ANALISIS KEAMANAN JARINGAN *WI-FI* MENGGUNAKAN METODE *SIGNAL SCANNING* DI FAKULTAS TEKNIK UNIVERSITAS PGRI YOGYAKARTA

Marti Widya Sari
Fakultas Teknik Universitas PGRI Yogyakarta
mwidyas@gmail.com

Abstract

Wi - Fi or Wireless Fidelity is a set of standards used for wireless local networks based on IEEE 802.11 specification. Wi - Fi operates using the basic IEEE 802.11 specification. In this specification, Wi - Fi using different specifications on every computer, laptop, or other electronic equipment with the intention of using the frequencies of different data transfer rates. The steps are performed in this study, the first is to scan the wireless signal at the study site using the tools inSSIDer and Vistumbler. Further analysis of the results of the scan process. Then test the security of wireless networks, namely through the replacement process macchanger ie MAC address to be entered into the network without having to log in using the username and password provided from PPTIK. The results of this study are the Wi-Fi network in the Faculty of Engineering is open use security on every device, that is all the users who will access the Wi- Fi network can directly access using a username and password, respectively, without the need to change the settings of the device existing network.

***Keywords** : signal scanning, wireless security, wi-fi, inSSIDer, Vistumbler*

Intisari

Wi-Fi atau *Wireless Fidelity* merupakan sekumpulan standar yang digunakan untuk jaringan lokal nirkabel yang didasari pada spesifikasi IEEE 802.11. Wi-Fi beroperasi dengan menggunakan spesifikasi dasar IEEE 802.11. Pada spesifikasi ini, Wi-Fi menggunakan spesifikasi-spesifikasi yang berbeda pada setiap komputer, laptop, maupun peralatan elektronik lainnya dengan tujuan untuk menggunakan frekuensi kecepatan transfer data yang berbeda. Langkah-langkah yang dilakukan dalam penelitian ini, yang pertama adalah melakukan scan sinyal *wireless* di lokasi penelitian menggunakan tools inSSIDer dan Vistumbler. Selanjutnya dilakukan analisa terhadap hasil dari proses scan tersebut. Kemudian dilakukan uji keamanan terhadap jaringan *wireless*, yaitu melalui proses MACchanger yaitu penggantian MAC address untuk dapat masuk ke jaringan tanpa melakukan login menggunakan *username* dan *password* yang diberikan dari PPTIK. Hasil dari penelitian ini adalah jaringan Wi-Fi di Fakultas Teknik UPY menggunakan keamanan bersifat *open* pada setiap perangkatnya, artinya adalah semua pengguna yang akan mengakses jaringan Wi-Fi dapat langsung mengakses dengan menggunakan *username* dan *password* masing-masing, tanpa perlu merubah setting dari perangkat jaringan yang ada.

Kata kunci : *signal scanning, wireless security, wi-fi, inSSIDer, Vistumbler*

1. PENDAHULUAN

Wireless Local Area Network (WLAN) merupakan teknologi jaringan lokal atau *Local Area Network* (LAN) yang menggunakan teknologi radio sebagai basis untuk menghubungkan komputer. (Reid and Seide, 2003). *Local Area Network* atau LAN merupakan sistem jaringan komputer yang memiliki konsep tentang jaringan konvensional atau penggunaan kabel UTP sebagai media perantara antar komputer. Jenis Penggunaan atau tipe LAN dapat dibagi menjadi 2 yaitu *Peer to Peer* dan *Server Based* (Priyambodo dan Heriadi, 2005). WLAN atau *Wireless Local Area Network* adalah teknologi jaringan lokal nirkabel yang mampu beroperasi atau bekerja secara efektif melalui sinyal gelombang radio dengan kapasitas *transfer* data antara satu hingga 2 Mbps *(Megabyte per seconds)* (Rogers and Edwards, 2003).

