dibutuhkan : Software dan Hardware yang diperlukan untuk wardriving antara lain: Smartphone dan WIGLE serta GoogleEarth.
* Pencarian Terikat : Enkripsi Channel Wireless, Default SSID Access Point, Merk AccessPoint, Capabilities Keamanan.
* Wilayah penelitian : Daerah Plaju,Tegal Binangun, Komplek opi.

### Persiapan dalam Wardriving

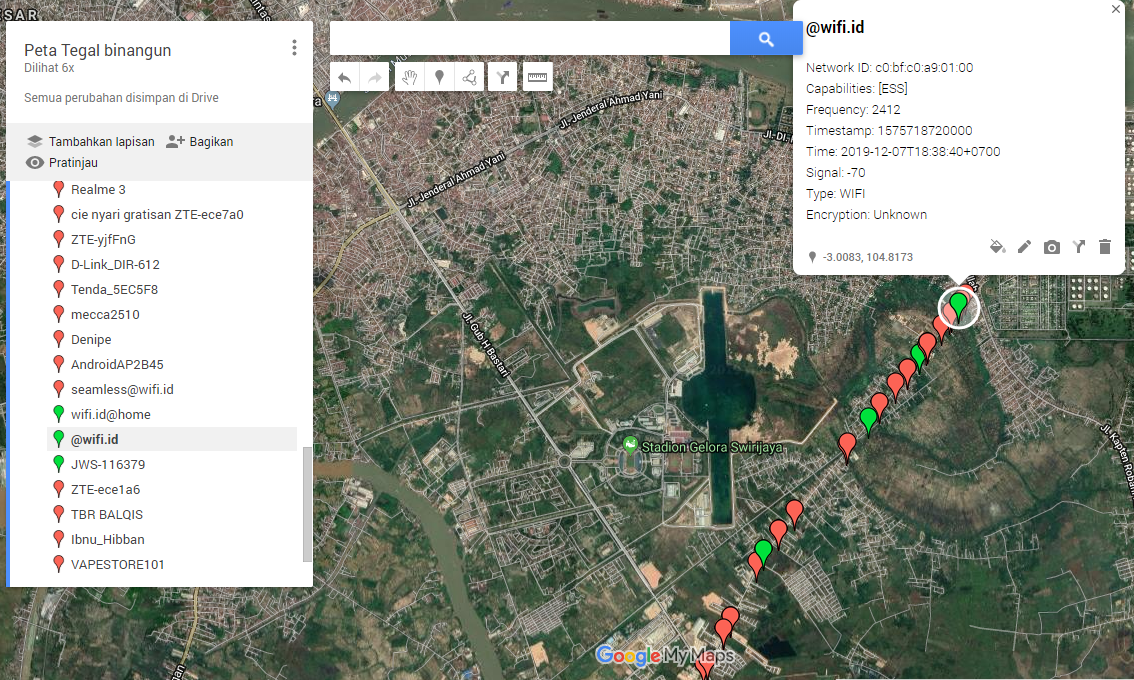
Dalam penelitian wardriving ini yang menjadi area dari penelitian yakni Kota Sumatra-Selatan, Batas-batas wilayah : Daerah Plaju,Tegal Binangun, Komplek opi.

