

**ANALISIS PENGGUNAAN *FLUXION PORTABLE*  
UNTUK MENGUJI WI-FI DENGAN KEAMANAN  
WPA/WPA2**

**SKRIPSI**

**Diajukan Oleh  
REJA ANGGARA SELIAN  
NIM. 180212023**

**Bidang Peminatan : Teknik Komputer dan Jaringan**

**Mahasiswa Fakultas Tarbiyah dan Keguruan  
Program Studi Pendidikan Teknologi Informasi**



**UNIVERSITAS ISLAM NEGERI AR-RANIRY  
FAKULTAS TARBIYAH DAN KEGURUAN  
PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMASI  
2023 M/ 1445 H**

**ANALISIS PENGGUNAAN FLUXION PORTABLE  
UNTUK MENGUJI WI-FI DENGAN KEAMANAN  
WPA/WPA2**

**SKRIPSI**

Diajukan Kepada Fakultas Tarbiyah dan Keguruan (FTK)  
Universitas Islam Negeri Ar-Raniry Darussalam Banda Aceh  
Sebagai Beban Studi Untuk Memperoleh Gelar Sarjana  
Dalam Ilmu Pendidikan Teknologi Informasi

**OLEH :**

**Reja Anggara Selian**

**NIM. 180212023**

**Mahasiswa Fakultas Tarbiyah dan Keguruan  
Program Studi Pendidikan Teknologi Informasi**

Disetujui Oleh :

**Pembimbing 1**



**(Mira Maisura, M.Sc)**

**NIP/NIDN. 198605272019032011**

**Pembimbing 2**



**(Aulia Syarif Aziz, S.Kom., M.Sc)**

**NIP/NIDN. 199305212022031001**

Lembar Pengesahan penguji sidang:

**ANALISIS PENGGUNAAN FLUXION PORTABLE  
UNTUK MENGUJI WI-FI DENGAN KEAMANAN  
WPA/WPA2**

**SKRIPSI**

Telah diuji oleh Panitia Ujian Munaqasyah Skripsi Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh dan Dinyatakan Lulus serta diterima sebagai salah satu beban studi Program Sarjana (S-1) dalam Pendidikan Teknologi

Informasi

Pada:

Senin, 11 Desember 2023

27 Jumadil Awal 1445 H

**Darussalam – Banda Aceh**

**Panitia Ujian Munaqasyah Skripsi**

Ketua



(Mira Maisura, M.Sc)  
NIP/NIDN. 198605272019032011

Sekretaris



(Aulia Syarif Aziz, S.Kom., M.Sc)  
NIP/NIDN. 199305212022031001

Penguji



(Sarini Vita Dewi, S.T., M.Eng)  
NIP/NIDN. 198712222022032001

Penguji 2



(Frimansyah, M.T)  
NIP/NIDN. 198704212015031002

**AR - RANIRY**

Mengetahui,

Dekan Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry  
Darussalam Banda Aceh



Prof. Saiful Luthfi, S.Ag., M.A., M.Ed., Ph.D.  
NIP/NIDN. 1953010211997031003



## LEMBAR PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan di bawah ini:

Nama : Reja Anggara Selian  
NIM : 180212023  
Program Studi : Pendidikan Teknologi Informasi  
Fakultas : Tarbiyah dan Keguruan  
Judul Skripsi : Analisis Penggunaan Fluxion Portable Untuk Menguji Wi-Fi Dengan Keamanan WPA/WPA2

Dengan ini menyatakan bahwa dalam penulisan skripsi ini, saya:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggungjawabkan.
2. Tidak melakukan plagiat terhadap naskah karya orang lain
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya
4. Tidak memanipulasi dan memalsukan data
5. Mengerjakan sendiri karya ini dan mampu bertanggung jawab atas karya ini

Bila dikemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggung jawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap dikenai sanksi berdasarkan aturan yang berlaku di Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh.

Demikian pernyataan ini saya buat dengan sesungguhnya.

Banda Aceh, 12 Desember 2023



menyatakan

Reja Anggara Selian

## ABSTRAK

Nama : Reja Anggara Selian  
NIM : 180212023  
Fakultas/Prodi : Tarbiyah dan Keguruan/Pendidikan Teknologi Informasi  
Judul : Analisis Penggunaan Fluxion Portable Untuk Menguji  
Wi-Fi Dengan Keamanan WPA/WPA2

Bidang Peminatan : Teknik Komputer dan Jaringan  
Jumlah Halaman : 66 Halaman  
Pembimbing I : Mira Maisura, M.Sc  
Pembimbing II : Aulia Syarif Aziz, S.Kom., M.Sc  
Kata Kunci : *Fluxion portable, Security, Action Research, WPA, WPA2*

Dengan kemudahan penggunaan yang diberikan oleh Wi-Fi, bermunculan pula berbagai tindakan ilegal yang menjadikan *password* Wi-Fi sebagai sasaran atau target utama. Penelitian ini bertujuan untuk menganalisis penggunaan dan keefektifan dari *fluxion portable* dalam menguji Wi-Fi dengan keamanan WPA/WPA2, yang dilakukan pada *router* ZTE-F609 dengan menggunakan metode *action research* atau tindakan. Hasil penelitian menunjukkan bahwa *fluxion portable* memang mampu dan efektif dalam mendapatkan *password* Wi-Fi dengan menggunakan teknik *social engineering* atau manipulasi psikologis melalui rekayasa sosial berupa serangan *online* yang jarang disadari oleh pengguna. Untuk mengatasi atau menghindari kemungkinan terjadinya serangan dari *fluxion portable* yaitu dengan menyembunyikan Wi-Fi dari *public* atau mengganti *router* yang mendukung fitur *whitelist*.

## KATA PENGANTAR

Puji syukur diucapkan kehadirat Allah SWT atas segala rahmatNya sehingga Skripsi ini dapat tersusun sampai dengan selesai. Tidak lupa kami mengucapkan terimakasih terhadap bantuan dari pihak yang telah berkontribusi dengan memberikan sumbangan baik pikiran maupun materinya. Penulis mengucapkan terima kasih kepada:

1. Kedua orang tua, Bapak dan Ibu yang telah memberikan segalanya selama menjalani Pendidikan
2. Ibu Mira Maisura, M.Sc selaku Ketua Program Studi Pendidikan Teknologi Informasi atas kesempatan dan bantuan yang diberikan kepada penulis dalam melakukan penelitian dan memperoleh informasi yang diperlukan selama penulisan proposal penelitian ini.
3. Bapak Aulia Syarif Aziz, S.Kom., M.Sc sebagai Dosen Pembimbing Proposal yang telah memberikan arahan dan semangat dalam penyusunan proposal
4. Bapak/Ibu Dosen program studi Pendidikan Teknologi Informasi yang tidak dapat saya sebutkan satu persatu yang telah mendidik dan memberikan bimbingan selama masa perkuliahan.
5. Teman-teman seperjuangan yang tidak dapat saya sebutkan satu persatu khususnya teman-teman yang membantu dalam penelitian ini.

Meskipun telah berusaha menyelesaikan Skripsi ini sebaik mungkin, penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun dari para pembaca guna menyempurnakan penyusunan Skripsi ini. Akhir kata, penulis berharap semoga Skripsi ini berguna bagi para pembaca dan pihak-pihak lain yang berkepentingan di kemudian hari.

