**LAPORAN KOMUNIKASI DATA**

**TRACKING SSID MENGGUNAKAN WIGLE WIFI**

****

**Di susun oleh:**

**Ahmad Ilham arismawan  
(09011381621064)**

**Dosen pengampu:**

**Deris stiawan, M.T, Ph.D.**

**SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**Daftar isi**

Daftar isi ………………………………………………………………………………………

Bab1 Pendahuluan …………………………………………………………………………….

Bab2 Dasar teori ………………………………………………………………………………

* 1. WEP …………………………………………………………………………………..
  2. WPA ………………………………………………………………………………….
  3. WPA2 …………………………………………………………………………………
  4. WPS …………………………………………………………………………………...
  5. ESS ……………………………………………………………………………………
  6. WiGle WiFi …………………………………………………………………………...

Bab3 Prosedur percobaan …………………………………………………………………….

Bab4 hasil dan pembahasan …………………………………………………………………..

Bab5 kesimpulan ………………………………………………………………………………

**Bab1**

**Pendahuluan**

Wireless Security merupakan salah satu sistem keamanan jaringan yang terdapat pada jaringan nirkabel atau jaringan tanpa kabel ( Wi-fi ), semakin banyaknya kebutuhan akan akses internet, membuat para penyedia jasa layanan Wi-fi seperti warnet atau Internet Hotspot semakin was - was dengan adanya pembobol jaringan Wi-fi, salah satu cara untuk mengantisipasi hal tersebut adalah dengan memanfaatkan Keamanan Wireless yang sudah tersedia, jenisnya pun beragam contohnya ada WEP, WPA, WPA2 Personal dan WPA2 Enterprise, istilah - istilah di atas mungkin masih terdengan asing bagi kita yang tidak mengetahuinya, padahal keamanan jaringan sangat di perlukan.

**Bab 2**

**Dasar teori**

**2.1** **WEP (Wired equivalent privacy)**

[WEP](http://goo.gl/m18NS) merupakan standart keamanan & enkripsi pertama yang digunakan pada wireless, WEP (Wired Equivalent Privacy) adalah suatu metode pengamanan jaringan nirkabel,atau 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.

Proses Shared Key Authentication:  
1. Client meminta asosiasi ke access point, langkah ini sama seperti Open System Authentication.  
2. Access point mengirimkan text challenge ke client secara transparan.  
3. Client akan memberikan respon dengan mengenkripsi text challenge dengan menggunakan kunci WEP dan mengirimkan kembali ke access point.  
4. Access point memberi respon atas tanggapan client, akses point akan melakukan decrypt terhadap respon enkripsi dari client untuk melakukan verifikasi bahwa text challenge dienkripsi dengan menggunakan WEP key yang sesuai. Pada proses ini, access point akan menentukan apakah client sudah memberikan kunci WEP yang sesuai. Apabila kunci WEP yang diberikan oleh client sudah benar, maka access point akan merespon positif dan langsung meng-authentikasi client. Namun bila kunci WEP yang dimasukkan client adalah salah, maka access point akan merespon negatif dan client tidak akan diberi authentikasi. Dengan demikian, client tidak akan terauthentikasi dan tidak tersambung dengan jaringan.

**Kelebihan WEP**

User lebih mudah menggunakan tipe kemanan jaringan ini karena akan secara otomatis masuk ke jaringan dengan hanya memasukan Username dan Password.  
  
**Kelemahan WEP**

Masalah kata sandi yang lemah, algoritma RC4 yang digunakan dapat di bobol. karena WEP menggunakan kunci yang bersifat statis.

**2.2 WPA (Wi-fi Protect access)**

WPA merupakan salah satu tipe keamanan jaringan nirkabel yang merupakan perkembangan dari WEP, WPA secara resmi di perkenalkan pada tahun 2003, setahun sebelum WEP resmi tidak di gunakan lagi. konfigurasi WPA yang paling umum adalah WPA-PSK ( Pre-Shared Key ). Enkripsi yang di gunakan oleh WPA adalah 256-bit, WPA mengimplementasikan layer IEEE yaitu Layer 802.11i . WPA di desain untuk menggantikan metode keamanan WEP, yang menggunakan kunci keamanan static, WPA menggunakan metode TKIP (Temporal Key Integrity Protocol) yang mampu berubah secara dinamis. Protokol TKIP akan mengambil kunci utama sebagai starting point yang kemudian secara reguler berubah sehingga tidak ada kunci enkripsi yang digunakan dua kali. WPA juga menggunakan alat tambahan yaitu PC, Alasannya karena PC berguna sebagai authentication server yang akan memberikan kunci berbeda pada masing - masing user.