Wi-Fi atau kependekan dari *Wireless Fidelity* yang memiliki pengertian sebagai sekumpulan standar yang digunakan untuk jaringan lokal nirkabel (WLAN – *Wireless Local Area Network)* yang didasari pada spesifikasi IEEE 802.11. *Wi-Fi* merupakan koneksi tanpa kabel yang menggunakan teknologi radio sehingga penggunanya dapat mentransfer data dengan cepat. *Wi-Fi* merupakan teknologi berbasis internet terbaru yang dikembangkan dari standar WLAN oleh sekelompok insinyur di Amerika Serikat yang bekerja pada suatu institut yang bernama *Institute of Electrical and Electronics Engineers* (IEEE) pada tahun 1990 (Rogers and Edwards, 2003). *Wi-Fi* beroperasi dengan menggunakan spesifikasi dasar IEEE 802.11. Pada spesifikasi ini, *Wi-Fi* menggunakan spesifikasi-spesifikasi yang berbeda pada setiap komputer, *laptop*, maupun peralatan elektronik lainnya dengan tujuan untuk menggunakan frekuensi kecepatan transfer data yang berbeda. Pada standar IEEE 802.11a memiliki kecepatan transfer data sebesar 54 mbps yang menggunakan gelombang frekuensi 5 GHz, IEEE 802.11b memiliki kecepatan kecepatan transfer data sebesar 11 mbps yang menggunakan gelombang frekuensi 2.4 GHz, IEEE 802.11g memiliki kecepatan kecepatan transfer data sebesar 54 mbps yang menggunakan gelombang frekuensi 2.4 GHz, dan IEEE 802.11n memiliki kecepatan kecepatan transfer data sebesar 100 mbps yang menggunakan gelombang frekuensi 2.4 GHz (Forouzan, 2007).

Saat ini di Fakultas Teknik Universitas PGRI Yogyakarta telah menggunakan fasilitas wifi untuk mendukung proses pembelajaran di kampus. Koneksi internet melalui wifi ini dapat digunakan oleh dosen, staf dan mahasiswa. Pengguna Wi-Fi di lingkungan Fakultas Teknik harus mendaftar terlebih dahulu ke PPTIK (Pusat Pelayanan Teknologi Informasi dan Komunikasi) untuk dapat mengakses internet, baik menggunakan laptop/notebook maupun telepon seluler. Selanjutnya pengguna akan diberikan *username* dan *password* dari PPTIK. Koneksi jaringan wireless yang ada saat ini dirasakan lambat oleh pengguna, terutama pada siang hari saat jam kuliah padat karena pengguna yang mengakses internet mencapai puncaknya.

2. KAJIAN LITERATUR

Penelitian yang dilakukan oleh Lawrence and Lawrence (2004), yang berjudul *Threats to The Mobile Enterprise: Jurisprudence Analysis of Wardriving and Warchalking*. Pada penelitian ini membahas tentang pengaruh *warchalking* dan *wardriving* dalam konteks hukum dan keamanan dengan melihat usulan perumusan kebijakan bagi teknisi, ilmuwan, manajer dan pengambil kebijakan dalam pemerintahan. Peneliti mengembangkan sebuah *framework* bernama *Mobile Enterprise Legal and Security* (MELS) yang berguna sebagai cara bagi perusahaan telepon seluler untuk memastikan bahwa perusahaan tersebut berada dalam wilayah kebijakan hukum dan keamanan untuk menjaga keamanan jaringannya.

Penelitian yang dilakukan oleh Jones and Liu (2007), tentang sebuah studi mengenai database *access point* yang berjumlah sekitar 5 juta titik, dengan menggunakan perlengkapan *wardriving* yang sudah sistematis dari *Skyhook Wireless*. Studi analisis dilakukan menyangkut perubahan pergerakan *access point* setiap waktu, penemuan data *access point* serta lokasinya. Hal tersebut dapat menjadi dasar untuk memahamai "*What, Where and Why*" dari *access point* Wi-Fi.

Penelitian yang dilakukan oleh Jones, Liu and Alizadeh-Shabdiz (2007) tentang perbaikan penempatan *wireless* berdasarkan pencocokan peta lokasi menggunakan metode *wardriving*.

Penelitian yang dilakukan oleh Ramadhani (2010) membahas tentang analisis keamanan jaringan *wireless* di beberapa fakultas di Universitas Gadjah Mada Yogyakarta menggunakan metode *wardriving*. Hasil

penelitian menunjukkan bahwa 32,2% jaringan wireless di UGM menggunakan sistem enkripsi untuk mendukung keamanan jaringan dan 67,8% menggunakan chlilispot dan SSO (*single sign on*). Hasil penelitian juga menunjukkan bahwa serangan seperti *eavesdropping*, *denial of service attack*, *sniffing* dan *crack* WEP dapat dilakukan dengan mudah berdasarkan pada informasi-informasi yang didapat melalui proses *wardriving*.