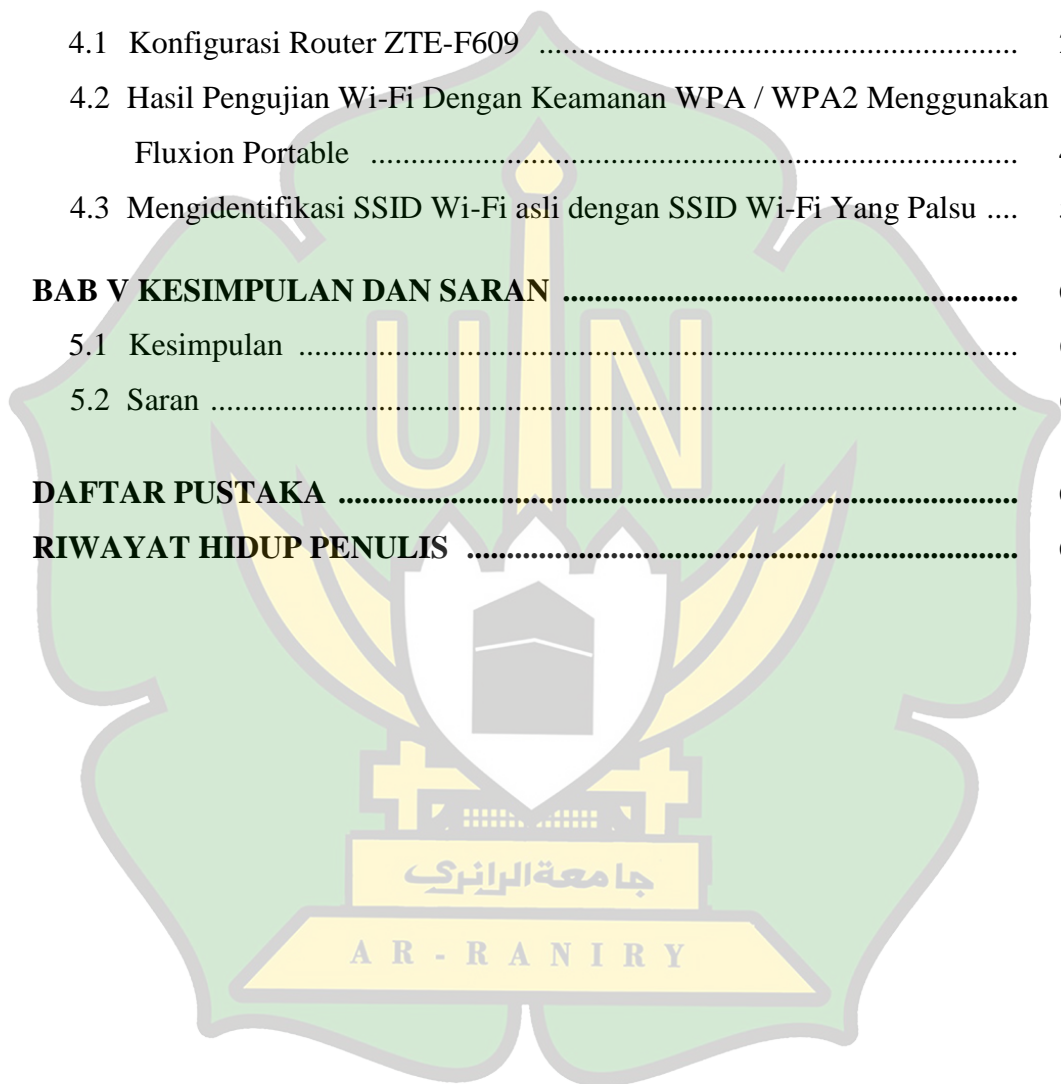
Banda Aceh, 12 Desember 2023

Penulis

## DAFTAR ISI

<b>HALAMAN SAMPUL JUDUL</b>	
<b>LEMBAR PENGESAHAN PEMBIMBING</b> .....	<b>i</b>
<b>LEMBAR PENGESAHAN SIDANG</b> .....	<b>ii</b>
<b>LEMBAR PERNYATAAN KEASLIAN KARYA ILMIAH</b> .....	<b>iii</b>
<b>ABSTRAK</b> .....	<b>iv</b>
<b>KATA PENGANTAR</b> .....	<b>v</b>
<b>DAFTAR ISI</b> .....	<b>vi</b>
<b>DAFTAR TABEL</b> .....	<b>viii</b>
<b>DAFTAR GAMBAR</b> .....	<b>ix</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah .....	3
1.3 Tujuan Penelitian .....	3
1.4 Batasan Penelitian .....	3
1.5 Manfaat Penelitian .....	3
1.6 Relevansi Penelitian Terdahulu .....	4
1.7 Sistematika Penulisan .....	8
<b>BAB II LANDASAN TEORITIS</b> .....	<b>9</b>
2.1 Dasar Teori .....	9
2.1.1 Wi-Fi .....	9
2.1.2 Router .....	11
2.1.3 Smartphone .....	14
2.1.4 Fluxion Portable .....	15
2.1.5 Keamanan Jaringan .....	15
<b>BAB III METODOLOGI PENELITIAN</b> .....	<b>19</b>
3.1 Peralatan Penelitian .....	19
3.1.1 Perangkat Penelitian .....	19

3.1.2 Metode Penelitian .....	20
3.1.3 Gambaran Umum Penelitian .....	21
3.1.4 Alur Penelitian .....	22
3.1.5 <i>Flowchart</i> Penelitian .....	23
3.1.6 Rancangan Sistem Penelitian .....	24
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>	<b>25</b>
4.1 Konfigurasi Router ZTE-F609 .....	25
4.2 Hasil Pengujian Wi-Fi Dengan Keamanan WPA / WPA2 Menggunakan Fluxion Portable .....	42
4.3 Mengidentifikasi SSID Wi-Fi asli dengan SSID Wi-Fi Yang Palsu ....	57
<b>BAB V KESIMPULAN DAN SARAN .....</b>	<b>60</b>
5.1 Kesimpulan .....	60
5.2 Saran .....	61
<b>DAFTAR PUSTAKA .....</b>	<b>62</b>
<b>RIWAYAT HIDUP PENULIS .....</b>	<b>66</b>





## DAFTAR TABEL

Tabel 1.1 Penelitian Terdahulu .....	4
Tabel 3.1 Perangkat Keras .....	19
Tabel 3.2 Perangkat Lunak .....	20



