

# ANALISIS KEAMANAN JARINGAN *WIRELESS* MENGUNAKAN METODE *WARDRIVING* PADA KANTOR PEMERINTAH KOTA PRABUMULIH

Hidayat Eral Putra<sup>1</sup>, Alex Wijaya, S.Kom., M.I.T<sup>2</sup>, RM. Nasrul Halim, D M.Kom<sup>3</sup>.

<sup>1</sup>Mahasiswa Teknik Informatika Universitas Bina Darma

<sup>2</sup>Dosen Ilmu Komputer<sup>3</sup>Dosen Ilmu Komputer.Jl Jend A.Yani No.12 Plaju,  
Palembang 30264

*Email*:saka\_distraction@yahoo.com<sup>1</sup>

**Abstrak.** Jaringan *Wireless* selama ini digunakan sebagai penyedia internet yang sangat baik. Dengan memanfaatkan jaringan *Wireless*, pengguna dapat menikmati internet tanpa harus tersambung pada sebuah kabel. Jaringan *Wireless* sudah menjadi kebutuhan penting bagi suatu instansi, lembaga pendidikan, maupun sebuah perusahaan. Internet yang diperoleh dari jaringan *Wireless* digunakan untuk mengolah data dan informasi. Pemerintah kota prabumulih sudah menggunakan *Wireless* sebagai penyedia internet yang dapat digunakan oleh pegawai yang sudah memiliki *login*. Jaringan *Wireless* yang baik haruslah memiliki keamanan yang baik agar terhindar dari ancaman kejahatan yang dapat mengganggu bahkan merusak data dan informasi pada kantor pemerintah kota prabumulih. Dengan banyaknya lembaga yang menggunakan jaringan *Wireless*, sering kali disalah gunakan oleh sekelompok orang. *Wardriving*, adalah suatu kegiatan dimana seseorang maupun sekelompok orang yang dibekali alat dan keahlian untuk mengakses sebuah jaringan *Wireless* secara gratis atau tanpa melakukan *login*. *Wardriving* merupakan ancaman bagi pemerintah kota prabumulih karena data penting yang diolah menggunakan jaringan *Wireless* tidak terjamin keamanannya. Untuk mengetahui seberapa kuat keamanan jaringan *Wireless* pada kantor pemerintah kota prabumulih, maka diperlukan analisis. Dari hasil analisis akan menjadi kesimpulan yang nantinya akan menjadi referensi bagi pengolahan jaringan wireless kantor pemerintah kota prabumulih.

Keyword : *Wireless*, *Wardriving*, Prabumulih,.

## 1. Pendahuluan

### 1.1. Latar Belakang

Jaringan *wireless* pada era digital saat ini sudah menjadi kebutuhan penting bagi suatu lembaga, jaringan *wireless* memudahkan para penggunanya untuk memperoleh internet yang dapat digunakan dalam memperoleh informasi. Pada suatu perusahaan atau perkantoran tentu mempunyai jaringan *wireless* yang diproteksi oleh keamanan, seperti menggunakan *user name* dan *password* untuk *login* agar dapat menggunakan jaringan *wireless* tersebut. Keberadaan jaringan *wireless* yang luas menimbulkan niat bagi orang atau sekelompok orang untuk mendapatkan jaringan *wireless* tersebut secara gratis ataupun dimanfaatkan untuk memperoleh data dari suatu lembaga maupun merusaknya.

Pada kantor pemerintahan kota prabumulih memiliki jaringan *wireless* yang berfungsi sebagai penyedia internet bagi pegawai yang akan digunakan untuk memperoleh informasi dan pengolahan data. Dinas Perhubungan Komunikasi dan Informatika (KOMINFO) merancang dan mengelolah *website* resmi Pemkot Prabumulih menggunakan jaringan *wireless*, tentunya penting menjaga suatu *website* agar tidak dirusak oleh orang yang tidak bertanggung jawab. Jaringan *wireless* pada kantor pemerintahan kota prabumulih cukup besar sehingga memungkinkan untuk melakukan *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).

Karena pentingnya menjaga keamanan jaringan *wireless*, maka diperlukan keamanan yang kuat. Untuk mengetahui seberapa kuat keamanan yang telah dibangun, maka dilakukan analisis yang nantinya hasil dari penelitian akan dijadikan kesimpulan dan saran bagi pengelola jaringan *wireless* pada pemerintah kota prabumulih. *Wardriving* menjadi ancaman yang ditakuti oleh instansi yang menggunakan *wireless*, khususnya bagi pemerintah kota prabumulih yang menggunakan *wireless* sebagai penyedia internet.