Menurut Forouzan (2007), standar ini mendefinisikan dua jenis layanan yaitu *basic service set* (BSS) dan *extended service set* (ESS). BSS merupakan susunan dari blok wireless LAN. BSS tersusun dari stasiun tak bergerak ataupun stasiun bergerak dan dapat juga berupa pusat pemancar yang dikenal dengan sebutan *access point* (AP). BSS tanpa *access point* merupakan *stand alone network* atau jaringan tunggal dan tidak dapat mengirim data ke BSS lain. Inilah yang disebut dengan arsitektur Ad Hoc. Pada aristektur ini, stasiun dapat terbentuk tanpa ada AP.

Extended service set (ESS) tersusun dari dua atau lebih BSS yang menggunakan access point. Dalam hal ini, BSS terkoneksi melalui sebuah sistem terdistribusi, yang biasanya berupa jaringan lokal memakai kabel. Sistem terdistribusi ini terhubung dengan AP di dalam BSS. IEEE 802.11 tidak membatasi sistem terdistribusi, ini dapat berupa IEEE LAN yang lain seperti Ethernet. Sebagai catatan, *extended service set* menggunakan dua tipe pemancar yaitu pemancar bergerak dan tidak bergerak. Ketika BSS terkoneksi, itulah yang disebut dengan jaringan Infrastruktur. Pada jaringan ini, pemancar yang menjangkau satu sama lain dapat berkomunikasi tanpa menggunakan AP. Bagaimanapun, komunikasi antara dua stasiun pada dua BSS yang berbeda biasanya terjadi melalui dua AP.

Menurut Forouzan (2004), standar ini menjelaskan tentang metode *orthogonal frequency division multiplexing* (OFDM) untuk kecepatan laju data 18 Mbps dan 54 Mbps. Untuk menggunakan standar 802.11a, perangkat-perangkat komputer memerlukan dukungan kecepatan komunikasi 6 Mbps, 12 Mbps dan 24 Mbps. Standar 802.11a juga mengoperasikan *channel* empat kali lebih banyak dari yang dapat dilakukan oleh standar 802.11 dan 802.11b. Walaupun standar 802.11a memiliki kesamaan dengan standar 802.11b pada lapisan *Media Access Control* (MAC), ternyata tetap tidak kompatibel dengan standar 802.11 atau 802.11b karena pada standar 802.11a menggunakan frekuensi 5 Ghz sementara pada standar 802.11b menggunakan frekuensi 2,4 GHz.

Standar ini menjelaskan tentang metode *high rate direct sequence spread spectrum* (HR-DSSS) untuk generasi sinyal pada lebar pita 2.40 – 2.48 GHz dengan kecepatan laju data 1 atau 2, 5.5, dan 11 Mbps. Standar 802.11b merupakan standar yang paling banyak digunakan di kelas standar 802.11. Standar 802.11b juga kompatibel dengan semua perangkat DSSS yang beroperasi pada standar 802.11. Saat ini kurang lebih 95% infrastruktur *wireless* LAN menggunakan produk 802.11b (Forouzan, 2004).

Ini merupakan spesifikasi yang baru menggunakan OFDM untuk generasi sinya pada lebar pita 2.40 - 2.48 GHz dengan kecepatan laju data 54 Mbps. Kecepatan laju data yang tinggi akan diterima menggunakan teknik modulasi yang kompleks. Standar 802.11g pada dasarnya hampir sama dengan standar 802.11a yaitu menyediakan jalur komunikasi kecepatan tinggi sampai dengan 54 Mbps. Dibandingkan dengan 802.11a, ternyata 802.11g memiliki kelebihan dalam hal kompatibilitas dengan jaringan standar 802.11b. Tetapi masalah yang mungkin muncul ketika perangkat-perangkat standar 802.11g yang mencoba berpindah ke jarinan 802.11b atau bahkan sebaliknya adalah masalah interferensi yang diakibatkan oleh penggunaan frekuensi 2,4 GHz. Karena frekuensi 2,4 GHz merupakan frekuensi yang paling banyak digunakan oleh perangkat-perangkat berbasis *wireless* lainnya (Forouzan, 2004).