**Kelebihan WPA**

Enkripsi data yang digunakan adalah Temporal Key Integrity Protocol (TKIP). enkripsi yang digunakan masih sama dengan WEP yaitu RC4, karena pada dasarnya WPA ini merupakan perbaikan dari WEP dan bukan suatu level keamanan yang benar – benar baru, walaupun beberapa device ada yang sudah mendukung enkripsi AES yaitu enkripsi dengan keamanan yang paling tinggi.  
  
**Kelemahan WPA**

Kelemahan WPA sampai saat ini adalah proses kalkulasi data yang lama. Dengan kata lain, proses transmisi data akan menjadi lebih lambat di bandingkan jika kita menggunakan protokol WEP tetapi Belum semua wireless mendukung, biasanya butuh upgrade firmware, driver atau bahkan menggunakan software tertentu.

**2.3 WPA2 (Wi-fi protect access 2)**

WPA telah dikembangkan pada 2006 dan secara resmi digantikan oleh WPA2. Salah satu perubahan yang paling signifikan antara WPA dan WPA2 adalah penggunaan algoritma AES dan pengenalan CCMP (Counter Cipher Mode dengan Blok Chaining Message Authentication Code Protocol) sebagai pengganti TKIP. perlu di ketahui bahwa algoritma AES merupakan Enkripsi yang memiliki keamanan paling tinggi. WPA sendiri di bagi menjadi dua jenis yaitu WPA2 Enterprise dan WPA2 Personal

**2.4 WPS (Wi-Fi protected setup)**

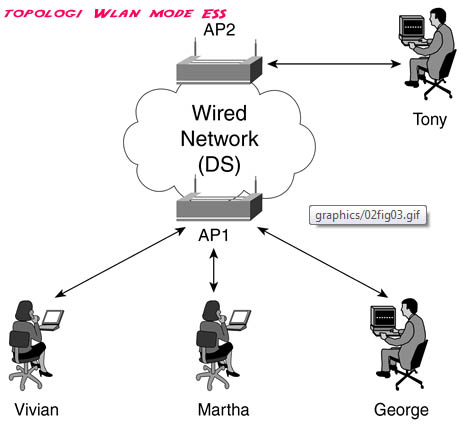
WPS adalah standar jaringan nirkabel yang mencoba untuk membuat koneksi antara router dan perangkat nirkabel lebih cepat dan lebih mudah. Ia bekerja hanya untuk jaringan nirkabel yang memiliki keamanan (secutiry) WPA Personal atau WPA2 Personal. WPS tidak memberikan dukungan untuk jaringan nirkabel menggunakan keamanan WEP lawas.

Dalam pengaturan normal, kamu tidak bisa menghubungkan perangkat nirkabel ke jaringan nirkabel kecuali kamu mengetahui nama jaringan (biasa disebut SSID) dan password (juga sering disebut key WPA-PSK). Pada perangkatmu, kamu harus terlebih dulu memilih jaringan yang ingin dihubungkan dan kemudian memasukkan password keamanan. Di sinilah fungsi WPS, yaitu menyederhanakan proses koneksi.

**2.5 ESS (Extended service set)**

Extended Service Sets (ESSs) adalah kumpulan dari beberapa topologi BSS. Pada topologi ESS terdapat lebih dari satu Access Point(AP), Access Point – Access Point dalam topologi ESS terhubung satu sama lain melalui port uplink. Alasan utama dipakainnya model topologi ini adalah untuk memperluas daya jangkau AP dan juga karena meningkatnya beban yang mesti dilayani oleh satu AP.

Beberapa hal yang mesti diperhatikan adalah dalam sebuah topologi ESS, AP-AP yang ada harus beroperasi dengan channel yang berbeda agar tidak saling meng- interferensi dan harus tetap menggunakan SSID yang sama.