## DAFTAR GAMBAR

Gambar 3.1 Alur Penelitian .....	22
Gambar 3.2 <i>Flowchart</i> Penelitian .....	23
Gambar 3.3 Rancangan Sistem Penelitian .....	24
Gambar 3.4 Penyerangan Wi-Fi .....	24
Gambar 4.1 Menghubungkan <i>router</i> dengan <i>adaptor</i> .....	25
Gambar 4.2 Menghubungkan <i>adaptor</i> pada sumber listrik .....	26
Gambar 4.3 Tombol <i>power</i> untuk menghidupkan <i>router</i> .....	26
Gambar 4.4 <i>Router</i> telah menyala .....	27
Gambar 4.5 <i>Reset router</i> .....	27
Gambar 4.6 Menghidupkan Wi-Fi pada <i>smartphone</i> .....	28
Gambar 4.7 Menghubungkan <i>smartphone</i> ke Wi-Fi .....	28
Gambar 4.8 SSID dan <i>password default</i> ZTE-F609 .....	29
Gambar 4.9 Membuka <i>browser</i> Chrome .....	29
Gambar 4.10 <i>Default IP address</i> .....	30
Gambar 4.11 <i>Enter</i> / Tombol panah kanan .....	30
Gambar 4.12 Halaman <i>login ruoter</i> ZTE-F609 .....	31
Gambar 4.13 <i>Username</i> dan <i>password login router</i> .....	31
Gambar 4.14 Halaman utama setelah <i>login</i> ke <i>router</i> .....	32
Gambar 4.15 Menu <i>Network</i> .....	32
Gambar 4.16 Halaman menu <i>Network</i> .....	33
Gambar 4.17 Halaman menu <i>Security</i> .....	33
Gambar 4.18 Halaman mengubah <i>password</i> Wi-Fi .....	34
Gambar 4.19 Menu <i>Choose SSID</i> .....	34
Gambar 4.20 Menu memilih SSID2 .....	35
Gambar 4.21 Menu mengubah <i>Authentication Type</i> .....	36
Gambar 4.22 Mengubah <i>password</i> SSID2 .....	36
Gambar 4.23 Menu <i>SSID Setting</i> .....	37
Gambar 4.24 Halaman menu <i>SSID Setting</i> .....	37
Gambar 4.25 Menu <i>Choose SSID</i> .....	38

Gambar 4.26 Halaman <i>enable</i> SSID2 .....	39
Gambar 4.27 Mengubah nama SSID2 .....	39
Gambar 4.28 Tombol <i>Logout</i> .....	40
Gambar 4.29 Mencari Wi-Fi yang sudah dibuat .....	40
Gambar 4.30 Menghubungkan <i>smartphone</i> pada Wi-Fi yang sudah dibuat ...	41
Gambar 4.31 Berhasil terhubung pada Wi-Fi yang sudah dibuat .....	41
Gambar 4.32 Menghubungkan <i>fluxion portable</i> pada listrik .....	42
Gambar 4.33 Munculnya Wi-Fi ATTRACTHOR .....	43
Gambar 4.34 Menghubungkan <i>smartphone</i> (penyerang) ke Wi-Fi ATTRACTHOR .....	44
Gambar 4.35 Alamat halaman untuk konfigurasi <i>fluxion portable</i> .....	44
Gambar 4.36 <i>Login</i> ke halaman konfigurasi <i>fluxion portable</i> .....	45
Gambar 4.37 <i>SETUP MODE</i> pada layar <i>fluxion portable</i> .....	45
Gambar 4.38 Halaman konfigurasi <i>fluxion portable</i> .....	46
Gambar 4.39 Daftar nama Wi-Fi di area sekitar .....	47
Gambar 4.40 Memulai penyerangan .....	48
Gambar 4.41 Keterangan pada layar <i>fluxion portable</i> berubah .....	49
Gambar 4.42 Wi-Fi target menjadi dua .....	49
Gambar 4.43 Halaman <i>login</i> Wi-Fi tiruan .....	50
Gambar 4.44 <i>Input password</i> yang salah .....	50
Gambar 4.45 <i>Login</i> ulang jika <i>password</i> yang dimasukkan salah .....	51
Gambar 4.46 <i>Smartphone</i> tetap tidak bisa terhubung pada Wi-Fi asli .....	51
Gambar 4.47 <i>Input password</i> yang benar .....	52
Gambar 4.48 Terhubung pada Wi-Fi asli dan Wi-Fi tiruan berubah nama .....	52
Gambar 4.49 <i>SETUP MODE password valid</i> .....	53
Gambar 4.50 Menghubungkan kembali <i>smartphone</i> penyerang pada Wi-Fi ATTRACTHOR .....	54
Gambar 4.51 <i>Login</i> kembali pada halaman konfigurasi <i>fluxion portable</i> .....	54
Gambar 4.52 Sub menu <i>STATUS</i> .....	55
Gambar 4.53 Daftar <i>password</i> yang sudah didapat .....	56
Gambar 4.54 Wi-Fi asli memiliki ikon gembok sedangkan yang palsu tidak .	57

Gambar 4.55 Perbedaan cara menghubungkan pada kedua Wi-Fi .....	57
Gambar 4.56 Perbedaan alamat ip dan <i>gateway</i> pada kedua Wi-Fi .....	58
Gambar 4.57 Centang pada kolom <i>Hide SSID</i> .....	59



# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Teknologi pada saat ini berkembang dengan sangat pesat sehingga mempengaruhi berbagai kegiatan manusia. Terlebih lagi saat sekarang ini, hampir semua kegiatan yang berkaitan dengan lembaga pendidikan, sosial, perkantoran, dan yang lainnya sudah bisa dilakukan secara *online*. Kegiatan yang bersifat *online* ini tentunya akan memerlukan koneksi *internet* dalam melakukan kegiatannya tersebut. Oleh karena itu banyak rumah-rumah yang telah menggunakan layanan Wi-Fi sebagai sumber *internet* yang bisa digunakan secara bersama-sama. Selain itu penggunaan layanan Wi-Fi tersebut adalah sebagai bentuk pengurangan pengeluaran biaya untuk membeli kuota *internet* yang relatif lebih mahal dan hanya bisa digunakan perindividu saja agar konektivitasnya bisa maksimal.

Di Indonesia, ada banyak sekali perusahaan penyedia layanan *internet*. Dilansir dari Data Indonesia.id, Badan Pusat Statistik (BPS) melaporkan ada 611 *internet service provider* (perusahaan penyedia layanan *internet*) di Indonesia tahun 2021[1]. Dan *internet service provider* yang paling banyak digunakan adalah indihome, melalui Blog Dipstrategy, dari survei yang dilakukan APJII pertahun 2022 indihome menjadi primadona *provider fixed broadband* dengan pengguna terbanyak yaitu 67,54%[2]. Ditahun 2021 PT. Telkom Aceh khususnya indihome memiliki 148.232 endorser di Aceh[3]. Dilansir dari Quira.com, alasan orang-orang memasang Wi-Fi di rumah mereka adalah karena kebutuhan akses *internet* serta kemudahan dalam mengakses. Alasan umum lainnya dari banyaknya pengguna Wi-Fi adalah karena kemudahan dan praktisnya penggunaan dari Wi-Fi tersebut[4].

Dengan kemudahan penggunaan yang diberikan oleh Wi-Fi, bermunculan pula berbagai tindakan ilegal guna dapat mengakses Wi-Fi tersebut. Meskipun Wi-Fi itu terpasang keamanan WPA/WPA2 tidak akan menutup kemungkinan untuk dijadikan target oleh pelaku tindakan ilegal tersebut. Hal menjadi target utama para pelaku tindakan ilegal ini adalah *password* dari Wi-Fi yang telah

menjadi target mereka. Cara yang mereka lakukan untuk mendapatkan *password* Wi-Fi target mereka adalah dengan menggunakan alat tambahan berupa *fluxion portable*. Tindakan ilegal yang mereka lakukan ini dapat berpotensi melanggar Undang-Undang dan akan diberikan sanksi yang tegas.