802.11n dikembangkan dengan menggabungkan teknologi 802.11b dan 802.11g. Teknologi yang diusung dikenal dengan istilah MIMO (*Multiple Input Multiple Output*) merupakan teknologi Wi-Fi terbaru. MIMO dibuat berdasarkan spesifikasi Pre-802.11n. Kata ”Pre-” menyatakan “*Prestandard versions of 802.11n*”. MIMO menawarkan peningkatan *throughput*, keunggulan reabilitas dan peningkatan jumlah klien yang terkoneksi. Secara teknis MIMO lebih unggul dibandingkan spesifikasi sebelumnya, 802.11a/b/g. *Access Point* MIMO dapat mengenali gelombang radio yang dipancarkan oleh adapter Wi-Fi 802.11a/b/g. Peralatan Wi-Fi MIMO dapat menghasilkan kecepatan transfer data sebesar 108 Mbps.

Metode *signal scanning* atau dapat disebut *wardriving* adalah kegiatan yang bergerak mengelilingi area tertentu dan memetakan

populasi *access point wireless* untuk tujuan statistik. *Scanner* bergerak mengelilingi area yang sudah dipetakan rutenya untuk menentukan *access point wireless* pada area tersebut. Menurut Hurley et al, peralatan yang digunakan untuk *wardriving* yaitu :

1. Hardware (laptop atau PDA)
2. *Wireless network card*
3. Antena luar
4. *Software wardriving*
5. GPS (*Global Positioning System*)

Beberapa hal yang dapat diperoleh dari kegiatan *signal scanning* adalah :

a) Menemukan *access point*
b) Autentikasi yang digunakan oleh *access point*
c) Mengetahui teknologi enkripsi yang digunakan
d) Client yang terhubung
e) *Gateway*
f) Data yang melalui jaringan, dapat berupa *username* dan *password*.

Semua informasi tersebut sangat berharga sehingga menjadi berbahaya jika disalahgunakan oleh *wardriver*. *Wardriving* perlu dilakukan karena semua informasi di atas tidak dapat diperoleh hanya dengan melihat bentuk fisik peralatan jaringan saja (Ramadhani, 2010).

Software yang dapat digunakan untuk *signal scanning* antara lain adalah inSSIDer, Vistumbler, Colasoft Capsa, Kismet dan MACchanger.

3. METODE PENELITIAN

Data primer merupakan data kualitatif dari hasil analisa pada infrastruktur jaringan yang menjadi sampel, misalnya hasil *scanning*, sistem enkripsi yang digunakan atau data yang diperoleh dari hasil wawancara dengan pengelola jaringan, dalam hal ini PPTIK (Pusat Pelayanan Teknologi Informasi dan Komunikasi) UPY seperti jumlah aset yang ada, ketersediaan dokumen kebijakan, dan lain-lain. Data primer yang digunakan sebagai bahan assessment adalah jumlah titik *access point* dan informasinya serta kebijakan keamanan jaringan *wireless* yang digunakan.

Data sekunder diperoleh dari studi literatur dan referensi yang digunakan dalam penelitian ini. Selain itu juga data yang diperoleh melalui pembahasan dalam forum-forum ilmiah tentang keamanan jaringan *wireless* dapat menambah wawasan dan pengetahuan mengenai analisis keamanan jaringan *wireless*.

Software aplikasi yang digunakan adalah inSSIDer dan Vistumbler yang berjalan di atas sistem operasi Windows.

Alat yang digunakan dalam penelitian ini adalah menggunakan komputer dengan spesifikasi sebagai berikut :

1. AMD Athlon Neo X2 Dual Core Processor L335 1.60 Ghz
2. Memori 2 Gb
3. Kapasitas harddisk 250 Gb
4. *Network Adapter* Broadcom 802.11/g

Jalan penelitian yang dilakukan meliputi survey ke lokasi penelitian, identifikasi masalah, mengumpulkan data, studi kepustakaan, analisis data kemudian membuat rekomendasi dari hasil penelitian yang dilakukan.

Salah satu jalan penelitian adalah melakukan survey langsung untuk mengumpulkan data untuk dilakukan analisis. Lokasi penelitian adalah Fakultas Teknik Universitas PGRI Yogyakarta.

Pada penelitian ini dilakukan identifikasi masalah yang menjadi obyek penelitian, masalah apa saja yang terjadi selama menggunakan jaringan *wireless*.