### Peralatan yang dibutuhkan

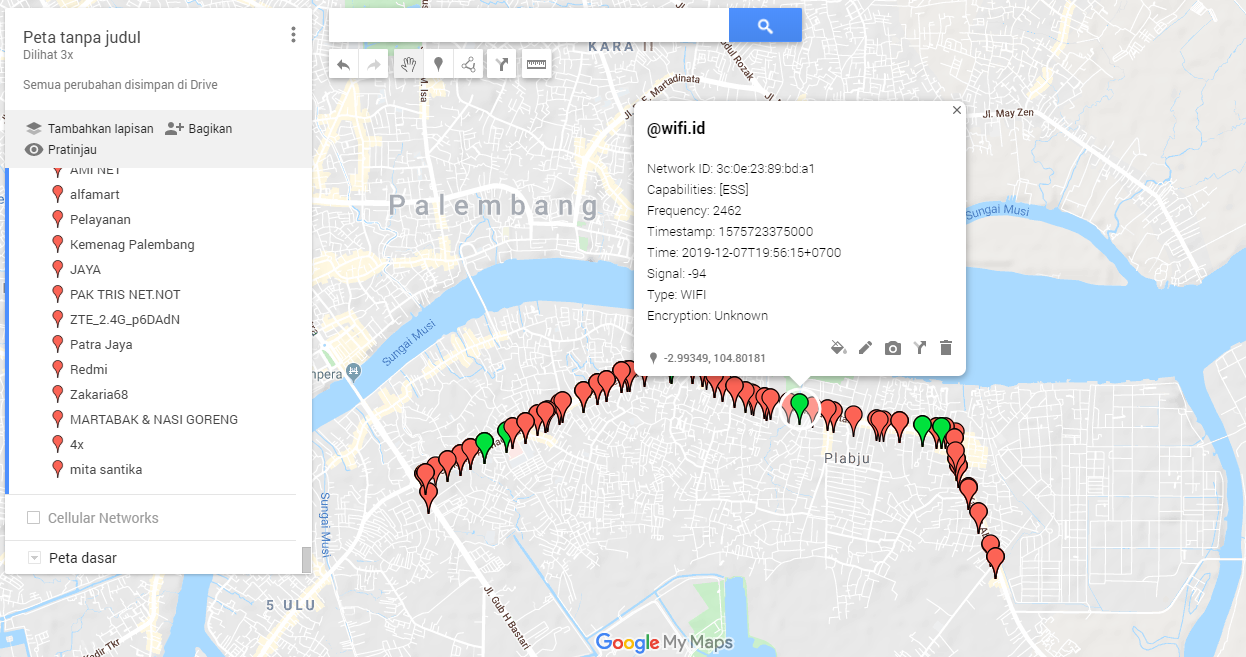
* Wardriving menggunakan Motor .
* Hardware : Smartphone Asus Max Pro M1
* Software : WIGLE Wifi dan GoogleEarth
  1. Langkah-Langkah Wardriving
* Buka smartphone Cari Aplikasi Wigle-Wifi.
* Kemudian Buka Aplikasi Wigle-Wifi Untuk membuat device android Terbaca dengan GPS & Wifi.
* Atur data conection Wifi maupun data, set location untuk mengsinkronisasi ke google Earth pada aplikasi WIGLE-WIFI sebagai Wireless Device .
* Setelah itu Lakukan proses scanning dan Wardriving selama beberapa menit.
* Ketika titik hospot telah terkmpul banyak simpaan data tersebut berupa format KML selanjutnya upload data ke wigle menuju googleEarth.
* Setelah itu data bisa kita lihat berdasarkan hasil scanning pada my google earth tersebut.

### Pemetaan dalam Wardriving

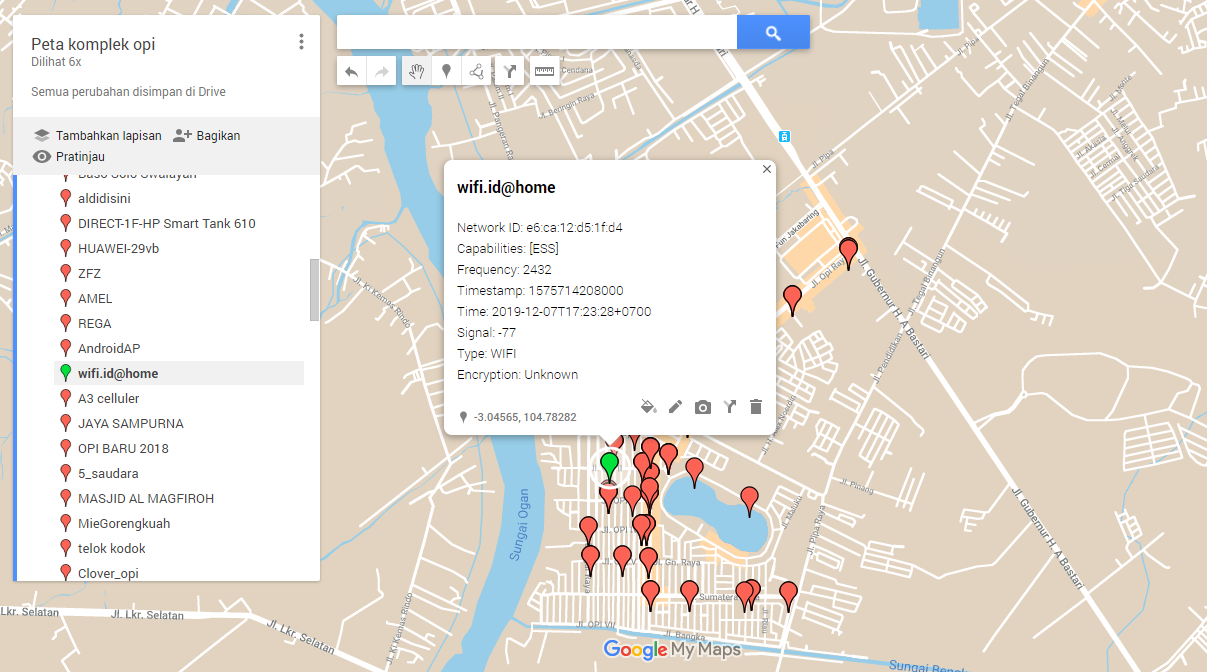
Untuk melakukan pemetaan dalam wardriving memanfaatkan fungsi maps dari google disebut Keyhole Markup Language. Setelah melakukan wardriving dilakukan export terhadap data ke format KML yang dapat dilihat pada google earth nantinya berikut merupakan contoh dari hasil KML pada google earth.



