Tugas Besar

Teknik penulisan karya ilmiah

“ Analisis Wardriving Wi-Fi Pada Area Jl. R.E. Martadinata

Menggunakan Sotfware Wigle “

Ditulis oleh

Nama : Muhammad Hafizzurrahman

NIM : 09030581822054

Prodi : Teknik Komputer 3B

Jurusan : Sistem Komputer

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2019

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa, karena hanya dengan rahmat-Nyalah penulis akhirnya bisa menyelesaikan karya ilmiah yang berjudul “Analisis Wardriving Wi-Fi Pada Area Jl. R.E. Martadinata Menggunakan Sotfware Wigle” ini dengan baik tepat pada waktunya.

Tidak lupa penulis menyampaikan rasa terima kasih kepada dosen pembimbing yang telah memberikan banyak bimbingan serta masukan yang bermanfaat dalam proses penyusunan karya ilmiah ini. Rasa terima kasih juga hendak penulis ucapkan kepada rekan-rekan mahasiswa yang telah memberikan kontribusinya baik secara langsung maupun tidak langsung sehingga karya ilmiah ini bisa selesai pada waktu yang telah ditentukan.

Meskipun penulis sudah mengumpulkan banyak referensi untuk menunjang penyusunan karya ilmiah ini, namun penulis menyadari bahwa di dalam karya ilmiah yang telah disusun ini masih terdapat banyak kesalahan serta kekurangan. Sehingga penulis mengharapkan saran serta masukan dari para pembaca demi tersusunnya karya ilmiah lain yang lebih lagi. Akhir kata, penulis berharap agar karya ilmiah ini...

Palembang, 8 Desember 2019

DAFTAR ISI

Abstrak

Di era yang serba digital sekarang ini, kita sering sekali menjumpai banyak tempat yang sudah ada Wi-fi nya, bahkan ditempat-tempat yang sering kali di kunjungi banyak orang sudah mungkin sudah banyak jaringan wifi atau titik hotspotnya. Wardriving pada dasarnya merupakan kegiatan untuk mencari sumber hotspot atau jaringan wifi tersebut dari akses poin sebanyak mungkin untuk mendapatkan informasi dari kumpulan dimana akses poin tersebut berada. Pada percobaan kali ini, penulis memilih tempat yang ramai lalu lalangnya di kota Palembang, yaitu di Jl. R.E. Martadinata mulai dari SPBU hingga Wifi.id Corner yang banyak titik hotspotnya, Pada percobaan wardriving kali ini tools yang digunakan adalah aplikasi Wigle WiFi dan Google Earth pada Smartphone Android yang penulis gunakan. Setelah melakukan scanning dengan menggunakan Wigle WiFi data hasil tersebut akan diupload ke server Wigle dengan format data kml. Lalu selanjutnya kita ekspor file ini ke Google Earth untuk pemetaan yang lebih spesifikasi untuk untuk melihat dimana posisinya berada.

Kata Kunci : *Wardriving, Wigle WiFi, Google Earth, GPS, WPA-PSK.*

1. Pendahuluan

Sekarang ini sering kali kita menjumpai banyak koneksi wireless network baik di gedung maupun di jalan. Dengan bermodalkan Smartphone saja kita bisa mendapatkan wireless network dengan mengaktifkan fasilitas Wi-fi dari smartphone, baik hotspot yang berasal dari operator selular, wireless network dari router yang dipasang pada sebuah gedung, maupun wireless network yang berasal dari smartphone pribadi (tethering) ataupun modem. Wireless network memiliki jarak jangkauan internet yang cukup luas sehingga orang selain pemilik pun bisa mengakses nya selagi masih pada jangkauan hotspotnya. Maka dari hal tersebutlah wardriving dilakukan, yaitu usaha untuk mendapatkan kumpulan dari wireless network yang terdapat di tempat-tempat 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 di install lewat desktop. Cukup berjalan atau berkendara di sekeliling lokasi tersebut yang menjadi target dan kita bias mendapatkan informasi jaringan wifi bahkan dengan authentication modenya apakah wifi tersebut menggunakan pengamanan atau tidak.