Pengumpulan data dilakukan melalui observasi langsung ke lokasi penelitian dan wawancara dengan administrator selaku penanggung jawab operasional IT secara *personal interview* yaitu bertatap muka secara langsung. Data yang terkumpul berupa permasalahan yang terjadi selama menggunakan jaringan *wireless*, teknologi enkripsi yang digunakan saat ini, software dan hardware pendukung yang digunakan serta hasil dari pengujian sistem yang saat ini digunakan.

Studi kepustakaan dilakukan untuk mencari literature yang berhubungan dengan obyek penelitian ini, serta untuk memahami konsep tentang *wireless local area network.* Selain itu, juga terdapat buku, jurnal ilmiah artikel, artikel di internet dan sebagainya.

Setelah data terkumpul, maka dilakukan analisa terhadap keseluruhan data yang sudah diperoleh. Analisa data yang dilakukan adalah dengan melihat hasil penelitian yang ada, yaitu hasil pengujian untuk keamanan jaringan *wireless* yang digunakan saat ini.

Rekomendasi atau usulan dibuat berdasarkan observasi di lokasi penelitian, wawancara dengan administrator maupun melalui analisa data. Rekomendasi juga dibuat berdasar

hasil penelitian yang sudah dilakukan. Pembuatan rekomendasi ini diharapkan dapat memberi masukan kepada pengelola jaringan untuk rencana sistem keamanan jaringan di masa mendatang.

4. HASIL DAN PEMBAHASAN

Lokasi Universitas PGRI Yogyakarta (UPY) berada di 3 (tiga) unit yang terpisah, yaitu Unit 1 terdiri dari Gedung A, B dan C, Unit 2 dan Unit 3. Di Unit 1 terdapat Gedung Pusat, Rektorat, Fakultas Teknik, Fakultas Ekonomi serta Fakultas Keguruan dan Ilmu Pendidikan (FKIP) untuk Program Studi Pendidikan Sejarah, Pendidikan Guru Sekolah Dasar.

Jaringan *wireless* yang ada di UPY juga dibagi menjadi tiga bagian, dengan pusat pengelolaan berada di Pusat Pelayanan Teknologi Informasi dan Komunikasi (PPTIK). Di Unit 1 terdapat server yang berada di PPTIK, kemudian terdapat 2 (dua) router yang berada di Gedung A dan B dan 10 *wireless access point*. Fakultas Teknik berada di Gedung B, menempati lantai 2 dan 3. Fakultas Teknik mempunyai satu program studi yaitu Program Studi Teknik Informatika. Di Fakultas Teknik terdapat 3 *wireless access point*.

Software inSSIDer yang digunakan untuk *scanning* berjalan di atas sistem operasi Windows. inSSIDer merupakan software untuk melakukan *scanning* sinyal *access point*. Seting *channel* yang digunakan adalah 2,4 GHz, karena sinyal *wireless* yang berada di Fakultas Teknik Gedung B adalah sinyal *wireless* yang bekerja pada frekuensi 2,4 GHz.

Hasil *scanning* di Kantor Fakultas Teknik adalah sebagai berikut.

Tabel 4.1 Hasil *scanning* di Kantor Fakultas Teknik

No	SSID	Signal	Ch	Security	802.11	Freq
1	@wifi.id	-76 dBm	11	Open	N	2,4 GHz
2	Flashzone-seamless	-76 dBm	11	WPA-2 Enterprise	N	2,4 GHz
3	Flash Zone	-76 dBm	11	Open	N	2,4 GHz
4	free@wifi.id	-76 dBm	11	Open	N	2,4 GHz
5	IndSchool@wifi.id	-76 dBm	11	Open	N	2,4 GHz
6	Speedy Instant@wifi.id	-77 dBm	11	Open	N	2,4 GHz
7	Hotspot UPY Gedung B	-77 dBm	1	Open	B	2,4 GHz
8	FlexiZone	-77 dBm	11	Open	N	2,4 GHz
9	Hotspot UPY Gedung A	-77 dBm	1	Open	B	2,4 GHz
10	Hotspot UPY Area 5	-77 dBm	1	Open	B	2,4 GHz
11	Flash Zone	-88 dBm	1	Open	N	2,4 GHz
12	Hotspot UPY Area 1	-89 dBm	1	Open	B	2,4 GHz
13	Hotspot UPY Area 3	-89 dBm	1	Open	B	2,4 GHz

