PERBANDINGAN KINERJA WIRESHARK DAN CAIN DALAM ANALISIS JARINGAN INTERNET

Edy Victor Haryanto[1] , Anderian[2]

[1,2] STMIK Potensi Utama
Jl. K. L Yos Sudarso Km.6,5 No.3A Tanjung Mulia Medan
Email : edyvictor@gmail.com, the.dark.heart19@gmail.com

Abstrak

Pengamanan data pada saat sangat dibutuhkan sekali, apalagi dalam hal jaringan komputer, siapapun dan dimanapun jaringan kita dapat dibobol atau diakses orang lain tanpa kita sendiri ketahui, maka dari itu perlu diketahui bagaimana seseorang dapat mengakses jaringan komputer kita atau orang lain, dalam penelitian ini akan dibahas mengenai metode wireshark dan cain dalam penggunaan jaringan internet

Kata Kunci : Jaringan komputer, sniffing, jaringan nirkabel, Cain.

1. PENDAHULUAN

Seiring dengan semakin berkembangnya teknologi *internet*, kejahatan yang memanfaatkan teknologi ini juga semakin meningkat. Hal ini ditambah lagi dengan semakin banyaknya peredaran aplikasi gratis yang dapat digunakan untuk melancarkan usaha pembobolan suatu sistem berbasis teknologi jaringan internet. Akan tetapi *internet* bukan tanpa resiko, karena maraknya kegiatan *cyber crime* akhir-akhir ini yang bisa mencuri data dan penyadapan transmisi pada jaringan. Oleh karena itulah dibutuhkan suatu aplikasi penganalisa jaringan yang bernama Cain dan Wireshark .

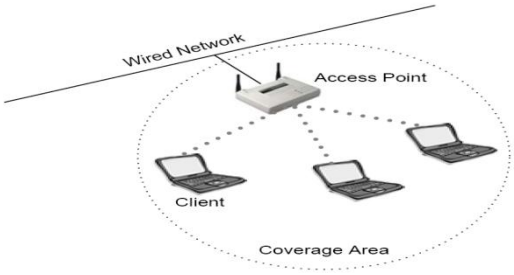
Cain adalah suatu aplikasi pemulihan sandi untuk sistem operasi Microsoft. Untuk itu Cain dapat melakukan pemulihan password dengan mengendus protocol jaringan yang ada, membuka password yang didekripsi melalui kamus, merekam percakapan VoIP, memecahkan kode secara acak, dan memulihkan kunci jaringan nirkabel.

2. Landasan Teori

2.2 Aplikasi Wireless LAN

2.2.1 Akses Role

Wireless LAN kebanyakan menyebar dalam suatu lapisan akses,maksudnya mereka digunakan sebagai suatu titik masukan ke dalam suatu kabeljaringan. Di masa lalu, akses telah digambarkan sebagai dial-up, ADSI, kabel / telegram, selular, Ethernet, Token Ring, Frame Relay, ATM, dan lain lain. Wireless cara sederhana yang lain untuk para user dalam mengakses jaringantersebut. Wireless LAN adalah lapisan jaringan Data-Link seperti cara akses semuanya hanya mendaftar saja. Dalam kaitan dengan kecepatan, jaringan nirkabel tidaklah tepat diterapkan dalam distributor atau sebagai inti dalam jaringan.

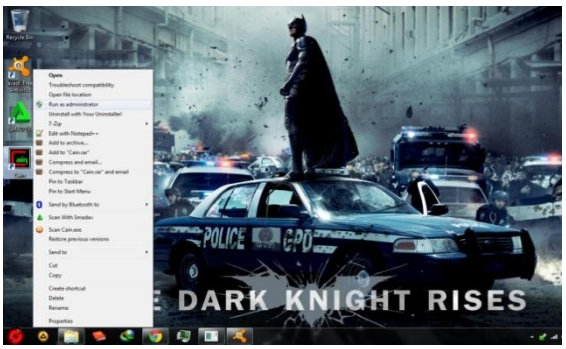


Gambar 1. Akses role dari wireless LAN

3. Analisis Hasil Pengujian

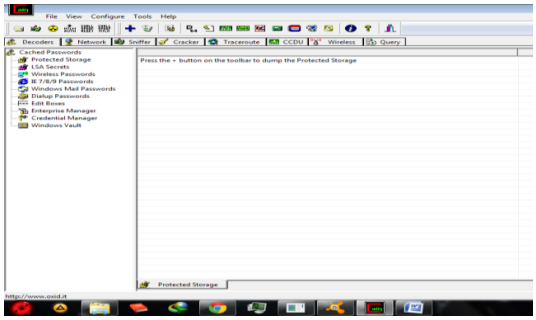
3.1 Hasil Pengujian Cain

Pengujian yang dilakukan disini adalah pada Wifi yang ada, yaitu SSID *Wi-Fi*. Ujicoba yang dilakukan adalah seperti berikut :
Untuk melakukan analisis dengan Cain, maka terlebih dahulu dibuka program aplikasi Cain, klik kanan pada *shortcut* Cain, lalu pilih *Run As Administrator*.



