Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.20196832
Vol. 6, No. 6, Desember 2019, hlm. 671-676 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018 e-ISSN: 2528-6579

STUDI EMPIRIS TERHADAP KINERJA & KEAMANAN WIFI (STUDI KASUS DI KOTA DEPOK)

Ahmad Fajri[1]
[1]Puskajibang Tekkamsisan, Badan Siber dan Sandi Negara
Email : [1]ahmad.fajri@bssn.go.id

(Naskah masuk: 25 Februari 2019, diterima untuk diterbitkan: 25 April 2019)

Abstrak

Pada tahun 2012, Kota Depok memperoleh penghargaan sebagai kota *Information and Communication Technology* (ICT) dari Kementerian Komunikasi dan Informatika. Salah satu parameter berkembangnya ICT di Kota Depok adalah meningkatnya jumlah pengguna internet dari berbagai sektor terutama perkantoran, hotel dan kampus dengan memanfaatkan jaringan *wifi* sebagai media transmisinya. Pada penelitian ini, kami melakukan audit terhadap keamanan jaringan *wifi* di Kota Depok dengan cara melakukan studi lapangan kinerja dan keamanan jaringan *wifi* menggunakan teknik *wardriving*. Studi ini mencakup sekitar 536 jaringan *wifi* di Jalan Margonda Depok. Hasil studi tersebut, kami menemukan bahwa 89% jaringan *wifi* menerapkan keamanan dengan menggunakan protokol WPA/WPA2, 1% menggunakan protokol WEP dan 10% bersifat terbuka. Kami juga menemukan sebanyak 20% jaringan *wifi* berada pada *channel* 1 dan 19% jaringan *wifi* berada pada *channel* 6 dan 11. *Channel* 1, 6 dan 11 merupakan *channel* yang terbaik bagi penggunaan jaringan *wifi* karena terbebas dari interferensi jaringan *wifi* lainnya. Oleh karena itu penilaian kinerja dan keamanan jaringan *wifi* di Kota Depok dinilai sudah baik sesuai dengan standar IEEE 802.11i yaitu tentang peningkatan pengamanan pada jaringan *Wifi* menggunakan WPA2 dan 802.11b tentang pengaturan *channel wifi* yang tidak menimbulkan interferensi.

Kata kunci : *ICT, Wifi, WPA2, WPA, WEP*

EMPIRICAL STUDY ON WIFI PERFORMANCE & SECURITY (CASE STUDY IN DEPOK CITY)

Abstract

In 2012, Depok City was awarded as the city of Information and Communication Technology (ICT) from the Ministry of Communication and Information Technology. One of the parameters of the development of ICT in Depok City is the increasing number of internet users from various sectors, especially offices, hotels and campuses by utilizing wifi networks as the transmission media. In this study, we conducted an audit of the security of wifi networks in Depok City by conducting field studies on the performance and security of wifi networks using wardriving techniques. This study covers about 536 wifi networks on Margonda Street Depok. The results of the study, we found that 89% of wifi networks implement security using the WPA / WPA2 protocol, 1% using the WEP protocol and 10% are open. We also found that as much as 20% of the wifi networks are on channel 1 and 19% of wifi networks are on channels 6 and 11. Channel 1, 6 and 11 are the best channels for using wifi networks because they are free from interference from other wifi networks. Therefore, performance assessment and wifi network security in Depok City are considered to be good in accordance with the IEEE 802.11i standard which is about increasing security on Wifi networks using WPA2 and 802.11b regarding wifi channel settings that do not cause interference.

Keywords : *ICT, Wifi, WPA2, WPA, WEP*

1. PENDAHULUAN

Kota Depok merupakan salah satu kota yang memperoleh penghargaan ICT pura dari Kementerian Komunikasi dan Informatika pada tahun 2012 karena dinilai berhasil dalam penerapan aplikasi Teknologi Informasi dan Komunikasi dengan kategori muda (Depok, 2012). Empat tahun kemudian, pada Tahun 2016 Kota Depok memperoleh peringkat ke-5 di Indonesia sebagai kota dengan penggunaan internet tertinggi setelah Jakarta, Surabaya, Bekasi dan Bandung (Depok, 2016).

