IMPLEMENTASI DAN ANALISIS JARINGAN MENGGUNAKAN WIRESHARK, CAIN AND ABELS, NETWORK MINNER (Studi Kasus: AMIK Dian Cipta Cendikia)

Didi Susianto[1], Anisa Rachmawati[2]
[1,2] *Jurusan Manajemen Informatika, AMIK Dian Cipta Cendikia Bandar Lampung*
Jl. Cut Nyak Dien No. 65 Durian Payung (Palapa) Bandar Lampung
E-mail: di2.susianto@dcc.ac.id[1)], Annisarachmawati36@gmail.com[2)]

ABSTRAKS
Pembelajaran menggunakan internet belum dapat diterapkan secara maksimal dikarnakan banyak mahasiswa saat belajar tidak membuka situs tentang materi tetapi situs yang lainya dan jaringan internet yang lambat mengakibatkan mahasiswa kurang puas dalam mengakses internet. Metode Penelitian yang digunakan dalam penelitian ini adalah dengan menggunakan Studi Kasus, Studi Kasus menggunakan cara-cara yang sistematis dalam melakukan pengamatan, pengumpulan data, analisis informasi, dan pelaporan hasilnya, pengamatan terhadap interaksi paket data dilakukan menggunakan Software Wireshark, Cain and Abels dan NetworkMiner, pelaksanaan pengamatan dilakukan dengan cara menginstalasi NetworkMinner pada laptop atau komputer lalu mengcapture (menangkap) paket paket data yang berinteraksi dalam jaringan internet menggunakan wireshark dan menganalisanya melalui NetworkMiner. Hasil yang diharapkan dari penelitian ini adalah agar dosen dapat mengetahui situs apa saja yang dibuka oleh mahasiswa yang terhubung pada jaringan AMIK Dian Cipta Cendikia Bandar Lampung dalam mengakses internet apakah mahasiswa menggunakan internet dengan benar untuk membuka situs tentang materi atau hanya bermain-main saat sedang terhubung pada WLAN (Wireless Local Area Network) AMIK Dian Cipta Cendikia Bandar Lampung.

Kata Kunci:Keamanan jaringan, Wireshark, Cain and Abels, Network Minner

1. PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer bukanlah sesuatu yang baru saat ini, hampir di setiap tempat terdapat jaringan komputer untuk memperlancar arus informasi pada tempat tersebut. Didalam sebuah jaringan komputer terdapat banyak sekali paket data yang berlalu lalang pada kabel jaringan, baik itu paket data yang mengandung informasi informasi seperti password, alamat sebuah situs, user name, ip user dan lain-lain. Untuk mengetahui atau memonitoring aktivitas user misalnya sedang membuka situs apa ketika sedang tekoneksi dengan internet, pembelajaran menggunakan internet belum dapat diterapkan secara maksimal dikarnakan banyak mahasiswa saat belajar tidak membuka situs tentang materi tetapi situs yang lainya dan jaringan internet yang lambat mengakibatkan mahasiswa kurang puas dalam mengakses internet, Untuk mengetahui atau mengontrol user pada WLAN (Wireless Local Area Network) dibutuhkan analisis jaringan menggunakan Aplikasi "Wireshark" yang dilakukan oleh pihak network analyzer dengan tujuan menganalisa jaringan dengan melakukan pengawasan yang dilakukan oleh User sehingga Administrator dapat mudah memonitoring aktivitas-aktivitas yang dilakukan oleh user.

Analisis jaringan komputer menggunakan aplikasi "Wireshark" diterapkan pada AMIK Dian Cipta Cendikia Bandar Lampung, agar dosen atau instruktur lab dapat mengawasi aktivitas yang dilakukan oleh siswa, apakah komputer digunakan secara maksimal untuk belajar atau hanya untuk hiburan semata, Instruktur lab juga dapat mengetahui jika siswa menggunakan internet tidak untuk belajar melainkan hanya untuk mainan maka instruktur lab dapat menegor terhadap siswanya.

Maka dari itu Tools yang sangat tepat digunakan untuk administrator dalam mengawasi jaringan adalah Tools Wireshark dimana tools ini sangat berguna untuk administrator dalam memonitoring jaringan, tools Wireshark mampu menangkap paket-paket data atau informasi yang berjalan dalam jaringan dan tools wireshark mampu menangkap dan menganalisa lalu-lintas jaringan WLAN (Wireless Local Area Network).