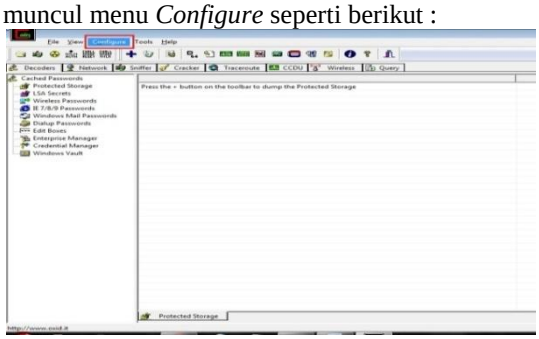
Gambar 7. Membuka aplikasi Cain pada Windows 7

Hasilnya dapat dilihat seperti pada gambar berikut :



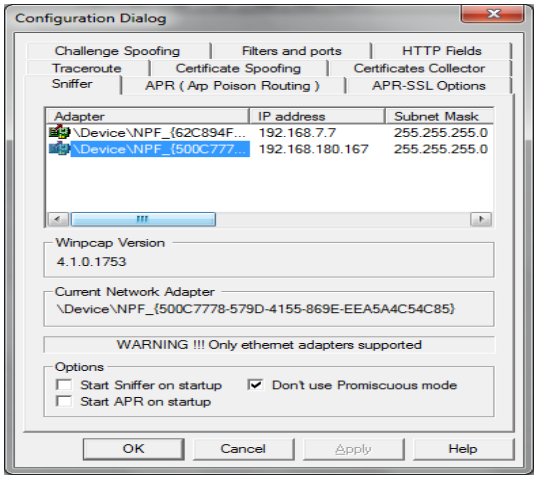
Gambar 8. Tampilan Menu Utama Cain

Selanjutnya, pilih menu *Configure*, lalu akan muncul menu *Configure* seperti berikut :



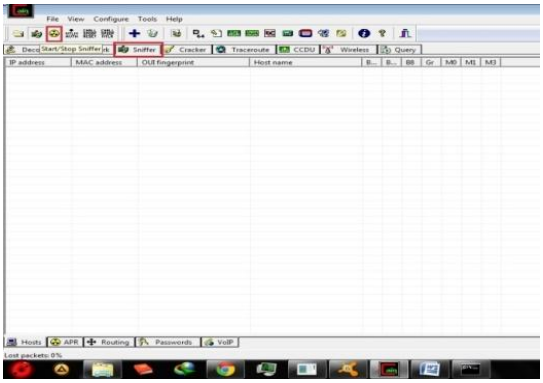
Gambar 9. Tampilan Letak Menu Configure pada Cain

Penulis akan melakukan suatu teknik penyadapan yang dinamakan *ARP Poisoning* atau yang lebih dikenal dengan istilah *Man In The Middle Attack*. Selanjutnya klik *configure* lalu tentukan interface yang digunakan, disini penulis menggunakan wireless. Untuk melihat lebih jelas apakah tersebut adalah LAN atau wireless, dapat di *scroll* ke kanan, lalu klik OK.



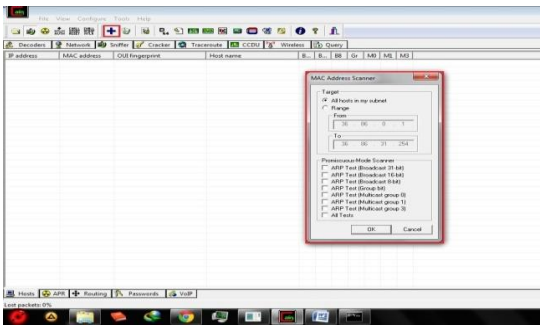
Gambar 10. Tampilan Pemilihan Interface yang Ingin Digunakan