Sumber utama tingginya pengguna internet di Kota Depok berasal dari pengguna jaringan *wifi* pada

area perkantoran, hotel, cafe, sekolah, kampus bahkan perumahan. Hal tersebut dikarenakan jaringan *wifi* memberikan kemudahan untuk dimanfaatkan sebagai sarana bertukar informasi. Bagaimanapun juga kemudahan penggunaan jaringan *wifi* diikuti dengan ancamana keamanan siber. Sifat *broadcast* dari *wifi* dapat memberikan risiko adanya penyusup yang dapat memperoleh akses yang tidak sah, sehingga menyebabkan data yang dipertukarkan rusak atau bahkan dimodifikasi.

Meskipun teknologi WPA dan WPA2 sudah tersedia untuk mengamankan jaringan *wifi* (IEEE 802.11) namun teknologi tersebut tidak selalu digunakan terutama karena kurangnya kesadaran akan keamanan informasi. Dalam hal kinerja penting untuk memaksimalkan kinerja *wifi* di Kota Depok dalam menghadapi era ekonomi digital. Sehingga jaringan *wifi* direkomendasikan berada pada *channel* 1, 6 atau 11 meskipun jaringan *wifi* secara *default* dapat beroperasi pada *channel* 1-11 (IEEE 802.11).

Studi empiris pada penelitian ini bertujuan untuk menghasilkan data yang akan diinformasikan kepada para pihak yang berkepentingan untuk mendukung Kota Depok sebagai kota *smart city* (Detik, 2018), selain itu hasil studi empiris ini juga dapat dimanfaatkan untuk melakukan perbaikan keamanan dan kinerja jaringan *wifi* di Kota Depok.

Metode penelitian yang digunakan pada studi empiris ini terdiri atas perancangan *tools* untuk audit kinerja dan keamanan jaringan *wifi* dan *wardriving*.

2. STUDI PUSTAKA

IEEE 802.11 merupakan seperangkat aturan spesifikasi teknis dalam mengimplementasikan jaringan WLAN. *Institute of Electrical and Electronic Engineering* (IEEE) sejak berdirinya pada tahun 1997 telah menciptakan beberapa standar yang dinamakan IEEE 802.11 kedalam beberapa versi yaitu standar implementasi jaringan *wireless* yang menangani berbagai jenis komunikasi. Pada tahun 1999 sekelompok vendor yang bergerak pada bidang peralatan *wireless* mengembangkan perangkat *wireless* yang sesuai dengan standar yang ditetapkan oleh IEEE 802.11 yang pada awal mula mereka menamakan diri sebagai *Wireless Ethernet Compatibility Alliance* (WECA) kemudian diganti menjadi *Wifi Alliance* hingga saat ini.

2.1 Wifi Security

Wifi Alliance sejak berdirinya hingga saat ini telah mengeluarkan 3 rekomendasi keamanan pada jaringan *wifi, yaitu* WEP, WPA dan WPA2.

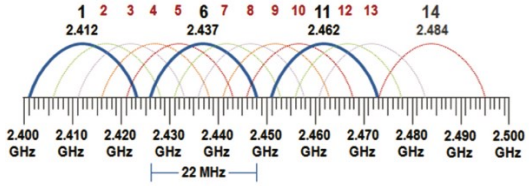
Protokol WEP diperkenalkan pada tahun 1999 oleh *Wifi Alliance*, dua tahun berjalan protokol ini dianggap sudah tidak aman lagi karena pada tahun 2001 salah satu grup riset di *University of California* yaitu Fluhrer, Mantin dan Shamir berhasil menemukan celah keamanan pada protokol WEP, celah keamanan tersebut didapatkan dengan memanfaatkan kelemahan dari metode *key scheduling algorithm RC4*, sehingga pada Tahun 2003 protokol WEP secara resmi digantikan dengan protokol WPA.

