Nusantara Journal of Multidisciplinary Science
Vol. 1, No. 6, Januari 2024
Hal 455-467
E-ISSN : 3024-8752
P-ISSN : 3024-8744
Site : https://jurnal.intekom.id/index.php/njms

Analisis Terhadap Kinerja Dan Keamanan Jaringan Nirkabel Menggunakan Teknik *Wardriving* Guna Mendukung Sistem Pemerintahan Berbasis Elektronik Di Kota Pontianak

Adry Nori[1], Helfi Nasution[2], Haried Novriando[3]
[1,2,3]Fakultas Teknik, Universitas Tanjungpura, Pontianak, Indonesia

Article Info

Article history:

Received January 10, 2024
Revised January 17, 2024
Accepted Januari 29, 2024

Keywords:

Pontianak,
Kuliner,
Srikaya Suka Hati

Keywords:

Pontianak,
Culinary,
Srikaya Suka Hati

ABSTRAK

Penggunaan internet yang tinggi di Kota Pontianak didominasi oleh pengguna WiFi, terutama di area bisnis, pendidikan, publik, dan perumahan. Meskipun jaringan nirkabel memberikan kemudahan informasi, keberadaannya juga membawa kerentanan terhadap kejahatan siber. Risiko penyusupan dan modifikasi data dapat terjadi karena sifat siaran jaringan nirkabel. Keamanan dan kinerja jaringan menjadi aspek penting dalam dunia teknologi informasi. Teknologi keamanan seperti WPA dan WPA2 sudah ada, namun belum selalu digunakan karena ketidaksadaran masyarakat. Maksimalkan kinerja jaringan nirkabel Kota Pontianak perlu pemilihan dan penentuan saluran yang tepat untuk mencegah interferensi. Aturan Kementerian Komunikasi dan Informatika mengenai radio frekuensi 2.4 GHz memberikan panduan dalam menyediakan saluran WiFi untuk mendukung kegiatan Asian Games. Penelitian ini bertujuan menganalisis kinerja dan keamanan jaringan nirkabel di Kota Pontianak dengan menggunakan Teknik Wardriving. Hasil penelitian menunjukkan bahwa 86% SSID menggunakan keamanan WPA2, 13% jaringan terbuka, dan 1% menggunakan WPA, sebagian besar menggunakan saluran 1, 6, dan 11, yang menciptakan kinerja jaringan yang baik dan aman dari interferensi.

ABSTRACT

High internet usage in Pontianak City is dominated by WiFi users, especially in business, education, public and residential areas. Although wireless networks provide easy information, their existence also brings vulnerability to cybercrime. The risk of data compromise and modification may occur due to the broadcast nature of wireless networks. Network security and performance are important aspects in the world of information technology. Security technologies such as WPA and WPA2 already exist, but are not always used due to public unawareness. Maximizing the performance of the Pontianak City wireless network requires selecting and determining the right channel to prevent interference. The Ministry of Communication and Information Technology regulations regarding 2.4 GHz radio frequencies provide guidance in providing WiFi channels to support Asian Games activities. This research aims to analyze the performance and security of wireless networks in Pontianak City using Wardriving Techniques. The research results show that 86% of SSIDs use WPA2 security, 13% open networks, and 1% use WPA, most of which use channels 1, 6, and 11, which creates good network performance and is safe from interference.

Corresponding Author:

Adry Nori
Fakultas Teknik, Universitas Tanjungpura,
Jakarta, Indonesia
Email: adrynori@student.untan.ac.id

1. PENDAHULUAN

Kota Pontianak merupakan salah satu kota yang memperoleh penghargaan *Smart City* kategori *Smart Branding* dalam program Gerakan Menuju *Smart City* dari Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo RI) pada hari Selasa tanggal 14 Desember 2021. Satu minggu kemudian Kota Pontianak kembali mendapatkan penghargaan dalam Riset Transformasi Digital dan Rating Kota Cerdas Indonesia 2021 yang digelar Pusat Inovasi Kota dan Komunitas Cerdas Institut Teknologi Bandung dalam kategori Kesiapan Digital Terbaik. Penghargaan ini diumumkan secara *virtual*, pada hari senin 27 Desember 2021. Penghargaan tersebut merupakan apresiasi bagi Kota Pontianak, apalagi riset dan rating ini diikuti oleh 93 daerah yang ada di Indonesia [1]. Rating dan riset yang dilakukan oleh Pusat Inovasi Kota dan Komunitas Cerdas Institut Teknologi Bandung ini bertujuan untuk mengukur kesiapan digital kota-kota yang ada di Indonesia, melakukan pengukuran kinerja terhadap pengelolaan kota, memberikan gambaran yang lebih komprehensif mengenai permasalahan dan potensi yang dihadapi setiap kota, memberikan gambaran bagi stakeholder kota dalam membangun layanan kota dan sebagai bahan evaluasi dan masukan untuk kemajuan perkembangan kota khususnya dan Indonesia umumnya.