2. Dasar Teori

a. Standarisasi Teknologi Wireless – WiFi (Wireless Fidelity)

WiFi (Wireless Fidelity) Alliance mendefinisikanWi-Fi sebagai sebagai produk Wireless Local Area Network (WLAN) yang didasarkan pada standar Institute of Electricaland Electronics Engineers (IEEE)802.11. IEEE 802.11 dibagi menjadi a/b/g/n atau IEEE 802.11a/b/g/n. IEEE802.11/a memiliki spesifikasi (Kecepatan ~54 Mb/s, Frekuensi 5 GHz), IEEE 802.11/b memiliki spesifikasi (Kecepatan 11 Mb/s, Frekuensi ~2.4 GHz), IEEE 802.11/g memiliki spesifikasi (Kecepatan 54 Mb/s, Frekuensi ~2.4GHz, kompatibel dengan IEEE 802.11b/g), IEEE 802.11/n memiliki spesifikasi (Kecepatan 100 Mb/s, Frekuensi ~2.4GHz, kompatibel dengan IEEE 802.11b/g/n). Standar teknis 802.11b/g/n diperuntukkan bagi perangkat WLAN yang

digunakan pada frekuensi 2,4 GHz atau disebut frekuensi ISM (Industrial, Scientific and Medical).

b. Sistem keamanan pada wireless network

Keamanan pada wireless network seperti Wi-fi diperlukan sebab teknologi seperti ini umumnya memiliki kelemahan. Salah satunya pada bagian fisik sebab menggunakan gelombang radio(udara)yang bersifat menyebar. Sehingga beberapa kemungkinan serangan oleh attacker, seperti : interception, injection, jamming, locating mobile nodes, access control dan hijacking sangat mungkin dilakukan.

Keamanan yang digunakan pada wireless network menggunakan enkripsi seperti berikut.

1. **WEP** (Wired Equivalent Privacy) merupakan standar keamanan & enkripsi pertama yang digunakan pada wireless, disebut juga dengan Shared Key Authentication. WEP menggunakan kunci yang dimasukkan oleh administrator ke client maupun access point. Berkeja dengan pencocokan kunci antara access point dan pengguna.

2. **WPA** (WiFi Protected Access). WPA terbagi menjadi WPA dan WPA2 merupakan penyempurnaan dari WEP. WPA mempunyai mekanisme enkripsi yang lebih handal. Teknik WPA dibentuk untuk menyediakan enkripsi data user authentication yang menjadi titik lemah WEP. Pada WPA2 merupakan sertifikasi produk yang tersedia melalui Wi-Fi Alliance. WPA2 sertifikasi produk yang secara resmi menggantikan WEP dan fitur keamanan lain yang asli standar IEEE 802.11. Tujuan dari sertifikasi ini adalah untuk mendukung tambahan fitur keamanan pada standar IEEE 802.11i

3. **WPA & WPA2-PSK** (WPA & WPA2 – Pre Shared Key). WPA-PSK merupakan teknik keamanan jaringan wireless tanpa memerlukan authentikasi server. Dengan demikian access point dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server. Sedangkan pada WPA2-PSK dengan fitut tambahan AES (Advanced Encryption Standard) dan TKIP (Temporal Key Integrity Protocol).

c. Wardriving

Wardriving adalah kegiatan atau aktivitas untuk mendapatkan informasi tentang suatu jaringan wireless dan mendapatkan akses terhadap jaringan wireless tersebut. Umumnya bertujuan untuk mendapatkan koneksi internet, tetapi banyak juga yang melakukan wardriving untuk maksud tertentu mulai dari rasa keingintahuan, coba-coba, research, tugas praktikum, kejahatan dan lain-lain (Sinambela, 2009), sedangkan menurut R. Hartono dan A. Purnomo (2011) menyebut bahwa wardriving pada umumnya sebuah kegiatan untuk mendapatkan informasi terkait teknologi wireless seperti WiFi (IEEE 802.11), melakukan mapping area dan fitur keamanan yang digunakan. Kegiatan dapat berupa mencari keberadaan WiFi (IEEE 802.11) dan menandai lokasi access point yang ditemukan, sambil berkendara maupun tanpa berkendara di suatu daerah tertentu, secara umum wardriving dibagi menjadi dua tahapan yaitu scanning dan mapping. Tahapan ini dapat memanfaatkan teknologi seperti GPS (Global Positioning System), serta mengkombinasikan tools software seperti Wigle dan Google Earth.

3. Metode Percobaan

Adapun Metode pengujian yang digunakan untuk penelitian ini adalah metode Wardriving. Wardriving adalah kegiatan seseorang yang melakukan kegiatan berkeliling ke berbagai ke tempat dalam usahanya mencari, mengekplorasi, bahkan mungkin juga mengekplotasi jaringan wireless yang ditemukannya. Kemudian orang yang melakukan kegiatan tersebut disebut sebagai Wardriver, dalam upanyanya itu dia melakukan pengumpulan data dan menganalisa sistem Security-nya (Zam, 2014). Tahapan dari metode Wardriving adalah :

3.1 Penentuan lokasi

Wardriving dilalukan ketika target lokasi telah di tentukan. Lokasi yang ditentukan kiranya ramai dan banyak pengunjung. Pada laporan ini lokasi yang dipilih adalah sekitaran jalan R.E. Martadinata (mulai dari SPBU 24.301.08 hingga Wifi.id corner).

