

**YAYASAN LEMBAGA PENDIDIKAN ISLAM DAERAH RIAU  
UNIVERSITAS ISLAM RIAU  
FAKULTAS TEKNIK**

---

Analisis Keamanan Jaringan Pada Fasilitas Internet (*Wifi*) Terhadap Serangan  
*Packet Sniffing* Pada Kantor Indosat Ooredoo  
Pekanbaru

**SKRIPSI**

Diajukan Untuk Memenuhi Salah Satu Syarat  
Mendapatkan Gelar Sarjana Pada Fakultas Teknik  
Universitas Islam Riau Pekanbaru



MUHAMMAD DENNY SANJAYA  
153510706

PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS ISLAM RIAU  
PEKANBARU  
2019

## LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama : Muhammad Denny Sanjaya  
NPM : 153510706  
Jurusan : Teknik  
Program Studi : Teknik Informatika  
Jenjang Pendidikan : Strata Satu (S1)  
Judul Skripsi : Analisis Keamanan Jaringan Pada Fasilitas Internet (WIFI) Terhadap Serangan DoS pada Kantor Indosat Ooredoo Pekanbaru

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini telah dipelajari dan dinilai relatif telah memenuhi ketentuan-ketentuan dan kriteria-kriteria dalam metode penulisan ilmiah. Oleh karena itu, skripsi ini dinilai layak dapat disetujui untuk disidangkan dalam ujian komprehensif.

Pekanbaru, 06 Desember 2019

Disetujui Oleh  
**PEKANBARU**

Dosen Pembimbing

ABDUL SYUKUR, S.Kom, M.Kom

Disahkan Oleh :



Dekan Fakultas Teknik

JEAN ABD. HUSNULZAINI, MT, MS., TR

AKUNTANSI 7.88 03 02 098

Ketua Prodi Teknik Informatika

dan SC Prodi

AUSE LABELAPANSA, ST, M.Cs., M.Kom



## LEMBAR PENGESAHAN TIM PENGUJI UJIAN SKRIPSI

Nama : Muhammad Denny Sanjaya  
NPM : 153510706  
Jurusan : Teknik  
Program Studi : Teknik Informatika  
Jenjang Pendidikan : Strata Satu (S1)  
Judul Skripsi : Analisis Keamanan Jaringan Pada Fasilitas Internet (WIFI) Terhadap Serangan Packet Sniffing Pada Kantor Indosat Ooredoo Pekanbaru

Skripsi ini secara keseluruhan dinilai telah memenuhi ketentuan-ketentuan dan kaidah-kaidah dalam penulisan penelitian ini. Serta telah diuji dan dapat dipertahankan dihadapan tim penguji. Oleh karena itu, Tim Penguji Ujian Skripsi Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan **Telah Lulus Mengikuti Ujian Komprehensif Pada Tanggal 06 Desember 2019** dan disetujui serta diterima untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Strata Satu Bidang Ilmu Teknik Informatika.

Pekanbaru, 06 Desember 2019

Tim Penguji

1. Ir. Hj Des Suryani

Sebagai Tim Penguji I

2. Yudhi Arta, ST., M. Kom

Sebagai Tim Penguji II

Disetujui Oleh

Dosen Pembimbing

ABDUL SYUKUR, S.Kom., M.Kom

Disahkan Oleh :

Dekan Fakultas Teknik

Ketua Prodi Teknik Informatika  
an seprodi

Dr. H. ABDUKUDUS ZAINI, MT., MS., TR  
NPM : 88 03 02 098

AUSE LABEL LAPANSA, ST., M.Cs., M.Kom

## LEMBAR PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

Nama : Muhammad Denny Sanjaya

Tempat/Tgl Lahir : Pekanbaru, 25 Mei 1997

Alamat : Jalan Muslim Kelurahan Tanjung Palas Kota Dumai.

Adalah mahasiswa Universitas Islam Riau yang terdaftar pada:

Fakultas : Teknik

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata-1 (S1)

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis adalah benar dan asli hasil dari penelitian yang telah saya lakukan dengan judul "Analisis Keamanan Jaringan Pada Fasilitas (Wifi) Terhadap Serangan *Packet Sniffing* Pada Kantor Indosat Ooredoo Pekanbaru.",

Apa bila dikemudian hari ada yang merasa dirugikan atau menuntut karena penelitian ini menggunakan sebagian hasil tulisan atau karya orang lain tanpa mencantumkan nama penulis yang bersangkutan, atau terbukti karya ilmiah ini bukan karya saya sendiri atau plagiat hasil karya orang lain, maka saya bersedia menerima sanksi sesuai dengan peraturan perundangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya untuk dapat digunakan sebagai mana mestinya.

Pekanbaru, 13 Desember 2019

Yang membuat pernyataan,



(Muhammad Denny Sanjaya)

## KATA PENGANTAR

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Panyayang, Penulis ucapkan puji syukur atas kehadiran-Nya, yang telah melimpahkan rahmat, hidayah, dan inayah-Nya kepada kami, sehingga penulis dapat menyelesaikan proposal skripsi yang berjudul “Analisis Keamanan Jaringan Pada Fasilitas Internet (*Wifi*) Terhadap Serangan *Packet Sniffing* Di Kantor Indosat Ooredoo Pekanbaru” ini tepat pada waktunya.

Proposal skripsi ini telah penulis susun dengan maksimal dan mendapatkan bantuan dari berbagai pihak sehingga dapat memperlancar pembuatan proposal skripsi ini. Untuk itu penulis menyampaikan banyak terima kasih kepada semua pihak yang telah berkontribusi dalam pembuatan proposal skripsi ini.

Terlepas dari semua itu, penulis menyadari sepenuhnya bahwa masih ada kekurangan baik dari segi susunan kalimat maupun tata bahasanya. Oleh karena itu dengan tangan terbuka penulis menerima segala saran dan kritik agar penulis dapat menyempurnakan laporan ini.

Akhir kata penulis berharap semoga proposal ini dapat memberikan manfaat, inspirasi, dan dapat dipergunakan oleh instansi terkait.

Pekanbaru, 20 September 2019

Penulis



## DAFTAR ISI

### KATA PENGANTAR

DAFTAR ISI.....	ii
DAFTAR TABEL .....	iv
DAFTAR GAMBAR.....	v
BAB I.....	1
PENDAHULUAN .....	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah .....	2
1.3 Rumusan Masalah .....	2
1.4 Batasan Masalah .....	3
1.5 Tujuan Penelitian.....	3
1.6 Manfaat Penelitian.....	4
BAB II .....	5
LANDASAN TEORI .....	5
2.1 Studi Kepustakaan.....	5
2.2 Dasar Teori.....	7
2.2.1 Konsep Kemanan Jaringan.....	7
2.2.2 Ancaman .....	7
2.2.3 Kelemahan .....	8
2.3 Jenis – Jenis Ancaman Keamanan Jaringan.....	9
2.3.1 <i>Packet Sniffer</i> .....	9
2.3.2 ARP Spoofing / ARP Poisoning .....	9
2.3.3 <i>Probe</i> .....	9
2.3.4 <i>Scan</i> .....	10
2.3.5 <i>Account Compromise</i> .....	10
2.3.6 Root Compromise .....	10
2.3.7 <i>Denial of Service (Dos)</i> .....	11
2.3.8 <i>Flowchart</i> .....	11
BAB III.....	16

<b>METODOLOGI PENELITIAN .....</b>	<b>16</b>
3.1 Metode Penelitian .....	16
3.1.1 Bahan dan Alat Penelitian.....	16
3.2 Flowchart Alur Penelitian .....	17
3.3 Tahapan-tahapan Instalasi dan Konfigurasi Software.....	19
3.4 Tahapan – Tahapan Penyerangan .....	29
<b>BAB IV.....</b>	<b>33</b>
4.1. Analisis Hasil Peneletian .....	33
4.2 Solusi Untuk Mencegah Serangan <i>Packet Sniffing</i> .....	46
<b>BAB V .....</b>	<b>48</b>
5.1 <b>Kesimpulan</b> .....	48
5.2 <b>Saran</b> .....	48
<b>DAFTAR PUSTAKA .....</b>	<b>50</b>

## DAFTAR TABEL

Tabel 2. 1 Simbol dan Fungsi <i>Flowchart</i> .....	11
---	----





## DAFTAR GAMBAR

Gambar 3. 1 <i>Flowchart</i> Alur Penelitian.....	18
Gambar 3. 2 <i>software netstumbler</i> . ....	20
Gambar 3. 3 Tampilan <i>software inSSIDer</i> pada <i>windows 10</i> .....	21
Gambar 3. 4 Penginstalan <i>Wireshark</i> Tahap Pertama.....	22
Gambar 3. 5 Penginstalan <i>Wireshark</i> Tahap Kedua .....	22
Gambar 3. 6 Penginstalan <i>Wireshark</i> Tahap Ketiga .....	23
Gambar 3. 7 Penginstalan <i>Wireshark</i> Tahap Keempat .....	24
Gambar 3. 8 Penginstalan <i>Wireshark</i> Tahap Kelima.....	25
Gambar 3. 9 Penginstalan <i>Wireshark</i> Tahap Keenam .....	26
Gambar 3. 10 Pengistalan <i>Wireshark</i> Tahap Ketujuh.....	27
Gambar 3. 11 Penginstalan <i>Wireshark</i> SELESAI.....	28
Gambar 3. 12 <i>Flowchart</i> Tahapan Penyerangan.....	29
Gambar 3. 13 Posisi tempat/lokasi penyerangan yang diizinkan pada gedung kantor PT Indosat. ....	30
Gambar 3. 14 Posisi tempat/lokasi penyerangan yang diizinkan pada gedung baru Kantor PT Indosat. ....	31
Gambar 3. 15 Tampilan <i>software inSSIDer</i> saat identifikasi <i>wifi</i> .....	32
Gambar 4. 1 Pukul 10.00 W.I.B – 11.00 W.I.B .....	34
Gambar 4. 2 Pukul 11.00 W.I.B – 12.00 W.I.B .....	35
Gambar 4. 3 Pukul 13.00 W.I.B s/d 14.00 W.I.B .....	35
Gambar 4. 4 Pukul 14.00 W.I.B s/d 15.00 W.I.B .....	36

Gambar 4. 5 Tahap Penyerangan Pertama Identifikasi Jaringan <i>Wifi</i> .....	38
Gambar 4. 6 Aktifitas Jaringan <i>Wifi</i> Pada Aplikasi <i>Wireshark</i> .....	39
Gambar 4. 7 <i>Website</i> Yang Tidak Memiliki Sistem Terenkripsi .....	40
Gambar 4. 8 Aktifitas <i>Website</i> Pada Aplikasi <i>Wireshark</i> .....	41
Gambar 4. 9 Hasil Pencarian IP <i>Website</i> Pada <i>Command Prompt</i> .....	42
Gambar 4. 10 Aktifitas <i>Website</i> Yang Sedang Berjalan .....	43
Gambar 4. 11 Cara Melihat Aktifitas Login <i>Website</i> .....	44
Gambar 4. 12 Pencarian Aktifitas Login Melalui <i>Find Text</i> .....	45
Gambar 4. 13 Perbedaan jaringan internet <i>wifi</i> kantor dan umum.....	46

## BAB I

### PENDAHULUAN

#### 1.1 Latar Belakang

Pada saat ini keamanan jaringan sangat penting dan harus diperhatikan terutama pada jaringan yang terhubung dengan internet atau suatu *wifi* , karena pada dasarnya jaringan tidak selalu aman dan selalu ada orang yang ingin mengeksploitasi jaringan tersebut, baik dari jaringan *wired LAN* maupun *wireless LAN*. Dalam pembangunan sebuah perancangan system keamanan yang telah terhubung ke suatu internet haruslah direncanakan dan dapat dipahami oleh pengguna agar dapat melindungi sumber daya yang berada di dalam jaringan tersebut dan bisa dapat meminimalisir serangan yang terjadi oleh seseorang yang tidak bertanggung jawab.

*Wireshark* adalah aplikasi *packet sniffer* yang berguna untuk melakukan sebuah analisa protocol keamanan jaringan. Aplikasi ini dapat memblokir lalu lintas pada jaringan *LAN*, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum.

Sedangkan *Netstumbler* adalah *tools wifi hacking* yang digunakan untuk mendeteksi dan mengidentifikasi sinyal *wireless* yang terbuka dan menyusup ke dalam jaringan.

Indosat didirikan sebagai perusahaan penanaman modal asing pertama di Indonesia yang menyediakan layanan telekomunikasi internasional melalui



satelit internasional. Saat ini Kantor Indosat Ooredoo Pekanbaru telah menerapkan jaringan komputer kabel maupun nirkabel sebagai media pertukaran data/informasi pelayanan umum, kepegawaian dan informasi penting lainnya. Terdapat jaringan yang terpasang dalam lingkup Kantor Indosat Ooredoo Pekanbaru yaitu terinstall pada gedung yang didalamnya terdapat ruang customer service dan ruangan teknisi dengan menerapkan jaringan kabel.

Berdasarkan uraian diatas, penulis tertarik untuk mempelajari cara untuk mengamankan suatu jaringan. Oleh karena itu, penulis mengambil bahan mengenai keamanan jaringan internet untuk judul skripsi “**Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Terhadap Serangan *Packet Sniffing***”.

### **1.2 Identifikasi Masalah**

Adapun identifikasi masalah yang dapat diambil dari penjelasan latar belakang tersebut adalah sebagai berikut “Kantor Indosat Ooredoo Pekanbaru perlu mempunyai pengawasan tentang bahaya nya jaringan komputer kantor dan umum dalam 1 jaringan yang berada di lingkungan Kantor Indosat Ooredoo Pekanbaru”.

### **1.3 Rumusan Masalah**

Berdasarkan latar belakang masalah dan hubungan dengan pemilihan judul tersebut, maka penulis merumuskan pokok permasalahan yaitu Evaluasi keamanan fasilitas internet (*wifi*) di Kantor Indosat Ooredoo Pekanbaru.