Konsep pembangunan *smart city* saat ini merupakan salah satu solusi bagi pemerintah dalam mengelola kotanya dengan efektif dan efisien. Melalui pendekatan ini diharapkan kinerja pelaksanaan pembangunan dan penyelenggaraan pemerintahan dan layanan publik menjadi semakin prima. *Smart City* sebagai salah satu solusi cerdas menjadi alternatif baru untuk Kota Pontianak saat ini. Solusi yang cerdas melibatkan minimal 3 (tiga) komponen, yakni teknologi, proses, dan manusia. Berbagai kemudahan diciptakan seiring dengan perkembangan Teknologi Informasi dan Komunikasi (TIK). Teknologi berperan sebagai *enabler* yang mempercepat terjadinya perubahan. Teknologi informasi dan komunikasi adalah salah satu contoh teknologi yang saat ini terbukti dapat memberikan perubahan gaya hidup manusia di dunia. Solusi membutuhkan perubahan proses dalam beraktivitas sehari-hari. Komponen manusia dibutuhkan karena manusialah penggerak utama perubahan proses dan yang memanfaatkan teknologi tersebut.

Dalam membangun *Smart City*, terlebih dahulu suatu kota/kabupaten harus memiliki Kesiapan Daerah Pintar atau *Smart City Readiness*. Terdapat beberapa elemen utama dalam kesiapan daerah pintar, yaitu potensi alam *(nature)*, struktur daerah *(structure),* infrastruktur *(infrastructure)* dan suprastruktur *(superstructure)*. Kerangka pikir berikutnya dari sebuah *Smart City* adalah dimensi-dimensi yang terdapat di dalam *Smart City* itu sendiri. Kerangka pikir Pontianak *Smart City* adalah menjadikan Kota Pontianak Kota yang pintar dengan berbagai elemen dan dimensi *smart city* yang telah digariskan serta menyelaraskannya dengan visi misi pembangunan daerah, program dan rencana pembangunan daerah yang telah disusun,

mulai dari RPJPD Kota Pontianak, RPJMD Kota Pontianak, RTRW Kota Pontianak dan dokumen lainnya yang mendukung tercapainya Pontianak Smart City.

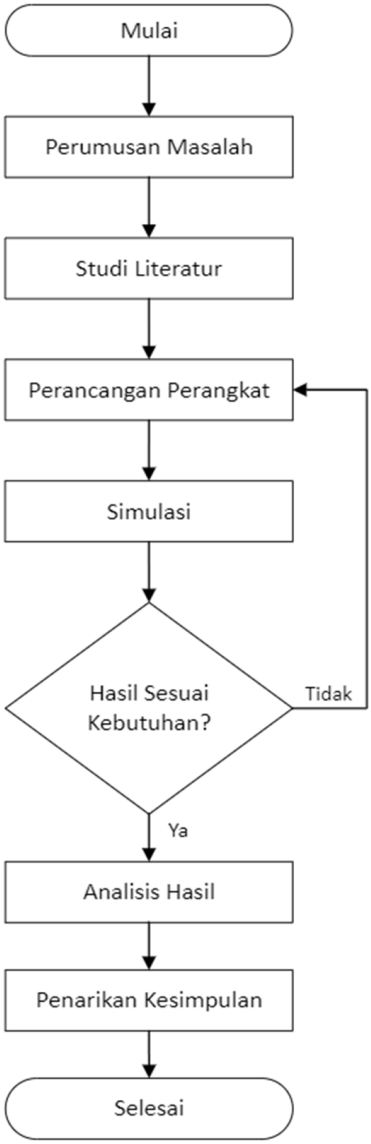
Pembangunan Pontianak *Smart City*, selain harus menjawab permasalahan kota Pontianak juga harus menghadirkan solusi yang berkelanjutan. Untuk itu kerjasama diantara pihak pemerintah, swasta, dan publik adalah sebuah keharusan untuk menjamin keberhasilan Pontianak *Smart City* [2]. Dalam upaya membantu pemerintah dalam pembangunan *smart city,* penulis ingin memberikan sedikit kontribusi dalam hal keamanan jaringan nirkabel yang ada di Kota Pontianak. Karena salah satu sumber utama tingginya pengguna *internet* di Kota Pontianak berasal dari pengguna jaringan nirkabel atau *Wi-Fi* pada area perkantoran, kampus, sekolah, café, bahkan perumahan. Hal tersebut dikarenakan jaringan nirkabel memberikan kemudahan sebagai sarana untuk saling bertukar informasi. Apalagi informasi yang bisa diakses melalui *Laptop*, *Smartphone*, *tablet* dan lain sebagainya. Seiring dengan kemudahan yang diberikan, jaringan nirkabel juga diikuti dengan ancaman siber. Sifat *Broadcast* dari jaringan nirkabel dapat memberikan resiko adanya celah bagi penyusup untuk mendapatkan akses yang tidak sah terhadap jaringan nirkabel, yang mana dapat menyebabkan data yang dipertukarkan melalui jaringan nirkabel menjadi rusak atau bahkan dimodifikasi.