Gambar 3.1 Hasil Wardriving Wilayah Tegal binangun



Gambar 3.2 Hasil Wardriving Wilayah Plaju



Gambar 3.3 Hasil Wardriving Wilayah Komplek opi

## Hasil dan Pembahasan

### Analisa Pemetaan pada Wardriving

Lokasi pertama pada wilayah tegal binangun terdapat 26 titik hospot pada hasil scanning yeng telah didapat Setelah melakukan scanning di kawasan tegal binangun didapatlah file format .kml yang kami export dari Wigle,dan kami langsung membuka file tersebut dengan menggunakan GoogleEarth, hasil yang didapat dari GoogleEarth adalah mapping yang bisa dilihat pada Gambar 3.1 , 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 3.1 merupakan hasil yang kami dapat setelah berberapa kali mengitari kawansan Tegal Binangun. Pada gambar 3.1 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.

Berdasarkan Tabel

* Hasil scanning di kawasan Tegal Binangun

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NO | SSID | SIGNAL | CAPABILITIES | TYPE | ENCRYPTION |
| 1 | AndroidAP | -94 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 2 | TBR | -88 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 3 | VAPESTORE101 | -84 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 4 | ZTE\_2.4G\_Dh6TDa | -90 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 5 | Wifi.id@home | -55 | [ESS] | WIFI | Unknown |
| 6 | D-Link\_DIR-612 | -74 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS | WIFI | WPA2 |
| 7 | Ibnu\_Hibban | -79 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS | WIFI | WPA2 |
| 8 | Redmi | -92 | [WPA2-PSK-CCMP][ESS] | WIFI | WPA2 |
| 9 | BERDIKARI | -87 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 10 | JWS-116379 | -94 | [ESS] | WIFI | Unknown |
| 11 | Imron toko | -88 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 12 | Tenda\_53C5F8 | -85 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 13 | Wifi // id | -91 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 14 | Lenovo P770 | -61 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 15 | @wifi.id | -92 | [ESS] | WIFI | Unknown |
| 16 | SMA\_FITRA\_ABDI | -92 | [ESS] | WIFI | Unknown |
| 17 | OPPO A1k | -88 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 18 | Bubbleboba | -93 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 19 | Denipe | -87 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 20 | AndroidAPA454 | -92 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 21 | Badoy | -89 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 22 | Cie nyari gratisan ZTE-ece7a0 | -84 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 23 | AndroidAPA0BB | -89 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 24 | @wifi.id | -70 | [ESS] | WIFI | Unknown |
| 25 | ZTE-ece1A6 | -85 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 26 | AndroidAPA454 | -77 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |

Lokasi kedua pada wilayah jalan plaju terdapat 44 titik hospot pada hasil scanning yeng telah didapat Setelah melakukan scanning di kawasan tegal binangun didapatlah file format .kml yang kami export dari Wigle,dan kami langsung membuka file tersebut dengan menggunakan GoogleEarth, hasil yang didapat dari GoogleEarth adalah mapping yang bisa dilihat pada Gambar 3.2, 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 3.2 merupakan hasil yang kami dapat setelah berberapa kali mengitari kawansan Tegal Binangun. Pada gambar 3.2 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.