1.2 Referensi

a. Nama Peneliti Sonny Rumalutur Jurusan Teknik Elektro, Fakultas Teknologi Industri, Universitas Gunadarma Jl. Margonda Raya No. 100, Pondok Cina, Depok 16424, jurnalnya berjudul "Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong" tahun jurnal " Jurnal Teknologi dan Rekayasa, Volume 19 No. 3, Desember 2014", masalah yang ada pada jurnal tersebut adalah Jaringan wireless sangatlah rentan ter-hadap serangan, hal ini dikarenakan jaringan wireless tidak dapat dibatasi oleh sebuah gedung seperti yang diterapkan pada jaringan berbasis kabel. Sinyal radio yang dipancarkan oleh perangkat wireless dalam melakukan proses transmisi data didalam sebuah jaringan dapat dengan mudah diterima/ditangkap oleh pengguna komputer lain selain pengguna dalam satu jaringan hanya

P-ISSN:0216-9436
E-ISSN:2622-6782

dengan menggunakan perangkat yang kompatibel dengan jaringan wireless seperti kartu jaringan wireless, metode yang digunakan penelitian ini adalah :

Metode 1 :

1. Melakukan koneksi berdasarkan informasi MAC Address dan Mendapatkan IP Address lalu membuka session koneksi Wireless dengan melakukan login ke Web Proxy dan terhubung dengan server.
2. Melakukan penyadapan paket untuk mendapatkan MAC Address yang sah dengan menggunakan software Network Stumbler serta memalsukan MAC Address miliknya dan melakukan koneksi dengan access point berdasarkan MAC address yang dipalsukan.

Metode 2 :

1. Melakukan koneksi dengan access point berdasarkan MAC Address yang dipalsukan dan mendapatkan IP Address dan koneksi Wireless LAN dibuka dengan melakukan login ke Web Proxy.
2. Melakukan koneksi dengan access point berdasarkan MAC address yang dipalsukan dan mendapatkan IP Address dan tidak dapat membuka session koneksi Wireless LAN saat login ke Web Proxy.

Hasil Analisis dengan Protokol WPA Dengan Protokol WPA dapat mengatasi kelemahan pada integritas data dan ketersediaan pada sistem. Dan penulis mencoba melakukan percobaan untuk membuktikan kelemahan protokol WPA jika diterapkan pada Wireless LAN, yaitu dengan melakukan serangan terhadap encryption (Network Key atau password) yang digunakan oleh access point.

Hasil Analisis Dengan Keamanan Web Proxy arsitektur Wireless LAN dan jaringan kabel merupakan bagian dari jaringan terintegrasi. Akses kontrol terhadap device yang ingin melakukan koneksi dilakukan dengan menggunakan MAC Address dari peng-guna yang disimpan dalam server LDAP (Lightweight Direction Access Protocol). Proses otentikasi ke dalam jaringan dilakukan dengan melalui Web Proxy yang menggunakan protokol Secure Socket Layer (SSL). SSL adalah protokol keamanan yang bekerja di atas lapisan ke 4 (empat) OSI (transport layer), dimana semua data-data yang melalui protokol ini akan dienkripsi. Setelah pengguna terotentikasi, maka pengguna akan mendapatkan hak akses kedalam jaringan kabel internal dan ke internal (dengan menggunakan proxy server). Pengguna Wireless LAN menggunakan Web Proxy dengan protokol SSL dalam proses otentifikasi, memberikan perlindungan keamanan terhadap pencurian informasi wireless username dan password karena data-data tersebut ditransmisikan dalam bentuk terenkripsi.