Meskipun teknologi keamanan jaringan nirkabel seperti *WPA* dan *WPA2* sudah tersedia untuk mengamankan jaringan nirkabel *(IEEE 802.11)* namun teknologi tersebut tidak selalu digunakan, bahkan tidak jarang ada jaringan nirkabel yang tidak menggunakan keamanan sama sekali atau *Open Network*. Hal ini terjadi dikarenakan kurangnya kesadaran akan keamanan jaringan terutama pada informasi yg beredar di jaringan nirkabel. Penelitian ini bertujuan untuk menghasilkan data yang nantinya akan diinformasikan kepada para pihak yang berkepentingan untuk mendukung Pelaksanaan Sistem Pemerintahan Berbasis Elektronik Kota Pontianak, yang mana Teknologi Informasi dan Komunikasi menjadi salah salah satu aspek, yaitu aspek 5 dan indikator 23 nomor 35, yaitu "Melakukan perencanaan, pembangunan, pemeliharaan dan/atau pengembangan jaringan intra pemerintah menggunakan Fiber Optik yang tertuang dalam Peta Rencana Sistem Pemerintahan Berbasis Elektronik [3].

Hasil penelitian ini juga dapat dimanfaatkan untuk mendukung pembangunan Kota Pontianak sebagai *Smart City,* yang mana hal ini menjadi salah satu poin dari pengembangan lanjutan pembangunan *Smart Governance,* yang merupakan salah satu point dari Strategi Pembangunan Pontianak *Smart City* yang diatur dalam PERATURAN WALIKOTA PONTIANAK NOMOR 25 TAHUN 2019 TENTANG MASTERPLAN PONTIANAK SMART CITY TAHUN 2019-2029 [2].

2. METODE

Penelitian ini menggunakan pendekatan kombinasi antara metode empiris dan simulasi komputer untuk menganalisis kinerja dan keamanan jaringan. Adapun tahapan yang digunakan pada penelitian ini akan dijelaskan pada gambar dibawah ini:



Gambar 1. Alur Metodologi Penelitian

2.1 Perancangan Perangkat

Sebelum melakukan *wardriving,* penulis akan melakukan perancangan perangkat untuk melakukan kegiatan *wardriving* terlebih dahulu. Adapun perangkat yang akan digunakan, yaitu Raspberry Pi, Globalsat USB, USB *Wireless Receiver,* Modem WiFi *Portable,* kabel UTP dan *Powerbank*. Sedangkan perangkat lunak yang digunakan untuk melakukan kegiatan *wardriving* ini adalah Juice SSH dan Kismet

2.2 Analisis Hasil

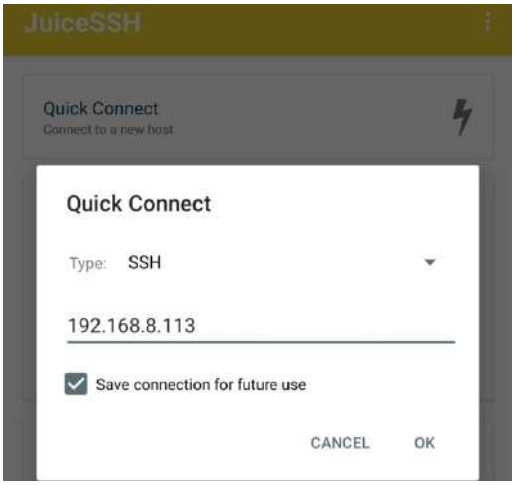
Setelah kegiatan *wardriving* berhasil dilakukan, maka langkah selanjutnya adalah melakukan analisis terhadap hasil dari kegiatan *wardriving* yang telah dilakukan. Kegiatan *wardriving* ini akan menghasilkan *capture* dari semua jaringan nirkabel yang terpasang di sepanjang area yang dilalui penulis pada rute *wardriving.* Adapun hasil yang akan didapat dari proses analisis adalah jumlah SSID yang terdeteksi, persentase jaringan nirkabel yang sudah mengaktifkan protokol keamanan *no encryption* WEP, WPA, WPA2 dan WPA3 dan persentase *channel* yang digunakan oleh setiap SSID yang terdeteksi.