Pada tabel di atas, dapat dilihat bahwa semua SSID yang ada bekerja pada frekuensi 2,4 GHz. Kekuatan sinyal berada pada kisaran -89 dBm sampai dengan -76 dBm. Untuk tipe keamanan, sebanyak 92,4% menggunakan model *Open security* dan 7,6% menggunakan WPA-2 Enterprise. *Open security* artinya adalah bahwa setiap pengguna dapat mengakses jaringan Wi-Fi setelah melakukan autentikasi menggunakan *user* dan *password* masing-masing. Setiap pengguna diberikan *user* dan *password* masing-masing oleh PPTIK. Untuk keamanan yang menggunakan WPA-2 Enterprise, berarti masih bawaan dari *vendor* perangkat yang digunakan. Hal tersebut akan mempersulit pengguna karena yang dapat mengakses adalah administrator jaringan.

Tabel 4.2 Hasil scanning di Lantai 2 Gedun B

No	SSID	Signal	Ch	Security	802.11	Freq
1	@wifi.id	-76 dBm	11	Open	n	2,4 GHz
2	Flashzone-seamless	-76 dBm	11	WPA-2 Enterprise	n	2,4 GHz
3	Flash Zone	-76 dBm	11	Open	n	2,4 GHz
4	free@wifi.id	-76 dBm	11	Open	n	2,4 GHz
5	IndSchool@wifi.id	-76 dBm	11	Open	n	2,4 GHz
6	Speedy Instant@wifi.id	-77 dBm	11	Open	n	2,4 GHz
7	Hotspot UPY Gedung B	-77 dBm	1	Open	b	2,4 GHz
8	FlexiZone	-77 dBm	11	Open	n	2,4 GHz
9	Hotspot UPY Gedung A	-77 dBm	1	Open	b	2,4 GHz
10	Hotspot UPY Area 5	-77 dBm	1	Open	b	2,4 GHz
11	Flash Zone	-88 dBm	1	Open	n	2,4 GHz
12	Hotspot UPY Area 1	-89 dBm	1	Open	b	2,4 GHz

13	Hotspot UPY Area 3	-89 dBm	1	Open	b	2,4 GHz

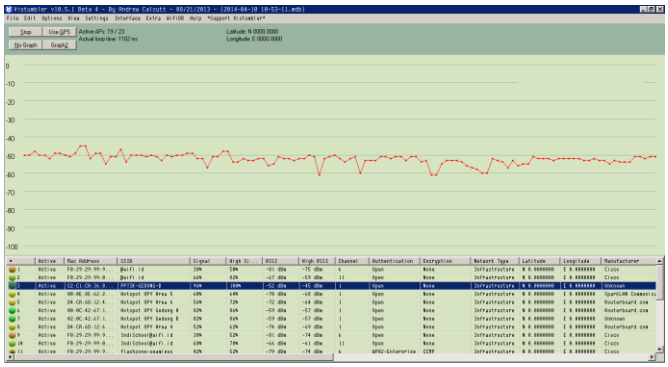
Pada Tabel 4.2 terlihat bahwa sinyal *wireless* dengan SSID Hotspot UPY Gedung B sebesar -72 dBm, lebih kuat dibandingkan dengan hasil *wardriving* di dalam Kantor Fakultas Teknik yaitu -77dBm. Kekuatan sinyal berada pada kisaran -77 dBm sampai dengan -66 dBm. Semua SSID yang ada bekerja pada frekuensi 2,4 GHz. Untuk tipe keamanan, sebanyak 92,4% menggunakan model *Open security* dan 7,6% menggunakan WPA-2 Enterprise.
Hasil *scanning* di Lantai 3 Fakultas Teknik adalah sebagai berikut.