#### 1.4 Batasan Masalah

Dalam pembuatan skripsi penulis membatasi masalah yang akan dikerjakan yaitu:

1. Penggunaan aplikasi *Wireshark* dalam melakukan simulasi penyerangan.
2. Penggunaan aplikasi *Wireshark*, dan *inSSIDer* untuk menganalisa keamanan jaringan di Kantor Indosat Ooredoo Pekanbaru.
3. Dalam skripsi penulis tidak melakukan implementasi peningkatan keamanan jaringan yang sudah ada, hanya memberikan solusi yang sebaiknya dilakukan untuk mengantisipasi terjadinya serangan seperti yang dilakukan penulis.
4. Untuk penelitian dilakukan percobaan beberapa hari dikantor untuk memahami konsep yang sedang berjalan dan membuat kembali simulasi dirumah jalan karya 1 gang miduk 1 yang memiliki koneksi internet.

#### 1.5 Tujuan Penelitian

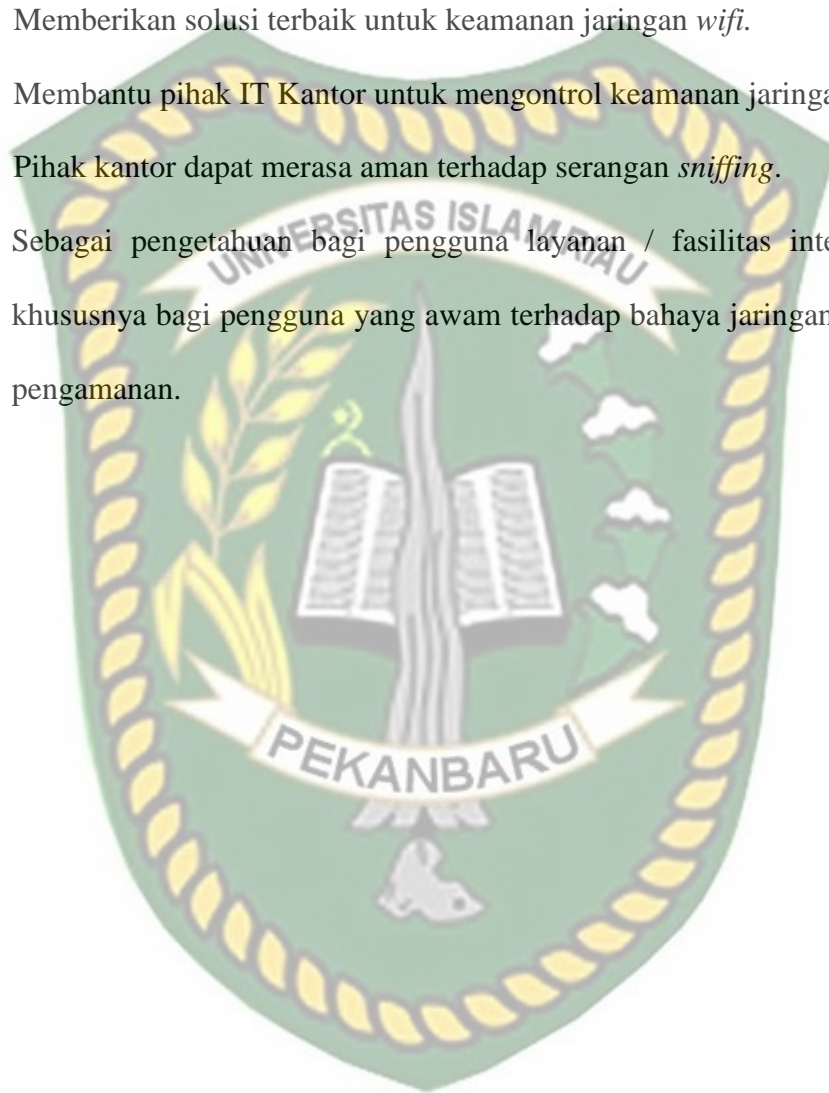
Tujuan yang hendak dicapai dalam penelitian ini adalah :

1. Meningkatkan keamanan jaringan *Wifi* pada Kantor Indosat Ooredoo Pekanbaru.
2. Jaringan *wifi* dikantor Indosat Ooredoo Pekanbaru dapat lebih diperhatikan terhadap penyadapan orang yang tidak bertanggung jawab.

## 1.6 Manfaat Penelitian

Penelitian ini bermanfaat untuk :

1. Memberikan solusi terbaik untuk keamanan jaringan *wifi*.
2. Membantu pihak IT Kantor untuk mengontrol keamanan jaringan *wifi*.
3. Pihak kantor dapat merasa aman terhadap serangan *sniffing*.
4. Sebagai pengetahuan bagi pengguna layanan / fasilitas internet (*wifi*) khususnya bagi pengguna yang awam terhadap bahaya jaringan *Wifi* tanpa pengamanan.







Dokumen ini adalah Arsip Miik :

**Perpustakaan Universitas Islam Riau**

## BAB II

### LANDASAN TEORI

#### 2.1 Studi Kepustakaan

Menurut Lalu Delsi Samsumar (2017), Penelitian yang ingin dilakukan oleh penulis ialah penulis tidak dapat menghasilkan suatu model untuk hasil dari penelitian yang dapat digunakan sebagai referensi pengembangan atau meningkatkan keamanan akses jaringan *Wired LAN* pada jaringan Kantor Indosat Ooredoo Pekanbaru. Penggunaan teknologi internet semakin banyak dan tidak terkontrol, hal ini disebabkan karena banyaknya oengguna internet di dunia dan hamper semua lapisan masyarakat mengetahui tentang adanya internet.

Perbedaan dengan Penelitian yang ingin dilakukan oleh penulis ialah penulis tidak menghasilkan sebuah model sebagai hasil dari penilaian yang dapat digunakan sebagai referensi untuk mengembangkan dan meningkatkan keamanan akses jaringan komputer nirkabel pada jaringan pada kantor PT.Indosat Ooredoo Pekanbaru.

Penelitian Aji Supriyanto (2006) ialah adanya batasan jangkauan radio dan interferensi menyebabkan ketersediaan servis menjadi terbatas. DoS attack dapat dilakukan dengan menginjeksikan *traffic* palsu. Pemakaian perangkat berbasis wlan pada saat ini sudah begitu banyak, baik digunakan untuk komunikasi suara maupun data. Karena banyak teknologi komunikasi lainnya menggunakan operator yang memberikan layanan komunikasi. Kelemahan jaringan wlan secara umum dapat dibagi menjadi 2 jenis yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah pada jaringan wlan terbentang atas empat layer dimana keempat lapis layer tersebut sebenarnya merupakan proses dari terjadinya komunikasi pada data media wlan.

Perbedaan dengan penelitian yang akan penulis bahas ialah adanya batasan jangkauan radio dan interferensi menyebabkan ketersediaan servis menjadi terbatas. DoS attack dapat dilakukan dengan menginjeksikan *traffic* palsu.

Menurut Hendri Noviyanto (2011) yang berjudul analisis keamanan wireless di universitas muhammadiyah Surakarta berisi tentang pengguna access point sangat mudah dan dapat dipakai di tempat yang terjangkau sinyal wireless tanpa harus berada di tempat tertentu. Seorang penyerang dapat melakukan koneksi dengan access point dengan melakukan satu koneksi dan seorang penyerang itu mulai melakukan scanning untuk pengguna yang sedang aktif.



Perbedaan keamanan jaringan yang akan penulis kerjakan ialah penyerang melakukan koneksi dengan Access point dengan melakukan suatu koneksi internet dan penyerang mulai melakukan scanning user yang aktif.

## **2.2 Dasar Teori**

### **2.2.1 Konsep Keamanan Jaringan**

Penulis memiliki acuan pada penelitian Noviyanto yang berjudul analisis keamanan wireless di universitas Muhammadiyah Surakarta yaitu pada saat ini suatu keamanan jaringan sangat penting dan patut di perhatikan, terutama untuk jaringan yang terhubung dengan internet atau *wifi* dan memiliki dasar tidak selalu aman dari penyadapan, baik dari jaringan wired LAN maupun wireless LAN. Pada pembangunan sebuah system keamanan jaringan internet haruslah di rencanakan dan dipahami agar dapat melindungi pengguna dan meminimalisir terjadi serangan oleh orang yang tidak bertanggung jawab.

Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Berikut ini akan dibahas mengenai ancaman , kelemahan, dan *policy* keamanan jaringan.

### **2.2.2 Ancaman**

Pada dasarnya, ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal ke dalam suatu jaringan komputer. Bagaimana tidak banyak ancaman-ancaman yang terjadi pada sistem informasi yang akan merugikan banyak pihak, baik individu, masyarakat, dan lain sebagainya. Oleh karena itu untuk mencegah ancaman-ancaman terhadap

sistem informasi yaitu perlu adanya keamanan yang sangat canggih agar dapat mendeteksi atau membenarkan dari sebagian sistem yang rusak akibat gangguan pada sistem informasi. Ada beberapa tujuan yang ingin dicapai oleh penyusup dan, sangat berguna apabila dapat membedakan tujuantujuan tersebut pada saat merencanakan sistem keamanan jaringan komputer. Beberapa tujuan para penyusup adalah:

- a. Setiap penyusup hanya ingin tau susunan sistem dan data yang ada pada suatu jaringan komputer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini disebut dengan *the curious*.
- b. Hanya ingin membuat sebuah sistem jaringan menjadi *down*, atau mengubah tampilan situs web. Penyusup yang mempunyai tujuan seperti ini disebut sebagai *the malicious*.
- c. Penyusup hanya berusaha untuk menggunakan sumber daya di dalam sistem jaringan komputer untuk memperoleh popularitas. Penyusup seperti ini disebut sebagai *the high-profile intruder*.
- d. Penyusup hanya ingin tau susunan data apa saja yang ada di dalam jaringan komputer dan selanjutnya dimanfaatkan untuk mendapatkan uang. Penyusup seperti ini disebut sebagai *the competition*.

### 2.2.3 Kelemahan

Kelemahan menggambarkan seberapa kuat sistem keamanan suatu jaringan komputer terhadap jaringan komputer yang lain, dan kemungkinan bagi seseorang untuk mendapat akses ilegal ke dalamnya.

## 2.3 Jenis – Jenis Ancaman Keamanan Jaringan

### 2.3.1 *Packet Sniffer*

Menurut Achmad Rizal Fauzi (2018), Packet sniffer ialah suatu teknik pemantauan setiap komunikasi dan transfer data yang lintas pada jaringan dan memonitor semua lalu lintas jaringan. Packet sniffer tidak sama dengan jaringan host standar yang hanya menerima dan mengirim lalu lintas khusus. Ancaman keamanan yang disajikan oleh penyadapan adalah kemampuan mereka untuk menangkap semua lalu lintas masuk dan keluar, termasuk password dan username atau bahan sensitif lainnya. Untuk dapat membaca dan menganalisa setiap protokol yang melintasi jaringan, diperlukan program yang bisa membelokkan paket ke komputer attacker. Biasa disebut serangan spoofing, attacker akan bertindak sebagai Man-In-the-Middle (Asrodia & Patel, 2012:1)

### 2.3.2 **ARP Spoofing / ARP Poisoning**

Menurut Fauzan F dengan judul Perancangan dan Analisis Keamanan Jaringan Terhadap ARP Spoofing pada Hotspot ialah Arp spoofing adalah suatu teknik untuk melakukan penyerangan kepada jaringan internet local baik menggunakan media kabel maupun nirkabel, yang dapat memungkinkan penyerang dapat mengendus frames data pada jaringan local atau penyerang dapat memodifikasi traffic bahkan menghentikan traffic.

### 2.3.3 *Probe*

Sebuah *probe* dapat dikenali dari adanya usaha-usaha yang tidak lazim untuk memperoleh akses ke dalam suatu sistem atau untuk menemukan informasi



tentang sistem tersebut. Salah satu contohnya adalah usaha untuk login ke dalam sebuah account yang tidak digunakan. *Probing* ini dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan yang dengan mencoba-coba apakah pintunya terkunci apa tidak.

#### 2.3.4 *Scan*

*Scan* adalah kegiatan *probe* dalam jumlah yang besar dengan menggunakan *tool* secara otomatis. *Tool* tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal maupun *host remote*, *IP address* yang aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju.

#### 2.3.5 *Account Compromise*

*Account compromise* adalah penggunaan *account* sebuah komputer secara ilegal oleh seseorang yang bukan pemilik *account* tersebut. *Account compromise* dapat mengakibatkan korban mengalami kehilangan atau kerusakan data. Sebuah insiden *account compromise* dapat berakibat lebih lanjut, yaitu terjadinya insiden *root compromise*, yang dapat menyebabkan kerusakan lebih besar.

#### 2.3.6 *Root Compromise*

*Root compromise* mirip dengan *account compromise*, dengan perbedaan *account* yang digunakan secara ilegal adalah *account* yang mempunyai *privilege* sebagai administrator sistem. Istilah *root* diturunkan dari sebuah *account* pada sistem berbasis *UNIX* yang mempunyai *privelege* tidak terbatas. Penyusup yang berhasil melakukan *root compromise* dapat melakukan apa saja pada sistem yang menjadi korban, termasuk menjalankan program, mengubah kinerja sistem, dan menyembunyikan jejak penyusupan.

### 2.3.7 *Denial of Service (Dos)*

Sumber daya jaringan yang berharga antara lain komputer dan database, serta pelayanan-pelayanan (service) yang disediakan oleh organisasi pemilik jaringan. Kebanyakan user jaringan memanfaatkan pelayanan-pelayanan tersebut agar pekerjaan mereka menjadi efisien. Bila pelayanan ini tidak dapat dipergunakan karena sebab-sebab tertentu, maka tentu saja akan menyebabkan kehilangan produktivitas. Sulit untuk memperkirakan penyebab *denial of service*. Berikut ini adalah contoh penyebab terjadinya *denial of service*:




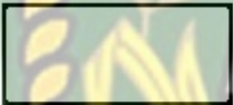


- a. Kemungkinan jaringan menjadi tidak berfungsi karena banjir traffic.
- b. Kemungkinan ada virus yang menyebar dan menyebabkan sistem komputer menjadi lambat atau bahkan lumpuh.
- c. Kemungkinan device yang melindungi jaringan dirusak.