3. HASIL DAN PEMBAHASAN

Pada tanggal 1 Juni 2023 pukul 11.40 WIB penulis melakukan sebuah simulasi *wardriving* dengan cara mengendarai sepeda motor dengan kecepatan 15 hingga 20 km/jam di sepanjang rute *wardriving* yang telah ditentukan yang berakhir pada pukul 12.16 WIB. Berikut adalah langkah-langkah dan hasil penelitian yang telah dilakukan.

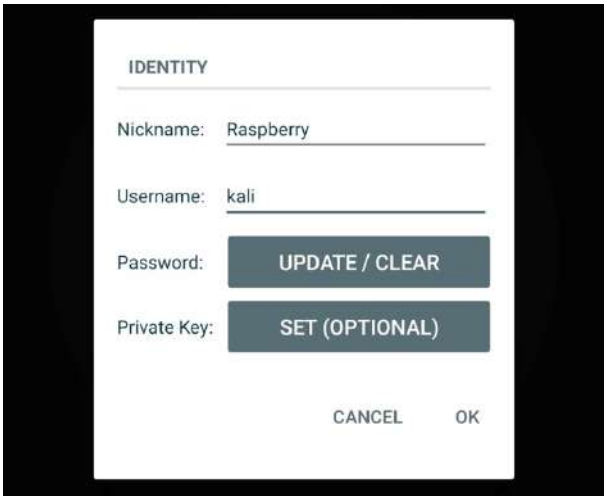
3.1 Simulasi

Setelah perancangan perangkat berhasil dilakukan, maka langkah selanjutnya adalah melakukan simulasi di sepanjang rute *wardriving* yang telah ditentukan. Langkah pertama dalam melakukan simulasi adalah menyiapkan dan menghubungkan *smartphone* dengan *wardriving rig*. Proses konfigurasi JuiceSSH untuk menghubungkan *smartphone* dengan *wardriving rig* disajikan pada gambar 2.



Gambar 2. Konfigurasi IP JuiceSSH

Pada gambar 2 di atas menggambarkan tampilan konfigurasi JuiceSSH dimana informasi *wardriving rig* yang perlu dimasukan adalah *IP Address* dari *wardriving rig,* yaitu 192.168.8.113 dan *connection type,* yaitu SSH. Setelah *IP address* dan *connection type* berhasil dimasukan, maka langkah selanjutnya adalah melakukan konfigurasi identitas untuk terhubung dengan *wardriving rig.* Konfigurasi identitas disajikan pada gambar 2.

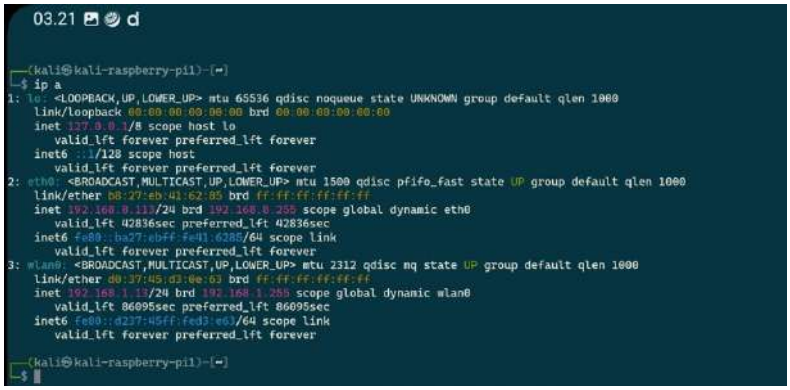


Gambar 3. Konfigurasi Identitas

Pada Gambar 3 di atas menggambarkan konfigurasi identitas untuk menghubungkan JuiceSSH dengan *wardriving rig*, yaitu Nickname yang bisa diisi sesuai keinginan, kemudian Username dan Password yang harus diisi dengan *username* dan *password* akun pada Kali Linux. Tampilan saat konfigurasi JuiceSSH berhasil dilakukan disajikan pada gambar 3.