b. Nama peneliti Tengku Mohd Diansyah, Sekolah Tinggi Teknik Harapan Medan, Jurusan Teknik Informatika, Judul Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Menggunakan Wireshark, nomor jurnal Vol. IV No 2 : 20-23, 2015 ISSN : 2337 – 3601, Masalah yang ada pada penelitian ini adalah dalam hal ini adalah gangguan dari pihak-pihak yang telah mengetahui kondisi keamanan dan kelemahan jaringan tersebut. Gangguan eksternal adalah gangguan yang memang berasal dari pihak luar yang ingin mencoba atau dengan sengaja ingin menembus keamanan yang telah ada. Gangguan eksternal biasanya lebih sering terjadi pada jaringan eksternal, seperti web server, telnet, FTP, SSH server, penelitian ini menggunakan Metode Eksperimen, Hasil pengujian ini adalah pengujian aktivitas yang berhasil di-capture oleh wireshark terhadap informasi sumber, tujuan protocol dan waktu capture-nya.
c. Nama Peneliti: Didi Susianto dan Iis Yulianti, AMIK Dian Cipta Cendikia Bandar Lampung, Jurusan Manajemen Informatika, Judul: Mengamankan Wireless Dengan Menggunakan Two Factor, Password dan Mac Address Filtering. Masalah: Banyak organisasi dan perusahaan menyediakan layanan hotspot untuk anggota atau karyawan tetapi karena sistem keamanan masih menggunakan password WPA sehingga banyak orang walaupun bukan anggota atau karyawan menggunakan layanan hotspot. Tentunya hal ini sangat merugikan pihak organisasi maupun perusahaan karena harus berbagi koneksi internet yang sama dengan pengguna lain yang tidak punya kewenangan. Hasil dari penelitian ini adalah penggunaa dua faktor keamanan yaitu keamanan WPA-PSK dan dengan menggunakan Mac Address Filtering, yang berarti jika ada sesorang yang ingin mengakses wifi harus mempunyai dua otentikasi, karena apabila hanya memiliki password WPA-PSK-nya saja maka tetap tidak akan bisa terkoneksi karena mac address pada perangkatnya tidak terdaftar.
d. Menurut Wicaksono (2009: 30), Wireshark adalah penganalisis paket gratis dan sumber terbuka. Perangkat ini digunakan untuk pemecahan masalah jaringan, analisis, perangkat lunak dan pengembangan protokol komunikasi, dan pendidikan.
e. Menurut Massimiliano Montoro program bantu cain&abel merupakan program hasil buah karya Massimiliano Montoro. Program ini dikhususkan dalam penanganan recovery password pada system operasi Microsoft Windows yang cenderung menangani masalah jaringan (baik aplikasi networking sampai dengan aplikasi yang menggunakan fitur database server) (http://www.oxid.it/cain.html).

P-ISSN:0216-9436
E-ISSN:2622-6782

f. Menurut Jogiyanto (2009:129), Analisis dapat didefinisikan sebagai penguraian dari suatu sistem informasi yang utuh kedalam bagian-bagian komponennya dengan maksud untuk mengidentifikasikan dan mengevaluasi permasalahan-permasalahan, kesempatan kesempatan, hambatan-hambatan yang terjadi dan kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikannya.

g. Menurut Pratama (2014:12), jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup semua jenis perangkat komputer (komputer desktop, smartphone , tablet) dan perangkat penghubung (router, switch, modem dan hub).

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah menggunakan studi kasus, studi kasus menggunakan cara-cara yang sistematis dalam melakukan pengamatan, pengumpulan data, analisis informasi, dan pelaporan hasilnya.

2.1 Teknik Pengumpulan Data

a. Metode yang digunakan dalam penelitian ini adalah menggunakan studi kasus, studi kasus menggunakan cara-cara yang sistematis dalam melakukan pengamatan, pengumpulan data, analisis informasi, dan pelaporan hasilnya.

b. Pengamatan terhadap interaksi paket data dilakukan menggunakan software wireshark, cain and abels dan networkminer, pelaksanaan pengamatan dilakukan dengan cara menginstalasi networkminer pada laptop atau komputer lalu mengcapture (menangkap) paket paket data yang berinteraksi dalam jaringan internet menggunakan wireshark dan menganalisanya melalui NetworkMiner.

2.2 Kebutuhan Fungsional

a. Sistem harus mampu menangkap paket data yang ada di dalam jaringan WLAN.

b. Sistem harus mampu menganalisa paket data yang ada di dalam jaringan WLAN.