Protokol WPA merupakan perbaikan dari protokol WEP, WPA menambahkan fungsi TKIP pada algoritma RC4, dengan adanya penambahan TKIP maka serangan pada algoritma WEP tidak akan berhasil jika diterapkan pada algoritma WPA, karena telah menghasilkan 128 bit untuk setiap paket dinamisnya. Pada algoritma WPA juga terdapat fungsi tambahan *integrity check algorithm* yaitu *Messege Integrity Code* yang berfungsi sebagai perbaikan dari algoritma CRC-32 pada protokol WEP.

Wifi Protected Access versi2 (WPA2) adalah sebuah protokol kriptografi yang berfungsi untuk mengamankan jaringan *wireless.* WPA2 diperkenalkan oleh *Wifi Alliance* pada tahun 2004, WPA2 memenuhi persyaratan standar yang ditetapkan oleh IEEE 802.11i. Dalam metode pengamanan WPA2 menggunakan algoritma AES sebagai proses enkripsi dan CBC-MAC sebagai proses enkripsi *traffic* pada jaringan dan melindungi integritas data.

2.2 *Wifi channels*

Wifi channels merupakan pengelompokan *channel* pada *wifi* berdasarkan panjang gelombang radio dan *frequency* yang digunakan. Terdapat 14 jenis *wifi channel* untuk jaringan *wifi* dimana masing-masing *channel* memiliki *frequency* dan panjang gelombang yang berbeda-beda. Berdasarkan pada teori rumusan panjang gelombang bahwa semakin kecil *frequency* sebuah gelombang maka semakin besar panjang gelombangnya sehingga semakin jauh jangkauannya. Pemilihan dan penentuan *channel* pada jaringan *wifi* sangatlah penting diantaranya karena, pemilihan dan pengaturan *channel* yang tepat akan meningkatkan daya jangkau sinyal *wifi* dan mencegah terjadinya interferensi. Pengelompokkan *wifi channels* disajikan pada Gambar 1.



Gambar 1. *Wifi channels*

Penggunaan *wifi channel* yang tidak tepat akan menimbulkan interferensi, sebagai contoh jika jaringan A menggunakan *channel* 6, sedangkan jaringan B menggunakan *channel* 8, maka akan terjadi interferensi yang akan berdampak pada gangguan sinyal gelombang elektromagnet yang disebabkan oleh sinyal lain sehingga kinerja *wifi* tidak maksimal.

3. METEDOLOGI

Metode penelitian yang diguanakan pada penelitian ini adalah perancangan *tools* dan *wardriving.*

3.1 Perancangan perangkat

Perangkat keras yang digunakan untuk melakukan kegitan *wardriving* yaitu, *raspberry pi, globalsat USB, micro sd, alfa network* dan *power bank.*

a. *Raspberry Pi* merupakan *sebuah SBC (Single Board Computer)* atau mini komputer yang memiliki dimensi kecil. Dalam perkembangannya, *raspberry pi* kini telah mencapai generasi ketiga. Sebagai mini komputer *raspberry pi* memiliki spesifikasi yang mirip dengan komputer biasa seperti *micro SD* sebagai media penyimpanan, *USB port, ethernet port, wireless LAN, bluetooth* dan sebagainya. *raspberry pi* menggunakan arsitektur CPU ARMv8 *quad core.*
b. *Globalsat USB* merupakan sebuah perangkat yang berfungsi untuk melakukan pencatatan posisi koordinat bumi *(network mapping)* dari hasil *wireless scanning.* Hasil koordinat yang didapat dari perangkat *globalsat USB* hanyalah lokasi relatif dari *access point,* tidak menunjukkan lokasi yang absolut dimana *access point* ditempatkan.
c. *Micro sd* merupakan sebuah perangkat yang berfungsi sebagai media penyimpanan pengganti dari *hadrdisk* pada sebuah komputer.
d. *Alfa network* merupakan *external USB wireless* yang berfungsi untuk *monitoring* jaringan *wifi (wireless scanning),* fungsi dari *alfa network* adalah sebagai perangkat untuk menjalankan fungsi kismet.
e. *Powerbank* berfungsi sebagai *power supply* untuk perangkat *Raspberry Pi*.