Lalu pilih tab sniffer, dan juga klik button sniffer



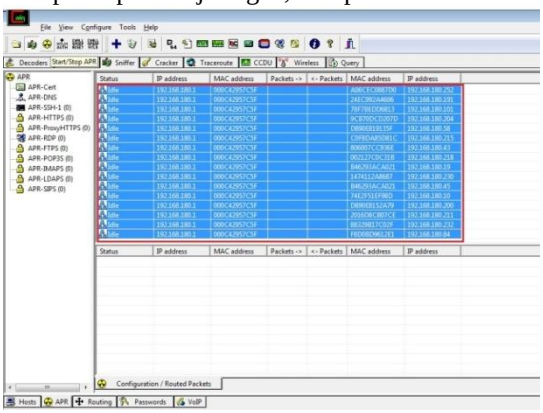
Gambar 11. Menghidupkan Sistem Sniffer Pada Cain

Lalu klik tombol *add to list* yang berwarna biru untuk menambahkan host yang akan di sniffing, lalu klik ok.



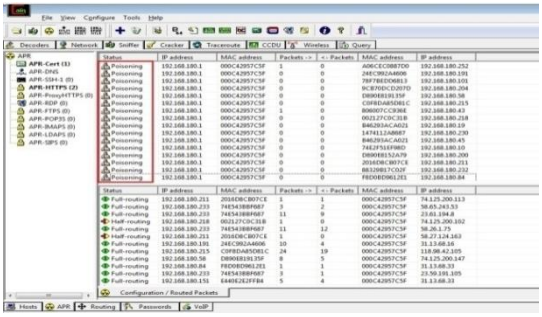
Gambar 12. Memasukkan Host yang Ada Pada Jaringan

Maka Cain akan menampilkan semua host yang terdapat pada jaringan, seperti berikut :



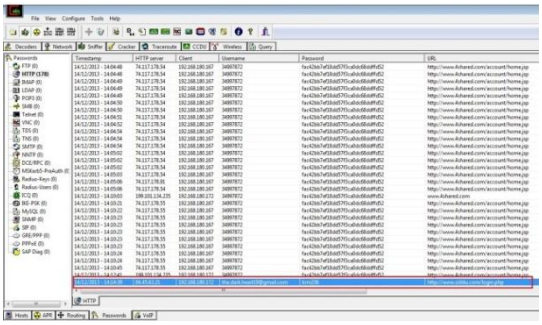
Gambar 13. Tampilan dari Semua Host Dalam Kondisi *Idle*

Bila dilihat pada gambar di atas, maka status dari semua host adalah *idle* artinya belum ada aktifitas yang didapat oleh Cain terhadap setiap host yang ada. Untuk itu, selanjutnya blok semua host dan klik button arp yang berwarna kuning sebelah atas, sehingga status semua host menjadi *poisoning.*



Gambar 14. Melakukan ARP Poisoning pada Host yang Sudah Didapat Oleh Cain

Pilih tab password yang berada di sebelah bawah, sehingga dapat terlihat apakah ada host yang melakukan login ke dalam suatu situs. Pada gambar di bawah di dapatkan username dan password dari salah satu host yang melakukan login ke situs http://www.ziddu.com, dengan username *the.dark.heart19@gmail.com* dan password *krm236*



Gambar 15. Hasil Dari Host yang Melakukan Login

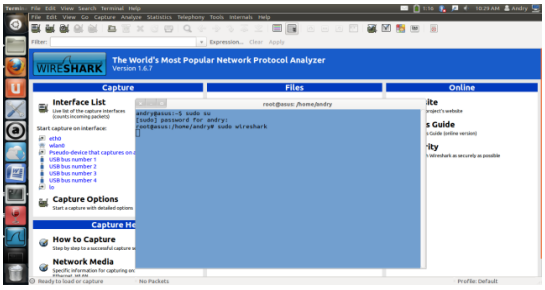
Dari hasil percobaan di atas, maka dapat diketahui bahwa Cain sangat berguna jika digunakan dengan baik oleh seorang administrator jaringan. hitung untuk kenaikan rata kuat sinyal *wireless* dari perangkat *access point* yang kuat sinyalnya dikuatkan dengan penguat sinyal yang menggunkaan kaleng minuman bekas dapat mempengaruhi penguatan sinyal sebesar 15.84158 % dari nilai kuat sinyal *access point* standart. Nilai sebesar 15.84158 merupakan nilai hasil rata – rata penguatan sinyal yang dilakukan terhadap 20 kali pengujian kuat sinyal. Hasil nilai prosentasi 15.84158 % dapat disimpulkan bahwa kaleng minuman bekas dapat menaikkan kuat sinyal transmisi *wireless* sebesar prosentasi penghitungan.

