Jurnal Cendikia Vol. XVI Cendikia 2018 Bandar Lampung, Oktober 2018 P-ISSN:0216-9436 E-ISSN:2622-6782

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

Didi Susianto<sup>1</sup>, Anisa Rachmawati<sup>2</sup>

<sup>1,2</sup> 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<sup>1</sup>, Annisarachmawati36@gmail.com<sup>2</sup>)

#### 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 mengganalisanya 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 internet, tekoneksi dengan 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 paketpaket 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 Rava 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 vang 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 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.
- 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 :
- 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.
- 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 datadata 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 karena terkoneksi 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).

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

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

riie T	view Configure	roois neip		
🛳 🏟 😔		+ 🛛 😼 🧣	. 🕥 💷 📟 🚾 📟 🥅	જી 🖾 🚺 🖇 🦺
👶 Decoders	🔮 Network 📸	Sniffer 🥑 Cracker 🕴	😋 Traceroute 🛛 CCDU 🕅	Wireless 🚯 Query
IP address	MAC address	OUI fingerprint	Host name	B B B8 Gr
192.168.43.1	2282C0ED6A7E			
		1.0		

**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

File V	iew Configure	Tools Help
🛛 🛥 🔹 🕉 🖞	ta Bee Ale 🖷	🕂 🦦   😼   🗞 🕥
歳 Decoders 💡	Network 🖼 S	niffer 🥑 Cracker 🗔 Tra
IP address	MAC address	OUI fingerprint
192.168.43.1	2282C0ED6A7E	
192.168.43.101	B43A281AE527	Samsung Electronics Co.,Ltd
192.168.43.176	6CE9075479A1	Nokia Corporation
📇 Hosts 😽 AF	PR 🕂 Routing	👫 Passwords 🛛 🚳 VoIP
Gaml	bar 5 IP Cli	ient 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(+).



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.

machine has not all other hosts on	the same performance your LAN.	of a router you could	cause DoS if you set	APR between your De	stault Gateway and
P address	MAC	Hostname	IP address	MAC	Hostname
92.169.43.1	2282C0ED6A7E		192.168.43.176	GCE 9075479A1	
92.168.43.101 92.168.43.176	6CE9075479A1		192.168.43.101	B43A281AE527	
c.					

Gambar 7 Block IP

3. Blok semua ip lalu Klik Start APR

Decoders 👰 Network	🔹 Sniffer 🧟	Cracker 🛄 T	raceroute 🛄 CC	:DU 😵 Wie	eless 🚯 Q	uery	
APR	Status	3P address	MAC address	Packets ->	<- Packets	MAC address	IP address
APR-Cert (0)	Alle						
APR-DNS	Alle	192.168.43.1	2282C01D6A7E	0	0	6CE9075479A3	192.368.43.176
APR-55H-1 (0)							
APR-HTTPS (0)							
APR-ProxyHTTPS (0)							
APE-FEDP (0)							
APK-PTPS (0)							
APR-PUP3S (0)	finder.	The set of second	MAC address	Backate	C. Backete	MAC address	10 address
APR-IMAPS (0)	ALCO S	a- address	mane, and ress	Packets - P	C-Patricis	Hunc address	a anness
ADD-CIDC (0)							
(v)							

Gambar 8 Block IP dan Start ARP

4. Maka Jaringan wifi telah berhasil di Routing

	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
lert (4)	A Poisoning	192.168.43.1	2282C0E06A7E		8	843A281AE527	192.168.43.101
NS H-1 (0)	APeisoning	192.168.43.1	2282C0ED6A7E	4	3	6CE9075479A1	192.168.43.176
TPS (0) wyHTTPS (0) P (0) PS (0)							
APR-POP35 (0) APR-BAAP5 (0) APR-LDAPS (0)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
	Half-rosting	192.168.43.101	843A281AE527	9	0	2282C0ED6A7E	74.125.200.101
IIPS (0)	S Full-routing	192.168.43.101	843A281AE527	10	6	2282C0ED6A7E	223.255.230.139
	Ful-couting	192.168.43.101	\$43A281AE527	28	23	2282C0ED6A7E	23.5.196.333
	Full-routing	192.168,43.101	843A291AE527	-40	61	2282C0ED6A7E	23.3.78.74
	Full-routing	192,368,43,176	6CE9075479A2	4	3	2282C0ED6A7E	107.167.115.241
	Full-routing	192,168,43,101	843A281AE527	12	30	2282C0ED6A7E	54,251,172,184
	Full-routing	192.168.43.176	6CE9075479A3	12	7	2282C0ED6A7E	107.167.115.239
	Full-routing	192,168,43,101	843A281AE527	9	6	2282C0ED6A7E	66.117.25.58
	Full-routing	192.168.41.176	6CER07547941	10		228200606075	107.167.115.252
	d blat motion	10216843176	600007547041	1	0	2282C0ED6A7E	173.252.127.254

#### **Gambar 9 Hasil Routing**

#### b. Software Wireshark

Della to to the B

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.