Perihal keamanan data pribadi ini telah diatur dalam Undang-Undang ITE Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang secara umum menjelaskan penegasan bahwa pemilik data pribadi berhak atas keamanan dan kerahasiaan data pribadinya dan setiap pengguna maupun penyelenggara sistem elektronik bertanggung jawab atas data pribadi yang terdapat dalam penguasaannya. Adapun sanksi bagi para pelanggar Undang-Undang ITE tersebut diatas telah diatur dalam Undang-Undang ITE Nomor 11 Tahun 2008 Pasal 27 Ayat 3 yang menyebutkan bahwa “*Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan atau mentransmisikan atau membuat dapat diaksesnya data elektronik dan atau dokumen elektronik yang memiliki muatan penghinaan dan atau pencemaran nama baik dipidana dengan pidana penjara paling lama 4 (empat) tahun dan atau denda paling banyak Rp750.000.000,- (tujuh ratus lima puluh juta rupiah)*”[5].

Berdasarkan Undang-Undang ITE Nomor 11 Tahun 2008 di atas, salah satu cara yang dapat dilakukan untuk mengukur tingkat keamanan sistem dalam menjaga data yang bersifat rahasia adalah dengan melakukan uji coba terhadap keamanan sistemnya. Salah satu cara untuk menguji keamanannya adalah dengan menggunakan *fluxion*. *Fluxion* adalah sebuah metode berupa program yang dirancang untuk menguji keamanan jaringan nirkabel. *Fluxion* terbukti berhasil mendapatkan *password* dari Wi-Fi target, namun bukan dengan teknik membobol melainkan dengan teknik menipu pengguna Wi-Fi melalui *form* halaman *login* yang dikirim oleh *fluxion* kepada pengguna Wi-Fi[6]. *Fluxion* awalnya hanyalah sebuah *software*, namun saat ini *fluxion* telah dikembangkan menjadi *hardware* dengan beragam bentuk dan nama sehingga lebih mudah dan praktis untuk digunakan.

Berdasarkan uraian permasalahan yang tersebut di atas, maka peneliti bermaksud dan tertarik untuk melakukan penelitian terhadap jaringan Wi-Fi dengan keamanan WPA/WPA2 menggunakan fluxion portable sehingga peneliti merumuskan judul penelitian ini menjadi “**Analisis Penggunaan Fluxion Portable untuk Menguji Wi-Fi dengan Keamanan WPA/WPA2**”.

## **1.2 Rumusan Masalah**

Melalui uraian latar belakang permasalahan, maka rumusan masalah dari penelitian ini dirumuskan menjadi :

1. Bagaimana cara *fluxion portable* memutus dan mengirimkan SSID tiruan ?
2. Bagaimana keefektifan dari *fluxion portable* jika dilakukan pada Wi-Fi dengan keamanan WPA/WPA2 ?
3. Bagaimana cara mengidentifikasi SSID asli dan palsu ?

## **1.3 Tujuan Penelitian**

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Untuk mengetahui bagaimana cara *fluxion portable* memutus dan mengirimkan SSID tiruan
2. Untuk mengetahui bagaimana keefektifan dari *fluxion portable* jika dilakukan pada Wi-Fi dengan keamanan WPA/WPA2
3. Untuk mengetahui cara mengidentifikasi SSID asli dengan yang palsu

## **1.4 Batasan Penelitian**

Agar penelitian ini menjadi lebih terarah, maka penulis memberikan batasan yakni :

1. Penelitian dilakukan menggunakan *router* ZTE-F609
2. Penelitian dilakukan menggunakan *smartphone* berbasis android

## **1.5 Manfaat Penelitian**

Adapun manfaat dari penelitian ini adalah sebagai berikut :

1. Manfaat Teoritis
  - Memberikan pemahaman terkait keamanan Wi-Fi dan cara penggunaan *fluxion portable* serta keefektifannya pada peneliti maupun pembaca

- Membantu peneliti dan pembaca untuk dapat mengidentifikasi dan memahami kerentanan keamanan Wi-Fi sehingga dapat meningkatkan keamanan Wi-Fi yang digunakan.

## 2. Manfaat Praktis

- Memberikan langkah-langkah konfigurasi *router* khususnya ZTE-F609 yang dapat diikuti oleh pembaca penelitian ini
- Melalui penelitian ini diharapkan dapat membantu pembaca agar dapat meminimalisir terjadinya pencurian password Wi-Fi yang dilakukan dengan menggunakan *fluxion portable*.

### 1.6 Relevansi Penelitian Terdahulu

Berikut ini adalah beberapa penelitian terdahulu yang berkaitan dengan penelitian yang penulis lakukan :

Tabel 1.1 Penelitian Terdahulu

No	Judul	Obyek penelitian	Hasil Penelitian
1	Analisis <i>Unauthorized Access Point</i> Menggunakan Teknik <i>Network Forensics</i>	<i>Router tp-LINK AC1350 High Power Wireless Dual Band Router</i>	<p>Pentester/penyerang menggunakan <i>Aircrack-ng</i> di <i>Fluxion</i> untuk menerima jabat tangan, membuat halaman <i>login</i> jaringan palsu, dan kemudian meluncurkan serangan yang benar-benar aneh yang disebut DoS ke AAP untuk mencegah korban/klien terhubung dan akhirnya masuk titik akses palsu.</p> <p>Halaman <i>login</i> palsu kemudian meminta korban untuk memasukkan kata sandi. Setelah kata sandi dimasukkan dan terdeteksi, penyerang dapat melihatnya</p>



			<p>melalui <i>Fluxion</i>.</p> <p>Sebagai tindakan pencegahan, perbedaan antara titik akses palsu dan titik akses asli dapat dilihat melalui adanya ikon gembok (Android) atau tanda seru. (Windows 10).</p>
2	<p>Analisis Uji Keamanan WPA2 Menggunakan <i>Fluxion</i> Pada PT. Andaglos Global Teknologi</p>	<p>PT. Andaglos Global Teknologi</p>	<p>Keamanan jaringan di PT. Andaglos Global Teknologi berjalan dengan baik dalam mengamankan kata sandi, tetapi terbukti bahwa <i>Fluxion</i> dapat memperoleh kata sandi jaringan, bukan dengan merusak keamanan, tetapi dengan menipu pengguna jaringan yang menggunakannya dengan membuat formulir <i>login</i> yang sama dengan yang digunakan <i>router</i> dari PT. Andaglos Global Teknologi. Sehingga pengguna jaringan tanpa sadar memberikan kata sandi kepada pengguna <i>Fluxion</i>, yang memungkinkan pengguna untuk mengakses jaringan secara ilegal.</p>
3	<p>Analisis Metode <i>Fluxion</i> Menggunakan <i>Wifi Deauther</i> Untuk Uji Keamanan WPA2 Pada Perangkat <i>Router Wireless Totolink</i></p>	<p><i>Router Wireless Totolink N300RT R</i></p>	<p>Pengambilan <i>password</i> masih sangat berpengaruh, jika <i>password</i> tidak ditemukan maka tidak akan berhasil dan minimal ada satu pengguna yang aktif agar <i>fluxion</i> berhasil mendapatkan <i>password</i>.</p> <p>Posisi awal perangkat dalam keadaan terhubung, kemudian akan terputus dan</p>