3.2. Hasil Pengujian Wireshark

3.2.1. Sniffing Paket HTTP

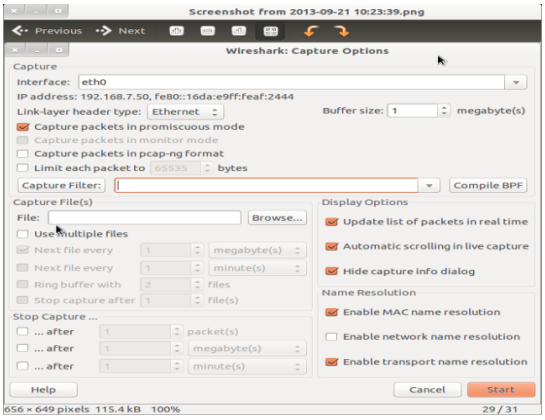
Uji coba analisis jaringan komputer melalui komputer user/sniffer mail server dilakukan melalui sistem operasi Ubuntu Dekstop 12.04, sedangkan client menggunakan sistem operasi windows, bisa juga digunakan sistem operasi lain, tetapi penulis pada uji coba perancangan client menggunakan sistem operasi windows. Disini penulis akan menjelaskan cara melakukan *sniffing* pada protocol HTTP (*Hypertext Transfer Protocol*), pada akses point WIFI. Protokol HTTP adalah protokol yang digunakan untuk transfer data di dalam internet antara *server* dan *client*.

Langkah pertama yang harus dilakukan adalah masuk sebagai root user dari terminal linux, ketik *ctrl+alt+t* dari keyboard untuk membuka terminal, lalu ketikkan *sudo su* untuk masuk sebagai *root user*, lalu masukkan passwordnya, dan ketik *sudo wireshark* untuk memanggil aplikasi Wireshark seperti pada gambar berikut ini :



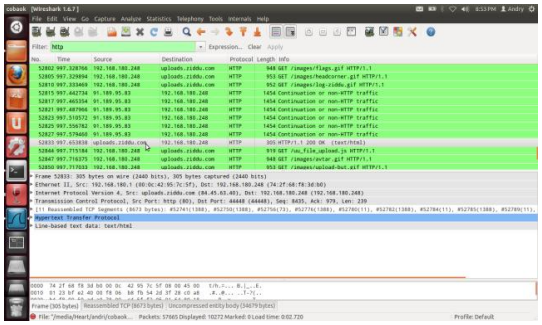
Gambar 16. Tampilan Perintah dan Menu Utama Wireshark

Setelah tampilan Wireshark muncul, pilih tab capture lalu capture option untuk memilih *interface* jaringan yang kita gunakan, disini penulis memakai LAN, sehingga *interface* dipilih adalah *eth0*.



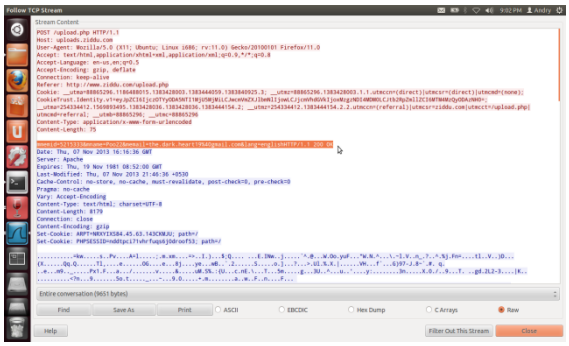
Gambar 17. Tampilan Capture Options Wireshark

Setelah itu, maka akan muncul hasil record yang didapat secara *real time* oleh Wireshark, tetapi karena Wireshark merekam semua lalu lintas yang terdapat dalam jaringan, maka semua informasi tersebut akan langsung di *capture* dalam tampilan Wireshark. Untuk itu diperlukan *filter* untuk menentukan paket apa saja yang ingin diketahui oleh *user*. Ketikkan *http* pada kolom *filter* sehingga paket yang muncul adalah yang memakai protokol http.



Gambar 18. Tampilan Wireshark dengan Filter Http

Lalu setelah ditemukan paket protokol yang diinginkan, seperti pada gambar, berasal dari situs http://www.ziddu.com. klik kanan pada paket tersebut, lalu klik *Follow TCP Stream* untuk melihat detail informasi yang didapatkan dari paket tersebut. Gambar berikut merupakan isi detail paket tersebut.