Tabel 4.3 Hasil *scanning* di Lantai 3 Fakultas Teknik

No	SSID	Signal	Ch	Security	802. 11	Freq
1	Flash Zone	-48 dBm	1	Open	n	2,4 GHz
2	Flashzone-seamless	-49 dBm	1	WPA2-Enterprise	n	2,4 GHz
3	free@wifi.id	-49 dBm	1	Open	n	2,4 GHz
4	IndSchool@wifi.id	-49 dBm	1	Open	n	2,4 GHz
5	Speedy Instan@wifi.id	-50 dBm	1	Open	n	2,4 GHz
6	FlexiZone	-50 dBm	1	Open	n	2,4 GHz
7	@wifi.id	-50 dBm	1	Open	n	2,4 GHz
8	Hotspot UPY Gedung B	-72 dBm	1	Open	b	2,4 GHz
9	Hotspot UPY Gedung A	-72 dBm	1	Open	b	2,4 GHz
10	Hotspot UPY Area 6	-77 dBm	1	Open	b	2,4 GHz
11	Hotspot UPY Auditorium	-81 dBm	8	Open	g	2,4 GHz
12	@wifi.id	-81 dBm	11	Open	n	2,4 Ghz
13	Hotspot UPY Area 5	-82 dBm	1	Open	b	2,4 GHz

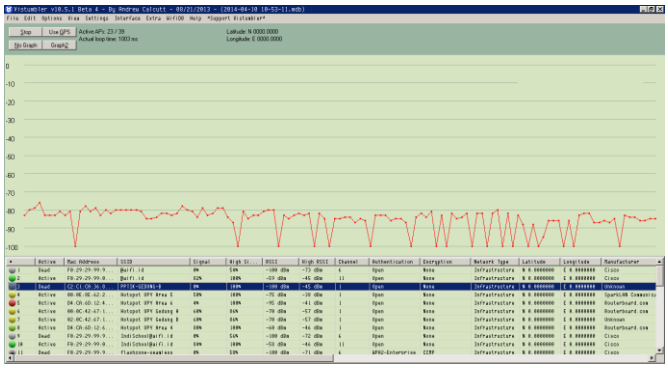
Pada Tabel 4.3 terlihat bahwa sinyal *wireless* dengan SSID Hotspot UPY Gedung B di lantai 3 sebesar -72 dBm, sama dengan hasil *wardriving* di lantai 2. Kekuatan sinyal berada pada kisaran -82 dBm sampai dengan -48 dBm. Semua SSID yang ada bekerja pada frekuensi 2,4 GHz. Untuk tipe keamanan, sebanyak 92,4% menggunakan model *Open security* dan 7,6% menggunakan WPA-2 Enterprise.

Dari hasil pengamatan sinyal PPPTIK Gedung B yang berada di dalam kantor cenderung stabil. Kuat sinyal dari access point tersebut adalah -50 dbm (Memakai Vistumbler).



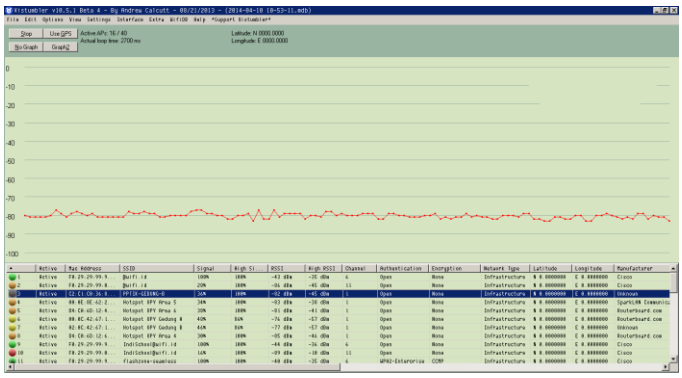
Gambar 4.1 *Signal scanning* menggunakan Vistumbler

Sedangkan sinyal yang berada di depan lab dasar adalah -80 dbm, bahkan sampai Down. Indikator ini ditandai dengan warna kuning pada access point PPTIK Gedung B.



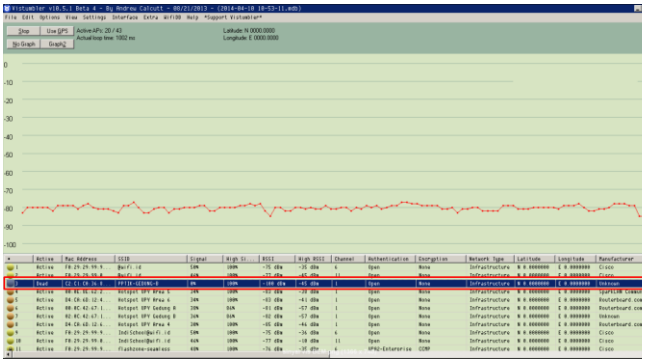
Gambar 4.2 *Signal scanning* di depan Lab Dasar

Sinyal PPTIK Depan 306, cenderung stabil namun indikator *access point* kurang kuat, ditandai dengan indikator yang berwarna kuning.