**2.6 WiGle WiFi**

WiGLE, atau (Wireless Geographic Logging Engine), adalah situs web untuk mengumpulkan informasi tentang berbagai hotspot nirkabel di seluruh dunia. Pengguna dapat mendaftar di situs web dan mengunggah data hotspot seperti koordinat GPS, SSID, alamat MAC dan jenis enkripsi yang digunakan pada hotspot yang ditemukan. Selain itu, data menara sel diunggah dan ditampilkan. Dengan memperoleh informasi tentang enkripsi berbagai hotspot, WiGLE mencoba untuk menciptakan kesadaran akan perlunya keamanan dengan menjalankan jaringan nirkabel. Rekaman hotspot pertama di WiGLE diunggah pada September 2001. Pada Juni 2017, WiGLE menghitung lebih dari 349 juta jaringan Wi-Fi yang tercatat dalam database-nya, yang mana 345 juta direkam dengan koordinat GPS dan lebih dari 4,8 miliar pengamatan rekaman unik. Selain itu, database sekarang mengandung 7,80 juta menara sel unik termasuk 7,75 juta dengan koordinat GPS.

**Bab 3**

**Prosedur peercobaan**

Pada percobaan yang dilakukan untuk mentracking SSID yang ada maka dibutuhkan sebuah aplikasi yang digunakan sebagai tracker SSID sepanjang jalur yang telah dituju. percobaan kali ini digunakan aplikasi yang bernama WiGle Wi-Fi. Dalam aplikasi Wigle wifi ini akan di tracking semua SSID yang berada dalam jangkauan sinyal sepanjang jalur, setelah di track maka didapatkan hasil berupa file yang memiliki enkstensi berupa kml, file inilah data dari SSID yang telah berhasil di track yang kemudian dapat di buka melalui Google Earth. Secara umum berikut merupakan langkah-langkahnya:

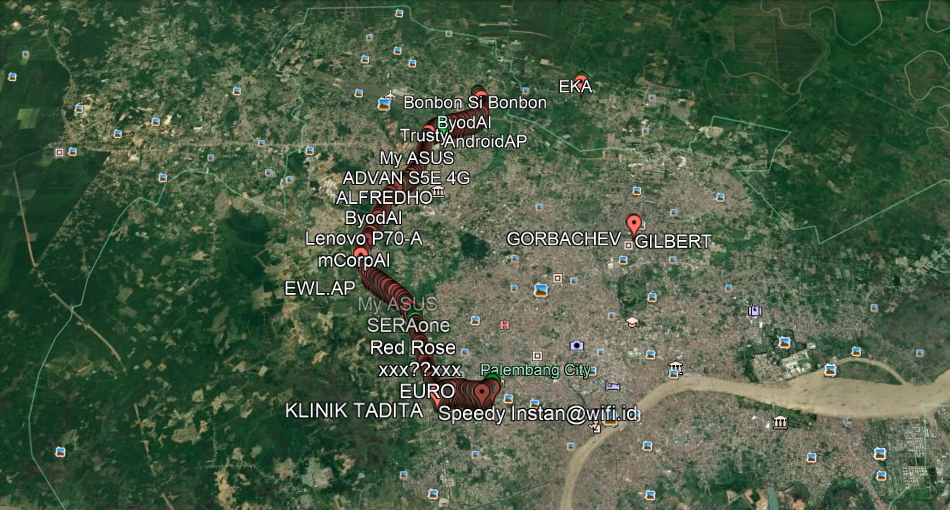
1. Menentukan jalur yang akan di tracking
2. Tracking SSID menggunakan WiGle Wi-Fi
3. Membuka data file menggunakan Google Earth
4. Analisa informasi data SSID

**Bab 4**

**Hasil dan pembahasan**

Pada tracking yang dilakukan didapatkan sekitar 100 lebih SSID yang ditemukan lengkap dengan informasi dari SSID tersebut. Berikut merupakan foto dari hasil tracking SSID menggunakan WiGle Wi-Fi.