Sedangkan perangkat lunak yang digunakan untuk melakukan kegiatan *wardriving* adalah *juiceSSH* dan *kismet.*

a. *JuiceSSH* berfungsi untuk melakukan fungsi *ssh* ke dalam perangkat *raspberry pi. JuiceSSH* merupakan perangkat lunak yang dapat diinstall pada perangkat pribadi *(handgphone)*.
b. Kismet adalah suatu program untuk mendeteksi jaringan *wireless* yang bekerja pada layer 2 *data link* dengan frekuensi 2,4 Ghz dan 5 Ghz. Kismet dapat bekerja menggunakan bantuan *wireless card* yang dapat menjalankan fungsi *monitoring*. Salah satu jenis *wireless card* yang *support* untuk menjalankan fungsi kismet adalah *alfa network.* Perangkat *wardriving* disajikan pada Gambar 2.

Gambar 2. Perangkat *Wardriving*

Langkah-langkah dalam melakukan perancangan *tools* adalah sebagai berikut :

a. Lakukan instalasi *software kali linux image (ARM)* ke dalam *micro sd.*
b. Lakukan instalasi *kismet* pada perangkat *raspberry pi.*
c. Lakukan konfigurasi *globalsat USB* pada *raspberrypi.*
d. Lakukan konfigurasi *alfa network,* sehingga *alfa network* berjalan dengan fungsi *monitoring.*
e. Lakukan konfigurasi *network* pada *raspberry pi,* dan *juiceSSH* sehingga berada dalam *network* yang sama.

3.2 *Wardriving*

Wardriving adalah tindakan mencari jaringan *wifi* dalam kendaraan bergerak. Kegiatan *wardriving* bertujuan untuk mengetahui kekurangan dan kelemahan jaringan *wifi* pada suatu wilayah tertentu melalui metode pemetaan lokasi. Beberapa informasi yang dapat diperoleh dari hasil kegiatan *wardriving,* yaitu menemukan *access point,* mengetahui autentikasi yang digunakan, mengetahui protokol yang digunakan dan mengetahui *client-client* yang terhubung. Langkah-langkah kegiatan *wardriving* adalah sebagai berikut :

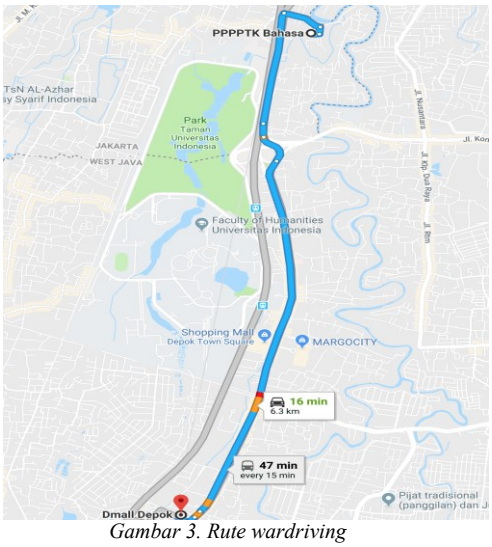
a. *Wireless scanning*
   Wireless scanning adalah kegiatan melacak keberadaan *access point* dengan cara berjalan/berkendara sesuai dengan jalur yang telah ditentukan. Ketika aplikasi *wireless scanning* menemukan sebuah *signal wireless* yang dipancarkan oleh *access point* berupa paket *beacon.* Aplikasi ini akan mencatat nama *ssid, channel* yang digunakan, kecepatan transmisi dan posisi koordinat bumi yang didapat dari perangkat globalsat USB.
b. *Network mapping*
   Hasil dari *wireless scanning* yang telah dilakukan, selanjutnya perlu digambarkan dalam bentuk pemetaan lokasi yang dilengkapi dengan informasi mengenai letak koordinat *access point.* aplikasi yang digunakan untuk melakukan *network mapping* adalah *google earth.* Aplikasi *google earth* hanya dapat membaca file dalam

format .kml dan .kmz, sehingga *output* dari proses *wireless scanning* yang berbentuk .netxml perlu dilakukan konfersi ke dalam format .kml dan .kmz.

c. Analisis hasil *wardriving*
Hasil dari kegiatan *wardriving* akan menghasilkan *snapshot* dari semua jaringan *wireless* yang terpasang sepanjang area yang telah dikunjungi. Adapun hasil yang akan didapat dari proses analisis adalah jumlah *access point* yang terdeteksi, persentase yang mengaktifkan protokol keamanan WEP, WPA dan WPA2, jumlah *access point* dengan *hidden SSID,* persentase *channel* yang digunakan.