2.3 Kebutuhan Non Fungsional

1. Kebutuhan Perangkat Keras
   Perangkat keras (Hardware) yang digunakan adalah laptop dengan spesifikasi berikut :
   a. Laptop Acer Aspire 4752
      - Sistem Operasi Windows
      - Prosessor Intel Core i3 2330M
      - RAM 2GB
      - Hardisk 500 GB
   b. Printer Canon iP 1980
2. Perangkat Lunak
   a. Windows 7
   b. Wireshark
   c. Cain and Abel
   d. NetworkMiner

2.4 Perancangan Sistem Teknik PGP

Dalam melakukan monitoring ini, peneliti masuk ke jaringan Wifi yang tersedia pada AMIK Dian Cipta Cendikia Bandar Lampung Khususnya di Kampus A yang dapat digunakan Mahasiswa AMIK Dian Cipta Cendikia Bandar Lampung. Sebelum melakukan monitoring, Software Cain and Abel dijalankan terlebih dahulu untuk melakukan routing agar traffic jaringan bisa terpantau. Lalu menggunakan Wireshark untuk mendapatkan hasil capture packet agar dapat dianalisis paket jaringan pada AMIK Dian Cipta Cendikia Bandar Lampung Kampus A dan paket data disimpan. Selanjutnya Paket data yang tersimpan pada wireshark di buka kembali melalui NetworkMiner Untuk melakukan analisis menggunakan NetworkMiner berguna untuk menampilkan website yang diakses.

a. Jaringan WLAN (Wireless Local Area Network)

Sebelum melihat paket data yang masuk pada jaringan, terlebih dahulu terhubung ke jaringan WLAN (Wireless Local Area Network) agar software mampu menganalisa paket data yang masuk pada jaringan WLAN (Wireless Local Area Network) di AMIK Dian Cipta Cendikia Bandar Lampung KampusA.

b. Software Cain and Abels

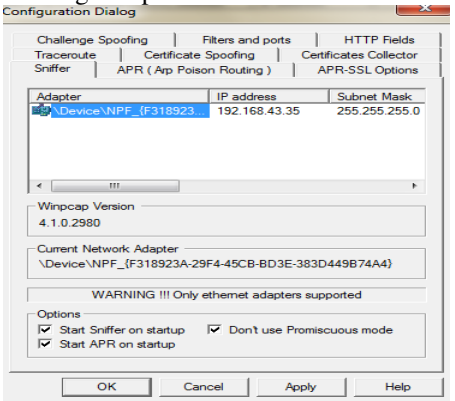
Software Cain and Abel dijalankan terlebih dahulu untuk melakukan routing agar traffic jaringan bisa terpantau.

Langkah-Langkah Routing Jaringan menggunakan Software Cain and Abels :

1. Buka software cain and abels

Gambar 1 Tampilan Awal Software Cain and Abels

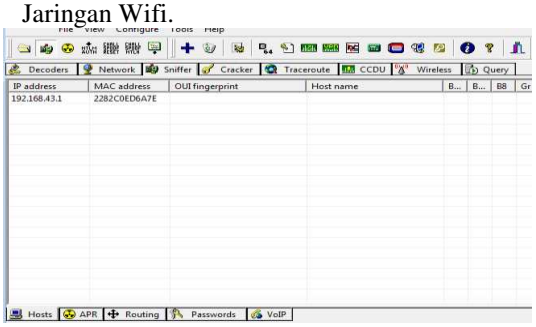
2. Klik menu configurate pilih device yang terhubung lalu pilih OK



Gambar 2 Configurate Software Cain And Abels

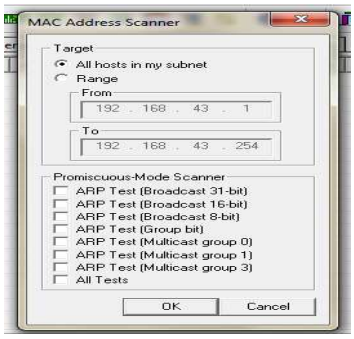
P-ISSN:0216-9436
E-ISSN:2622-6782

3. Selanjutnya Klik Start Sniffer, Lalu Klik Gambar Tambah untuk Melihat Host IP yang ada pada Jaringan Wifi.



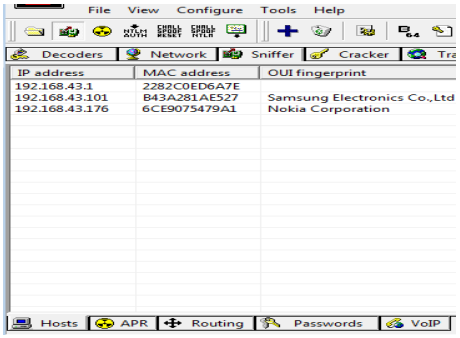
Gambar 3 Start Sniffer

4. Maka akan muncul seperti gambar dibawah ini Lalu Klik OK.



Gambar 4 Start IP Client

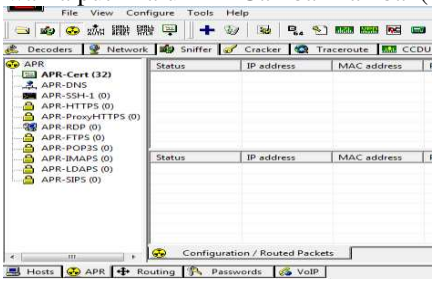
5. Maka Ip yang berada pada jaringan Wifi sudah Terlihat