Untuk menghindari *wardriving*, maka dilakukan analisis keamanan jaringan *wireless* pada pemerintah kota prabumulih. Berdasarkan hal diatas maka penulis akan melakukan penelitian dengan judul “**Analisis Keamanan Jaringan Wireless Menggunakan Metode Wardriving Pada Kantor Pemerintah Kota Prabumulih**”.

## 2. Metode Penelitian

Metode penelitian yang digunakan adalah metode penelitian tindakan (*action research*) adalah salah satu bentuk rancangan penelitian, dalam penelitian tindakan peneliti mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial pada waktu yang bersamaan dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi. *Action research* dalam pandangan tradisional adalah suatu kerangka penelitian pemecahan masalah, dimana terjadi kolaborasi antara peneliti dengan *client* dalam mencapai tujuan (Kurt Lewin, 1973 disitasi Sulaksana, 2004), sedangkan pendapat Davison, Martinsons & Kock (2004), menyebutkan penelitian tindakan, sebagai sebuah metode penelitian, didirikan atas asumsi bahwa teori dan praktik dapat secara tertutup diintegrasikan dengan pembelajaran dari hasil intervensi yang direncanakan setelah diagnosis yang rinci terhadap konteks masalahnya.

Metode pengujian pada pemkot prabumulih adalah *wardriving*, langkah-langkah dalam melakukan *wardriving* adalah:

1. Penguatan sinyal, Untuk mendapatkan sinyal lebih kuat, peneliti akan menggunakan Wajan Bolic. Penggunaan Wajan Bolic agar sinyal dari jaringan *wireless* pada kantor pemerintah kota prabumulih dapat ditembus dari jarak yang lebih jauh.
2. *Scanning*, Untuk melakukan *Scanning*, peneliti akan menggunakan *Tools* G-MoN yang dioperasikan di Android. *Software* ini akan memberikan informasi tentang *Channel*, *MAC address*, *SSID*, *Speed*, tipe Enkripsi, dari jaringan *wireless* yang akan di teliti yaitu jaringan *wireless* pada kantor pemkot prabumulih.

3. Pemetaan, Setelah dilakukan *Wardriving*, Informasi yang dihasilkan dari G-MoN akan diolah menggunakan Laptop sistem Operasi *Windows*. Titik-titik *Hotspot* yang sudah di *capture* menggunakan G-MoN akan disambungkan ke *Google Earth* sehingga hasil dari *Wardriving* dapat dipetakan.
4. *Cracking*, Setelah mendapatkan informasi berupa AP (*Access Point*), MAC address (*Media Access Control Address*), Tipe Enkripsi dan BSSID (*Basic Service Set Identification*), peneliti akan melakukan *Crack* untuk mendapatkan akses dari *wireless* tersebut sesuai dari Tipe keamanan. Peneliti akan menggunakan *software* *CommView for Wifi* versi 6 dan *Aircrack* jika tipe keamanan yang digunakan adalah WEP. Jika Tipe keamanan yang digunakan adalah WPA atau WPA2 peneliti akan menambahkan teknik *Brute Force Attack* sebagai usaha untuk mendapatkan akses internet pada jaringan *wireless* pemkot prabumulih.

### 3. Hasil dan Pembahasan

Dari hasil *Scanning* menggunakan *Software* G-Mon yang dioperasikan menggunakan Android Acer Z500. G-Mon menghasilkan file yang berformat KML, file ini dapat dibuka menggunakan *Google Earth*. Pada penelitian ini peneliti menggunakan laptop yang telah ter-*instal Google Earth*. Berikut ini adalah hasil dari proses *scanning* yang telah dipetakan melalui *google earth*. Gambar 4.1 adalah hasil dari proses *scanning* yang dilakukan menggunakan *software* G-Mon yang dioperasikan menggunakan Android Acer Z500.

Titik-titik berwarna hijau, kuning, orange dan merah pada gambar 4.1 adalah titik *hotspot* yang tertangkap. Dari hasil yang diperoleh, dapat kita ketahui jumlah titik *hotspot* yang ada dan mengetahui beberapa informasi didalamnya. Dengan mengklik salah satu titik dapat mengetahui informasi berupa SSID, *Signal Strenght* (kekuatan sinyal), *Channel* dan juga tipe keamanan. Hasil dari pemetaan memudahkan peneliti untuk memilih titik *hotspot* mana yang akan dijadikan target untuk melakukan aksi *cracking* yang bertujuan mendapatkan *keys/password*.