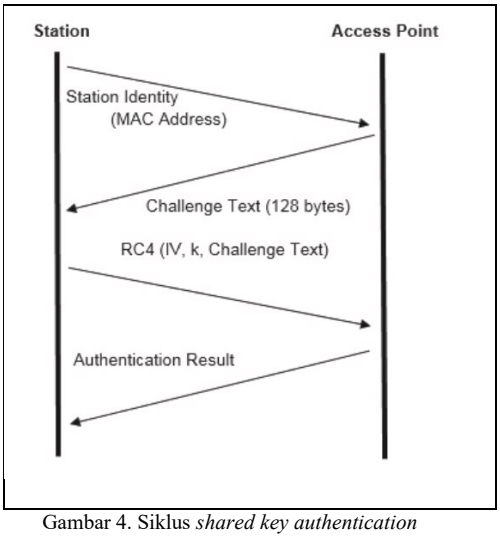
4. SIMULASI

Penulis melakukan simulasi *wireless scanning* dengan cara mengendarai sepeda motor sepanjang jalan Margonda, Depok. Dengan rute dimulai dari perbatasan Kota Depok dengan Jakarta Selatan hingga Depok Mall. Sepanjang perjalanan ditemui gedung-gedung pemerintahan, kampus, sekolah, serta banyak perusahaan-perusahaan yang bergerak dalam bidang bisnis seperti hotel, mall, dan kafe. Dalam penelitian ini kami menemukan sebanyak 536 jaringan *wifi.* Rute *wardriving* disajikan pada Gambar 3.



Gambar 3. Rute wardriving

Cara kerja *alfa network* dalam mengumpulkan data tentang jaringan disekitarnya adalah melalui dua metode yang didefinisikan pada IEEE 802.11. Metode pertama didasarkan pada *frame beacon* yang secara berkala dikirimkan oleh *access point* dengan cara *broadcast* kepada *radius* disekitarnya. Metode kedua *alfa network* secara *broadcast* mengirimkan *request frame* dan menunggu *probe response* dari *access point* yang menerima *requset.* Ketika proses *request* dan *response* berhasil dilakukan maka telah terjadi satu siklus *shared key authentication.* Seperti disajikan pada Gambar 4.



Gambar 4. Siklus *shared key authentication*

Hasil dari *wireless scanning* kemudian dipetakan ke dalam *google earth.* Yaitu dengan cara melakukan *network mapping.* Hasil dari *netwok mapping* disajikan pada Gambar 5.

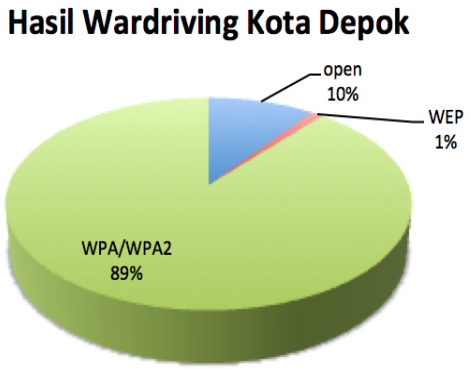
Gambar 5. Hasil *network mapping*

5. HASIL

5.1 *Wifi Security*

Pada gambar 6 menginformasikan persentase jaringan *wifi* di Kota Depok yang dikelompokan berdasarkan *security level* yang digunakan yaitu *no encryption,* WEP, WPA atau WPA2.