	N300RT		SSID akan muncul ganda, jika memilih pada Wi-Fi yang asli maka akan langsung terhubung tanpa <i>login</i> ulang, tapi jika salah memilih maka akan diperintahkan untuk <i>login</i> ulang.
--	--------	--	--

Berdasarkan penelitian yang dilakukan oleh Felicia Paramita, Madeline, Olga Alvina, Rahel Esther Sentia dan Ade Kurniawan (2019) dengan judul “Analisis *Unauthorized Access Point* Menggunakan Teknik *Network Forensics*”. Teknologi jaringan Wi-Fi berkembang dengan sangat pesat diseluruh penjuru dunia yang bisa digunakan untuk komunikasi data maupun yang lainnya. Teknologi jaringan Wi-Fi sendiri menggunakan sinyal frekuensi dalam mengirimkan paket datanya, sehingga memberikan celah keamanan yang dapat diserang untuk mendapatkan data berupa *password* oleh penyerang. Penyerang dapat mengetahui *password* keamanan WPA2-PSK pada saat pengguna terhubung ke jaringan Wi-Fi yang sudah menjadi target dari penyerang tersebut. *Password* didapatkan melalui beberapa teknik dan pengujian diantaranya pengujian PIN WPS, SSID palsu dan memanfaatkan pengguna yang terhubung pada Wi-Fi tersebut.

Serangan dilakukan menggunakan *fake access point*, yang berguna untuk meniru *authorized Wi-Fi access point* atau *access point* Wi-Fi yang asli dan menyebabkan *access point* tersebut menjadi *down* dan tidak dapat digunakan, sehingga pengguna beralih ke *fake access point* yang mana nantinya pengguna akan dialihkan secara otomatis pada sebuah halaman *login* pada *browser* yang ada pada perangkat pengguna dan diminta untuk mengisi ulang *password* Wi-Fi yang akan dibaca dan disimpan oleh *fake access point* tersebut[7].

Berdasarkan penelitian yang telah dilakukan oleh Dwi Nanda Widiatama (2018) dengan judul “Analisis Uji Keamanan WPA2 Menggunakan *Fluxion* Pada PT. Andaglos Global Teknologi”. *Fluxion* terbukti berhasil dalam mendapatkan kata sandi dari Wi-Fi target bukan dengan teknik membobol

melainkan dengan teknik menipu pengguna jaringan Wi-Fi tersebut dengan membuat *form* halaman *login* yang sama dengan yang digunakan oleh Wi-Fi target. Sehingga tanpa mereka sadari, mereka telah memberikan kata sandi Wi-Fi tersebut pada pengguna *fluxion* yang menyebabkan Wi-Fi itu dapat diakses oleh pengguna *fluxion* melalui kata sandi yang telah mereka berikan[6].

Berdasarkan penelitian yang dilakukan oleh Rafita Manda Sari (2021) dengan judul “Analisis metode *Fluxion* Menggunakan Wi-Fi *Deauther* Untuk Uji Keamanan WPA2 Pada Perangkat *Router Wireless* TOTOLINK N300RT”. Metode *fluxion* menggunakan Wi-Fi *deauther* menggunakan *script* dalam proses pengambilan *password* dari Wi-Fi targetnya. *Script* ini akan berhasil jika Wi-Fi yang menjadi target memiliki satu atau lebih *user* yang sedang *online*, hal ini bertujuan agar pengambilan data berupa kata sandi bisa dilakukan dengan lebih mudah dan cepat. Akan tetapi *script* tersebut juga bisa gagal jika Wi-Fi yang sudah menjadi target tidak memiliki satupun *user* yang sedang *online*.

*Handphone* yang terhubung akan terputus dengan Wi-Fi yang sudah menjadi target, kemudian Wi-Fi *deauther* menggunakan *script fluxion* akan membuat SSID menjadi ganda, yang mana SSID ini salah satunya adalah palsu dan yang satunya lagi adalah yang asli. Dengan begitu *user* yang *handphonenya* sudah terputus dengan Wi-Fi akan kaget dan merasa kebingungan dan memilih salah satu dari kedua SSID tersebut, jika SSID palsu yang terpilih maka *user* akan dialihkan ke halaman *login* pada *browser handphone user* tersebut dan kemudian *user* diminta untuk memasukkan ulang kata sandi yang apabila *user* memasukkan kata sandi akan otomatis terbaca oleh *script fluxion* ini. Akan tetapi apabila *user* memilih SSID asli maka tidak akan terjadi proses *login* ulang dan *script* dianggap gagal[8].

Melalui hasil beberapa penelitian diatas, dapat dipahami bahwa *fluxion* pada awalnya hanyalah sebuah program yang seiring waktu dikembangkan menjadi sebuah perangkat keras. Cara kerjanya pun tergolong hampir sama dengan *fluxion* yang masih berbentuk program. Meski demikian tentu akan

memiliki perbedaan dari sisi penggunaan misalnya, *fluxion portable* ini mudah dioperasikan karena berbentuk *hardware* dan *tool-tools* yang diberikan oleh *fluxion portable* ini juga tidak sukar untuk dipahami. Berbeda dengan *fluxion* yang masih berbentuk program, yang mana pengguna harus melakukan instalasi *linux* terlebih dahulu pada perangkat mereka kemudian harus melakukan *setting* dan konfigurasi dan pemahaman *tool-tools* yang ada, tentu hal ini akan membuat kebanyakan orang menjadi kesulitan terlebih lagi mereka yang tidak memiliki latar belakang IT.

## **1.7 Sistematika Penulisan**

### **Bab 1 : Pendahuluan**

Bab I menjelaskan tentang latar belakang permasalahan yang akan diteliti, rumusan masalah, tujuan, manfaat, batasan dan relevansi penelitian terdahulu serta sistematika penulisan.

### **Bab 2 : Landasan Teoretis**

Bab II menjelaskan teori-teori yang digunakan untuk penelitian dan juga teori-teori yang baru digunakan.

### **Bab 3 : Metodologi Penelitian**

Bab III menjelaskan tentang peralatan yang digunakan dalam penelitian, metode penelitian, alur penelitian, dan rancangan sistem penelitian.

### **Bab 4 : Hasil dan Pembahasan**

Bab IV menjelaskan tentang pembahasan penelitian berupa pelaksanaan dari perencanaan yang ada ada Bab III serta menjelaskan tentang bagaimana hasil dari penelitian yang telah dilakukan.

### **Bab 5 : Penutup**

Bab V menjelaskan tentang kesimpulan yang diperoleh dari penelitian berdasarkan hasil yang sudah didapat pada Bab IV, dan juga berisikan saran untuk penelitian yang dilakukan.

## BAB II

### LANDASAN TEORITIS

#### 2.1 Dasar Teori

##### 2.1.1 Wi-Fi

Wi-Fi adalah kependekan dari *Wireless Fidelity*, yang memiliki pengertian sekumpulan standar yang digunakan untuk jaringan lokal nirkabel. Wi-Fi adalah standar koneksi yang digunakan sebagai penghubung antara satu perangkat dengan perangkat lain atau banyak perangkat yang membentuk sebuah jaringan untuk berinteraksi dengan *internet*[9].