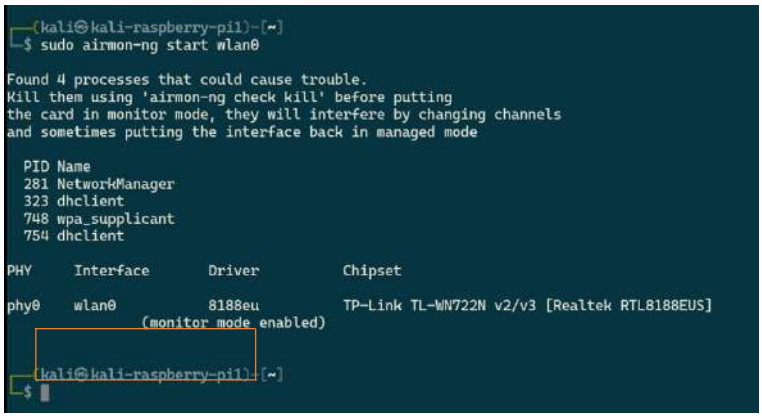
Gambar 4. Tampilan JuiceSSH Berhasil Terhubung

Pada gambar 4 di atas menggambarkan tampilan JuiceSSH saat berhasil terhubung dengan *wardriving rig.* Setelah JuiceSSH berhasil terhubung dengan *wardriving rig,* maka langkah selanjutnya adalah melakukan pengecekan nama *interface* USB *wireless receiver* pada *wardriving rig* dengan memberikan perintah ”ip a” pada terminal. Tampilan *interfaces* pada *wardriving rig* disajikan pada gambar 4.



Gambar 5. Tampilan Interfaces pada Wardriving Rig

Pada gambar 5. di atas menampilkan *interfaces* pada *wardriving rig*. Berdasarkan informasi pada gambar 4.4 diketahui bahwa *interface* USB *wireless receiver* adalan wlan0. Setelah *interface* USB *wireless receiver* diketahui, maka langkah selanjutnya adalah melakukan konfigurasi terhadap USB *wireless receiver* menjadi *monitoring mode* dengan memberikan perintah ”sudo airmon-ng start wlan0” pada terminal. Tampilan konfigurasi USB *wireless receiver* menjadi *monitoring mode* disajikan pada gambar 5.



Gambar 6. Konfigurasi USB Wireless Receiver menjadi Monitoring Mode

Pada gambar 6. di atas menggambarkan tampilan konfigurasi USB *wireless receiver* menjadi *monitoring mode*. Setelah konfigurasi USB *wireless receiver* menjadi *monitoring mode* berhasil dilakukan, maka langkah selanjutnya adalah membuat sebuah *folder* untuk menyimpan *file wardriving.* Dalam hal ini penulis membuat sebuah *folder* dengan nama "simulasi" dengan memberikan perintah "mkdir simulasi" pada terminal. Setelah *folder* untuk menyimpan *file wardriving* berhasil dibuat, maka langkah selanjutnya adalah menjalankan aplikasi kismet dengan memberikan perintah "kismet -c wlan0" pada terminal di *folder* yang sudah dibuat untuk menyimpan *file wardriving*. Tampilan saat aplikasi Kismet dijalankan disajikan pada gambar 6.

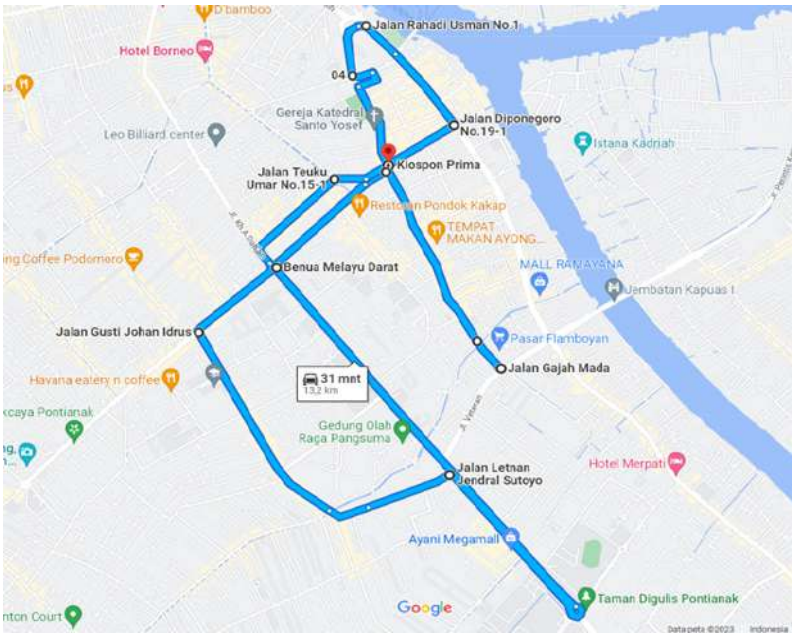
Gambar 7. Tampilan saat Aplikasi Kismet dijalankan

Pada gambar 7 di atas menggambarkan tampilan saat aplikasi Kismet dijalankan dimana terdapat beberapa informasi yang tercantum, yaitu USB *wireless receiver,* GPS *Module* dan aplikasi Kismet berhasil dijalankan.