Berdasarkan hasil persantase tersebut, didapatkan hasil sebanyak 89% sudah menerapkan *security* WPA/WPA2, 1% menerapkan *security* WEP, 10% tidak menerapkan *security (wifi* bersifat terbuka*)*. Hal tersebut mengindikasikan bahwa mayoritas pengguna jaringan *wifi* di Kota Depok sudah menerapkan *security* WPA/WPA2.



Gambar 6. Persentase jaringan *wifi* di Kota Depok

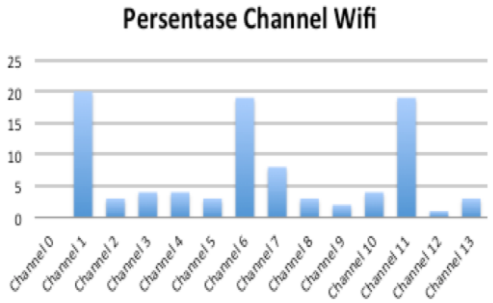
Dengan kata lain, teknisi ataupun pengguna jaringan *wifi* di Kota Depok memiliki kesadaran keamanan informasi yang cukup tinggi.

Pengguna *wifi* dengan penerapan metode keamanan WEP di Kota Depok sebesar 1%. WEP merupakan protokol enkripsi yang cukup lama. Dan sangat mudah untuk dilakukan *carcking password,* karena protokol WEP memiliki beberapa kelemahan dalam hal kunci, *initialization vector, data integrity* (yang menggunakan algoritma crc32).

Pengguna *wifi* tanpa menggunakan protokol dan algoritma enkripsi adalah sebesar 10%. Artinya siapa pun dapat mengakses jaringan *wifi* tanpa memasukkan *password.* Penggunaan *wifi* tanpa *password* pada praktiknya akan menimbulkan ancaman seperti pencurian data pribadi, bahaya penyebaran virus, iklan yang mengganggu yang dapat mengandung *malicious software* dan *snooper* atau mata-mata.

5.2 Wifi Performance

Gambar 7 menginformasikan persentase penyebaran *wifi channel* di Kota Depok.



Gambar 7. Persentase *channel wifi* di Kota Depok

Persentase tertinggi penyebaran *wifi channel* di Kota Depok adalah pada *channel* 1 sebesar 20%, *channel* 6 sebesar 19% dan *channel* 11 sebesar 19%. Tingginya penggunaan *channel* 1, 6 dan 11 pada Kota Depok merepresentasikan bahwa Kota Depok sangat memperhatikan kinerja penggunaan *wifi. Channel* 1, 6 dan 11 merupakan *channel* terbaik karena aman terhadap gangguan interferensi, sehingga kinerja *wifi* akan maksimal.

5. ANALISIS

Pengaturan penggunaan *channel wifi* di Indonesia sudah ditetapkan oleh Pemerintah melalui Peraturan Menteri Perhubungan nomor K.M 2 Tahun 2005 tentang penggunaan pita frekuensi. Pada Peraturan Menteri Perhubungan tersebut secara umum hanya memberikan batasan interval diperbolehkannya penggunaan pita frekuensi saja yaitu pada 2400-2483.5 MHz, hal tersebut mengartikan *channel wifi* yang diperbolehkan oleh pihak regulator di Indonesia kepada pihak penyedia jaringan internet yaitu antara *channel 1-13.*

Setiap negara memiliki aturan tersendiri dalam mengelola penggunaan *channel wifi* di Negaranya masing-masing. Seperti contoh, di Amerika Utara, Amerika Serikat dan Kanada hanya dapat menggunakan *channel wifi* pada *channel 1-11,* di Eropa dapat menggunakan *channel 1-13* dan di Jepang hanya dapat menggunakan *channel 14 saja.* Pengaturan dalam hal penggunaan *channel* akan berdampak pada tingkat kekuatan interferensi gelombang frekuensi *wifi*.