Dalam kehidupan sehari-hari, secara umum Wi-Fi berfungsi sebagai penghubung antar perangkat seperti komputer, laptop, *smartphone*, *smart television* dan sebagainya pada *internet*. Agar Wi-Fi ini dapat digunakan maka sebuah Wi-Fi harus memiliki *access point* atau *router* yang menghubungkan antara perangkat dengan *internet*. *Router* akan menerima dan mengirimkan koneksi *internet* yang diberikan oleh *provider internet* ke semua ataupun sejumlah perangkat melalui sinyal gelombang[10].

Ada dua hal yang menjadi komponen penting pada Wi-Fi diantaranya ialah :

a. SSID

SSID (*Service Set Identifier*) biasa diartikan sebagai nama dari sebuah komputer yang memiliki *card USB* atau perangkat *wireless* dan yang mana setiap perangkat harus memiliki sebuah nama yang digunakan sebagai identitas. *Service set Identifier* (SSID) juga sering disebut sebagai serangkaian karakter atau nama yang digunakan untuk mendefinisikan suatu domain roaming dalam suatu *access point* (AP) dalam sebuah jaringan nirkabel yang terdiri dari beberapa *Access Point* (AP).

Pada awalnya SSID ini digunakan sebagai sebuah kata

sandi untuk masuk ke dalam sebuah jaringan nirkabel, tanpa mengetahui SSID *client* tidak akan bisa tergabung ke jaringan. Namun ada banyak sekali program-program atau aplikasi yang bisa digunakan untuk melacak SSID tersebut. Jadi kalau kita menggunakan SSID ini sebagai kata sandi maka sama saja tidak berguna[11]. Singkatnya, SSID ini adalah nama dari sebuah *router* atau *access point* sebagai pembeda antara *access point* satu dengan yang lain.

b. Enkripsi

Secara sederhana enkripsi pada Wi-Fi ini bisa disebut sebagai kode rahasia dari sebuah Wi-Fi. Enkripsi ini berguna untuk mengamankan suatu data berupa kode yang sifatnya rahasia supaya orang lain tidak dapat mengetahuinya, yang mana enkripsi pada Wi-Fi ini memiliki berbagai macam jenis dan tingkatan Berikut ini adalah jenis-jenis enkripsi yang ada pada teknologi Wi-Fi diantaranya :

a. Terbuka (*Open*)

Jaringan Wi-Fi yang terbuka biasanya tidak memiliki kata sandi dan siapapun bisa mengaksesnya.

b. WEP (*Wired Equivalent Privacy*)

Standar keamanan yang sudah lama dan sangat rentan untuk dirusak. WEP ada dua versi, WEP 64 dan WEP 128. WEP 128 memiliki ukuran kunci enkripsi yang lebih besar daripada WEP 64, meskipun begitu WEP 128 juga masih tergolong rentan untuk dirusak. Adapun panjang karakter dari enkripsi jenis ini adalah 5-13 karakter.

c. WPA-PSK (*Wi-Fi Protected Access-Pre-Shared Key*)

Standar keamanan yang lebih baik setelah WEP yang dipublikasikan pertama kali pada tahun 2003. WPA adalah enkripsi termutakhir dan terbaik diantara semua jenis enkripsi yang ada. Biasanya fitur jenis ini telah digantikan

oleh WPA2 dan tergolong tidak aman. WPA-PSK ini juga terbagi dua versi, TKIP (*Temporal Key Integrity Protocol*) dan AES (*Advanced Encryption System*). TKIP menggunakan versi asli dari protokol WPA, biasanya fitur jenis ini telah digantikan oleh WPA2. AES juga menggunakan versi asli dari protokol WPA namun menggantikan TKIP dengan enkripsi yang lebih modern dan hampir semua AES mendukung keamanan WPA2.

d. WPA2-PSK

Merupakan tingkat keamanan tertinggi dalam enkripsi yang dipublikasikan pada 2004. WPA2 adalah enkripsi terbaru dan hasil pengembangan dari WPA sebelumnya. WPA2 jenis ini juga terbagi kedalam dua versi, TKIP dan AES. TKIP menggunakan enkripsi modern yang lebih tua dari AES yang lebih baik dari kedua versi WPA. AES adalah standar keamanan terbaru pada Wi-Fi dan lebih baik dari semua keamanan sebelumnya dan merupakan pilihan keamanan yang paling aman dan ideal. TKIP/AES merupakan kombinasi antara TKIP dan AES yang menyediakan kompatibilitas maksimum dengan perangkat lawas yang mungkin masih banyak dimiliki oleh orang lain. Hanya saja keamanan jenis ini tidak lebih baik dari WPA2-PSK (AES). Adapun panjang karakter yang terdapat pada WPA dan WPA2 adalah berkisar diantara 8-64 karakter[12].

### 2.1.2 Router

*Router* adalah sebuah alat atau program aplikasi yang bertugas untuk menentukan titik mana suatu paket data harus diteruskan ke jaringan lain, *router* akan memilih rute terdekat untuk meneruskan paket data. *Router* dapat menentukan jaringan mana yang berwenang

untuk menggunakan paket data yang disediakan oleh *router* tersebut. Oleh karena itu *router* dapat dipasang atau disambungkan dengan dua jaringan atau lebih. *Router* biasanya terletak di *gateway* yang terhubung ke jaringan. *Router* memiliki daftar rute dan dapat memilih rute terbaik untuk paket data atau disebut juga sebagai *routing table*[13].

*Router* adalah alat yang digunakan untuk mengirimkan data melalui jaringan atau *internet* menuju tujuannya melewati sebuah proses yang disebut dengan *routing*. *Routing* adalah proses pengiriman paket data melalui jaringan dari satu perangkat ke perangkat lainnya. *Router* secara konstan memindai jaringan untuk melacak penambahan, perubahan, dan penghapusan lalu lintas atau titik akses. *Router* menggunakan informasi ini untuk membuat peta jaringan internal. Sebuah *router* secara berkala bertukar informasi di tabel internalnya dengan *router* lain untuk mendapatkan informasi tentang jaringan lain yang terhubung langsung pada *router*[14].

Berdasarkan mekanismenya, *router* terbagi dua yakni *router* statis dan dinamis. *Router* statis merupakan *router* yang cocok untuk kebutuhan jaringan *internet* dengan skala kecil. Hal ini dikarenakan *router* jenis ini memiliki tabel *routing* yang tetap dan sifatnya manual yang hanya bisa dilakukan oleh admin jaringan. Sedangkan *router* dinamis merupakan versi kebalikan dari *router* statis, yakni dengan *table routing* yang berubah-ubah, serta mempelajari arus terbaik untuk meneruskan paket data secara otomatis sesuai dengan instruksi dari admin jaringannya. Kebanyakan dari *router* ini digunakan pada kebutuhan jaringan *internet* dengan skala yang lebih besar.

Jika dilihat dari bentuknya, *router* ini dibagi menjadi tiga yakni *router software*, *hardware*, dan PC. *Router software* adalah *router* yang dapat diunduh pada perangkat komputer dan digunakan sebagai aplikasi yang penggunaannya bergantung pada perangkat keras yang tersedia. *Router hardware*, adalah *router* yang berbentuk benda atau yang dapat disentuh dengan fisik. *Router* jenis ini adalah *router* yang



paling banyak dan umum digunakan. *Router* PC, hampir mirip dengan *router software* yang bisa diunduh diperangkat komputer. Akan tetapi untuk memakainya *router* ini dapat langsung digunakan menggunakan komputer dengan *processor* minimal intel pentium II.