1. **Data foto keseluruhan**



Seperti yang terlihat pada hasil tersebut, jalur yang di ambil ialah jalur sepanjang jalan dari simpang bandara Sultan Mahmud Badaruddin II hingga kampus Uiversitas Sriwijaya dan ditemukan hingga lebih dari 100 SSID yang terlacak.

1. **Data foto secara dekat**





Pada foto kali ini saya memperbesar data kml yang dibuka menggunakan Google Earth secara acak, terlihat ada beberapa perbedaan pada SSID yang didapatkan yaitu berupa warna dari SSID tersebut. Warna yang saya dapatkan yaitu berupa warna merah, kuning dan hijau.

1. **SSID warna merah**

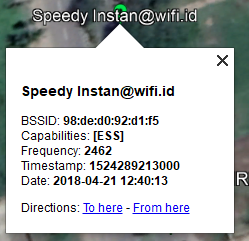




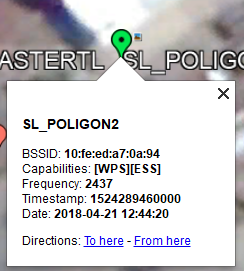
Diambil dari hasil dari file kml diambil 2 SSID yang memiliki warna merah secara acak, hasilnya terlihat beberapa kesamaan yang dimiliki yaitu pada hal capabilities/kapabilitas nya. Pada SSID bernama RAMOS PRIMA MANDIRI kapabilitas yang dimiliki berupa keamanan jaringan berbasis WPA-PSK-CCMP+TKIP dan juga WPA-PSK-CCMP+TKIP, selain itu terlihat pula topologi yang digunakan yaitu berupa topologi berbasis ESS. Ini berarti jaringan SSID yang berwarna merah memiliki tingkat kerentanan akan peretasan jaringan sangatlah kecil atau susah untuk ditembus atau bisa juga dibilang cukup aman karena memiliki keamanan jaringan double dengan metode yang sangat aman seperti penggunaan konfigurasi PSK, hingga konfigurasi keamanan CCMP dan TKIP yang mampu merubah key secara dinamis pada masing masing WPA dan WPA2.

1. **SSID warna hijau**



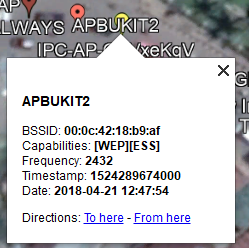


Kemudian diambil juga secara acak kembali 2 SSID yang memiliki warna hijau, pada foto dari data SSID tersebut, kedua SSID memiliki kesamaan pada hal capabilities/kapabilitasnya yaitu berupa informasi topologi yang digunakan berupa topologi ESS. Dalam hal ini berbeda dengan informasi SSID yang memiliki warna merah, SSID warna hijau tidak memiliki pengaturan keamanan jaringan wireless layaknya SSID pada warna merah, pada hal ini SSID berarti memiliki sifat terbuka pada seluruh device yang memperbolehkan mengakses jaringan tersebut sehingga SSID warna hijau memiliki kerentanan yang sangat besar akan aktifitas peretasan yang dilakukan oleh pihak pihak yang tidak bertanggung jawab. Namun pada data yang diambil kembali ditemukan perbedaan dalam SSID yang memiliki wana hijau.

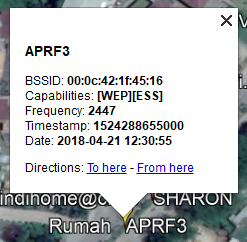


Seperti yang terlihat pada SSID warna hijau kali ini ditemukan informasi yang baru berupa keamanan jaringan yang digunakan yaitu dengan metode WPS, seperti pada penjelasan dalam dasar teori keamanan jaringan yang digunakan ini hanyalah sebagai penyederhanaan proses koneksi device terhadap jaringan SSID tersebut sehingga tidak perlu lagi memasukan password. Alasan mengapa SSID ini memiliki warna hijau meskipun menggunakan WPS kemungkinan adalah karena dengan penyederhanaan tersebut device luar yang telah terhubung sebelumnya tidak akan perlu memasukan key kembali, sehingga jika orang luar sebelumnya ingin membobol jaringan tersebut tidak perlu lagi memasukan key sehingga dapat dikatakan kurang aman.