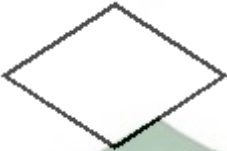


### 2.3.8 *Flowchart*

*Flowchart* adalah bagan-bagan yang mempunyai arus yang menggambarkan langkah-langkah penyelesaian suatu masalah. *Flowchart* merupakan cara penyajian dari suatu algoritma. Simbol *flowchart* dan fungsinya dapat dilihat pada tabel sebagai berikut (Ladjamudin, 2006:265) :

**Tabel 2. 1 Simbol dan Fungsi *Flowchart***

No	Simbol	Nama	Fungsi

1		Terminator	Permulaan / pengakhiran program
2		Flow Line	Arah aliran program
3		Preparation	Proses inisialisasi/pemberian nilai awal
4		Process	Proses pengolahan data
5		Input/Output Data	Proses input/output data,parameter, informasi
6		Predefined Process	Permulaan sub program / proses menjalankan sub program

7		Decision	Perbandingan pernyataan, penyeleksian data yang memberikan pilihan untuk langkah selanjutnya
8		On Page Connector	Penghubung bagian-bagian flowchart yang berada pada satu halaman
9		Off page Connector	Penghubung bagian-bagian flowchart yang berada pada halaman berbeda





Dokumen ini adalah Arsip Miik :

**Perpustakaan Universitas Islam Riau**

## BAB III

### METODOLOGI PENELITIAN

#### 3.1 Metode Penelitian

Pada simulasi ini menggambarkan suatu *mode* kecil topologi jaringan internet Kantor Indosat Ooredoo Pekanbaru yang dalam jaringan *wifi* nya digunakan oleh pihak Kantor dan Umum (pengunjung), dan tidak memisahkan penggunaan nya antara jaringan *wifi* kantor dengan *wifi* untuk umum (pengunjung). Hingga perlu adanya pengawasan tentang bahaya nya jaringan *wifi* terhadap penyadapan data. Berikut langkah-langkah metode simulasi yang harus dilakukan.

Pada simulasi penelitian ini menggambarkan suatu *mode* kecil topologi jaringan internet Kantor Indosat Ooredoo Pekanbaru yang dalam jaringan *wifi* nya digunakan oleh pihak Kantor dan Umum (pengunjung), dan tidak memisahkan penggunaan nya antara jaringan *wifi* kantor dengan *wifi* untuk umum (pengunjung). Hingga perlu adanya pengawasan tentang bahaya nya jaringan *wifi* terhadap penyadapan data. Berikut langkah-langkah metode simulasi yang harus dilakukan.

##### 3.1.1 Bahan dan Alat Penelitian

Pada saat melakukan penelitian ini Penulis menggunakan beberapa *software* dan *hardware* sebagai penunjang penelitian yang akan dilakukan oleh penulis. Untuk spesifikasi alat yang digunakan penelitian adalah sebagai berikut:

1. Kebutuhan perangkat keras dan sistem operasi.

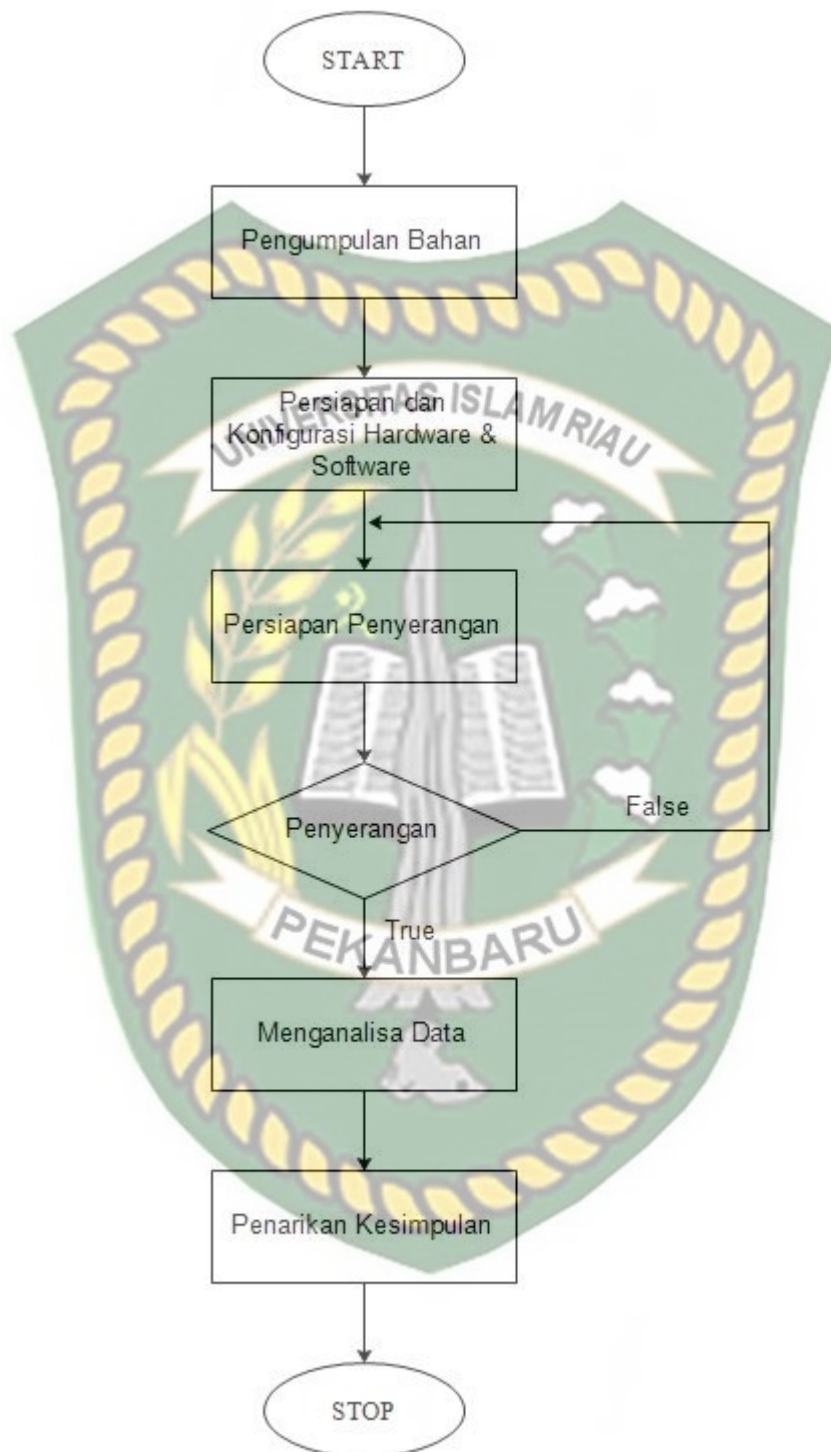
- a. Laptop Asus X441N, *Processor intel 2Core 2,4 Ghz*, Memori 2 GB
- b. Sistem operasi *Windows 10*.

2. Kebutuhan perangkat lunak.

- a. Software *Wireshark* (untuk serangan *Packet sniffing*).
- b. Software *Netstumbler* versi 0.4.0 (untuk melihat keberadaan *wifi*)
- c. Software *inSSIDer*

### 3.2 Flowchart Alur Penelitian

Dalam menjelaskan sebuah permasalahan alur penelitian dibuat untuk mempermudah pemahaman dalam penelitian tersebut. Metode tersebut dibuat dalam *flowchart* alur penelitian.



**Gambar 3.1** *Flowchart* Alur Penelitian.

Sesuai dengan *flowchart* alur penelitian pada gambar 3.1 penelitian ini dilakukan dalam beberapa tahapan.



- a. Sebelum memulai penelitian penulis menyiapkan semua literatur, buku, ebook dan artikel untuk membantu menunjang penelitian.
- b. Penulis harus memenuhi persyaratan/prosedur perizinan penelitian yang diberikan oleh pihak Kantor PT.Indosat Ooredoo Pekanbaru, karena tidak semua tempat/lokasi boleh masuk kecuali karyawan tertentu yang berhak.
- c. Penulis mencari informasi data yang ada, konfigurasi jaringan *wifi* yang terpasang di seluruh ruangan Kantor PT.Indosat Ooredoo Pekanbaru meliputi tempat, SSID, BSSID, enkripsi yang digunakan.
- d. Penulis menyiapkan *hardware* dan *software* yang dibutuhkan untuk mendukung pelaksanaan penelitian.
- e. Penulis melangkah untuk melakukan sebuah percobaan penyerangan kepada jaringan *wifi* untuk mendapatkan informasi tentang keamanannya.
- f. Penulis bisa menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan jaringan kabel LAN dan *wifi* melihat dari sisi pengguna.

### 3.3 Tahapan-tahapan Instalasi dan Konfigurasi Software

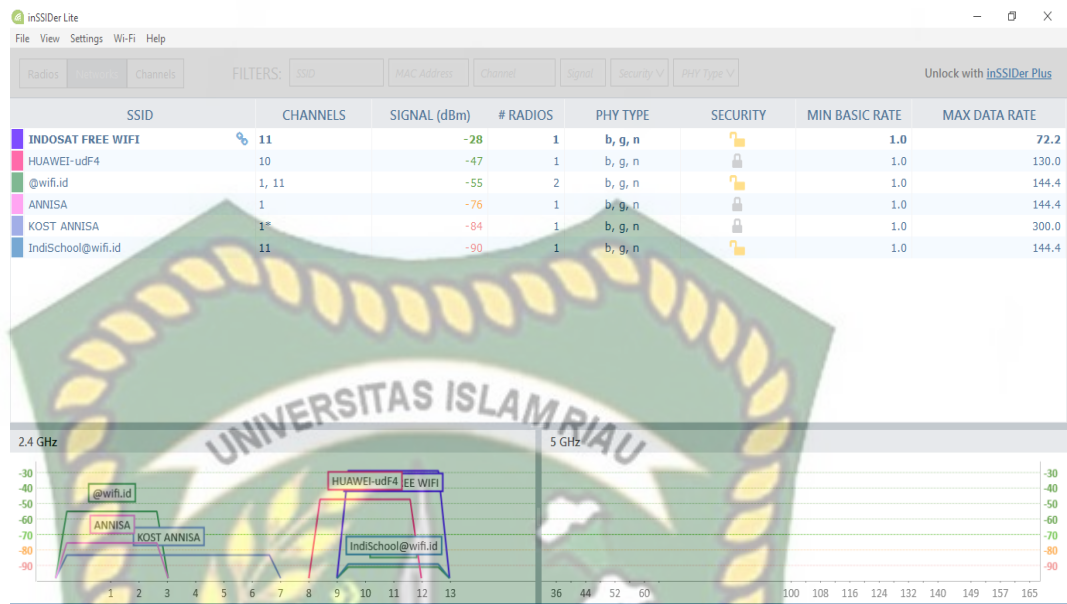
1. Instalasi software *Netstumbler* pada *windows 10*
  - a. Klik 2x pada file *netstumblerinstaller\_0\_4\_0.exe* untuk instalasi, kemudian ikuti perintah selanjutnya dengan klik *i agree*, *next* dan *install* sampai selesai.

- b. Konfigurasi *device network* yang terhubung dengan laptop pada netstumbler dengan cara meng-klik pilihan device, seperti pada gambar 3.2. berikut :



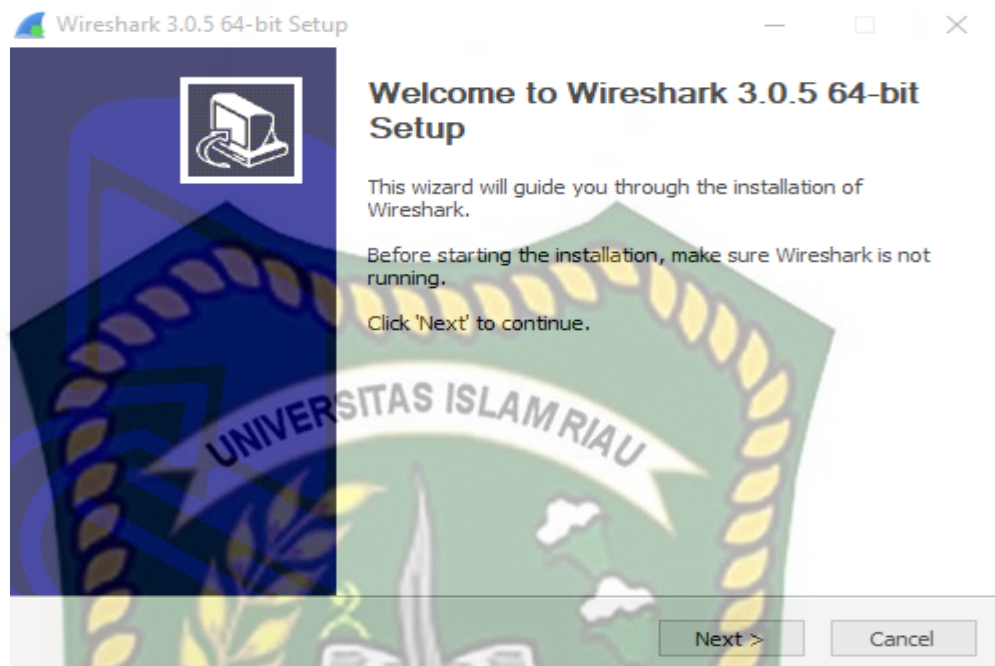
**Gambar 3. 2** *software netstumbler.*

- c. Setelah melihat gambar 3.2 ternyata *device network adaptor* yang terhubung dengan laptop penulis tidak *support*, karena *software netstumbler* hanya dapat berjalan sempurna pada *windows XP* dan tidak dapat berjalan sempurna pada *windows 10*. Kemudian penulis menggantinya dengan *software inSSIDer* sebagai alternatif *software netstumbler* untuk *windows 10*.