Kementerian Komunikasi dan Informatika baru-baru ini mengeluarkan aturan mengenai penggunaan pita frekuensi radio 2.4 GHz yang dituangkan dalam Surat Edaran Direktur Jenderal Sumber Daya dan Perangkat Pos dan Informatika nomor 595 Tahun 2018 tentang Ketentuan Penggunaan Pita Frekuensi Radio 2.4 GHz dan 5 Ghz untuk Penyedia Jaringan Internet Wifi Pada Asian Games XVIII. Pada surat edaran tersebut disebutkan bahwa *channel wifi* yang harus disediakan oleh pihak penyedia dalam mendukung kegiatan asian games yaitu *channel wifi* yang berada pada *channel* 1, 6 dan 11. Hal tersebut untuk memaksimalkan kinerja *wifi* dan menghindari adanya interferensi gelombang frekuensi *wifi* yang dapat menurunkan kualitas jaringan internet.

Oleh karena itu guna menjadikan Kota Depok sebagai kota *smart city*, maka perlu adanya suatu aturan tersendiri dari Pemerintah Kota Depok dalam hal ini, Dinas Komunikasi dan Informatika Depok dalam mengeluarkan surat edaran terkait dengan peggunaan *channel wifi.* Namun persentase penyebaran *channel wifi* di Kota Depok berdasarkan hasil penelitian sudah dapat dikatan baik, karena sebagain besar sudah berada pada *channel* 1, 6 dan 11.

6. KESIMPULAN

Berdasarkan hasil *wardriving,* Kota Depok dinilai sebagai kota yang sudah sadar akan keamanan informasi khusunya dalam penggunaan *wifi* dan siap untuk menghadapi era ekonomi digital karena persentase terbesar yaitu sebesar 89% telah menerapkan keamanan protokol WPA2. Selain itu *wifi* di Kota Depok juga memiliki kinerja yang maksimal karena mayoritas *channel wifi* yang digunakan bekerja pada *channel* 1, 6 dan 11 yang aman dari adanya interferensi.

Oleh karena itu penilaian keamanan jaringan *wifi* di Kota Depok dinilai sudah baik karena sudah sesuai dengan standar IEEE 802.11i yaitu tentang peningkatan pengamanan pada jaringan *Wifi* menggunakan WPA2 dan penilaian kinerja jaringan *wifi* di Kota Depok juga dinilai sudah baik karena sesuai dengan standar IEEE 802.11b tentang pengaturan *channel wifi* yang tidak menimbulkan interferensi.

DAFTAR PUSTAKA

IEEE 802.11. 2008. Tersedia di: http://standards.ieee.org, [Diakses 15 Oktober 2018]

ALEXANDER, GOSTEV, 2007. The Wardriving in London. Tersedia di: https://securelist.com/analysis/publications/36135/wardriving-inlondon-2007 [Diakses 15 Oktober 2018]

SEBBAR A, BOULAHYA, S.E, MEZZOUR G. 2016. An Empericial study of Wifi Security and performance in Morocco – WarDriving in Rabat. "2nd International Conference on electrical and Information Technologies ICEIT 2016"

HANWEI HSIAO, TIENHE CHANG, AND CHICCHE CHANG. 2013. Wireless security analysis using wardrive investigation in kaohsiung areas. In The 3rd International workshop on Intelligent Data Analysis and Management, Springer.

KLEIN ANDREAS. 2006, Attack on the RC4 stream cipher.

PERATURAN MENTERI PERHUBUNGAN Nomor KM.2 Tahun 2005 tentang Penggunaan Pita Frekuensi 2400 – 2483.5 MHZ

SURAT EDARAN DIREKTUR JENDERAL SUMBER DAYA DAN PERANGKAT POS DAN INFORMATIKA Nomor 595 Tahun 2018 tentang Ketentuan Penggunaan Pita Frekuensi Radio 2.4 GHz dan 5 Ghz untuk penyedia jaringan internet *Wifi* pada Asian Games XVIII

VIRGONO, A., SUMADJUDIN, B., ROSY, A., & HUTOMO, P. 2009. Analisa Pengaruh Besar Area Hotspot dan Interferensi Pada WLAN IEEE 802.11. Jurnal Penelitian dan Pengembangan Telekomunikasi, Vol 14, No.1

PURBO, O. 2008. Buku Pegangan Internet *Wireless* dan *Hotspot.* Jakarta : PT. Gramedia.