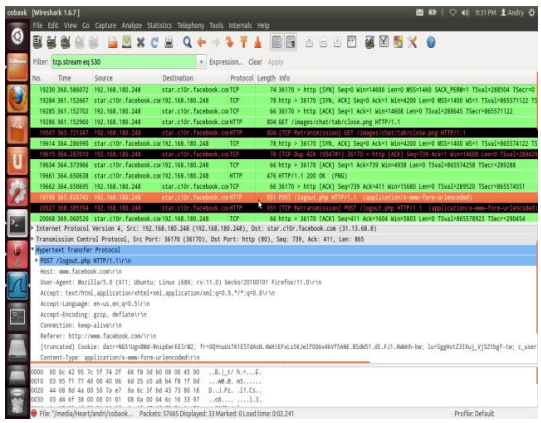
Gambar 19. Tampilan Detail Paket HTTP yang Dicapture

3.2.1.1. Analisis Paket HTTP

Berdasarkan paket yang didapat, *host* tujuan yang digunakan adalah http://www.ziddu.com, hal tersebut berdasarkan pada baris informasi paket yaitu Referer: http://www.ziddu.com/upload.php. Tanggal pengambilan paket terlihat pada baris Date: Thu, 07 Nov 2013 16:16:36 GMT, yaitu hari Kamis, 7 November 2013. Server host ziddu menggunakan Apache, sesuai dengan baris informasi Server: Apache. Pada baris yang diseleksi, terdapat informasi mengenai akun pengguna yaitu username : Poo22, dan email : the.dark.heart19@gmail.com. Hal tersebut merupakan salah satu kelemahan protokol HTTP, karena tidak memiliki enkripsi, sehingga seringkali username dan password pengguna dapat tertangkap oleh pengguna yang tidak berhak. Untuk itu tidak ada, transaksi *internet banking*, dan pembayaran lainnya menggunakan protokol ini.

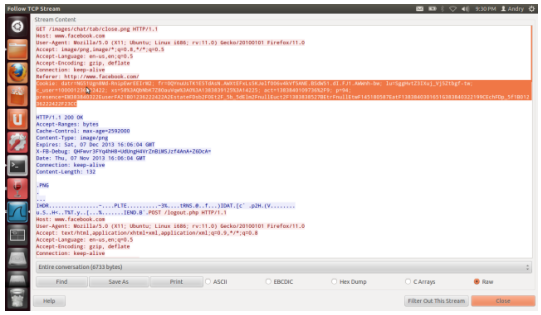
3.3. Sniffing Paket HTTPS (HTTP *Secure*)

Untuk mengetahui perbedaannya dengan protokol HTTP, maka penulis akan menjabarkan analisis paket pada protokol HTTPS. Masih dalam *live capture* yang sama, penulis akan menganalisis salah satu paket yang terekam dari situs http://www.facebook.com yaitu paket *logout* dari salah satu user, seperti terlihat dalam gambar IV.5 berikut ini.



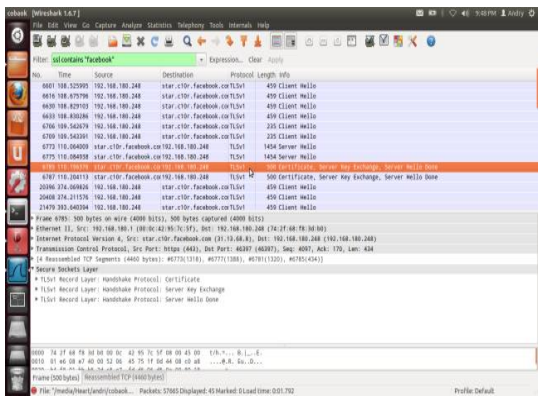
Gambar 20. Paket Logout dari Host Facebook

Klik kanan, dan pilih *Follow TCP String* untuk melihat detailnya, dan akan muncul seperti gambar berikut ini.

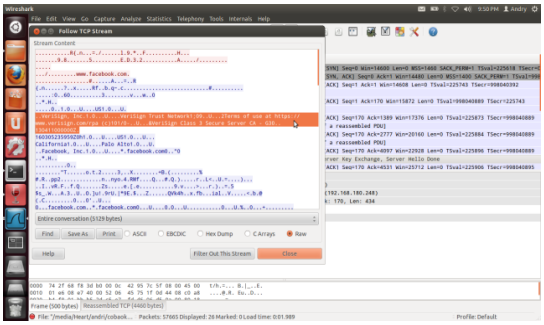


Gambar 21. Detail Paket dari Logout Facebook

Untuk melihat server enkripsi yang digunakan situs ini, maka dapat dilakukan dengan mengetik pada *filter*, sintaks berikut : *ssl contains "facebook"*. Maka akan muncul paket data protokol SSL (*Secure Socket Layer*) yaitu protokol keamanan data yang digunakan untuk menjaga pengiriman data antar *server* dan *client*.