3.2 Scanning

Untuk melakukan scanning, penulis menggunakan software Wigle pada smartphone android untuk mencari dan menagkap titik-titik access point serta menampilkan informasi-informasi pada Wifi tersebut seperti MAC Address, SSID, Signal, Frekuensi, tipe enkripsi dan sebagainya di lokasi tersebut.

3.3 Mapping

Setelah mendapatkan data hasil scanning. Mapping atau pemetaan dilakukan, yakni bertujuan untuk memetakan titik-titik hotspot yang telah tertangkap dalam oleh wigle dalam format baik .kml maupun .csv. Kemudian di-import kedalam Google Earth untuk menampilkan petanya.

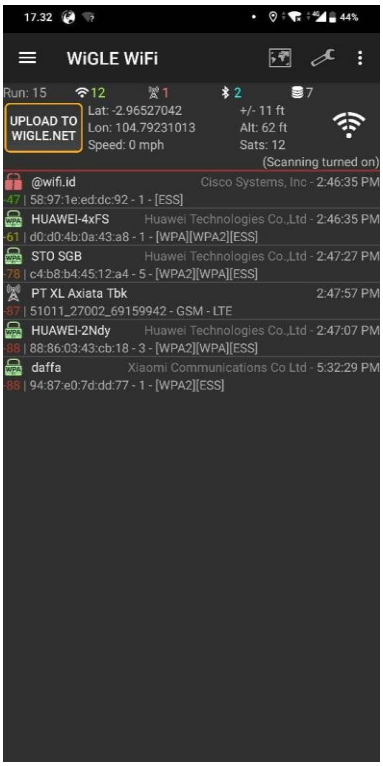
3.4 Analisis hasil scanning dan mapping.

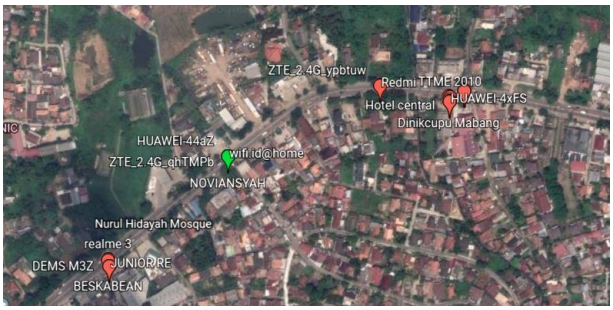
Menentukan fitur keamanan yang paling apa saja yang digunakan pada teknologi wireless seperti WiFi dan mengukur persentase qualitas sinyal pada setiap WiFi.

4. Hasil dan Pembahasan

Lokasi sekitaran Jl. R.E.Martadinata dimana dari SPBU 24.301.08 hingga Wifi.id corner berada pada keramaian. Sehingga lokasi ini dinilai memenuhi kriteria untuk melakukan kegiatan wardriving WiFi. Untuk melakukan kegiatan wardriving beberapa spesifikasi hardware dan tools software yang penulis persiapkan adalah sebagi berikut :

1. Hardware : - Smartphone Asus max pro M2
   - Laptop Asus notebook x441uv
2. Operating System : Android 9/ pie
3. Tools Software : Wigle wi-fi
4. GPS (Global Positioning System) support Asus max pro M2
5. Mapping : Google Earth.





Gambar 1. Hasil scanning wigle

Gambar 2. Hasil pemetaan menggunakan Google earth

Pada **Gambar 1.** saat wigle menjalankan proses scanning, fitur Wi-fi dan Gps dan Bluetooth akan otomatis aktif. Kemudian list wifi akan otomastis ditampilkan pada dashboard termasuk SSID, MAC Address, channel, vendor, dan enkripsinya.