D 10 X 1			too water Tele Ma			
A H ( A) = /	Copier Angle 28	064				
a a se a co	A Stat	Ofel	(W) 1 1 1 1			
CR Depart Control and	II See	Orbul				
	d Report	Orf-R				
	Capture Filters					
	Refrech Interfaces	15				
	EPERCOLAUNACION	N CH MEL				
	EIPERCOBAAN.pcap	(33 MB)				
	D'Rigkblogroup (356	7 1021				
	Dr.TA 541449.000ED4406.3008.EA WEED4406.Au/27 met/9-12/proprie (JETM 60)					
	Drifts Salak-FutersHaterLataut Ka WESHARK.april 20 net Gangacaping (29 NB)					
	DYTA SALAH INTERSHARKUNAN KA WERDHARKUNAN BANKUNAN ON HEI ANALAMI (HWH HEI ANALAMI (HWH)					
	DUTA SALAH MERSIAAN JANE DA WERSIAAN MARTING (Jan 13: 00) arama (20:140)					
	DI/TA SALAHUNIRESH	ARK/JOKOB	4005 propeg (3148 KB)			
	Dr.TA SALAHI MESHAND ANNADAR (2023 RD					
	EV7A SALAH METAAMIYANG KANANG KANA					
	Capture					
	ump the film:	der a capitare	Ny	al eterlaces shown *		
	Window Natural Con	I feetang				

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.

the East Vent Ger	Capture Londyes Halliday	Talaphony Wanters Teals	
• • • • • • • • •	SO G = TT	# 1723 (100 VS. 03. 03. 89	
		an even state of the lost	
			· Copressor. 8
e Des	Game	Cardy alter: Prot	largh bis
and ITS. IITING	282.108.42.22	229,299,299,298 310	ALL MITTER & MITTERLA
ANT 121, 181800	382.588.45.39	197,338,45,3 090	IN STANDARD DARY'S BUDDIN & Assistication, Pr. sourt, con
and STT. OFFICE	342.188.43.00	119.41.222.04 840	the Standard case's Kulley Docume (22781) clearant attacked Lake's process (42884) charant attacked Lake's Pack.
468 177.5EHEPO	342.248,42.5	182.108.41.18 888	100 Standard many, requires dealers is good firstion. Ff arous, one (SDNE seal)tion .Pf, search com (SDNE graditites, esh-
458 122.771478	330.43.352.40	107.108.62.38 040	Ale university sportation (12) En/218/Telfuranty Packet)
			on allow o dial (1981) heard alreaded land doubled when her press
458-334-574508	17-136-43-52	192.556.45.35 30	on every a second point, while being access adjusted parent minimum advectory back primes
455 334,579532	892.109.43.25	17.134.45.53 80	18 40274 + ETAL [ACL] SEPT 40241 HEAVENING
954 124, 189831	392.568.49.25	17.114.45.53 50	her works a much fact' work prior with class for the believe on a components and
all Its campage	22,228,49,58	195.558.45.58	on state of the second s
NUM LIN, SHEPLY	381.189.41.91	F7.494.400 8F1	PHE PHY //REALINED HTT//I. CHESTERIAL CONTENTION
817 174.181144	77.10.01.01	177.058.00.05 855	BUR BYTY/ALS BUR BUR FILME [1993/1004]
			the state of state (5.44, and ) and other states and states of the
and the second	CONTRACTOR OF CONTRACTOR		NATE TATION PARAMETARY AND ADDRESS AND ADDRESS
	201 144 43 15	101.100.01.000 800	the proof of the proof of the other states of the first first first and the proof of the proof of the state o
and the simple	100 100 43 35	123 255 225 158	and writing a property of
ALL LOS LABORS	THE RELEASE AND INC. THE	Charles and the second water	at two fast the last the fast half the last the at a
and the network	Substant 18 de las	TRUTH ( A shinks for some	de ver tan an weite an te
AND THE DESIGN	Constanti VE.00.00	Tandard Tanah IT and	AT THE VER AT 1 IS AT THIS AT THIS AT THE ANALY
ADE TIP, NEWLAR	Duncaria, To-de-da	made an other and	42 192 198 40.5 16 at 20 15 87 78 40 40
MAT SAX MALINE	342.388.95.98	239,255,255,258,258	and MITTER + APPRIL 1
Frame L. av inten Etherret II, bui Schweiderte Protosol Schweiderte Ereit 40 Ma 22 of 40 ad 50 of 60 W 20 de 60	LY 4/14 (142 5/14), 49 5 Quarters, 75,00 44 (26) 5 Warder S, Wei 20, 160 Mill Freiner, Sr. Wei 20, 160 Mill Freiner, Sr. Wei 20, 160 Mill Freiner, Sr. Wei 20, 160 Mill St. Mill S, 17, 20 40 40 Mill S, 20 10 41 41 41 41 41 10 21 41 41 41 41 41 41 41		And the second
O 7 Abrica lanuari	Communition 2: Velver cognitions in proop	-	Painty 47 (assure 47 (assure 47)