Gambar 1 Hasil *Scanning* dan Pemetaan

NO	SSID	Tipe keamanan	Channel
1	DPPKAD 01	WPA	1
2	DPPKAD 02	WPA	1
3	DPPKAD 04	WPA	1
4	DPPKAD 12	WPA	7
5	DPPKAD 22	WPA	7
6	DPPKAD 51	WPA	7
7	DPPKAD 52	WPA	7
8	DPPKAD 61	WPA	7
9	Kominfo Lt.1A	WPA	6
10	Kominfo Lt.1B	WPA	6
11	Kominfo Lt.3A	WPA	6
12	Kominfo Lt.5A	WPA	6
13	Kominfo Lt.7B	WPA	6
14	HOTSPOT SPEEDY 03	WPA	4
15	HOTSPOT SPEEDY 04	WPA2	4
16	PID PEMKOT-1	WPA2	3
17	DISHUB KOMINFO	WPA2	9
18	DINAS PU	WPA2	9
19	Groovia 5E48	WPA2	12
20	DINAS PERTANIAN	WPA2	6
21	INSTPEKTORAT 01	Open	1
22	Jaringan Bebas	WEP	5

Tabel 1 Tabel Pemetaan

Dari hasil pemetaan yang dilakukan menggunakan software G-Mon dapat dilihat jumlah titik *hotspot* yang berhasil ter-*capture*, SSID, tipe keamanan dan juga *channel*. Pada saat melakukan pemetaan menggunakan software G-Mon peneliti juga mendapati titik *hotspot* diluar dari gedung pemkot, selain itu peneliti juga mendapati *hotspot* dengan *Hidden* SSID atau *hotspot* yang tidak menampilkan SSID. Peneliti juga mendapati *Hotspot* dengan penggunaan berbayar. Berikut ini adalah *hotspot* yang dimaksud dalam bentuk tabel.

NO	SSID	Tipe keamanan	Channel
1	Wifid	Open	3
2	Speedy Instanwifid	Open	3
3	Speedy Instanwifid	Open	9
4	WirelessNet	Open	5
5	RUMDIS KAPOLRES	WPA	2
6	Reskrim	WPA2	5
7	UNKNOWN	WPA2	2
8	UNKNOWN	WPA	2

Tabel 2 Tabel Pemetaan Lainnya

Pada Tabel 2 adalah hasil pemetaan G-Mon yang didapati tanpa SSID, diluar dari gedung pemkot dan *hotspot* penggunaan yang berbayar. *Hotspot* Wifid,

Speedyinstantwifiid dan *WirelessNet* adalah *hotspot* dengan penggunaan berbayar, artinya untuk menggunakan *hotspot* tersebut harus melakukan pembayaran atau registrasi sebelumnya berupa tagihan operator seluler (pulsa). *Hotspot* RUMDIS KAPOLRES dan Reskrim adalah *hotspot* yang berada diluar gedung pemkot yang ikut *ter-capture* pada saat peneliti melakukan pemetaan menggunakan *software* G-Mon. *Hotspot* UNKNOWN adalah *hotspot* yang *Hidden SSID* atau *hotspot* yang tidak menampilkan SSID.

#### 4. Pembahasan

Dalam melakukan penelitian, peneliti mendapati beberapa kendala. Kendala yang dihadapi adalah seperti sulitnya mendapat posisi parkir mobil yang pas, baterai laptop habis, angin yang membuat sinyal tidak stabil dan juga *blue screen* (layar biru) atau laptop eror saat melakukan injeksi paket. Karena metode yang digunakan adalah *wardriving*, peneliti melakukan *cracking* didalam mobil, sehingga posisi parkir yang pas menunjang keberhasilan proses *cracking*. Proses *cracking* juga membutuhkan waktu yang cukup lama, energi baterai yang digunakan pada laptop terbatas sehingga proses *cracking* terkadang terhenti dikarenakan baterai pada laptop habis. Angin juga mempengaruhi sinyal, keberadaan peneliti pada luar ruangan dan titik *hotspot* yang tinggi membuat sinyal tidak stabil sehingga membuat proses *cracking* terganggu dan gagal. Disaat melakukan injeksi paket, peneliti sering kali mendapati *blue screen* atau bisa disebut laptop eror. Hal ini terjadi karena disaat melakukan injeksi paket dibutuhkan RAM laptop yang kuat.