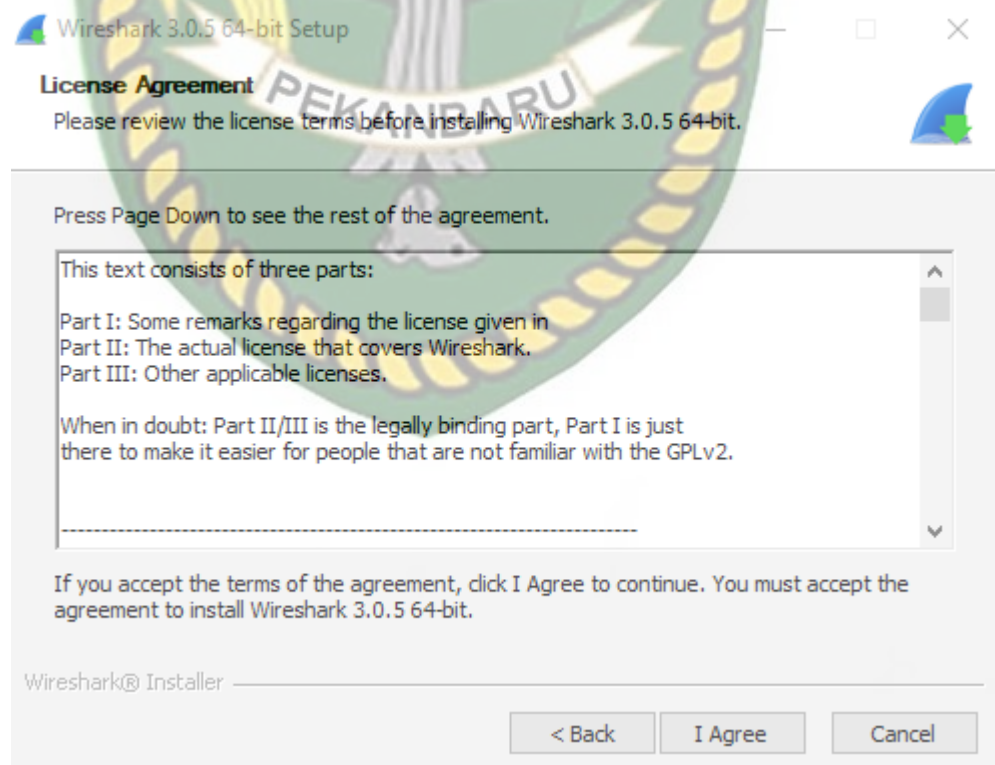
**Gambar 3. 3** Tampilan software inSSIDer pada windows 10.

2. Instalasi software Wireshark pada Windows 10
  - a. Klik 2 kali pada file *wireshark-win640-3.0.5* yang telah di download sebelum nya untuk memulai install aplikasi *wireshark*.
  - b. Selanjut nya akan muncul seperti gambar 3.4 dan klik *Next* yang akan melanjutkan kehalaman selanjutnya



**Gambar 3. 4** Penginstalan *Wireshark* Tahap Pertama

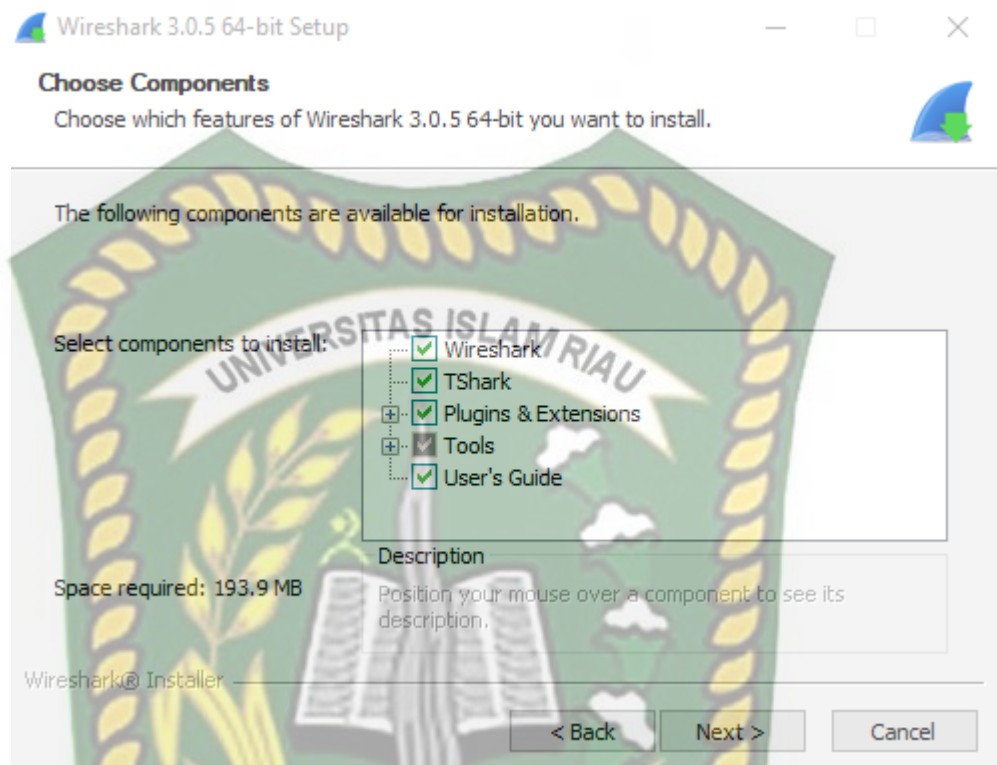
- c. Tahap selanjut nya tekan *I agree* seperti gambar 3.5



**Gambar 3. 5** Penginstalan *Wireshark* Tahap Kedua

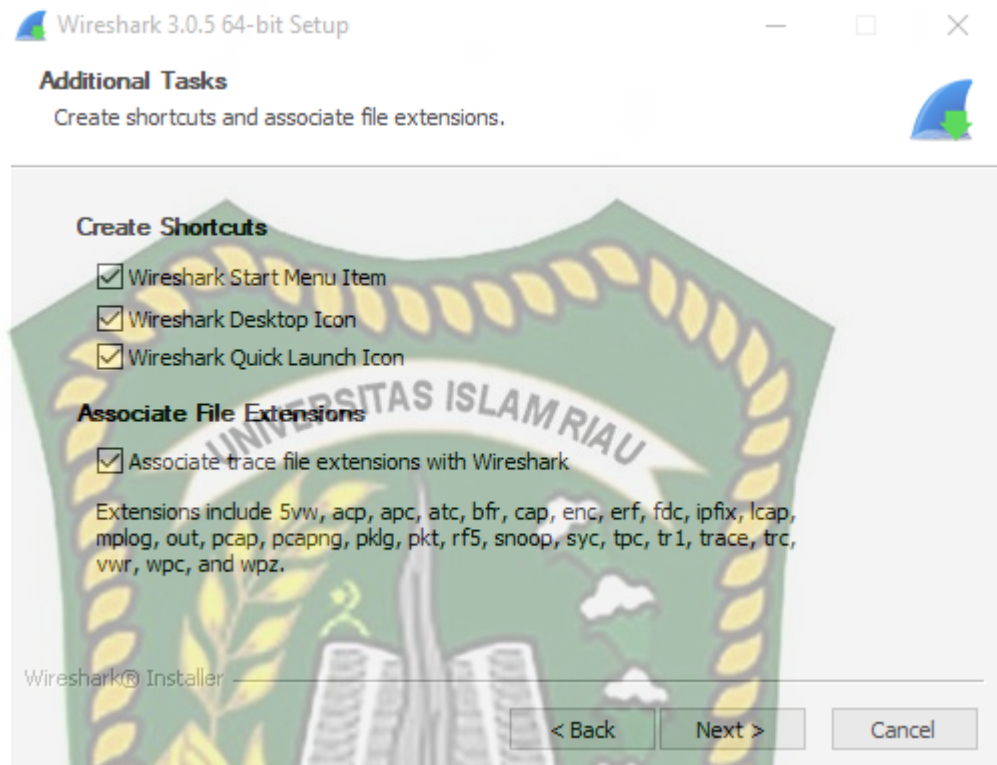


- d. Selanjut nya ceklis semua pilihan lalu tekan *Next* perhatikan digambar 3.6



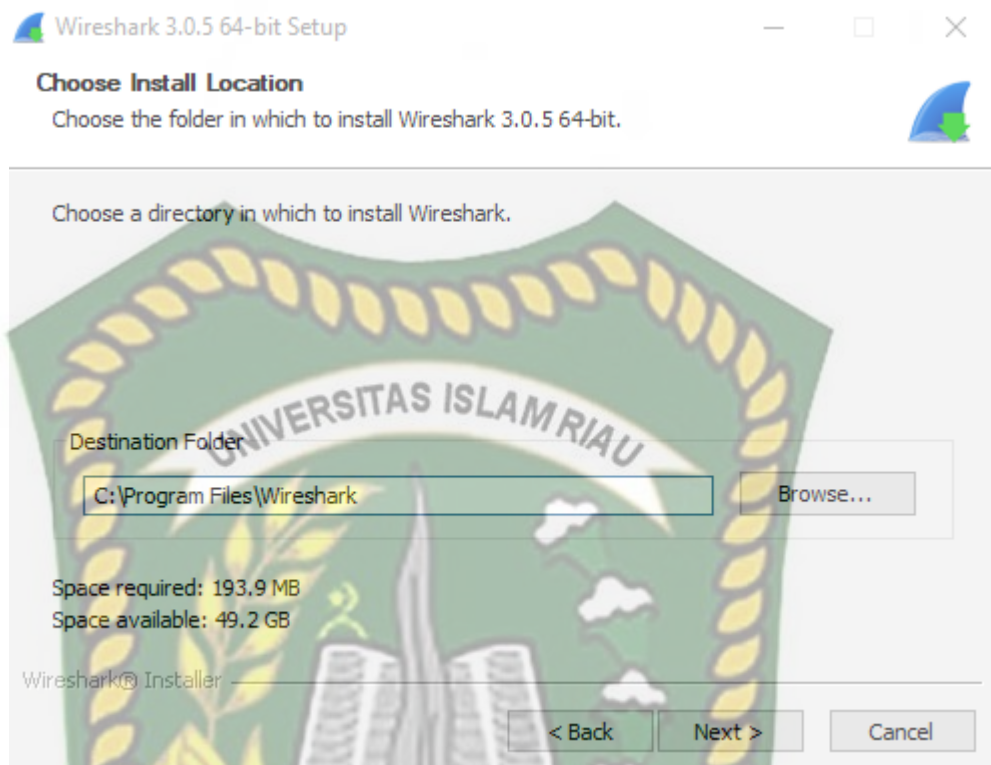
**Gambar 3. 6** Penginstalan *Wireshark* Tahap Ketiga

- e. Selanjutnya ceklis kolom yang tersedia agar aplikasi *wireshark* berada di *desktop* dan tombol *start* lalu tekan *next*, perhatikan gambar 3.7



**Gambar 3. 7** Penginstalan *Wireshark* Tahap Keempat

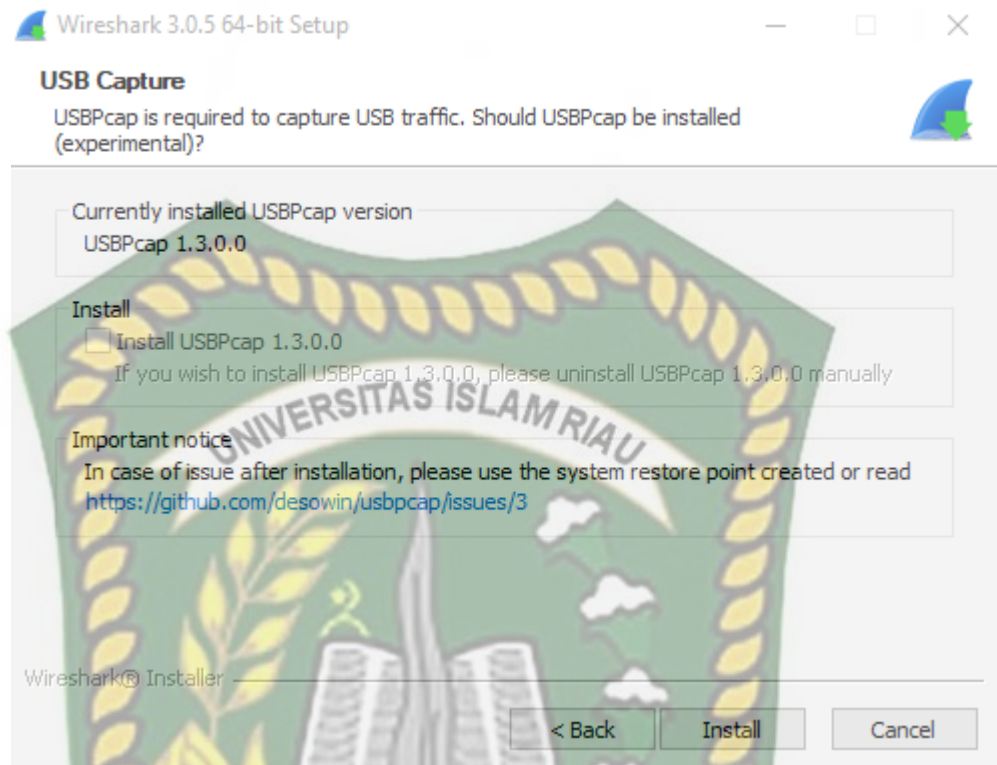
- f. Selanjutnya pilih tempat penyimpanan yang diinginkan dengan menekan *browser* untuk memilih tempat penyimpanan lalu tekan *next* untuk menuju tahap selanjutnya, perhatikan gambar 3.8



**Gambar 3. 8** Penginstalan *Wireshark* Tahap Kelima

- g. Selanjutnya tekan *install* untuk memulai penginstalan seperti gambar

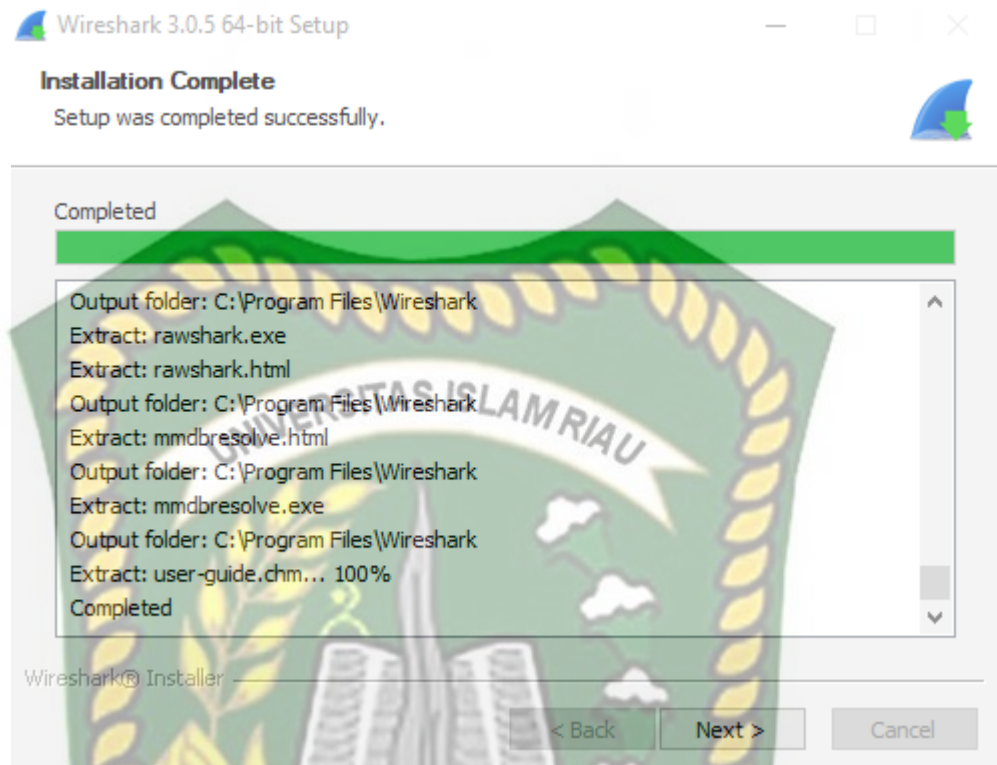
3.9



**Gambar 3. 9** Penginstalan *Wireshark* Tahap Keenam

- h. Selanjutnya tunggu penginstalan hingga selesai tekan next setelah penginstalan selesai, perhatikan gambar 3.10