Gambar 4.3 *Signal scanning* di depan Ruang 306

Untuk sinyal PPTIK Gedung B didepan BEM FT tidak terjangkau ditandai dengan indikator sinyal berwarna abu-abu dan bertuliskan DEAD.



Gambar 4.4 *Signal scanning* di depan Ruang BEM FT

5. Kesimpulan

Kesimpulan dari penelitian ini adalah sebagai berikut.

1. Proses *signal scanning* yang sudah dilakukan di Fakultas Teknik UPY menggunakan *software* aplikasi insider, kismet, *MACchanger* dan Collasoft Capsa dapat digunakan untuk mengetahui jaringan Wi-Fi yang berada di Fakultas Teknik dan sekitarnya. Selain itu, dapat diketahui juga perangkat-perangkat jaringan serta *client* yang terkoneksi dengan jaringan Wi-Fi tersebut.
2. Keamanan *wireless* di Fakultas Teknik UPY menggunakan autentikasi *user* dan *password*, yang dapat diperoleh dengan mendaftar dahulu ke PPTIK (Pusat Pelayanan Teknologi Informasi dan Komunikasi)
3. Jaringan *Wi-Fi* di Fakultas Teknik UPY menggunakan keamanan bersifat *open* pada setiap perangkatnya, artinya adalah semua *user* yang akan mengakses jaringan *Wi-Fi* dapat langsung mengakses dengan menggunakan *user* dan *password* masing-masing, tanpa perlu merubah setting dari perangkat jaringan yang ada.
4. Keamanan jaringan *Wi-Fi* di Fakultas Teknik masih dapat ditembus, dibuktikan dengan proses *MACchanger*, yaitu proses merubah suatu MAC *address* dari seorang *user* untuk dapat masuk ke jaringan *Wi-Fi* tanpa perlu memasukkan *user* dan *password*.
5. Pada proses *signal scanning* di Fakultas Teknik UPY menggunakan aplikasi inSSIDer, yang dilakukan di lantai 2 dan 3 Gedung B, untuk tipe keamanan, sebanyak 92,4% menggunakan model *Open security* dan 7,6% menggunakan WPA-2 Enterprise.

6. REFERANSI

Barken, L., Ermel, E., Eder, J., Fanady, M., Mee, M., Palumbo, M., Koebrick, A. 2004. *Wireless Hacking Projects for Wi-Fi Enthusiasts*. Syngress Publishing, Inc. Rockland. MA.

Bastien, G; Degu, C.A. 2004. *CCSP Secure Exam Certification Guide*. Cisco Press. Indianapolis, USA

Brown, L. 2003. *Lecture Notes for Use with Cryptography and Network Security by Willliam Stallings*.

Edwards, J., & Rogers, G.S. 2003. An Introduction to Wireless Technology. Prentice Hall. New Jersey.

Forouzan, B. 2004. *Data and Communication Network*. McGraw-Hill Companies. New York.

Forouzan, B. 2007. *TCP/IP Protocol Suite (Third Edition)*. McGraw-Hill Companies. New York.

Heriadi, D. & Priyambodo, T.K. 2005. *Jaringan Wi-Fi: Teori dan implikasi.* Andi. Yogyakarta.

Hurley, C., Puchol, M., Rogers, R., Thornton, F. 2004. *WarDriving: Drive, Detect, Defend: Guide to Wireless Security*. Syngress Publishing. Rockland, MA.

Lawrence E, & Lawrence J. 2004. *Threats to The Mobile Enterprise: Jurisprudence Analysis of Wardriving and Warchalking*. IEEE Journal.

Liu, L & Jones, K. 2007. *What Where Wi: An Analysis of Millions of Wi-Fi Access Point.* IEEE Journal.

Liu, L, Jones, K & Alizadeh-Shabdiz. 2007. *Improving Wireless Positioning with Look-Ahead Map-Matching*. IEEE Journal.

Ramadhani, E. 2010. *Analisis Kemanan Jaringan Wireless di Universitas Gadjah Mada dengan Menggunakan Metode Wardriving*. Magister Teknologi Informasi Universitas Gadjah Mada. Yogyakarta.

Reid, N., & Seide R. 2003. *Wi-Fi Networking Handbook*. McGraw-Hill. California.