Pada *Hotspot* Kominfo Lt.1A peneliti berhasil mendapatkan atau meng-*crack keys/password*. Setelah mendapatkan *password*, peneliti dapat mengakses jaringan *wireless* pada *hotspot* kominfo Lt.1A menggunakan *password* yang telah didapat dengan cara *login* seperti biasa. Peneliti juga mencoba login pada beberapa *hotspot* menggunakan *password* yang sama yaitu *hotspot* Kominfo Lt.1B, *hotspot* Kominfo Lt.3A, *hotspot* Kominfo Lt 5A dan *hotspot* Kominfo LT 7B. Peneliti berhasil *login* pada beberapa *hotspot* tersebut menggunakan *password* yang sama dengan yang *password* yang digunakan pada *hotspot* Kominfo Lt.1A.

Pada *Hotspot* DPPKAD 01 dan *Hotspot* DPPKAD 02 peneliti tidak berhasil melakukan *cracking* karena tidak ditemukannya *handshake* atau tidak adanya *client* yang melakukan *login* terhadap *hotspot* DPPKAD 01 dan *hotspot* DPKKAD 02 saat peneliti melakukan injeksi paket. Hal ini bisa disebabkan karena sedikitnya pengguna *hotspot* tersebut atau juga terbatasnya waktu peneliti saat melakukan injeksi paket sehingga belum sempat didapatkan *client* yang *login* dengan mengetikkan *password* pada *hotspot* DPKKAD 01 dan *hotspot* DPPKAD 02.

Pada *Hotspot* DISHUB KOMINFO, peneliti mendapati *handshake* tetapi tidak bisa mendapatkan *keys/password*. Peneliti sudah mencoba beberapa *dictionary file* atau kamus *password* dan tetap tidak berhasil. Hal ini dikarenakan *password* yang digunakan pada *hotspot* DISHUB KOMINFO sudah kuat atau menggunakan *password* yang unik yaitu berupa huruf kecil, huruf besar, angka dan simbol. Berbeda dengan *hotspot* DISHUB KOMINFO, *hotspot* Kominfo Lt.1A tidak memiliki *password* yang kuat atau unik. *Keys/password* yang digunakan pada *hotspot* Kominfo Lt.1A adalah berupa huruf kecil yang berjumlah 8 karakter tanpa kombinasi huruf besar, angka atau simbol. Hal ini membuat *Hotspot* Kominfo Lt.1A cukup mudah untuk di-*Crack*. Pada beberapa *hotspot* lainnya yang berada pada gedung pemkot

prabumulih, peneliti tidak mendapati izin penuh sehingga penelitian hanya meneliti beberapa *hotspot* saja yang telah diberikan izin dari pihak pemkot.

Setelah dilakukan pengujian, peneliti dapat melakukan *cracking* dan berhasil mendapatkan akses internet pada *Hotspot* Kominfo Lt.1A dan juga berhasil login pada beberapa *hotspot* yang menggunakan *password* yang sama dengan *password* yang digunakan pada *hotspot* Kominfo Lt.1A. Hal ini tentu berbahaya jika dilakukan oleh orang yang tidak bertanggung jawab. Seperti teknik *Sniffing*, *client* yang tidak bertanggung jawab bisa saja melakukan *sniffing* untuk mendapatkan *password client* lain yang melakukan *login email*, *facebook*, *twitter* dan lainnya. Atau juga melakukan aksi pencurian data dengan memanfaatkan kelalaian pengguna lain yang sedang melakukan *file sharing*. Pada penelitian ini peneliti tidak diizinkan untuk melakukan aksi tambahan.

Seperti yang diketahui bahwa suatu jaringan *wireless* dapat dikatakan aman jika memenuhi prinsip dasar keamanan jaringan yaitu Kerahasiaan (*secrecy*), Integritas (*integrity*) dan ketersediaan (*availability*). Pada penelitian ini, peneliti berhasil mendapatkan *keys/password* dan berhasil login pada jaringan *wireless* pemkot prabumulih, artinya keamanan jaringan *wireless* pada pemkot prabumulih tidak memenuhi prinsip dasar keamanan jaringan pada point 3 yaitu ketersediaan (*availability*) yang tertulis bahwa suatu keamanan jaringan *wireless* dapat dikatakan aman jika diakses atau dimanfaatkan oleh pihak yang berhak. Dari hasil analisa yang dilakukan, peneliti dapat menyimpulkan bahwa jaringan *wireless* pada pemkot prabumulih tidak aman.