3.2 *Wireless Scanning*

Setelah proses wireless scanning berhasil dilakukan, maka ditemukan persentase keamanan jaringan dan channel yang digunakan oleh setiap SSID yang berhasil di-capture di

sepanjang rute wardriving. Berikut ini adalah penjelasan mengenai hasil dari penelitian yang telah dilakukan. Berdasarkan hasil dari *wireless scanning* yang telah dilakukan, penulis menemukan sebanyak 2.333 SSID disepanjang rute *wardriving.* Rute *wardriving* disajikan pada gambar 8.



Gambar 8. Rute Wardriving

3.2.1 Jalan Gajah Mada

Wireless scanning yang dilakukan berhasil membaca sebanyak 728 SSID yang ada di sepanjang Jalan Gajah Mada. terdapat sebanyak 84% atau 610 SSID sudah menerapkan keamanan WPA2, 1% atau 10 SSID menerapkan keamanan WPA dan 15% atau 108 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Gajah Mada sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Gajah Mada memiliki kesadaran keamanan informasi yang cukup tinggi

3.2.2 Jalan H. Agus Salim

Wireless scanning yang dilakukan berhasil membaca sebanyak 31 SSID yang ada di sepanjang Jalan H. Agus Salim. Menginformasikan bahwa terdapat sebanyak 97% atau 30 SSID sudah menerapkan keamanan WPA2, 3% atau 1 SSID menerapkan keamanan WPA dan tidak ditemukan SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan H. Agus Salim sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan H. Agus Salim memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.3 Jalan Gusti Sulung Lelanang

Wireless scanning yang dilakukan berhasil membaca sebanyak 147 SSID yang ada di sepanjang Jalan Gusti Sulung lelanang. Menginformasikan bahwa terdapat sebanyak 82% atau 120 SSID sudah menerapkan keamanan WPA2, 2% atau 3 SSID menerapkan keamanan WPA

dan 16% atau 24 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Gusti Sulung Lelanang sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Gusti Sulung Lelanang memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.4 Jalan Jenderal Ahmad Yani

Wireless scanning yang dilakukan berhasil membaca sebanyak 532 SSID yang ada di sepanjang Jalan Jenderal Ahmad Yani. menginformasikan bahwa terdapat sebanyak 82% atau 434 SSID sudah menerapkan keamanan WPA2, 1% atau 3 SSID menerapkan keamanan WPA dan 17% atau 95 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Jenderal Ahmad Yani sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Jenderal Ahmad Yani memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.5 Jalan Lenan Jendral Sutoyo

Wireless scanning yang dilakukan berhasil membaca sebanyak 81 SSID yang ada di sepanjang Jalan Letnan Jendral Sutoyo. menginformasikan bahwa terdapat sebanyak 82% atau 66 SSID sudah menerapkan keamanan WPA2, 1% atau 1 SSID menerapkan keamanan WPA dan 17% atau 14 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Letnan Jendral Sutoyo sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Letnan Jendral Sutoyo memiliki kesadaran keamanan informasi yang cukup tinggi

3.2.6. Jalan Moh. Sohor

Wireless scanning yang dilakukan berhasil membaca sebanyak 193 SSID yang ada di sepanjang Jalan Moh. Sohor. Menginformasikan bahwa terdapat sebanyak 91% atau 176 SSID sudah menerapkan keamanan WPA2, 1% atau 1 SSID menerapkan keamanan WPA dan 8% atau 16 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Moh. Sohor sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Moh. Sohor memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.7 Jalan Slt. Abdurrahman

Wireless scanning yang dilakukan berhasil membaca sebanyak 186 SSID yang ada di sepanjang Jalan Slt. Menginformasikan bahwa terdapat sebanyak 82% atau 153 SSID sudah menerapkan keamanan WPA2, 1% atau 2 SSID menerapkan keamanan WPA dan 17% atau 31 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Slt. Abdurrahman sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Slt. Abdurrahman memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.8. Jalan Kh. Ahmad Dahlan

Wireless scanning yang dilakukan berhasil membaca sebanyak 9 SSID yang ada di sepanjang Jalan Kh. Ahmad Dahlan. Menginformasikan bahwa terdapat sebanyak 100% atau 9 SSID sudah menerapkan keamanan WPA2 dan tidak terdapat SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Kh. Ahmad Dahlan sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Kh. Ahmad Dahlan memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.9 Jalan Teuku Umar