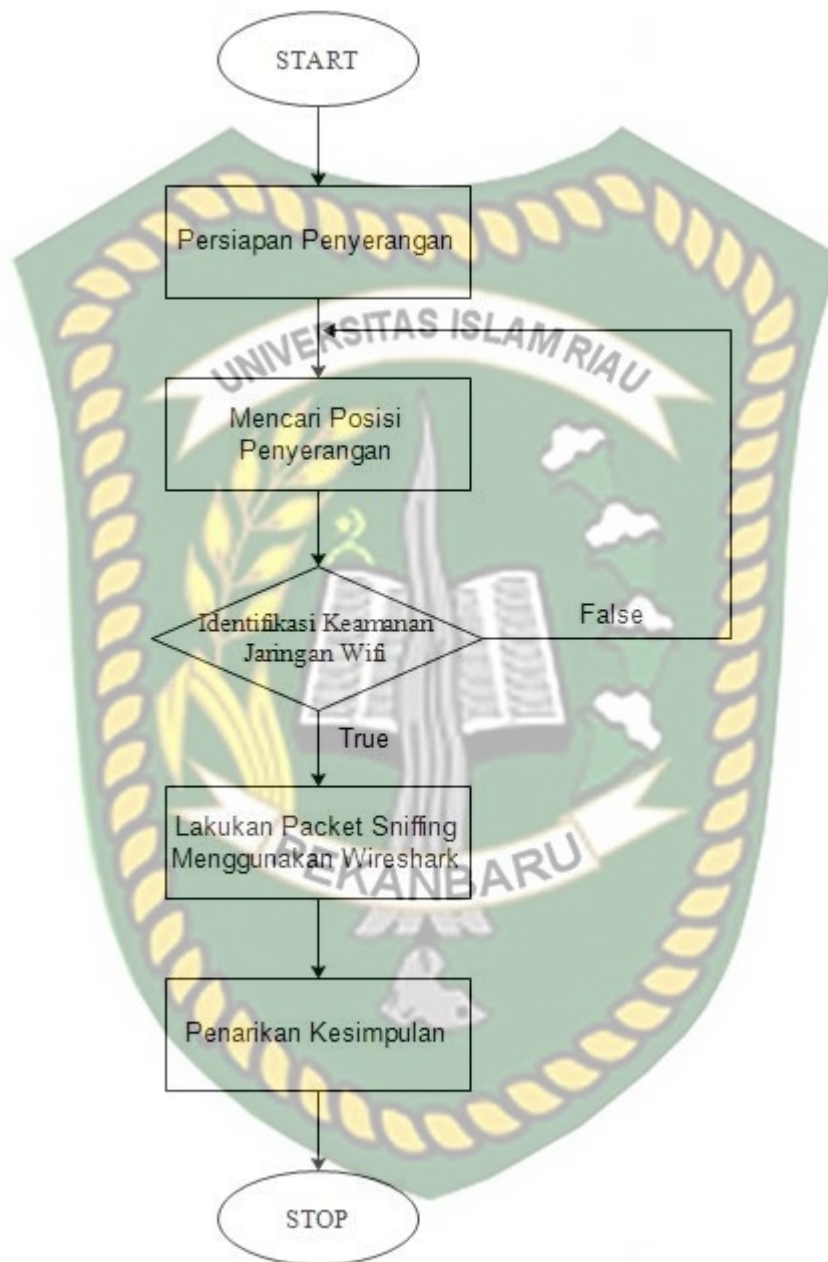
**Gambar 3. 10** Pengistalan *Wireshark* Tahap Ketujuh

- i. Selesai dalam melakukan penginstalan aplikasi *Wireshark* dan siap digunakan tekan *finish* untuk menutup penginstalan, perhatikan gambar 3.11



**Gambar 3. 11** Penginstalan *Wireshark* SELESAI

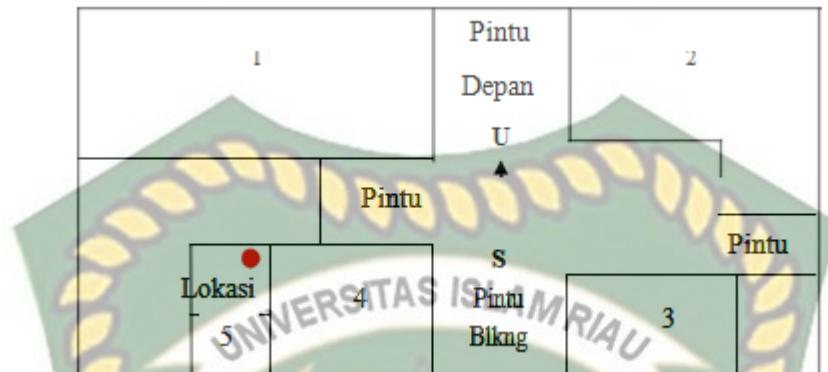
### 3.4 Tahapan – Tahapan Penyerangan



**Gambar 3. 12** *Flowchart* Tahapan Penyerangan

Sesuai dengan *flowchart* tahapan penyerangan diatas, penyerangan ini dilakukan dalam beberapa tahapan.

1. Penulis mencari posisi tempat penyerangan yang diizinkan.

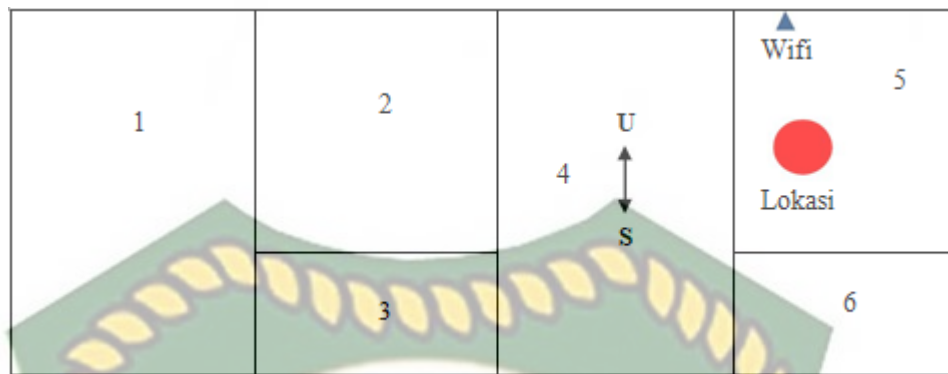


**Gambar 3. 13** Posisi tempat/lokasi penyerangan yang diizinkan pada gedung kantor PT Indosat.

Gambar 3.7 adalah denah lokasi dimana penulis melakukan penelitian pada gedung kantor PT Indosat Ooredoo Pekanbaru, angka – angka yang tertulis diatas merupakan perwakilan dari beberapa ruangan, berikut penjelasannya :

- Ruang 1 terdapat Ruang Karyawan Pelayanan Customer.
- Ruang 2 terdapat Ruang Karyawan Administrasi Keuangan, dan Kasir.
- Ruang 3 terdapat Ruang Supervisor Operasi & Teknik.
- Ruang 4 terdapat Ruang Karyawan Kebersihan & Peralatan.
- Ruang 5 adalah Ruang Rapat yang penulis gunakan sebagai tempat penelitian, yang didalam ruangan tersebut terdapat *switch* dan modem ADSL Provider.





**Gambar 3. 14** Posisi tempat/lokasi penyerangan yang diizinkan pada gedung baru Kantor PT Indosat.

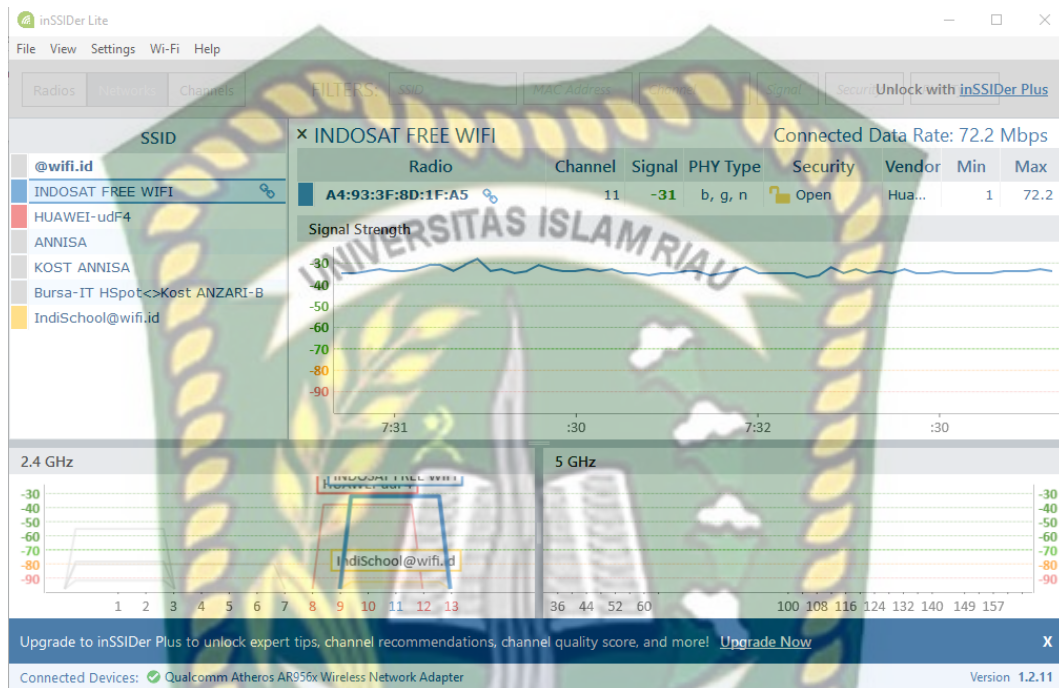
Gambar 3.8 adalah denah lokasi dimana penulis melakukan penelitian pada gedung kantor PT Indosat Ooredoo Pekanbaru, angka – angka yang tertulis diatas merupakan perwakilan dari beberapa ruangan, berikut penjelasannya :

- Ruang 1 adalah ruangan server.
- Ruang 2 adalah ruang karyawan PT Indosat Ooredoo.
- Ruang 3 adalah ruang supervisor PT Indosat Ooredoo.
- Ruang 4 adalah ruang tunggu.
- Ruang 5 adalah ruang monitoring jaringan komputer yang penulis gunakan sebagai tempat penelitian.
- Ruang 6 adalah Gudang.

## 2. Pengidentifikasian keamanan Wifi menggunakan software inSSIDer

Penulis menjalankan software inSSIDer pada windows 10 dan secara otomatis akan menampilkan informasi tentang keberadaan wifi dengan lengkap

dengan nama SSID, *mac address*, *vendor*, *channel* yang dipakai, *network type* dan *security* atau keamanan yang digunakan.



**Gambar 3. 15** Tampilan software inSSIDer saat identifikasi *wifi*.

## BAB IV

### HASIL DAN PEMBAHASAN

Analisis ini perlu dilakukan agar dapat mengetahui seberapa aman tingkat keamanan yang ada dalam sebuah jaringan *wireless* pada PT.Indosat Ooredoo Pekanbaru. Seperti pada umumnya tingkat keamanan bukan berasal dari *hardware* dan *software* yang sudah ada namun terdapat peran penting dari manusia/pengguna jaringan yang melakukan kontak atau koneksi dari perancangan jaringan itu sendiri.

Keamanan jaringan komputer yang terpasang di area PT.Indosat Ooredoo Pekanbaru pada umumnya masih perlu peningkatan kewanaman, terbukti pada *wifi* yang terpasang tidak menggunakan keamanan atau terbuka. Disamping itu masih banyak pegawai dan konsumen yang masih awam tentang keamanan jaringan *wifi*.

#### 4.1. Analisis Hasil Penelitian

##### a. Mengidentifikasi Wifi

Percobaan ini penulis lakukan untuk mengidentifikasi keberadaan *wifi* dalam berbentuk informasi lengkap dengan nama SSID, *mac address*, RSSI, *vendor*, *channel* yang memakai *network type* dan *security* atau keamanan yang digunakan. Hal ini hanya untuk memudahkan penulis melakukan penyerangan untuk mendapatkan koneksi dengan jaringan *wifi* yang ada. Dalam mengidentifikasi ini penulis mendapatkan jaringan *wifi* tanpa pengaman atau terbuka yang berada di area PT.Indosat Ooredoo Pekanbaru.

## b. Analisis jaringan wifi

Percobaan analisis ini dilakukan untuk memastikan website yang sering di kunjungi pihak kantor PT. Indosat Pekanbaru, dan untuk memastikan bahwa website tersebut bebas dari serangan *packet sniffing*. Hal ini dapat memudahkan penulis untuk memastikan website yang dapat terbebas dari serangan dan tidak, agar pihak kantor tidak perlu khawatir menggunakan jaringan *wifi* yang berada di wilayah kerja kantor PT.Indosat Ooredoo Pekanbaru.