Agar keamanan jaringan *wireless* pada pemkot lebih optimal, perlunya menambahkan keamanan yang lebih kuat pada semua titik *hotspot* yang digunakan. Seperti menggunakan *password* yang rumit yaitu *password* dengan kombinasi huruf kecil, huruf besar, angka dan simbol. Atau dengan mengaktifkan *MAC Address Filtering* sehingga hanya perangkat dengan *MAC address* tertentu saja yang boleh mengakses kedalam jaringan *wireless* yang dikelola. Untuk menghindari Injeksi paket saat seseorang melakukan *cracking* adalah dengan mengaktifkan mode *Connect Automatically* yaitu dengan men-centang bagian *Connect Automatically* pada saat melakukan *login* ke jaringan *wireless*. Cara tersebut dapat mencegah injeksi paket karena disaat seseorang melakukan injeksi paket yang dibutuhkan adalah *client* yang login ke sebuah jaringan *wireless* dengan mengetikkan *password*. Jika didapati PC yang menggunakan *software Deep Freeze*, sebaiknya *software* tersebut di-*uninstall* selanjutnya lakukan *login* dengan mengaktifkan mode *Connect Automatically*, lalu pasang kembali *software Deep Freeze*.

Pada saat melakukan Pemetaan dan *cracking*, peneliti tidak mendapati kecurigaan dari pihak pemkot prabumulih, artinya keamanan pada lahan parkir di kantor pemkot prabumulih kurang optimal. Sehingga masyarakat umum dapat memasuki lahan parkir dengan mudah dan kegiatan yang dilakukan pada lahan parkir gedung pemkot tidak terpantau dengan baik. Hal ini membuat pelaku *wardriving* dapat dengan mudah melakukan *wardriving* pada pemkot prabumulih. Jika keamanan pada gedung pemkot dapat dioptimalkan, kegiatan *wardriving* dapat diminimalisir bahkan dicegah.

## 5. Kesimpulan

Setelah dilakukan analisa terhadap keamanan jaringan *wireless* pada kantor pemerintah kota prabumulih dengan menggunakan metode *wardriving*, peneliti dapat menyimpulkan hasil dari penelitian sebagai berikut:

- a. Jaringan *wireless* pada kantor pemerintah kota prabumulih tidak aman, karena masih ada titik hotspot yang bisa dilakukan *cracking* dan berhasil mendapatkan *password/keys*.
- b. Pada *hotspot* Kominfo Lt.1A digunakan *password* yang ringan yaitu menggunakan huruf kecil tanpa kombinasi angka, huruf besar ataupun simbol.
- c. *Password* yang digunakan pada *hotspot* Kominfo Lt.1B, Kominfo Lt.3A, Kominfo Lt 5A, Kominfo LT 7B sama dengan *password* yang digunakan pada *hotspot* Kominfo Lt.1A.
- d. Kurangnya pengawasan terhadap lahan parkir gedung pemkot prabumulih.

## Referensi

Aditya Wahyu Setyawan, Gunawan Adi, Muhammad Ary Murti (2007). *Analisis sistem keamanan jaringan wirelesslan dengan menggunakan metode wardriving*.

Dari:<http://repository.telkomuniversity.ac.id/pustaka/files/90474/resume/analisis-sistem-keamanan-jaringan-wirelesslan-dengan-menggunakan-metode-wardriving.pdf> diakses pada desember 2015.

Ch.sai priya, Syed umar, T sirisha (2006). *The impact of wardriving on wireless networks*.

Dari:<http://ijcset.net/docs/volumes/volume3issue6/ijcset2013030605.pdf> diakses pada desember 2015.

Efvy Zamidra Zam (2014) *Wireless Hacking*

Hira sathu (2006). *Wardriving dilemmas*. Dari: [citrenz.ac.nz/conferences/2006/papers/237.pdf](http://citrenz.ac.nz/conferences/2006/papers/237.pdf) diakses pada desember 2015.