Gambar 5 IP Client Masuk

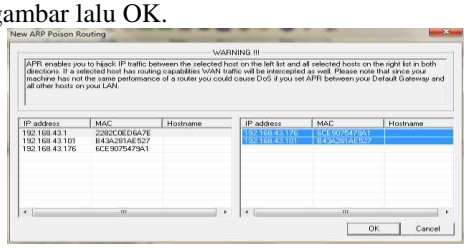
Untuk Memulai Proses Selanjutnya kita akan routing jaringan wifi yang tersedia :

1. Klik Gambar Star ARP , Lalu Klik tulisan ARP yang berada di bawah, Klik kotak kosong berwarna putih lalu Klik Gambar Tambah(+).



Gambar 6 Start APR

2. Maka akan muncul gambar seperti dibawah ini, Klik Ip yang berada di atas bagian kiri gambar dan blok semua Ip yang berada pada Kanan gambar lalu OK.



Gambar 7 Block IP

3. Blok semua ip lalu Klik Start APR

Gambar 8 Block IP dan Start ARP

4. Maka Jaringan wifi telah berhasil di Routing

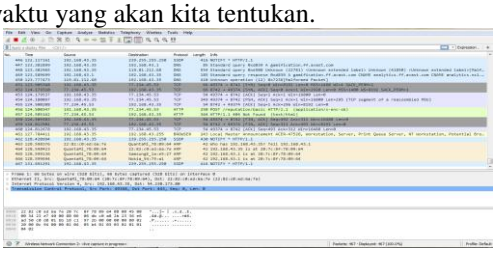
Gambar 9 Hasil Routing

b. Software Wireshark

1. Buka Software Wireshark untuk melihat paket data yang masuk Pada Jaringan Wifi dan Klik jaringan yang sudah Terhubung yaitu Wireless Network Connection selanjutnya pilih Capture Lalu Klik Start.

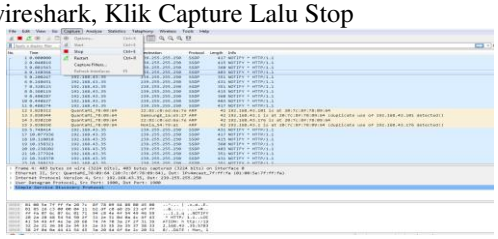
Gambar 10 Start Software Wireshark

2. Lalu Wireshark akan langsung menangkap paket paket data yang berada pada jaringan wifi, biarkan software wireshark berjalan sampai waktu yang akan kita tentukan.



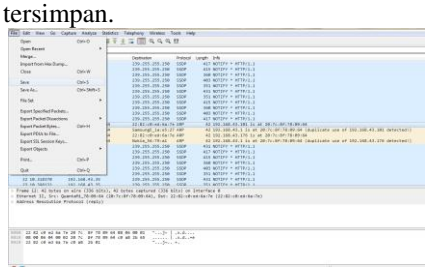
Gambar 11 Capture Paket Data Wireshark

3. Jika sudah maka kita akan stop software wireshark, Klik Capture Lalu Stop



Gambar 12 Stop Software Wireshark

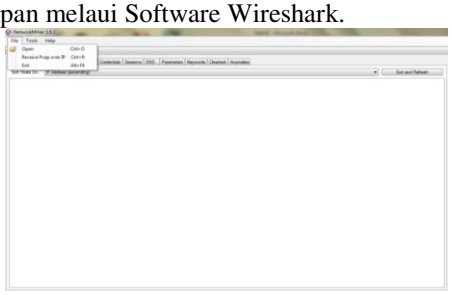
4. Data yang tercapture dari wiresshark akan disimpa agar dapat dianalisa oleh software Network Minner, Klik file lalu save maka paket data tersimpan.