1. **SSID warna kuning**



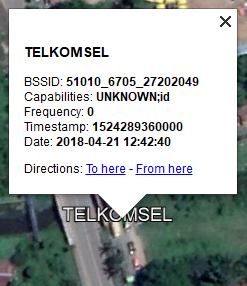




Pada SSID warna kuning diambil 2 SSID secara aca pada 2 tempat yang berjauhan, hasilnya kesamaan yang dimiliki sama yaitu pada capabilities/kapabilitasnya berupa informasi keamanan jaringan yang digunakan yaitu menggunakan keamanan jaringan dengan metode WEP dan informasi topologi jaringan yang digunakan yaitu ESS. Seperti yang dijelaskan pada dasar teori metode keamanan jaringan WEP ini kurang handal dibandingkan dengan WPA yang menggunakan PSK, CCMP dan TKIP. Keamanan WEP mudah untuk diretas karena menggunakan konfigurasi keamanan Shared key authentication yang bersifat statis, sehingga memudahkan pihak lain untuk membobol keamanan jaringan ini.

1. **Bukan berupa SSID WLAN**

Pada hasil berikut ada beberapa jaringan yang terdeteksi namun bukanlah berupa suatu SSID WLAN namun berupa nama sebuah operator layanan jaringan dengan informasi yang tidak diketahui, kemungkinan hal ini merupakan interferensi yang ditimbulkan oleh sinyal penyedia jasa layanan jaringan tersebut.



**Bab 5**

**Kesimpulan**

Berdasarkan pada hasil yang didapatkan serta pembahasan dan Analisa yang telah dijelaskan maka dapat ditarik beberapa kesimpulan yang dapat di ambil:

1. WiGle Wi-Fi dapat digunakan sebagai alat tracking SSID secara baik dengan diberikannya informasi yang cukup lengkap.
2. SSID memiliki beberapa sistem keamanan jaringan yang digunakan berupa WEP,WPA dan WPA2
3. Topologi jaringan pada SSID WLAN kebanyakan sama yaitu menggunakan topologi ESS
4. SSID dengan sistem keamanan WPA serta WPA2 paling banyak digunakan karena memiliki sistem keamanan yang tinggi

**Daftar pustaka**

**Santri bantat, “Mengenal keamanan wireless wep dan wpa” diperoleh 8 mei 2018, Dari** [**http://santri-bantat.blogspot.co.id/2011/10/mengenal-keamanan-wireless-wep-dan-wpa.html**](http://santri-bantat.blogspot.co.id/2011/10/mengenal-keamanan-wireless-wep-dan-wpa.html)

**Government of HKSAR, “Wireless networking security” diperoleh 8 mei 2018, Dari** [**https://www.infosec.gov.hk/english/technical/files/wireless.pdf**](https://www.infosec.gov.hk/english/technical/files/wireless.pdf)

**Techopedia, “Extended service set” diperoleh 8 mei 2018, Dari** [**https://www.techopedia.com/definition/24968/extended-service-set-ess**](https://www.techopedia.com/definition/24968/extended-service-set-ess)

**Routekno, “Jenis-jenis keamanan pada jaringan” diperoleh 8 mei 2018, Dari**

[**http://routekno.blogspot.co.id/2016/02/jenis-jenis-keamanan-pada-jaringan.html**](http://routekno.blogspot.co.id/2016/02/jenis-jenis-keamanan-pada-jaringan.html)

**Anto, “Tiga jenis topologi wireless yang mesti diketahui” diperoleh 8 mei 2018, Dari**

[**http://www.norisanto.com/wireless/tiga-jenis-topologi-wireless-yang-mesti-diketahui/**](http://www.norisanto.com/wireless/tiga-jenis-topologi-wireless-yang-mesti-diketahui/)

**Informasi seputar pengetahuan, “Apa itu WPS? Apa itu fungsinya? WPS adalah …” diperoleh 8 mei 2018, Dari**

[**https://inseptek.wordpress.com/2017/01/17/apa-itu-wps-apa-fungsinya-wps-adalah/**](https://inseptek.wordpress.com/2017/01/17/apa-itu-wps-apa-fungsinya-wps-adalah/)

**Wikipedia, “WiGle” diperoleh 8 mei 2018, Dari**

**https://en.wikipedia.org/wiki/WiGLE**