Gambar 11 Capture Paket Data Wireshark

Jurnal Cendikia Vol. XVI Cendikia 2018 Bandar Lampung, Oktober 2018

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.

P	]	-		-					-	-	No.	Vebsite ang di	ouka
Pen	gguna	na hat	Images   Messages   Cest	erstale (1)   Seco	ore (127) C		1	ers (43)   Ke	presentine ( Cir	eated A	ronales	1	
~~~~		1	Clert.	Clers Pot	Server	Sever P.	1.	ONS TT	Tars.	Type	DIVS Query	Ohis An.	Alexa T.
6648	7/16/2018 4 22 2	4 F14	192.168.43.101 Easter	43002	192.168	63.	64	00 11 46	0xE310	0x000	eyndication /wither core	104.244	NAP
5643	7)16/2018 4:22:2	4.756	192 168 43 101 (Linus)	43002	192,160	.53	64	001146	045390	0+000	syndication twitter com	104.244	NX.Pt
\$641	7/16/2018 4:22 2	4 756	192.168.43.101 (Linux)	43002	192.168	53	54	00.11.46	042330	0+000	syndication twitter core	104.244	NXP.
664)	7/16/2018 4 22 2	4 P54	192.168.43.101 (Janar)	45002	192.168	53	64	00 11 46	046210	0+000.	syndication Invitter core	104.244	N/A/Pt
6645	7:16/2018 4:22.2	4.958	192.168.43.101 (Linux)	43002	192 168	53	64	001146	045390	0+000.	syndication twitter core	104.244	NAPE
2014	7/16/2018 4:20-5	0.64	152.168.43.101 (Level)	55106	192.165	53	64	00:02:04	DrC448	0x000	tp00 evenettech.net akadre	66.117.2	NAP:
2615	7/16/2018 4 20 5	O PM	192.168.43.101 Eanal	55106	192.168	53	64	00 02 04	0-C448	0+000	1000 eventtech net all admit	66.117.2	NAP
1048	7) 16/2018 4:20:2	5 P.M	192,168.43.101 (Linux)	2627	192.160	53	64	02:03:47	0x1034	0+000	widcard alock con edgekey	a11956	NAM
1048	7/16/2018 4 20 2	9.756	192.168.43.101 (Jinus)	3627	192.165	53	64	00.03.47	0:1034	0+000	addcard alods.com edgekey	e11956	NAP
654	7/16/2018 4:19 5	5 PM	192.168.43.101 (Janua)	14508	192.168	53	64	03 32 33	0-6061	0+000	wildcard taobao lacada edge	+14205	N/A/Pr
655	7/16/2018 4 19:5	5 F54	192.168.43.101 (Linux)	14500	192.168	53	64	03 32 33	045061	0.000	wildcard taobax lazada edge	+14205	NAP
001	7/16/2018 4:20 1	9 714	192 168 43 101 (Linux)	25427	192.165	53	64	03.32.08	0.0884	0+000	eddcard lackes lazada edge	+14205	NAP
612	7/16/2018 4 20 1	3 FM	192.168.43.101 (Linux)	21427	192.168	53	64	03 32 08	0-C884	Ge000.	widcard taxbao lasada edge	e14205	N/A/Pt
6299	7/16/2018 4:22 2	3 P56	192 168 43 101 (Linus)	22994	192.168	53	64	00.00.12	0x760C	0+000	wildcard twing.com	104.244	NAP
6205	2/16/2018 4 22 2	3.64	192.168.43.101 (Jana)	23990	192.168	53	64	00:00:12	6,7600	0+000	wildcard twing.com	104.244	NAP
6290	7/16/2018 4 22 2	3 PM	192.165.43.101 Einwi	23996	192.168	53	64	00:00 12	b/%00	0+000	wildcard twing.com	104.244	N/A/Pr
6290	7/16/2018 4 22 2	3 P56	192 168 43 101 (Linua)	22998	192.168	53	64	00.00.12	0x760C	0.000	wildcard lwmg.com	104.244	NAP