Analisis ini dilakukan beberapa kali dalam keadaan jam kerja,berikut contoh analisis yang dilakukan :

### 1. Jam kerja pukul 10.00 W.I.B – 12.00 W.I.B

No.	Time	Source	Destination	Protocol	Length	Info
66630	1105.934560	10.126.75.175	13.107.4.50	TCP	74	[TCP Dup ACK 66614#3] 59664 → 80 [ACK] Seq=8928 Ack=3196750 Win=64240 Len=0 SLE=3202590 SRE=3204050 SLE=3198210...
66631	1105.934656	10.126.75.175	13.107.4.50	TCP	74	[TCP Dup ACK 66614#4] 59664 → 80 [ACK] Seq=8928 Ack=3196750 Win=64240 Len=0 SLE=3202590 SRE=3205510 SLE=3198210...
66632	1105.948293	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
66633	1105.948294	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
66634	1105.948295	13.107.4.50	10.126.75.175	TCP	1514	80 → 59665 [ACK] Seq=3361819 Ack=12617 Win=16996 Len=1460 [TCP segment of a reassembled PDU]
66635	1105.948295	13.107.4.50	10.126.75.175	TCP	1514	80 → 59665 [ACK] Seq=3363279 Ack=12617 Win=16996 Len=1460 [TCP segment of a reassembled PDU]
66636	1105.948381	10.126.75.175	13.107.4.50	TCP	74	[TCP Dup ACK 66614#5] 59664 → 80 [ACK] Seq=8928 Ack=3196750 Win=64240 Len=0 SLE=3202590 SRE=3206970 SLE=3198210...
66637	1105.948476	10.126.75.175	13.107.4.50	TCP	74	[TCP Dup ACK 66614#6] 59664 → 80 [ACK] Seq=8928 Ack=3196750 Win=64240 Len=0 SLE=3202590 SRE=3208430 SLE=3198210...
66638	1105.948518	10.126.75.175	13.107.4.50	TCP	54	59665 → 80 [ACK] Seq=12617 Ack=3364739 Win=64240 Len=0
66639	1105.982517	13.107.4.50	10.126.75.175	TCP	1514	[TCP Out-Of-Order] 80 → 59665 [ACK] Seq=3196750 Ack=8928 Win=13307 Len=1460
66640	1105.982527	13.107.4.50	10.126.75.175	TCP	635	[TCP Previous segment not captured] 80 → 59665 [ACK] Seq=3366199 Ack=12617 Win=16996 Len=581 [TCP segment of a ...]
66641	1105.982528	13.107.4.50	10.126.75.175	TCP	1514	[TCP Out-Of-Order] 80 → 59665 [ACK] Seq=3364739 Ack=12617 Win=16996 Len=1460 [TCP segment of a reassembled PDU]
66642	1105.982529	13.107.4.50	10.126.75.175	TCP	1514	80 → 59665 [ACK] Seq=3366780 Ack=12617 Win=16996 Len=1460 [TCP segment of a reassembled PDU]
66643	1105.982530	13.107.4.50	10.126.75.175	TCP	1514	80 → 59665 [ACK] Seq=3368240 Ack=12617 Win=16996 Len=1460 [TCP segment of a reassembled PDU]
66644	1105.982532	13.107.4.50	10.126.75.175	TCP	1514	80 → 59665 [ACK] Seq=3369700 Ack=12617 Win=16996 Len=1460 [TCP segment of a reassembled PDU]
66645	1105.982702	10.126.75.175	13.107.4.50	TCP	66	59664 → 80 [ACK] Seq=8928 Ack=3201130 Win=64240 Len=0 SLE=3202590 SRE=3208430
66646	1105.982868	10.126.75.175	13.107.4.50	TCP	66	[TCP Dup ACK 66638#1] 59665 → 80 [ACK] Seq=12617 Ack=3364739 Win=64240 Len=0 SLE=3366199 SRE=3366780
66647	1105.982959	10.126.75.175	13.107.4.50	TCP	54	59665 → 80 [ACK] Seq=12617 Ack=3366780 Win=64240 Len=0
66648	1105.983040	10.126.75.175	13.107.4.50	TCP	54	59665 → 80 [ACK] Seq=12617 Ack=3371160 Win=64240 Len=0
66649	1106.094442	10.126.104.109	10.126.255.255	UDP	305	54915 → 54915 Len=263
66650	1106.094444	10.126.107.159	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
66651	1106.114642	13.107.4.50	10.126.75.175	TCP	1514	80 → 59665 [PSH, ACK] Seq=3371160 Ack=12617 Win=16996 Len=1460 [TCP segment of a reassembled PDU]
66652	1106.114644	13.107.4.50	10.126.75.175	TCP	1514	80 → 59665 [PSH, ACK] Seq=3372620 Ack=12617 Win=16996 Len=1460 [TCP segment of a reassembled PDU]
66653	1106.114645	13.107.4.50	10.126.75.175	TCP	1514	[TCP Previous segment not captured] 80 → 59665 [ACK] Seq=3376432 Ack=12617 Win=16996 Len=1460 [TCP segment of a ...]
66654	1106.114775	10.126.75.175	13.107.4.50	TCP	66	59665 → 80 [ACK] Seq=12617 Ack=3374980 Win=64240 Len=0 SLE=3376432 SRE=3377892
66655	1106.121868	52.139.250.253	10.126.75.175	TCP	66	[TCP Dup ACK 640834] 443 → 59542 [ACK] Seq=1 Ack=1 Win=7990 Len=0 TSval=3225614525 TSecr=11568456
66656	1106.121949	10.126.75.175	52.139.250.253	TCP	54	[TCP Dup ACK 645834] [TCP ACKed unseen segment] 59522 → 443 [ACK] Seq=1 Ack=2 Win=514 Len=0
66657	1106.242859	10.126.20.131	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
66658	1106.242861	10.126.107.213	10.126.255.255	NBNS	92	Name query NB ISATAP<00>

**Gambar 4. 1** Pukul 10.00 W.I.B – 11.00 W.I.B



No.	Time	Source	Destination	Protocol	Length	Info
69671	1135.924812	13.107.4.50	10.126.75.175	HTTP	627	[TCP Previous segment not captured] Continuation
69682	1136.064497	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69685	1136.086861	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69686	1136.086863	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69693	1136.086872	36.89.220.115	10.126.75.175	HTTP	946	Continuation
69694	1136.086873	36.89.220.115	10.126.75.175	HTTP	1514	Continuation
69695	1136.086873	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69697	1136.086874	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69704	1136.087522	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69713	1136.234935	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69714	1136.234937	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69715	1136.234938	36.89.220.115	10.126.75.175	HTTP	1514	Continuation
69716	1136.234947	36.89.220.115	10.126.75.175	HTTP	1514	Continuation
69717	1136.234948	13.107.4.50	10.126.75.175	HTTP	1514	[TCP Previous segment not captured] Continuation
69725	1136.656416	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69726	1136.656419	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69727	1136.656420	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69728	1136.656422	36.89.220.115	10.126.75.175	HTTP	1514	[TCP Previous segment not captured] Continuation
69729	1136.656423	36.89.220.115	10.126.75.175	HTTP	1514	Continuation
69758	1137.166927	13.107.4.50	10.126.75.175	HTTP	1514	[TCP Previous segment not captured] Continuation
69823	1139.210522	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69825	1139.558906	36.89.220.115	10.126.75.175	HTTP	1514	Continuation
69847	1140.240543	36.89.220.115	10.126.75.175	HTTP	1514	Continuation
69870	1140.435161	13.107.4.50	10.126.75.175	HTTP	1514	[TCP Previous segment not captured] Continuation
69872	1140.438904	13.107.4.50	10.126.75.175	HTTP	1514	Continuation
69876	1140.453525	36.89.220.115	10.126.75.175	HTTP	1514	[TCP Spurious Retransmission] Continuation
69877	1140.453531	36.89.220.115	10.126.75.175	HTTP	1514	Continuation
69881	1140.474566	36.89.220.115	10.126.75.175	HTTP	1514	[TCP Previous segment not captured] Continuation

Gambar 4. 2 Pukul 11.00 W.I.B – 12.00 W.I.B

## 2. Jam kerja 13.00 W.I.B s/d 15.00 W.I.B

No.	Time	Source	Destination	Protocol	Length	Info
16049	466.963384	10.126.168.230	10.126.255.255	NBNS	92	Name query NB NB.ZABHXQQ.NET<00>
16050	466.996693	10.126.168.230	10.126.255.255	NBNS	92	Name query NB NB.ZABHXQQ.NET<00>
16051	467.102478	10.126.183.152	10.126.255.255	UDP	305	54915 → 54915 Len=263
16052	467.103642	10.126.111.234	10.126.255.255	NBNS	92	Name query NB DESKTOP-GP4VUG41c<1c>
16053	467.249098	10.126.12.224	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
16054	467.251987	10.126.72.181	10.126.255.255	UDP	305	54915 → 54915 Len=263
16055	467.304108	10.126.34.63	255.255.255.255	UDP	82	57621 → 57621 Len=40
16056	467.461008	10.126.168.129	10.126.255.255	BROWSER	243	Host Announcement HP-PC, Workstation, Server, Print Queue Server, NT Workstation
16057	467.462046	10.126.111.128	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
16058	467.632711	10.126.209.99	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
16059	467.633840	10.126.245.200	10.126.255.255	NBNS	92	Name query NB BRWFC017C48252E<00>
16060	467.636299	10.126.168.230	10.126.255.255	NBNS	92	Name query NB NB.WQJPGVF.NET<00>
16061	467.980413	10.126.111.234	10.126.255.255	NBNS	92	Name query NB DESKTOP-GP4VUG41c<1c>
16062	467.981555	10.126.237.230	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
16063	467.982603	10.126.156.23	255.255.255.255	UDP	82	57621 → 57621 Len=40
16064	467.983757	10.126.12.224	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
16065	467.986125	10.126.255.65	10.126.255.255	BROWSER	243	Host Announcement ACERKU-PC, Workstation, Server, NT Workstation, Potential Browser
16066	468.045074	10.126.12.146	192.168.1.255	TCP	66	[TCP Retransmission] 59079 → 1688 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16067	468.103331	10.126.72.181	10.126.255.255	UDP	305	54915 → 54915 Len=263
16068	468.220600	10.126.111.128	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
16069	468.244842	10.126.73.63	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
16070	468.355129	10.126.12.134	10.126.255.255	NBNS	92	Name query NB WPAD<00>
16071	468.356185	10.126.209.99	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
16072	468.558373	10.126.245.200	10.126.255.255	NBNS	92	Name query NB BRWFC017C48252E<00>
16073	468.559760	10.126.168.230	10.126.255.255	NBNS	92	Name query NB NB.WQJPGVF.NET<00>
16074	468.560972	10.126.237.230	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
16075	468.563238	10.126.5.72	10.126.255.255	BROWSER	228	Request Announcement MINDOMS-BVSBUTE
16076	468.921268	10.126.168.234	10.126.255.255	NBNS	92	Name query NB WPAD<00>

Gambar 4. 3 Pukul 13.00 W.I.B s/d 14.00 W.I.B

No.	Time	Source	Destination	Protocol	Length	Info
17878	529.459661	10.126.33.56	10.126.255.255	BROWSER	243	Host Announcement: DESKTOP-POT531J, Workstation, Server, NT Workstation, Potential Browser
17879	529.671701	10.126.245.200	10.126.255.255	NBNS	92	Name query NB BRWFC017C4B252E<00>
17880	529.675647	10.126.162.73	10.126.255.255	NBNS	110	Registration NB WORKGROUP<00>
17881	529.678173	10.126.145.249	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
17882	529.680600	10.126.8.229	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17883	529.714083	10.126.173.96	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17884	529.715169	10.126.173.96	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17885	529.716365	10.126.173.96	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17886	529.870324	10.126.193.111	10.126.255.255	BROWSER	243	Host Announcement: ARYANDISCOUT24, Workstation, Server, NT Workstation, Potential Browser
17887	529.870934	10.126.12.146	192.168.1.255	TCP	66	[TCP Retransmission] 59079 → 1688 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
17888	529.871224	10.126.208.105	10.126.255.255	NBNS	92	Name query NB SISOHU.COM<00>
17889	530.080385	10.126.183.152	10.126.255.255	UDP	305	54915 → 54915 Len=263
17890	530.083206	10.126.72.181	10.126.255.255	UDP	305	54915 → 54915 Len=263
17891	530.183475	10.126.30.162	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17892	530.190550	10.126.127.233	10.126.255.255	BROWSER	240	Browser Election Request
17893	530.191676	10.126.208.191	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17894	530.203908	10.126.93.57	10.126.255.255	UDP	1462	889 → 889 Len=1420
17895	530.208035	10.126.8.214	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17896	530.208212	10.126.245.200	10.126.255.255	NBNS	92	Name query NB BRWFC017C4B252E<00>
17897	530.335871	10.126.123.122	10.126.255.255	NBNS	92	Name query NB ISATAP<00>
17898	530.337026	10.126.8.214	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17899	530.338222	10.126.8.214	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17900	530.402628	10.126.40.75	255.255.255.255	UDP	82	57621 → 57621 Len=40
17901	530.404952	10.126.173.96	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17902	530.406069	10.126.173.96	10.126.255.255	NBNS	92	Name query NB WPAD<00>
17903	530.456067	10.126.162.168	10.126.255.255	NBNS	92	Name query NB SISOHU.COM<00>
17904	530.604446	10.126.47.112	10.126.255.255	NBNS	92	Name query NB WORKGROUP<1c>
17905	530.923013	10.126.8.229	10.126.255.255	NBNS	92	Name query NB WPAD<00>

**Gambar 4. 4** Pukul 14.00 W.I.B s/d 15.00 W.I.B

### c. Packet Sniffing

Penelitian ini dilakukan untuk dapat melihat informasi penting seperti *account username, password*, akses DNS yang akan di tuju dan informasi lainnya. Penelitian ini dilakukan agar penyerang dapat melakukan akses internet secara tidak sah dan untuk menguntungkan diri sendiri tapi dapat merugikan bagi orang lain yang menggunakan jaringan yang sama dengan penyerang. Pada penelitian ini penyerang berhasil mendapatkan beberapa *username* dan *password* dari salah satu pengguna yang berada di dalam jaringan. Dengan demikian penulis dapat memberi pernyataan bahwa jaringan yang digunakan tidak aman karena semua kegiatan pengguna di dalam jaringan dapat terekam dengan mudah dan dapat dicuri yang hanya menguntungkan diri sendiri.