Wireless scanning yang dilakukan berhasil membaca sebanyak 98 SSID yang ada di sepanjang Jalan Teuku Umar. Menginformasikan bahwa terdapat sebanyak 97% atau 95 SSID sudah menerapkan keamanan WPA2, 1% atau 1 SSID menerapkan keamanan WPA dan 2% atau 2 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Teuku Umar sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Teuku Umar memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.10 Jalan Hos Cokroaminoto

Wireless scanning yang dilakukan berhasil membaca sebanyak 32 SSID yang ada di sepanjang Jalan Hos Cokroaminoto. Menginformasikan bahwa terdapat sebanyak 94% atau 30 SSID sudah menerapkan keamanan WPA2 dan terdapat 6% atau 2 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Hos Cokroaminoto sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Hos Cokroaminoto memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.11 Jalan Diponegoro

Wireless scanning yang dilakukan berhasil membaca sebanyak 87 SSID yang ada di sepanjang Jalan Diponegoro. Menginformasikan bahwa terdapat sebanyak 99% atau 86 SSID sudah menerapkan keamanan WPA2 dan terdapat 1% atau 1 SSID yang menerapkan keamanan WPA. Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Diponegoro sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Diponegoro memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.12 Jalan Tanjung Pura

Wireless scanning yang dilakukan berhasil membaca sebanyak 95 SSID yang ada di sepanjang Jalan Tanjung Pura. Menginformasikan bahwa terdapat sebanyak 94% atau 89 SSID sudah menerapkan keamanan WPA2 dan terdapat 1% atau 1 SSID yang menerapkan keamanan WPA dan terdapat 5% atau 5 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Tanjung Pura sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan

nirkabel di sepanjang Jalan Tanjung Pura memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.13 Jalan Rahadi Usman

Wireless scanning yang dilakukan berhasil membaca sebanyak 23 SSID yang ada di sepanjang Jalan Rahadi Usman. Menginformasikan bahwa terdapat sebanyak 100% atau 23 SSID sudah menerapkan keamanan WPA2 dan tidak ditemukan SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Rahadi Usman sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Rahadi Usman memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.14 Jalan Zainuddin

Wireless scanning yang dilakukan berhasil membaca sebanyak 20 SSID yang ada di sepanjang Jalan Zainuddin. Menginformasikan bahwa terdapat sebanyak 100% atau 20 SSID sudah menerapkan keamanan WPA2 dan tidak ditemukan SSID yang tidak menerapkan keamanan atau *open network.*. Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Zainuddin sudah menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Zainuddin memiliki kesadaran keamanan informasi yang cukup tinggi.

3.2.15. Jalan Nusa Indah Baru

Wireless scanning yang dilakukan berhasil membaca sebanyak 9 SSID yang ada di sepanjang Jalan Nusa Indah Baru. Menginformasikan bahwa terdapat sebanyak 56% atau 9 SSID sudah menerapkan keamanan WPA2 dan ditemukan 44% atau 4 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Nusa Indah Baru belum cukup menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Nusa Indah Baru memiliki kesadaran keamanan informasi yang menengah.

3.2.16 Jalan Patimura

Wireless scanning yang dilakukan berhasil membaca sebanyak 63 SSID yang ada di sepanjang Jalan Patimura. Menginformasikan bahwa terdapat sebanyak 90% atau 57 SSID sudah menerapkan keamanan WPA2, 5% atau 3 SSID yang menggunakan keamanan WPA dan terdapat 3% atau 3 SSID yang tidak menerapkan keamanan atau *open network.* Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan nirkabel di sepanjang Jalan Patimua belum cukup menerapkan keamanan WPA2. Dengan kata lain, pengguna jaringan nirkabel di sepanjang Jalan Patimura memiliki kesadaran keamanan informasi yang tinggi

3.3. *Network Mapping*

Hasil dari *wireless scanning* kemudian dipetakan ke dalam Google Earth dengan cara melakukan konfersi *file* .kismet ke *file* .csv terlebih dahulu dengan memberikan perintah "kismetdb_to_wiglecsv -i nama_file_yang_ingin_dikonfersi -o nama_file_output.csv" pada terminal, kemudian *file* .csv akan dikonfersi ke *file* .kml. menggunakan aplikasi CSV to KML

Online Converter. Setelah *file* .kismet berhasil dikonfersi menjadi *file* .kml maka *file* tersebut sudah bisa dibuka menggunakan aplikasi Google Earth untuk dipetakan.