Berdasarkan Tabel

* Hasil scanning di kawasan plaju

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NO | SSID | SIGNAL | CAPABILITIES | TYPE | ENCRYPTION |
| 1 | RAJA AYAM | -82 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 2 | Vivo Y93 | -75 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 3 | Wifi@home | -89 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 4 | KLINIK MARISA | -83 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 5 | abcd | -81 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 6 | Linotine Alumunium | -92 | [WPA2-PSKCCCMP] [ESS] | WIFI | WPA2 |
| 7 | Ruli | -75 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS | WIFI | WPA2 |
| 8 | Ppp | -88 | [WPA2-PSK-CCMP][ESS] | WIFI | WPA2 |
| 9 | IMEL BOOY | -88 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 10 | Zakaria68 | -85 | WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 11 | ZTE\_2.4G\_p6DAdN | -88 | WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 12 | Bams elektronik | -73 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 13 | Redmi | -92 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 14 | HUAWEI-9PS4 | -84 | WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 15 | Speedy Instan@wifi.id | -93 | [ESS] | WIFI | Unknown |
| 16 | BiKz-YWJkdxraG9 | -84 | [ESS] | WIFI | Unknown |
| 17 | Mairus | -87 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 18 | MAULANA 88 | -91 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 19 | MARTABAK & NASI GORENG | -81 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 20 | Ayudia | -92 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 21 | Bang Tebby | -94 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 22 | Aiisyah faiha salsabila | -91 | [WPA2-PSK-CCMP] [ESS][WPS] | WIFI | WPA2 |
| 23 | Alfamart | -94 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 24 | Wifi Terus Sampe Mampus | -87 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 25 | @wifi.id | -94 | [ESS] | WIFI | unknown |
| 27 | Patra jaya | -94 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 28 | Naniksalto | -92 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 29 | Private 2 (10mb/s) | -84 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 30 | L300 | -92 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 31 | IO-PALEMBANG | -95 | [ESS] | WIFI | Unknown |
| 33 | Tenda\_4CE848 | -59 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA |
| 34 | 0711510058@wifi.id | -95 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 35 | Mika santika | -67 | [WPA2-PSK-CCMP] [ESS] [WPS] | WIFI | WPA2 |
| 36 | @Wifi.id | -97 | [ESS] | WIFI | unknown |
| 37 | Wifi.id@home | -87 | [ESS] | WIFI | unknown |
| 38 | KM.AGPG | -78 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 39 | HUAWEI-3J8C | -91 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 40 | Bepeker lah oii kawan | -63 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 41 | Rian Joker | -69 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 42 | Union Motor | -63 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 43 | Eric cantona | -83 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 44 | AndroidAP\_6656 | -92 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |

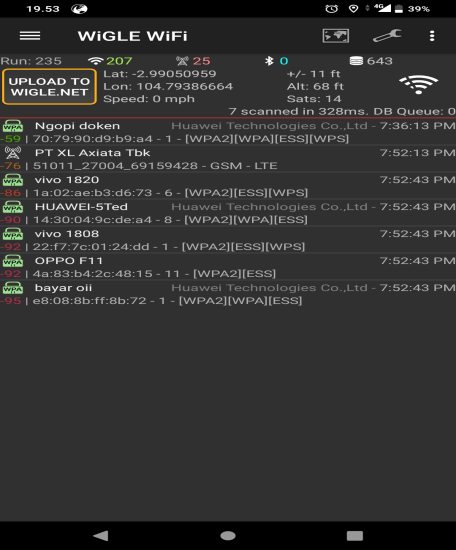
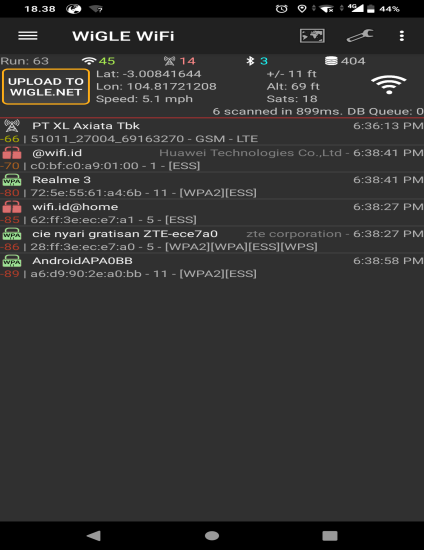
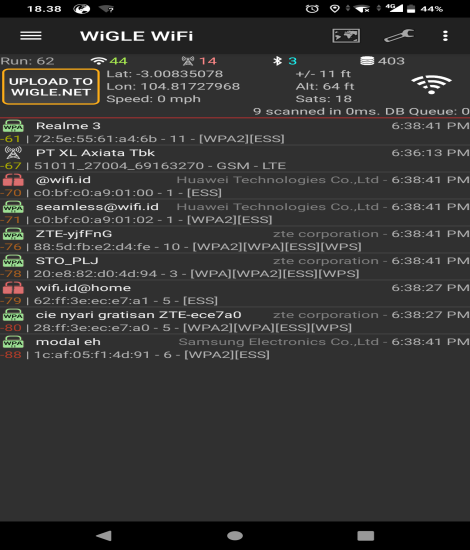
Lokasi ketiga pada wilayah komplek opi terdapat 32 titik hospot pada hasil scanning yeng telah didapat Setelah melakukan scanning di kawasan tegal binangun didapatlah file format .kml yang kami export dari Wigle,dan kami langsung membuka file tersebut dengan menggunakan GoogleEarth, hasil yang didapat dari GoogleEarth adalah mapping yang bisa dilihat pada Gambar 3.3, 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 3.3 merupakan hasil yang kami dapat setelah berberapa kali mengitari kawansan Tegal Binangun. Pada gambar 3.3 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.