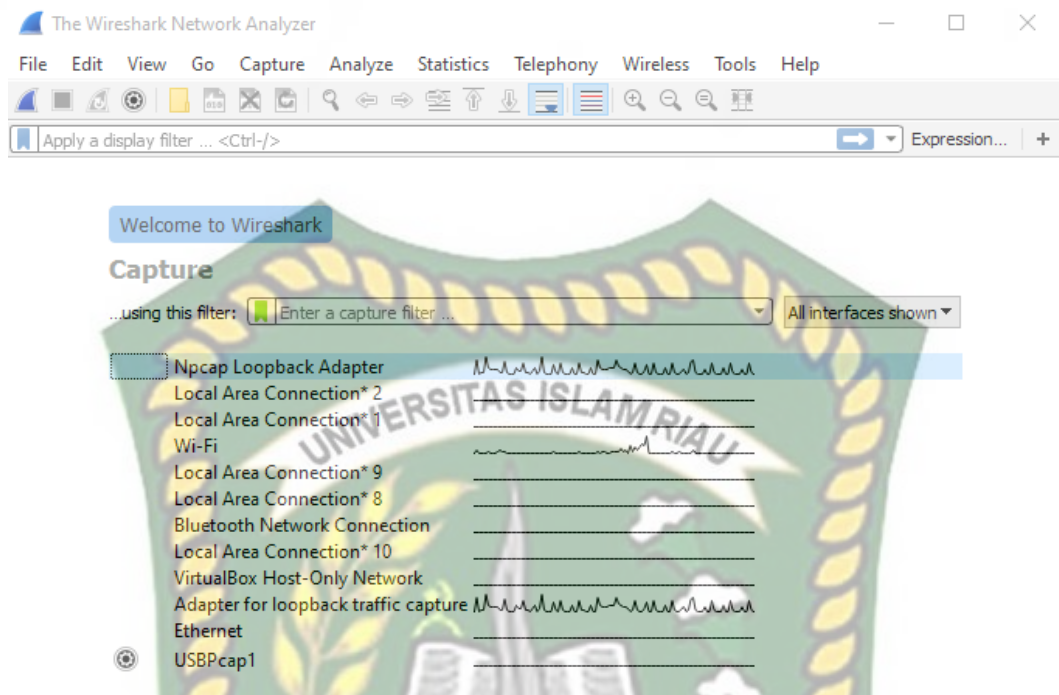
Skenario dimana penyerang sedang melakukan penyerangan dengan membagi kelompok target menjadi dua kelompok yaitu target 1 dan target 2 dimana target 1 atau target utama tidak merespon atau tidak melakukan aktifitas

apapun maka penyerang akan langsung otomatis berpindah ke target 2 begitu pula sebaliknya hingga penyerang dapat merekam semua akses dan aktifitas yang berjalan pada target.

Karena dalam penyerangan ini selama beberapa jam kerja penyerang tidak menemukan aktifitas yang sedang mengakses seperti email dan password, maka penyerang melakukan 1 skenario lagi yaitu :

- a. Berikut langkah langkah dari skenario yang dilakukan:
  1. Penyerang memastikan target berada didalam satu jaringan yang sama dengan penyerang
  2. Penyerang mencari sebuah website yang tidak memiliki sistem keamanan yang terenkripsi
  3. Penyerang melakukan login pada sistem informasi tersebut.
  4. Akun yang di coba login adalah akun yang salah karena penyerang hanya mencoba sistem keamanan website tersebut.
  5. Penyerang berhasil merekam beberapa aktifitas dari target yang sudah masuk dengan menggunakan software *wireshark*.
- b. Hasil penyerangan skenario yang dilakukan penyerang
  1. Memastikan penyerang berada dalam jaringan yang sama dengan target pada aplikasi *wireshark*. Seperti gambar 4.5.

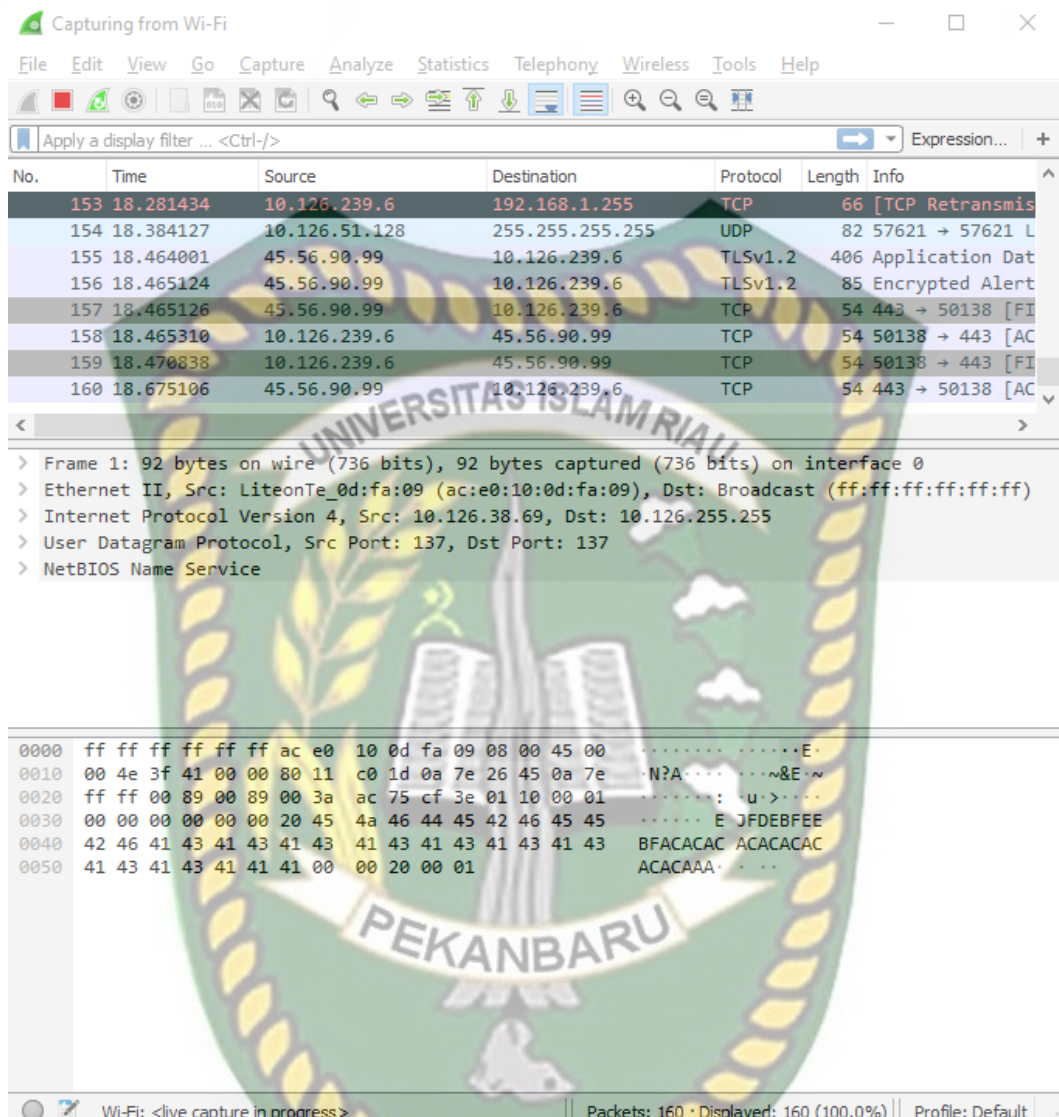




**Gambar 4. 5** Tahap Penyerangan Pertama Identifikasi Jaringan *Wifi*

- Setelah memilih jaringan yang ingin diiginkan penyerang dapat melihat aktifitas jaringan tersebut seperti gambar 4.6.





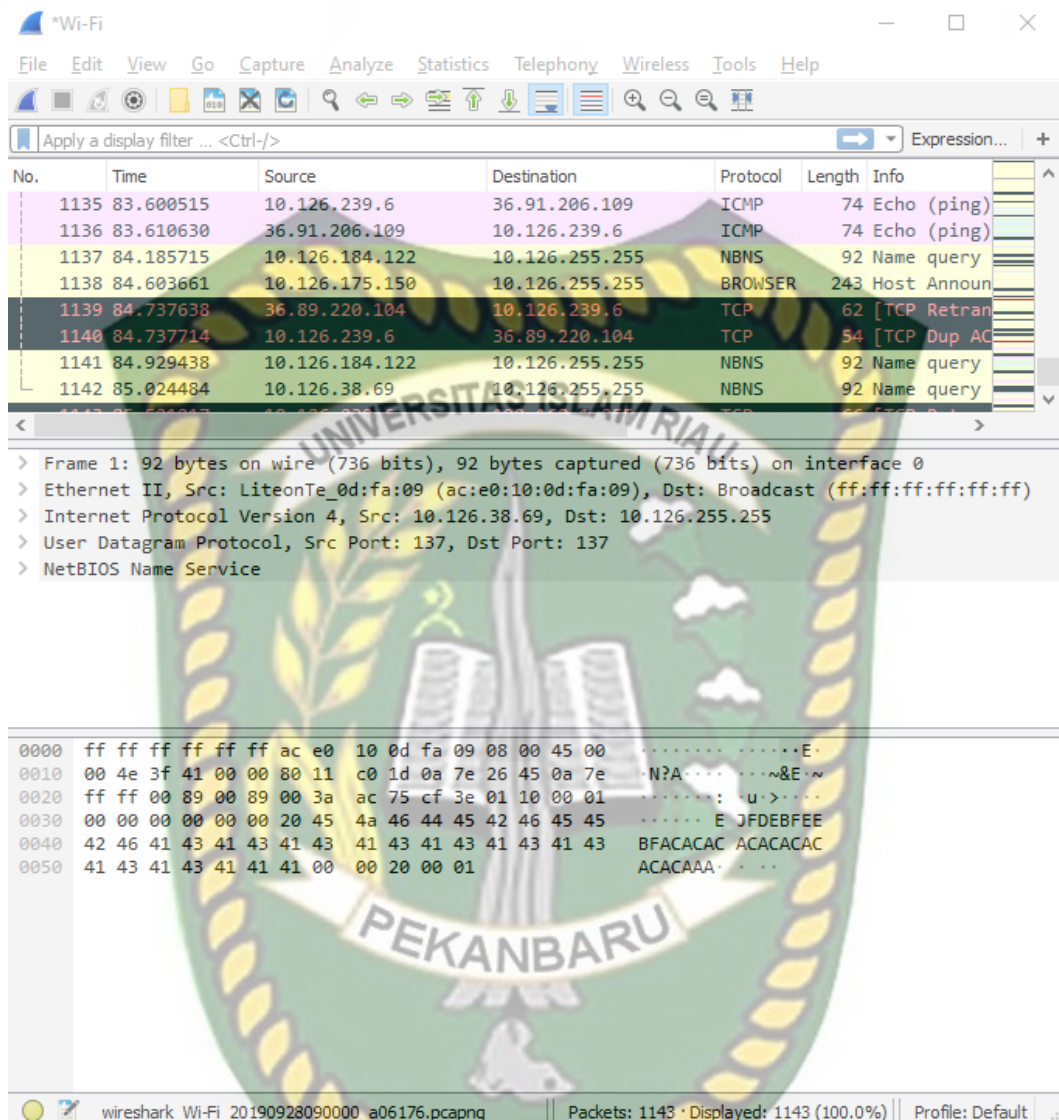
Gambar 4. 6 Aktivitas Jaringan Wifi Pada Aplikasi Wireshark

- Setelah itu penyerang dapat mencari website yang tidak memiliki keamanan yang terenkripsi. Dan setelah penyerang dapat website yang tidak memiliki system keamanan terenkripsi penyerang dapat mengisi kolom *username* dan *password* yang salah karena system akan tetap membaca apapun yang terisi pada sistem yang akan diserang. Contoh website yang tidak terenkripsi dapat dilihat pada gambar 4.7.



**Gambar 4.7** Website Yang Tidak Memiliki Sistem Terenkripsi

4. Setelah itu penyerang dapat melihat aktifitas pada *website* pada aplikasi *wireshark*. Seperti gambar 4.8.



Gambar 4. 8 Aktivitas Website Pada Aplikasi Wireshark

5. Jika pada aktivitas *wireshark* penyerang tidak dapat melihat IP dari *Website* yang akan di serang maka penyerang bisa melihat IP *website* melalui *command prompt*, seperti gambar 4.9.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Asus>ping portalmhs.stia-lk-dumai.ac.id

Pinging portalmhs.stia-lk-dumai.ac.id [36.91.206.109] with 32 bytes of data:
Reply from 36.91.206.109: bytes=32 time=7ms TTL=60
Reply from 36.91.206.109: bytes=32 time=7ms TTL=60
Reply from 36.91.206.109: bytes=32 time=7ms TTL=60
Reply from 36.91.206.109: bytes=32 time=10ms TTL=60

Ping statistics for 36.91.206.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 10ms, Average = 7ms