*Router* berfungsi untuk mengirimkan informasi, menghubungkan jaringan, menyaring paket data, membagikan file, dan menghubungkan jaringan ke jaringan lokal. *Router* bekerja dengan memastikan *internet* atau paket data sampai pada semua *client* yang terhubung secara efektif dengan bantuan *table routing* untuk menganalisis dan mengirimkan paket data. Sebelum menentukan arus pengiriman paket data, *router* akan terlebih dahulu membaca *header* dari paket tersebut. Cara kerja *router* ini meliputi analisis arus yang cepat dan efisien untuk menjangkau alamat IP tujuan. Kemudian *router* mengirimkan paket jaringan pada arus yang sudah ditentukan melalui *table routing* sebelumnya.

Setiap paket data yang dikirim oleh *router* berisi beberapa bagian, termasuk informasi seperti tipe data, informasi pengirim, dan alamat IP tujuan. Informasi ini dikirim melalui beberapa jaringan bersama dengan bagian lain dari *router* hingga mencapai komputer atau jaringan tujuan[15].

Dalam melakukan konfigurasi *router* ini ada dua hal yang perlu untuk diperhatikan yakni :

- IP Address

IP Address adalah singkatan dari *Internet Protokol Address*, merupakan identitas sebuah perangkat yang terhubung pada sebuah jaringan *internet*[16].

IP Address tersusun atas sederet atau serangkaian angka yang dipisah dengan tanda titik. IP Address berfungsi untuk memastikan agar data yang dikirim sampai pada penerima yang tepat[17].

- *Gateway*

*Gateway* merupakan sebuah teknologi yang memungkinkan perangkat satu terhubung dengan perangkat lainnya. Penggunaan *gateway* ini disebabkan oleh *protocol* yang digunakan oleh tiap-tiap perangkat berbeda, sehingga untuk menghubungkan perangkat-perangkat maka digunakanlah *gateway* sebagai penghubungnya[18].

Istilah *gateway* merujuk pada perangkat keras atau perangkat lunak yang menjadi jembatan dua jaringan atau aplikasi yang tidak sama. Pengertian lain yang bisa dipakai untuk mendefinisikan *gateway* ini ialah, sebuah mekanisme yang menyediakan akses ke sebuah sistem lain yang terhubung pada sebuah jaringan[19].

### 2.1.3 *Smartphone*

*Smartphone* atau ponsel cerdas merupakan kombinasi antara PDA ( *Personal Digital Assistant*) dan *Mobile Phone* (Ponsel). PDA ( *Personal Digital Assistant* ) merupakan sebuah telepon mini yang mampu mengkombinasikan fitur fungsi dari komputer, telepon, faximile, *internet* dan jaringan. *Mobile Phone* atau yang sering juga dikenal dengan sebutan ponsel merupakan sebuah alat komunikasi yang terkoneksi dengan jaringan komunikasi melalui gelombang radio dan transmisi satelit.

Seperti yang sudah disebutkan, *smartphone* merupakan gabungan dari PDA dan *mobile phone*, namun lebih fokus pada bagian mobile-nya. *Smartphone* ini memadukan fungsi ponsel dengan fungsi komputer. *Smartphone* dapat menyimpan data, mengirim *email* dan menginstal aplikasi, Sebagian besar perangkat *mobile* yang melebihi kemampuan ponsel dapat dikategorikan sebagai *smartphone*. Sebenarnya tidak ada definisi standar mengenai *smartphone* ini Umumnya suatu ponsel dikatakan sebagai *smartphone* bila dapat

berjalan pada perangkat lunak *operating system* atau sistem operasi yang lengkap[20]

#### **2.1.4 Fluxion Portable**

*Fluxion* merupakan alat yang dapat digunakan untuk melakukan peretasan terhadap Wi-Fi dengan semua keamanan termasuk WPA/WPA2. *Fluxion* menggunakan teknik *Man In The Middle Attack*. *Fluxion* ini merupakan cikal bakal masa depan peretasan Wi-Fi dengan menggabungkan teknik rekayasa dan sosial yang mengharuskan pengguna memasukkan *password* Wi-Fi yang benar pada sebuah *form* yang dikirimkan oleh penyerang agar Wi-Fi yang sebelumnya digunakan dapat digunakan kembali[21].

*Fluxion* adalah audit keamanan dan sebuah alat penelitian rekayasa sosial. *Fluxion* awalnya hanyalah sebuah program dan hanya orang-orang tertentu saja yang bisa menggunakannya, tapi kini *fluxion* sudah disandingkan dengan perangkat keras yang lebih praktis dan mudah untuk digunakan. Adapun cara kerja *fluxion* ini adalah sebagai berikut :

- Memindai jaringan nirkabel target
- Memunculkan gangguan komunikasi dan memutuskan semua *client* yang terhubung pada *Access Point*.
- Memunculkan *Access Point* palsu dengan meniru yang asli
- Memunculkan halaman web yang meminta *client* untuk memasukkan ulang kata sandi
- Semua yang diinput *client* pada halaman web sebelumnya akan disimpan di server[8].

#### **2.1.5 Keamanan Jaringan**

Keamanan jaringan adalah perlindungan sumber daya dari orang yang tidak berwenang untuk mengubah dan menghancurkannya. Beberapa ahli jaringan mengatakan bahwa hanya ada satu cara yang sederhana dan efektif untuk membuat sistem jaringan yang aman, yaitu

dengan menggunakan pemisah sekitar satu inci antara perangkat dengan jaringan. Dengan kata lain, hanya perangkat yang tidak terhubung ke jaringanlah yang mendapat perlindungan penuh. .

Untuk menjamin keamanan dan kerahasiaan data, diperlukan enkripsi sehingga informasi tersebut hanya dapat dibaca atau dipahami oleh penerima yang sah. Selain untuk melindungi data, hal ini bertujuan untuk meningkatkan keamanan data, melindungi data agar tidak dapat dibaca oleh orang yang tidak berhak, dan mencegah orang yang tidak berwenang untuk menambah, memodifikasi atau menghapus data[22].

Pada jaringan Wi-Fi terdapat banyak sekali jenis enkripsi seperti yang telah disebutkan diatas. Meski demikian tetap saja data yang dienkripsi tersebut dapat bocor dan bisa diakses oleh pihak-pihak tertentu. Adapun beberapa metode yang umum dan sering digunakan dalam melakukan serangan kewan untuk mendapatkan data yang dienkripsi diantaranya adalah sebagai berikut :

a. *Sniffing*

*Sniffing* adalah aktivitas memantau dan menangkap data yang dikirim menggunakan jaringan *internet*. Teknik *sniffing* ini biasanya dilakukan oleh pihak-pihak yang tidak bertanggung jawab untuk mencuri informasi penting saat adanya komunikasi data pada jaringan *internet*[23].

b. *Interruption (NetCut)*

*Interruption* adalah metode serangan yang banyak dijumpai pada kasus-kasus keamanan jaringan yang mengganggu ketersediaan data dan informasi pada sistem komputer dengan cara dirusak, dibuang, dan membuatnya menjadi tidak berguna. *Interruption* ini dapat merusak perangkat lunak, data dan juga jalur komunikasi yang terdapat didalam suatu sistem yang terhubung pada jaringan. Seperti yang dijelaskan diatas, serangan pada perangkat lunak dapat dilakukan dengan cara dihapus maupun dirusak. Sedangkan pada jalur komunikasi dapat diputus dan

dirusak serta pemotongan jalur komunikasi dengan menggunakan aplikasi *NetCut*.