Gambar 22. Tampilan Filter SSL Facebook



Gambar 23. Detail Paket Protokol SSLv1 pada Facebook

3.3.1. Analisis Paket HTTPS (HTTP Secure)

Berdasarkan paket *logout* yang terekam, maka dapat dilihat bahwa paket dalam keadaan sudah terenkripsi, hal tersebut terlihat pada baris yang diseleksi yaitu *cookie*, seperti *datr* = NG51Ugn8Md-RnipEwrEEIrM2, dan facebook menulis data ID pengguna yaitu pada *c_user* = 100001236222422 dan selanjutnya. Facebook menggunakan jasa suatu server untuk keperluan enkripsi. Hasilnya berdasarkan gambar, diketahui bahwa server yang mememberikan tanda tangan digital dalam keperluan dekripsi, terlihat pada gambar, yaitu *www.verisign.com*.

Perbandingan antara Wireshark dan Cain

Wireshark	Cain
Untuk penggunaan pada OS Linux, dibutuhkan aplikasi pendukung seperti Ettercap agar mendapat hasil sniffing yang lebih baik.	Tidak tersedia untuk Linux, dan tidak memerlukan aplikasi lain sebagai pembantu.
Memiliki banyak fungsi seperti pemeliharaan jaringan, mencari pengguna arp poisoning, dll.	Fungsinya lebih ke enkripsi kata sandi jaringan

4. Kesimpulan

Berdasarkan dari proses pengujian yang telah dilakukan, dapat disimpulkan bahwa keamanan yang dimiliki oleh jaringan tanpa kabel atau wireless cukup rentan akan penyadapan, karena dengan melalui Cain, serangan *Man In The Middle Attack* dapat dilakukan tanpa adanya rintangan atau kemanan yang harus dilalui.

Daftar Rujukan

[1] Witono Timotius. 2006. Linux-Based *Access point* Dalam *Wireless* LAN. (Jurnal Informatika, Vol. 2, No.2). Bandung : Sekretariat Jurnal Informatika UKM

[2] Arifin Zaenal. 2008. Sistem Pengamanan Jaringan *Wireless* LAN. Yogyakarta : ANDI

[3] Purbo, Onno.W, 1998, *TCP/IP Standar, Desain dan Implementasi*, PT. Elex Media Komputindo, Jakarta.

[4] Joko I. Mumpuni dan Adisuryo Wardono. 2006. Meningkatkan Kemampuan Jaringan

[5] Komputer. Yogyakarta : ANDI

[6] Prakoso Samuel. 2005. Jaringan Komputer Linux Konsep Dasar, Instalasi, Aplikasi, Keamanan, dan Penerapan. Yogyakarta : ANDI

[7] Nuraksa Makodian dan Lingga Wardhana. 2009. Teknologi Wireless Communication dan Wireless Broadband. Yogyakarta : ANDI

[8] Stalling W, Data and Computer Communication, Macmillan Publishing, 1985.

[9] Hartono,Jogianto.1999.Pengenalan omputer, dasar ilmu komputer, pemrograman,sistem informasi dan intelegnsi buatan.Yogyakarta : Penerbit ANDI

[10] Stalling, W.Local Network, Macmillan Publishing Company, 1985

[11] Arifin Zainal.2005.Langkah Mudah Membangun Jaringan Komputer. Yogyakarta :Penerbit ANDI

[12] IEEEb http://www.IEEE802.org/11/ Diakses terakhir pada tanggal 11 November 2012 , pukul 22.55 WITA

[13] Wireless Technology

[14] Hidayat Risanuri.2003. Wireless LAN. Yogyakarta

[15] http://compnetworking.about.com/cs/*wireless*80211/a/aa80211standard.htm/ Diakses terkahir pada tanggal 20 November 2012, pukul 18:05 Signal Interferensi

[16] http://www.far-far-away.com/~yousif/articles/wifi-sig.php Diakses terakhir pada tanggal 25 Oktober 2012 , pukul 22.00 WITA.