C:\Users\Asus>

```

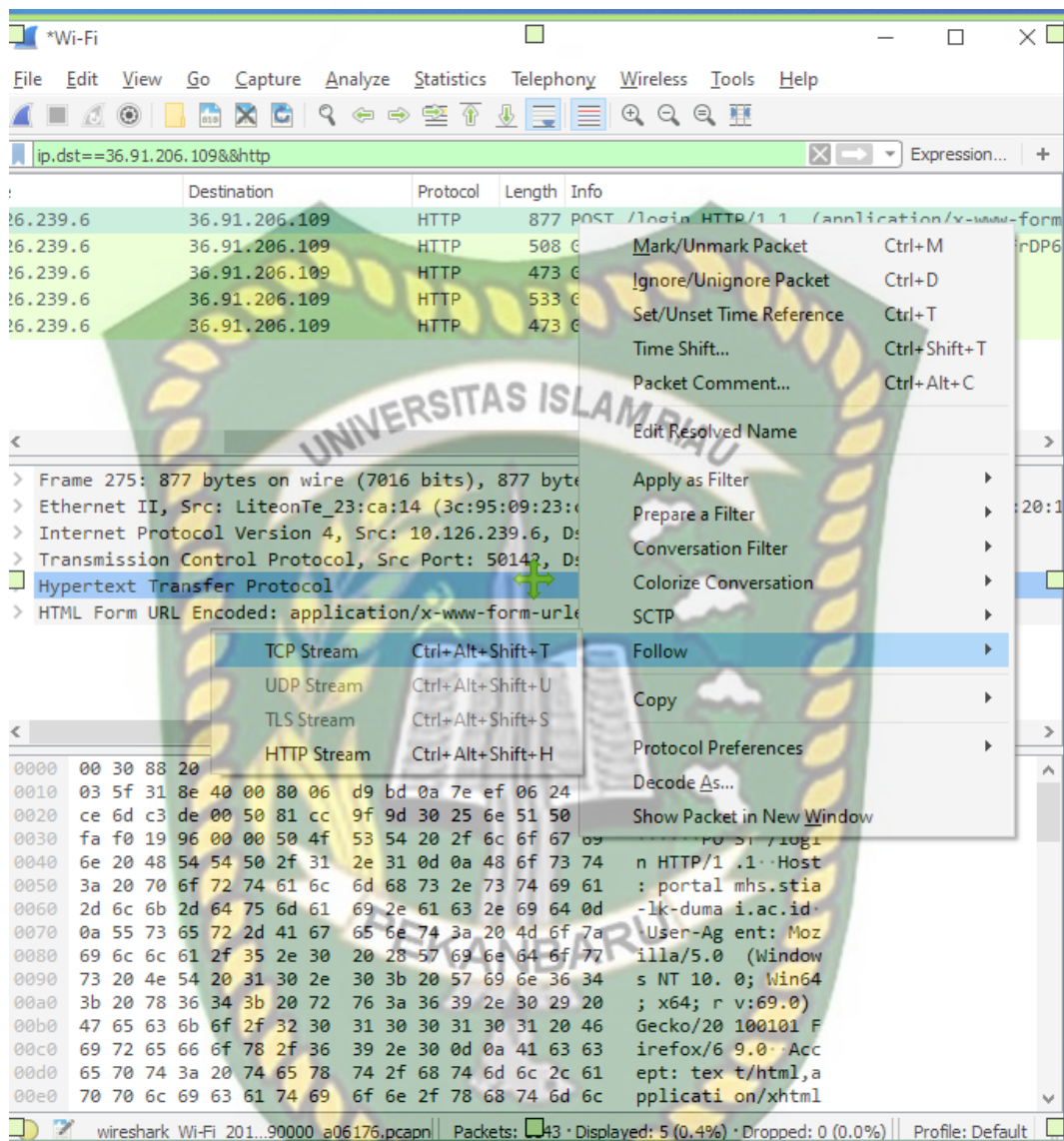
**Gambar 4. 9** Hasil Pencarian IP *Website* Pada *Command Prompt*

6. Setelah penyerang mendapat IP *Website* penyerang dapat mencari aktifitas *website* tersebut di aplikasi *wireshark* seperti pada gambar 4.10.



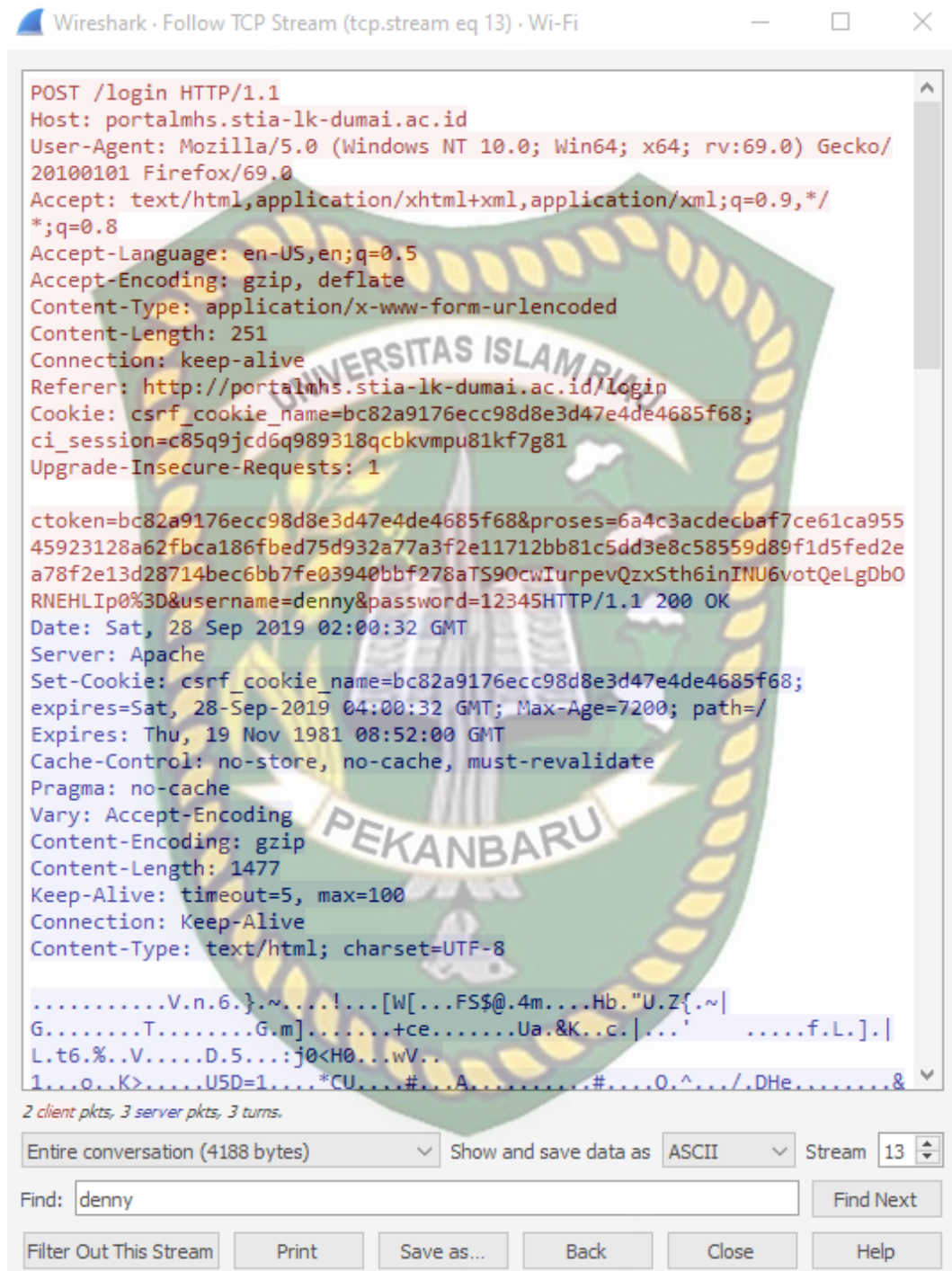


7. Setelah dapat melihat aktifitas apa saja pada website penyerang bisa dapat melihat aktifitas login website dengan cara seperti gambar 4.11.



**Gambar 4. 11** Cara Melihat Aktifitas Login Website

8. Selanjutnya tampilan pencarian aktifitas login penyerang dapat mencari melalui *find text* seperti gambar 4.12.



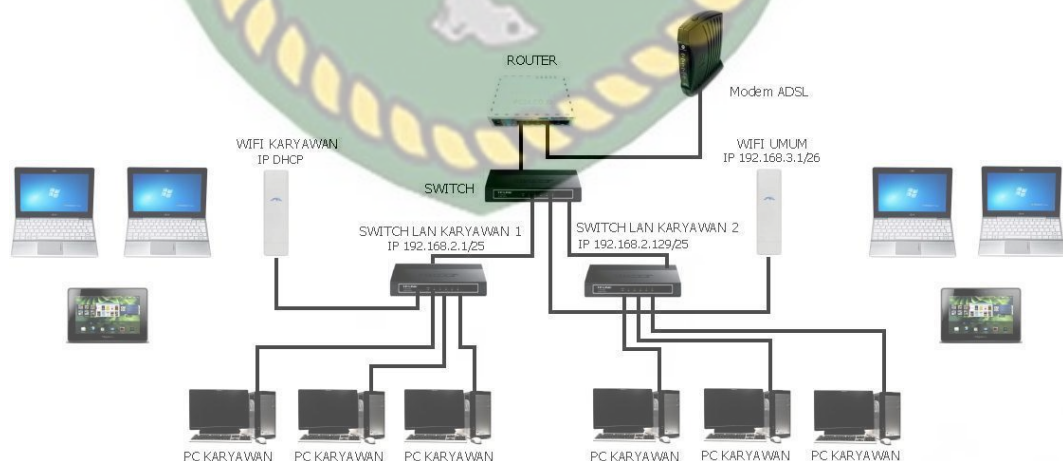
**Gambar 4. 12** Pencarian Aktifitas Login Melalui *Find Text*



#### 4.2 Solusi Untuk Mencegah Serangan *Packet Sniffing*

Setelah melakukan beberapa penyerangan dan skenario penulis telah menyiapkan beberapa rekomendasi untuk meningkatkan keamanan sebuah jaringan pada wifi yang tanpa pengaman agar terhindar dari suatu serangan seperti yang dapat dilakukan oleh penulis. Untuk dapat menganalisis suatu keamanan jaringan *wifi* yang dapat diterapkan yaitu seperti :

1. Selalu bedakan antara jaringan *wifi* untuk pemakaian kantor dengan *wifi* untuk pengguna umum atau kostumer, karena ketika seorang penyerang atau orang yang tidak bertanggung jawab menggunakan teknik *packet sniffing* seperti yang di lakukan penulis tidak dapat menembus jaringan *wifi* kantor. Secara teknis solusi diatas dapat di lakukan dengan melakukan setting ulang *subnetting*, untuk jaringan *wifi* kantor misalnya dengan IP 192.168.2.1/25 dan untuk jaringan *wifi* umum dengan IP 192.168.3.1/26 untuk 64 host.



**Gambar 4. 13** Perbedaan jaringan internet *wifi* kantor dan umum



Pada gambar 4.13 dijelaskan dengan membedakan pemakaian antara jaringan *wifi* kantor dan umum maka serangan *packet sniffing* tidak dapat masuk kedalam jaringan kantor untuk menyadap lalu lintas data yang sedang berjalan, karena secara sistem *packet sniffing* berjalan di layer 2.

## 2. Binding IP dan Mac Address

Salah satu cara yang digunakan untuk mengatasi *ARP Spoofing* pada suatu jaringan adalah dengan *Binding IP dan Mac Address*. Metode ini dapat bekerja dengan cara mendaftarkan setiap pengguna yang terkoneksi dengan jaringan *gateway*. Setiap pengguna diikat *IP address* dan *MAC address*nya sehingga *gateway* tidak salah dalam mengirimkan pesan atau paket kepada pengguna, maka *ARP Spoofing* dapat di hindari.

3. Selalu gunakan keamanan enkripsi WPA2-PSK dan radius yang hanya berada di dalam ruangan kantor, karena untuk mengamankan jaringan *wifi* kantor agar sinyal jaringan tidak dapat di jangkau oleh pengguna umum dan hanya karyawan yang mengetahui nya.



Dokumen ini adalah Arsip Miik :

**Perpustakaan Universitas Islam Riau**

## BAB V

### KESIMPULAN DAN SARAN

#### 5.1 Kesimpulan

Berdasarkan pembahasan yang sudah penulis lakukan dalam penelitian ini yang berjudul “Analisis Keamanan Jaringan *Wifi* Terhadap Penyerangan Packet Sniffing Pada Kantor PT Indosat Ooredoo Pekanbaru” masih perlu peningkatan keamanan , maka hasil penelitian ini dapat di simpulkan sebagai berikut :

1. Penyerangan *Packet Sniffing* dapat merekam dan menampilkan *username* dan *password* target dengan menggunakan aplikasi *Wireshark*.
2. Dengan melakukan penelitian ini pihak kantor PT Indosat Ooredoo Pekanbaru dapat mengetahui bahayanya penggunaan *wifi* tanpa pengaman dan yang berada dalam satu jaringan dengan pengguna umum.
3. Pihak kantor PT Indosat Ooredoo Pekanbaru dapat meningkatkan keamanan *wifi* kantor dengan memisahkan pemakaian *wifi* kantor dan pengguna umum

#### 5.2 Saran

Simulasi yang penulis lakukan ini sangat jauh dari kata sempurna banyak terdapat kekurangan. Untuk itu penulis sangat perlu pengembangan lebih lanjut agar simulasi ini terlihat sempurna, adapun saran-saran dari simulasi ini agar dapat dipertimbangkan untuk ke depannya adalah sebagai berikut :

1. Simulasi ini hanya menggunakan 1 PC untuk menggunakan 2 PC harus menggunakan *Operation System* (OS) linux sedangkan penulis hanya memakai *Operation System* (OS) Windows 10.
2. Diperlukan pembagian jaringan untuk membedakan pemakaian *wifi* kantor dan pemakaian *wifi* umum agar tidak terjadi serangan yang dilakukan melalui jaringan *wifi* umum oleh pihak yang tidak bertanggung jawab untuk mendapatkan informasi penting demi keuntungan pribadi.
3. Diperlukan nya pengamanan *wifi* berupa WPA2-PSK sebagai keamanan *wifi* awal untuk dapat meminimalisir terjadi nya *packet sniffing*.
4. Lakukan lah pergantian *password* secara berkala setelah login menggunakan *wifi* umum.
5. Lakukan pengecekan jaringan secara berkala untuk menghindari kesalahan/*error* pada jaringan yang membuat kinerja jaringan menjadi lambat.



## DAFTAR PUSTAKA

- Rumalutur, Sonny. 2012. “Analisis Keamanan Jaringan Wireless Lan (WLAN) Pada PT.PLN(PERSERO) Wilayah P2B Area Sorong”. Sorong : Politeknik Katolik Saint Paul Sorong.
- Samsumar, Lalu Delsi. 2017. “Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (WLAN); Studi Kasus Di Kampus STMIK Mataram”. Mataram : STMIK Mataram.
- Supriyanto, Aji. 2006. “Analisis Kelemahan Keamanan Pada Jaringan Wireless”. Semarang : Tugas Akhir Universitas Stikubank Semarang,
- Setiawan, Thomas. 2004. “Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal”. Bandung : Tugas Akhir Institut Teknologi Bandung,
- Noviyanto, Hendri. 2011. Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta. Surakarta : Tugas Akhir Universitas Muhammadiyah Surakarta.
- Sinambela, Josua M. 2007. “ Hacking Wifi “
- Oktavianto, Digit. 2012. “ Mencegah ARP Spoofing Dan ARP Poisoning Di Linux “
- Fadillah, Fauzan. 2012. “ Perancangan dan Analisis Keamanan Jaringan Terhadap ARP Spoofing pada Hotspot “,
- Rumalutur, Sonny. 2012. “Analisis Keamanan Jaringan Wireless Lan (WLAN) Pada PT.PLN(PERSERO) Wilayah P2B Area Sorong”. Sorong : Politeknik Katolik Saint Paul Sorong.