Berdasarkan Tabel

* Hasil scanning di kawasan komplek

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NO | SSID | SIGNAL | CAPABILITIES | TYPE | ENCRYPTION |
| 1 | A3 celluler | -80 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 2 | Redmi | -81 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 3 | ZTE\_2.4G\_KamNeA | -91 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 4 | KEVIN | -97 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 5 | ZFZ | -93 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 6 | Router-wifi-222C | -88 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 7 | AndroidAP6FAE | -82 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 8 | @JKB01 | -92 | [WPA2-PSK-CCMP][ESS] | WIFI | WPA |
| 9 | ESTHEIM | -80 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 10 | REGA | -89 | WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 11 | Eddy 288 | -80 | WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 12 | JEHOVA | -82 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 13 | Redmi | -92 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 14 | ZTE\_2.4\_mbHQ4r | -76 | WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 15 | @ANNUR | -88 | WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS][WPS] | WIFI | WPA2 |
| 16 | WAYA WAYA ES | -81 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 17 | Tenda\_4C3428 | -79 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 18 | E 60 | -75 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 19 | Ady sofyan | -84 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 20 | Nubieter | -63 | [WPA2-PSK-CCCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 21 | RAY | -92 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] [WPS] | WIFI | WPA2 |
| 22 | LUKITAROSMARI | -86 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 23 | corvobianco | -92 | [WPA2-PSK-CCCMP] [ESS] [WPS] | WIFI | WPA2 |
| 24 | Rhasel | -81 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 25 | MADIL F | -94 | WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 27 | ALIYA PUTRI YUDISTIRA | -95 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 28 | Eginnnnnn | -90 | [WPA2-PSK-CCMP] [ESS] | WIFI | WPA2 |
| 29 | Ipin Upin | -84 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 30 | Toko ICAN | -93 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 31 | HUAWAEI-dW95 | -92 | [WPA2-PSK-CCMP+TKIP] [WPA2-PSK-CCMP+TKIP] [ESS] | WIFI | WPA2 |
| 32 | Budi | -77 | [WPA2-PSK-CCMP] [ESS] [WPS] | WIFI | WPA2 |

Pada gambar dibawah ketika sedang terjadinya scaning titik hotspot yang dilakukan pada wadriving.



### Analisa Channel Wireless

Setelah melakukan scanning di kawasan Plaju,Tegal binangun,opi 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 3.1 merupakan hasil yang kami dapat setelah berberapa kali mengitari kawansan Plaju. Pada gambar 3.1 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) begitupun dengan kawasan pada wilayah plaju dn komplek opi tersebut. wireless di ketika kawasan ini hampir 70% mengalami interferensi yang dimana interferensi itu akan mengganggu stabilitas dan perfomance dari signal jaringan wireless.Dengan keamaan yang metode autentikasi WEP/WPA PSK/WPA2-PSK.

# BAB III

# PENUTUP

## Kesimpulan :

Wigle sebagai Tools yang digunakan pada smartprhone bisa menggantikan fungsi 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. Pada penelitian kali ini juga menggunakan GoogleEarth bisa untuk mapping sebuah jaringan wireless sebagai pendukung kegiatan Wardriving, dan juga dapat mengetahui SSID serta BSSID yang ada pada jaringan wireless tersebut ,tentu saja mapping bisa dilakukan dengan format file .kml yang diberikan oleh Wigle.