Gambar 13 Save Paket Data

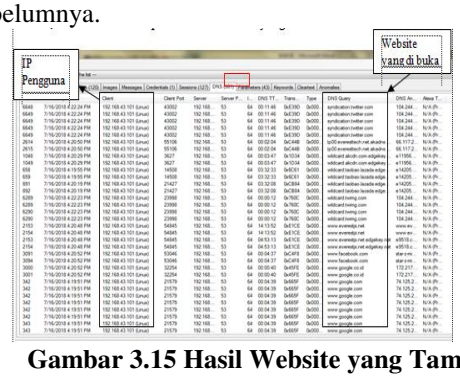
c. Software NetworkMinner

1. Buka Software NetworkMinner agar paket data yang tercapture dari wireshark dapat dianalisa. Klik File Open lalu cari paket data yang sudah di simpan melaui Software Wireshark.



Gambar 14 Open Paket Data

2. Maka akan tampil data data yang sudah di tangkap Melalui Software Wireshark sebelumnya.



Gambar 3.15 Hasil Website yang Tampil

Hasil data yang di dapat dari analisa di atas yaitu:

Tanggal/Waktu	IP	Website
16-07-2018/ 04:16:35 PM	162.168.43.101	- www.google.com - whatsapp - www.lazada.com - www.twitter.com - mail.google.com - www.youtube.com - www.gstatic.com - www.facebook.com
16-07-2018/ 04:19:54 PM	162.168.43.101	- www.operamini.com - www.facebook.com

Gambar 16 Contoh Hasil Data Website

Dari hasil yang didapat diatas bahwa website yang paling bayak dibuka oleh pengguna yaitu www.facebook.com.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Berikut ini adalah hasil penelitian Analisa Website yang dibuka pada AMIK Dian Cipta Cendikia Bandar Lampung yaitu :

No	Tanggal/Waktu	IP	Website
1	23-07-2018/ 12:34:35 PM	192.168.1.4	- baca.co.id - amazonaws.com - xiaomi.com
2	11:20:28 AM	192.168.1.13	- www.google.com
3	11:19:27 AM	192.168.1.15	- whatsapp - facebook.com - youtube - www.google.com - grabtaxi.com - doubleclick.net - picsart.com - mopud.com - supersonicad.com - inmobi.com - adrta.com - www.ssacdn.com - www.googlemanager.com
4	13:24:23 PM	192.168.1.23	- youtube - gmail - shoope.co.id - googlevidio.com - akamai.net - play.google.com - doubleclick.net
5	11:19:15 AM	192.168.1.1.27	- facebook - whatsapp - bbm - instagram - www.bing.com

Gambar 17 Hasil Analisa Website

3.2 Pembahasan

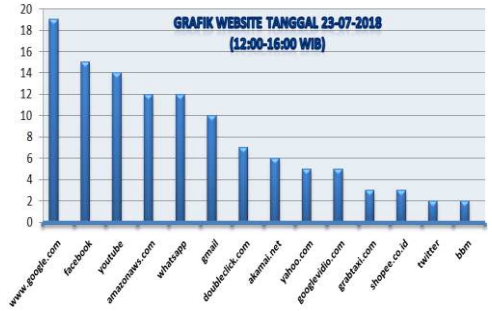
Berdasarkan hasil penelitian di atas maka peneliti akan membahas hasil penelitian di atas sebagai berikut :

1. Pada tanggal 23-07-2018 penelitian dilakukan siang hari yaitu pada jam 11:00-16:00 WIB, dari hasil penelitian di atas ada 36 user yang masuk, dan ada 71 website yang di buka oleh user pada jam 11:00-16:00, website yang banyak di buka yaitu :

1. www.google.com = 19 user
2. facebook = 15 user
3. youtube = 14 user
4. amazonaws.com = 12 user
5. whatsapp = 12 user
6. gmail = 10 user
7. doubleclick.com = 7 user
8. akamai.net = 6 user
9. yahoo.com = 5 user
10. googlevidio.com= 5 user
11. grabtaxi.com = 3 user
12. shopee.co.id = 3 user
13. twitter = 2 user

P-ISSN:0216-9436
E-ISSN:2622-6782

14. bbm = 2 user



Gambar 18 Grafik Hasil Analisa Website

Website yang paling banyak di buka yaitu www.google.com sebanyak 19 user.