Pada **Gambar 2** hasil scanning menggunakan wigle akan di export menjadi format .kml. Kemudian diimport ke Google earth dan menghasilkan mapping area WiFi. Pemetaan di google earth dapat menampilkan dua atau lebih simbol berbeda yang mana pada percobaan ini muncul dua simbol berbeda, simbol dengan warna merah merupakan simbol koneksi wireless yang menggunakan enkripsi sedangkan simbol yang berwarna hijau merupakan simbol koneksi wireless yang tidak menggunakan enkripsi selain itu hasil mapping wardriving menggunakan google earth juga menghasilkan informasi berupa MAC Address, SSID, Authentication Mode, channel, RSSI, dan informasi lainnya**.** Namun dalam laporan ini penulis hanya mengambil

beberapa informasi diantaranya MAC Address, Authentication Mode, dan RSSI seperti ditunjukan pada Tabel 1 berikut ini :

Tabel 1. Informasi Hasil Scanning dan Mapping

No.	MAC Address	Authentication Mode	RSSI
1	58:97:1e:ed:dc:92	[ESS]	-38
2	d0:d0:4b:0a:43:a8	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP]	-52
3	88:5d:fb:c1:fe:30	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-80
4	88:86:03:43:ca:d	[WPA2-PSK-CCMP+TKIP][WPA-PSK-CCMP+TKIP][ESS]	-76
5	34:e9:11:1e:93:53	[WPA2-PSK-CCMP][ESS]	-82
6	e4:ca:12:92:2a:2e	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-86
7	c2:87:eb:a7:36:71	[WPA2-PSK-CCMP][ESS]	-69
8	34:0a:7b:27:21:7b	[WPA2-PSK-CCMP][ESS]	-71
9	c8:8d:83:38:c5:04	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-75
10	88:86:03:43:cb:18	[WPA2-PSK-CCMP+TKIP][WPA-PSK-CCMP+TKIP]	-80
11	e4:ca:12:91:a2:62	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-81
12	3e:b6:b7:29:3e:6b	[WPA2-PSK-CCMP][ESS][WPS]	-82
13	c4:b8:b4:45:12:a4	[WPA2-PSK-CCMP+TKIP][WPA-PSK-CCMP+TKIP][ESS]	-87
14	20:e8:82:c0:25:a4	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-84
15	0c:37:47:9d:5f:df	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-88
16	00:27:15:17:16:7e	[WPA2-PSK-CCMP][ESS]	-73
17	24:d3:f2:e5:b8:fc	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-86
18	ce:2d:83:9c:a8:71	[WPA-PSK-CCMP+TKIP][ESS][WPS]	-76
19	18:f0:e4:52:80:52	[WPA2-PSK-CCMP][ESS]	-91
20	24:7e:51:87:97:ce	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-66
21	22:e8:82:dc:d3:f4	[ESS]	-70
22	24:d3:f2:ea:4a:18	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-74
23	88:5d:fb:ce:f7:e2	[WPA2-PSK-CCMP][WPA-PSK-CCMP][ESS][WPS]	-74
24	24:d3:f2:ea:4d:de	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-74
25	34:da:b7:fe:8b:20	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-76
26	70:c7:f2:8f:86:54	[WPA2-PSK-CCMP+TKIP][WPA-PSK-CCMP+TKIP][ESS]	-76
27	26:d3:f2:da:4a:8a	[ESS]	-76
28	98:da:c4:48:44:6a	[WPA2-PSK-CCMP][ESS][WPS]	-76
29	24:d3:f2:ea:4a:8a	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-77
30	d0:c7:89:e9:13:30	[ESS]	-77
31	d0:c7:89:e9:13:31	[ESS]	-80

32	48:8e:ef:92:7b:ac	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-64
33	48:8e:ef:92:7b:ad	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-65
34	3c:1e:04:0d:94:c2	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-69
35	5a:85:a2:5e:91:c7	[WPA2-PSK-CCMP][ESS]	-70
36	e4:ca:12:c5:6d:44	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-81
37	9e:71:3a:68:4a:71	[WPA2-PSK-CCMP+TKIP][WPA-PSK-CCMP+TKIP]	-69
38	b0:be:76:8a:ba:40	[WPA2-PSK-TKIP+CCMP][ESS][WPS]	-86
39	90:c7:d8:9b:e4:1b	[WPA-PSK-TKIP+CCMP][WPA2-PSK-TKIP+CCMP][ESS]	-72
40	60:f1:8a:f9:b4:e8	[WPA2-PSK-CCMP+TKIP][WPA-PSK-CCMP+TKIP]	-85
41	f0:63:f9:9d:c5:c0	[WPA2-PSK-CCMP+TKIP][WPA-PSK-CCMP+TKIP]	-91