2155	7/16/2018 4 20 4	2 754	192 168 43 101 (Linus)	54845	192,165	53	64	14 13 52	Get ICE	0-000	more evenedia ret		NAM
2154	7/15/2018 4 20-4	8.956	192.168.43.101.6.mail	54345	192 168	\$3	64	14 13 52	DECE	0.000	anny eventia rel	www.ev	NAP
2153	7/16/2018 4 20 4	1 PM	192.168.43.101 (Linua)	54845	192.168	53	64	04.53.13	D-E1CE	Ge000	www.evenedji.ret.edgek.ey.i	+1518.4	NAP
2154	7/16/2018 4:20-4	1.754	192 168 43 101 (Leval)	54545	192 168	53	64	(4 53 13	DETCE	0.000	answ averedja, ret, edgekay i	# +3518c.	NAP.
3091	7/16/2018 4 20:5	2.8%	192 168 43 101 Email	53046	192.168	53	64	00:04:37	DC4F8	0.000	www.facebook.com	daren.	N/A.Pt
3094	7/16/2018 4 20:5	2 PM	192 168 43 101 (JALA)	53046	192.168	53	64	00.04.37	0-C4F8	0+000	www.facebook.com	44.14	NAP
3000	7/16/2018 4 20-5	2.FM	192 168 43 101 (Linus)	32254	192.168	53	64	00.00.40	0.4571	0+000	enviv google to id	172.217.	NAP
3021	7:15/2018 4:20:5	2.634	192 168 43 101 (Jacob)	32254	192.168	53	64	00.00.40	0.071	0-000.	array google on id	172.217	NOLPH
342	7/16/2018 4 19 5	1 PM	192.168.43.101 (Linua)	21579	192.168	53	64	00:04:39	0-6657	0+000	www.google.com	74.125.2	N/A-PI
342	2/16/2018 4:19:5	1 PM	192 168 43 101 (Linua)	21579	192.168	53	64	00.64.29	0-565/	0+000	www.google.com	74 125.2	NAP
342	7/16/2018 4 19 5	1 FM	192.168.43.101 (Linux)	21579	192.168	53	64	00.04.29	0-54.57	0-000	www.google.com	74.125.2	NAP
342	7/16/2018 4 19 5	1 P56	192 168 43 101 (Linua)	21579	192.168	53	64	00.04.39	0.6657	0+000	www.google.com	74.125.2	NXP
342	7/16/2018 4 19:5	1 PM	192 168 43 101 (Linua)	21579	192.168	53	64	00.04.29	04657	0+000	enviry google com	74.125.2	NAP
342	7/16/2018 4:19:5	1.856	192.168.43.101 (Linux)	21579	192.168	53	- 64	02:04:39	0465F	0-000.	www.google.com	74.125.2	NOUP
343	7/16/2018 4 19:5	1 PM	192 168 43 101 (Jana)	21579	192 168	\$3	- 64	00:04:39	0-6657	0+000	www.google.com	74.125.2	NAP
10	7/16/2018 4 19 5	1 PM	192 168 43 101 Einun)	21579	192.168	53	64	00.04.39	0-6657	0.000	snew google.com	74 125.2	NAP

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	<ul> <li>www.google.com</li> <li>whatsapp</li> <li>www.lazada.com</li> <li>www.twitter.com</li> <li>mail.google.com</li> <li>www.youtube.com</li> <li>www.gstatic.com</li> <li>www.facebook.com</li> </ul>
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     immobi.com     adrta.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 - doublectick.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. what sapp = 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

Jurnal Cendikia Vol. XVI Cendikia 2018 Bandar Lampung, Oktober 2018

#### 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/instalasiprogram-monitoring-jaringan-wireshark, tanggal akses 15 April 2018.
- http://www.oxid.it/cain.html