4. KESIMPULAN

Setelah dilakukan hasil analisa dan pembahasan penelitian, dapat diperoleh kesimpulan sebagai berikut:

1. Hasil yang telah dianalisa didapatkan bahwa penggunaan wifi belum dimanfaatkan secara penuh oleh mahasiswa, dikarnakan banyak mahasiswa mengakses sosial media paling banyak.
2. Jumlah user pengunjung website pada pagi hari sebanyak 62 user dengan website yang paling banyak diakses yaitu facebook sebanyak 28 user dan siang hari sebanyak 104 user dengan website yang paling banyak diakses yaitu facebook sebanyak 36 user.
3. Berdasarkan hasil perhitungan penggunaan website pada AMIK Dian Cipta Cendikia Bandar Lampung dapat diketahui pengguna Website terbanyak yaitu facebook.com 64 user, whatsapp 61 user, www.google.com 55 user, youtube.com 47 user, amazonaws.com 45user.
4. Jumlah pengunjung website secara keseluruhan sebanyak 166 user dan jumlah keseluruhan website yang di akses ada 272 website, Dari jumlah tersebut website facebook yang sering diakses oleh mahasiswa, dengan alasan karena facebook sebagai jaringan komunikasi yang banyak disukai oleh mahasiswa.

Berdasarkan kesimpulan di atas, maka kelebihan dan kekurangan dapat menjadi masukan serta referensi untuk kedepannya. Saran yang dapat dipertimbangkan, antara lain :

1. Untuk Administrator, perlunya adanya monitoring minimal setiap bulan secara rutin di wifi AMIK Dian Cipta Cendikia Bandar Lampung sehingga dapat dilihat penggunaannya apakah dimanfaatkan secara baik atau tidak dalam menunjang perkuliahan.
2. Bagi peneliti lain, mengingat kelemahan hasil penelitian pada peroleh data masih kurang, sehingga bagi peneliti selanjutnya dalam pengumpulan data perlu memperhatikan lama waktu yang digunakan, sehingga data-data yang dikumpulkan lebih banyak dan hasilnya akan lebih baik lagi.

PUSTAKA

Adiba Kamalia, fitur-fitur pada wireshark,http://ilmukomputer.org/2014/09/14/ Fitur-fitur-wireshark/, tanggal akses 15 April 2018.

Anonim., 2014, Modul Pelatihan Sniffing Jaringan Menggunakan Cain&Abel.

Bangkit Kurnia Ari Setyawan, Melwin Syafrizal., 2012, Analisis Keamanan Jaringan Wireless Yang Menggunakan Captive Portal, Vol. 13, No, 3 September 2012, Yogyakarta, Page 1-7.

Imam Prasetyo., Pengenalan dan instalasi Wireshark, http://ilmukomputer.org/2013/05 /26/pengenalan-dan-instalasi-wireshark-2, tanggal akses 15 April 2018.

Jogiyanto, 2009. Sistem Informasi Manajemen. Yogyakarta: Penerbit Andi.

Naufal Samir, Irwansyah, Helda Yudiastuti., Analisis Dan Monitoring penggunaan Hotspot Pada Kantor Disdikpora Kota Palembang Terhadap Dampak Kinerja Jaringan.

Pratama. I Putu Agus, "Handbook Jaringan Komputer Teori dan Praktik Berbasiskan Open Source, 1st ed, Bandung: BI-Obses, 2014

Ridlwan Pahala., 2015, Perancangan Sistem Pencegahan Flooding Data pada jaringan Komputer, Tugas Akhir, Fakultas Komunikasi Dan Informatika Universitas Muhammadiyah, Surakarta.

Susianto, D., & Yulianti, I. (2015). Mengamankan Wireless dengan Menggunakan Two Factor, Password dan Mac Address Filtering. EXPERT, 5(2).

Sonny Rumalutur (2014). Analisis Keamanan Jaringan *Wireless* LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong. Jurnal Teknologi dan Rekayasa.

Diansyah, T. M. (2016). Analisa pencegahan aktivitas ilegal didalam jaringan menggunakan Wireshark. Jurnal Times, 4(2), 20-23.

Wicaksono, Rizki.2009. Sniffing SSL Traffic using oSpy. http://www.ilmuhacking.com/

Yama Fresdian Dwi Saputro., Instalasi Program Monitoring Jaringan Wireshark, http://ilmukomputer.org/2014/09/11/instalasi-program-monitoring-jaringan-wireshark, tanggal akses 15 April 2018.

http://www.oxid.it/cain.html