Tabel 1 diatas memperlihatkan bahwa ESS (Extended Service Set) dihampir semua fitur authentication. ESS merupakan jaringan yang terdiri dari beberapa BSS (Basic Service Set). Sedangkan definisi dari BSS itu sendiri merupakan kumpulan dari perangkat wireless yang terhubung satu sama lain dengan perantaraan sebuah perangkat access point. Dalam hal ini BSS dan ESS merupakan service set untuk pengelompokan teknologi wireless IEEE 802.11 secara logic. Dengan demikian Wigle mendefinisikan ESS pada hasil scanning sebagai fitur basic authentication pada teknologi wireless IEEE 802.11 seperti WiFi. Begitu juga TKIP dan CCMP, TKIP (Temporal Key Integrity Protocol) digunakan sebagai enkripsi untuk melindungi wireless network. Enkripsi ini biasa digunakan pada autentikasi WPA (WPA-TKIP). Sedangkan CCMP (Counter Mode CDC-MAC Protocol) atau lebih dikenal AES CCMP merupakan mekanisme yang menggantikan pendahulunya TKIP yang memiliki mekasnisme algoritma yang mudah untuk di pecahkan. Biasa digunakan sebagai standar enkripsi WPA2.

Berdasarkan hasil yang diperoleh dari penelitian tersebut menunjukanan adanya perbedaan RSSI. RSSI (Received Signal Strength Indicator) adalah pengukuran terhadap daya yang diterima oleh sebuah perangkat wireless. Pengukuran melibatkan kalibrasi nilai RSSI untuk setiap node referensi. Untuk mendapatkan kuatilas kekuatan sinyal wifi, RSSI harus di konversi menggunakan rumus berikut.

```
quality = 2 * (dBm + 100) where dBm: [-100 to -50]

dBm = (quality / 2) - 100 where quality: [0 to 100]
```

Dimana quality sebagai kualitas kuat sinyal yang berjarak 0 hingga 100 dan dBm sebagai kuat siynal berjarak -100 hingga -50. Jadi kualitas sinyal dari setiap SSID tabel diatas di dapat seperti tabel 2 berikut.

Tabel 2. Persentase signal strength

No.	RSSI	Quality (%)
1	-38	124
2	-52	96
3	-80	40
4	-76	48
5	-82	36
6	-86	28
7	-69	62
8	-71	58
9	-75	50
10	-80	40
11	-81	38
12	-82	36
13	-87	26
14	-84	32
15	-88	24
16	-73	54
17	-86	28
18	-76	48
19	-91	18
20	-66	68
21	-70	60
22	-74	52
23	-74	52
24	-74	52
25	-76	48
26	-76	48
27	-76	48
28	-76	48
29	-77	46
30	-77	46

31	-80	40
32	-64	72
33	-65	70
34	-69	62
35	-70	60
36	-81	38
37	-69	62
38	-86	28
39	-72	56
40	-85	30
41	-91	18

Dari hasil tabel diatas dapat simpulkan bahwa semakin besar dBm-nya maka makin besar juga persentase-nya. Dan semakin kecil dBm-nya maka makin kecil pula persentase-nya. Namun tidak menutup kemungkinan nilai tersebut akan mengalami penurunan bila ada satu user yang menghubungkan ke AP tersebut untuk terhubung ke internet atau transfer data secara otomatis ada penurun kuat sinyal (RSSI) 4 hingga 5 persen.

5. **Kesimpulan**

1. Dengan melakukan wardriving kita tidak hanya mendapatkan titik hotspot saja, tapi kita juga mendapatkan beberapa informasi dari titik hotspot atau access point tersebut.
2. Semakin jauh jarak yang kita ambil saat wardriving, kemungkinan access point yang tertangkap akan lebih banyak.
3. Sebagian besar mekanisme keamanan yang digunakan yakni WPA-PSK dan WPA2-PSK dengan enkripsi CCMP yang cukup aman dari TKIP.
4. Semakin besar dBm signal maka semakin bagus pula kualitas kuat sinyal yang diterima dan sebaliknya, namun tergantung berapa orang yang terhubung pada access point tersebut.

DAFTAR PUSTAKA

[1] J. M. Sinambela, "*Keamanan Wireless LAN (Wifi)*," no. April, 2007.

[2] R. Hartono and A. Purnomo, "*Wireless Network 802.11*," pp. 1–23, 2011.

[3] https://media.neliti.com/media/publications/173230-ID-pengkajian-kualitas-sinyal-dan-posisi-wi.pdf

[4] Wahyudi Dimas, "*Analisa Wardriving WiFi menggunakan Wigle pada Area Komplek Pertamina-Persada Indralaya*", 2013

[5] Hidayat Eral Putra, Alex Wijaya, RM Nasrul Halim, "*ANALISIS KEAMANAN JARINGAN WIRELESS MENGGUNAKAN METODE WARDRIVING PADA KANTOR PEMERINTAH KOTA PRABUMULIH*"

[6]https://www.acrylicwifi.com/en/blog/about-wpa-psk-tkip-ccmp-wi-fi-security-information/