4. KESIMPULAN

Berdasarkan hasil *wardriving* yang telah disajikan pada bab 4, persentase keamanan jaringan yang sudah diterapkan, yaitu dari 2.333 SSID yang berhasil di-*capture* di sepanjang rute *wardriving,* terdapat 86% SSID yang sudah menggunakan keamanan WPA2, 13% SSID tidak menggunakan keamanan atau *open network,* 1% SSID menggunakan keamanan WPA dan tidak ditemukan SSID yang menggunakan keamanan jaringan WEP.

Dalam hal pemilihan *channel* jaringan nirkabel, dari total 2.333 SSID yang berhasil di-*capture,* mayoritas jaringan nirkabel sudah mulai seragam dalam hal pemilihan *channel* jaringan nirkabel, yaitu sebanyak 1.589 atau 68% SSID jaringan nirkabel sudah menggunakan grup *channel* jaringan nirkabel 1, 6 dan 11, sebanyak 254 atau 11% SSID menggunakan kelompok *channel* jaringan 2, 7 dan 12, sebanyak 212 atau 9% SSID menggunakan kelompok *channel* jaringan 3, 8 dan 13. Berdasarkan data tersebut, terdapat 2055 atau 88% SSID sudah menggunakan kelompok *channel* yang direkomendasikan dan terdapat 278 atau 12% SSID belum menggunakan kelompok *channel* yang direkomendasikan.

Berdasarkan data diatas, dapat ditarik kesimpulan bahwa keamanan jaringan nirkabel yang ada di Kota Pontianak dinilai sudah cukup baik karena sudah sesuai dengan standar IEEE 802.11i, yaitu tentang peningkatan pengamanan pada jaringan nirkabel menggunakan WPA2 dan penilaian kinerja jaringan nirkabel di Kota Pontianak juga dinilai sudah cukup baik karena sudah menggunakan kelompok *channel* yang dapat mengurangi kemungkinan interferensi

REFERENSI

[1] Pontianak Informasi. (2021, 12 15). *Kota Pontianak Terima Penghargaan Smart City Kategori Smart Branding dari Kemenkominfo RI*. Dipetik Mei 15, 2023, dari Pontianak Informasi: https://pontianakinformasi.co.id/lokal/bangga-kota-pontianak-terima-penghargaan-smart-city-kategori-smart-branding-dari-kemenkominfo-ri/

[2] Mulyadi. (2013, Maret 12). MASTERPLAN PONTIANAK SMART CITY TAHUN 2019-2028. Pontianak, Kalimantan Barat, Indonesia. Dipetik Mei 15, 2023

[3] Admin SPBE. (2021, Agustus 12). *Peta Rencana SPBE*. Dipetik Juli 23, 2023, dari Website Resmi SPBE Kota Pontianak: https://spbe.pontianak.go.id/artikel/peta-rencana-spbe

[4] Asnawi, M. F., & Nugroho, M. A. (2022). PENGUJIAN KEAMANAN JARINGAN MENGGUNAKAN METODE PENETRASI TES PADA JARINGAN SMK MUHAMMADIYAH 1 WONOSOBO. *Jurnal DEVICE*, 160-168. Dipetik Juli 20, 2023

[5] Darwis, M. (2020). Penambahan Fitur Tampilan LCD dan Micro SD Card Reader pada mesin Laser Engraver and Cutter di Laboratorium Pengemudian Listrik. *Jurnal Pengelolaan Laboratorium Pendidikan*, 8-18. Dipetik Juli 20, 2023

[6] Desmira, & Wiryadinata, R. (2022). Rancang Bangun Keamanan Port Secure Shell (SSH). *Jurnal Ilmu Komputer dan Sistem Informasi*, 28-33. Dipetik Juli 20, 2023

[7] Dinata, A. (2022, Oktober 28). *Jaringan Nirkabel: Pengertian, Sejarah, Cara Kerja dan Manfaat*. Dipetik November 20, 2022, dari TEKNOVIDIA: https://www.teknovidia.com/jaringan-nirkabel-adalah/

[8] Fajri, A. (2019). STUDI EMPIRIS TERHADAP KINERJA & KEAMANAN WIFI (STUDI KASUS DI KOTA DEPOK). *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 671-676. Dipetik November 20, 2022

[9] Fatimah. (2022). Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing

di Universitas PGRI Sumatra Barat. *Jurnal Teknologi Informasi*, 7-11. Dipetik Juli 20, 2023

[10] Hypernet. (2020, Juli 7). *Fungsi Dan Cara Kerja WIFI Router Untuk Bisnis*. Dipetik November 22, 2022, dari hypernet.co.id: https://hypernet.co.id/id/2020/07/07/fungsi-dan-cara-kerja-wifi-router-untuk-bisnis/