Gondohanindijo, *Sistem Keamanan Jaringan NIRKABEL* (2012) dari [https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjEm43NnffKAhVGZCYKHSU7CXQQFgkMAE&url=http%3A%2F%2Fwww.unaki.ac.id%2Fejournal%2Findex.php%2Fjurnal-](https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjEm43NnffKAhVGZCYKHSU7CXQQFgkMAE&url=http%3A%2F%2Fwww.unaki.ac.id%2Fejournal%2Findex.php%2Fjurnal-informatika%2Farticle%2Fdownload%2F20%2F19&usq=AFQjCNETOKNfyN2NeY9d7 tD9eWzAuJZQ&bvm=bv.114195076,d.eWE)

[informatika%2Farticle%2Fdownload%2F20%2F19&usq=AFQjCNETOKNfyN2NeY9d7 tD9eWzAuJZQ&bvm=bv.114195076,d.eWE](https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjEm43NnffKAhVGZCYKHSU7CXQQFgkMAE&url=http%3A%2F%2Fwww.unaki.ac.id%2Fejournal%2Findex.php%2Fjurnal-informatika%2Farticle%2Fdownload%2F20%2F19&usq=AFQjCNETOKNfyN2NeY9d7 tD9eWzAuJZQ&bvm=bv.114195076,d.eWE) diakses pada desember 2015

<https://en.wikipedia.org/wiki/Wardriving> diakses pada desember 2015.

<http://library.binus.ac.id/eColls/eThesisdoc/Bab2HTML/20131013451FBab2001/page12.html> diakses pada desember 2015

[https://id.wikipedia.org/wiki/Wired\\_Equivalent\\_Privacy](https://id.wikipedia.org/wiki/Wired_Equivalent_Privacy) diakses pada desember 2015.

<http://sir.stikom.edu/273/6/BAB%20III.pdf> diakses pada September 2015.

<http://www.adalahcara.com/2013/05/pengertian-kelas-ip-address-adalah.html> diakses pada september 2015.

- <http://adefachreza.blogspot.com/2013/09/pengertian-access-point-dan-fungsinya.html>  
diakses pada september 2015.
- Kern, Benjamin D (2005). *Whacking, joyriding and war-driving: roaming use of wi-fi and the law*. Dari: <http://digitalcommons.law.scu.edu/chtli/vol21/iss1/3>  
diakses pada september 2015.
- Nugroho (2012). *Analisa Keamanan Jaringan wireless Local Area Network Dengan Access Point Tp-Link Wa500g*. Dari [http://eprints.ums.ac.id/20254/20/Naskah\\_Agung\\_Nugroho\\_L200080023.pdf](http://eprints.ums.ac.id/20254/20/Naskah_Agung_Nugroho_L200080023.pdf)  
Diakses pada september 2015.
- Reza jalaluddin Al-haroh(2012). *Wardriving dan testing penetrasi wi-fi lanjut di wilayah kota Yogyakarta*, dari: [http://repository.amikom.ac.id/files/publikasi\\_08.11.2153.pdf](http://repository.amikom.ac.id/files/publikasi_08.11.2153.pdf) diakses pada desember 2015.
- Rushadi (2009). *Konsep Keamanan Jaringan Komputer dengan Infrastruktur Demilitarized Zone*. Dari [http://www.academia.edu/11938528/Konsep\\_Keamanaan\\_Jaringan\\_Komputer\\_dengan\\_Infrastruktur\\_Demilitarized\\_Zone](http://www.academia.edu/11938528/Konsep_Keamanaan_Jaringan_Komputer_dengan_Infrastruktur_Demilitarized_Zone) diakses pada september 2015.
- [Securekomodo.com/hacking-wpa-wpa2-encrypted-networks/](http://Securekomodo.com/hacking-wpa-wpa2-encrypted-networks/) diakses pada September 2015.
- Stiawan (2008), *Wireless Fundamental, Instalation & Implemetations*. Dari : <http://amikom.ac.id/research/index.php/KIM/article/viewFile/3160/1494>  
diakses pada desember 2015.
- Tabrani (2008). *Metode Authentikasi Jaringan Wireless Modus Infrastruktur (Hotspot)*. Dari [https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiMoIKnpvfKAhVISyYKHZstBqQQFggeMAA&url=http%3A%2F%2Fwww.unsri.ac.id%2Fupload%2Farsip%2FAdri1%2520Tabrani%252009061002012.doc&usg=AFQjCNFOIZmI\\_S8CKAg869X05cOqcNpjEg&bvm=bv.114195076,d.eWE](https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiMoIKnpvfKAhVISyYKHZstBqQQFggeMAA&url=http%3A%2F%2Fwww.unsri.ac.id%2Fupload%2Farsip%2FAdri1%2520Tabrani%252009061002012.doc&usg=AFQjCNFOIZmI_S8CKAg869X05cOqcNpjEg&bvm=bv.114195076,d.eWE) diakses pada September 2015
- Vyctoria (2014) *Tips & Trik Jaringan Wireless*