Sekilas mengenai *NetCut*, yaitu salah satu aplikasi jenis *interruption* yang belakangan ini banyak digunakan oleh pelaku penyerangan pada jaringan komputer. *NetCut* adalah aplikasi yang berfungsi untuk memblokir akses jaringan *internet* sehingga *client* tidak bisa menggunakan fasilitas *internet* tersebut[24].

c. *Brute Force*

*Brute force* adalah pendekatan langsung untuk memecahkan masalah, biasanya berdasarkan fakta masalah dan definisi konsep. *Brute force* memecahkan masalah dengan cara yang sangat sederhana, langsung dan sangat jelas. Sebagai permulaan, *brute force* akan mencocokkan serangkaian karakter pada awal teks, kemudian bergerak ke kiri dan kanan dengan membandingkan setiap karakter yang ada didalam string dengan karakter yang bersesuaian didalam teks. Jika perbandingan tersebut sesuai maka akan mengeluarkan hasil. Akan tetapi jika *string* belum ditemukan kecocokan sementara teks belum habis maka akan geser *string* satu karakter ke kanan dan mengulangi lagi perintah yang sama seperti sebelumnya[25].

d. *Social Engineering*

Merupakan sebuah teknik mencuri atau mengambil data maupun informasi penting dan rahasia dari seseorang dengan cara melakukan pendekatan manusiawi melalui interaksi sosial. Pelaku *social engineering* memanfaatkan sifat alamiah manusia dengan cara memuji, ramah, dan melakukan sesuatu hal secara lebih agar dapat lebih dekat dengan target sehingga target tidak menyadari tabiat buruk dari pelaku. Dengan begitu target juga tidak merasa curiga dan memberikan informasi rahasianya pada pelaku[26].

e. *Man In The Middle Attack (MITM Attack)*

*Man In The Middle Attack* merupakan serangan yang memanfaatkan celah pada jaringan untuk melihat, mengambil maupun mencuri data yang terdapat pada jalur komunikasi[27]. MITM atau *Man In The Middle Attack* dilakukan dengan cara menyusup ke dalam jaringan kemudian menyadap komunikasi yang sedang terjadi antara pengguna dengan pengguna yang lain maupun pengguna dengan *server* tujuan. MITM melakukan penyamaran sebagai jaringan asli kemudian membuat korban seolah-olah berada pada jaringan yang benar sehingga korban tidak menyadari bahwa mereka berada pada jaringan yang salah[28].

f. *Evil Twin*

*Evil Twin* adalah serangan yang menggunakan *teknik man-in-the-middle* (MITM). Dengan menggunakan teknik ini, penyerang dapat mengarahkan korban ke halaman *login* palsu dengan SSID duplikat. *Evil twin* adalah serangan yang dapat menyamar sebagai titik akses dan juga sebagai perangkat yang mampu memalsukan SSID, alamat MAC, dan lalu lintas dari titik akses asli[29].

Adapun cara mengamankan Wi-Fi yang bisa dilakukan untuk meminimalisir terjadinya pembobolan sandi dan perubahan konfigurasi oleh pihak yang tidak berizin yakni dengan cara :

- Menggunakan enkripsi terbaru.
- Menggunakan *password* atau kata sandi yang kuat dengan menggabungkan antara huruf besar dan kecil dengan karakter lain dan angka.
- Mengganti nama SSID standar dengan yang baru.
- Mengaktifkan *MAC Filtering*[30].

## BAB III METODOLOGI PENELITIAN

### 3.1 Peralatan Penelitian

#### 3.1.1 Perangkat Penelitian

Dalam penelitian ini, guna mendukung kelancaran dan kesuksesan penelitian, penulis menggunakan beberapa alat dalam upaya menganalisa bagaimana cara kerja dari *fluxion portable* ini dalam menguji Wi-Fi dengan keamanan WPA/WPA2. Adapun peralatan yang penulis gunakan pada penelitian ini berupa perangkat keras (*hardware*) dan perangkat lunak (*software*).

##### 1. Perangkat Keras (*Hardware*)

Adapun perangkat keras yang digunakan pada penelitian ini adalah sebagai berikut :

Tabel 3.1 Perangkat Keras

No	Nama	Spesifikasi	Jumlah	Fungsi
1	<i>Smartphone</i>	Android	2	Sebagai media untuk mengatur <i>fluxion</i> , mendeteksi, dan melakukan penyerangan pada Wi-Fi dengan keamanan WPA/WPA2.
2	<i>Router</i>	ZTE-F609	1	Sebagai pemancar sinyal Wi-Fi
3	<i>Fluxion</i>	<i>Fluxion Portable</i>	1	Sebagai media penangkap, pemutus, dan

				pengambil <i>password</i> Wi-Fi.
4	USB	<i>Micro</i> USB		Sumber daya listrik untuk <i>Fluxion portable</i>

## 2. Perangkat Lunak (*Software*)

Adapun perangkat lunak yang digunakan pada penelitian ini adalah sebagai berikut :

Tabel 3.2 Perangkat Lunak

No	Nama	Spesifikasi	Fungsi
1	<i>Browser</i>	Chrome	Sebagai tempat pengujian dan juga melakukan <i>setting router ZTE-F609</i> .

### 3.1.2 Metode Penelitian

Dalam penelitian ini penulis menggunakan metode Tindakan ( *Action Research* ). Metode tindakan merupakan sebuah metode penelitian yang penelitinya ikut serta menjadi subjek dari penelitian tersebut. Adapun tahapan-tahapan yang ada pada metode tindakan ini diantara lain :

a. *Diagnosing*

Melakukan diagnosa pada sistem jaringan Wi-Fi

b. *Action Planning*

Melakukan perencanaan yang akan dilakukan dengan membuat perancangan dan pengujian pada sistem jaringan Wi-Fi

c. *Action Taking*

Mengimplementasikan perencanaan yang telah dibuat sebelumnya, dan mencari kelemahan pada sistem jaringan Wi-Fi



d. *Evaluating*

Melakukan evaluasi terhadap hasil analisis dari *fluxion portable* yang digunakan untuk menemukan *password* Wi-Fi yang terpasang keamanan WPA/WPA2[31].

### 3.1.3 Gambaran Umum Penelitian

Berikut ini ilustrasi skema jaringan sederhana untuk implementasi uji Wi-Fi dengan keamanan WPA/WPA2 pada perangkat *router wireless* ZTE-F609 menggunakan *fluxion portable*. Dalam ilustrasi ini, ada sebuah warung yang menyediakan Wi-Fi gratis, dalam warung ini memiliki sebuah *access point* atau *router* yang bertugas menyebarkan jaringan internet dan menampung *client*.

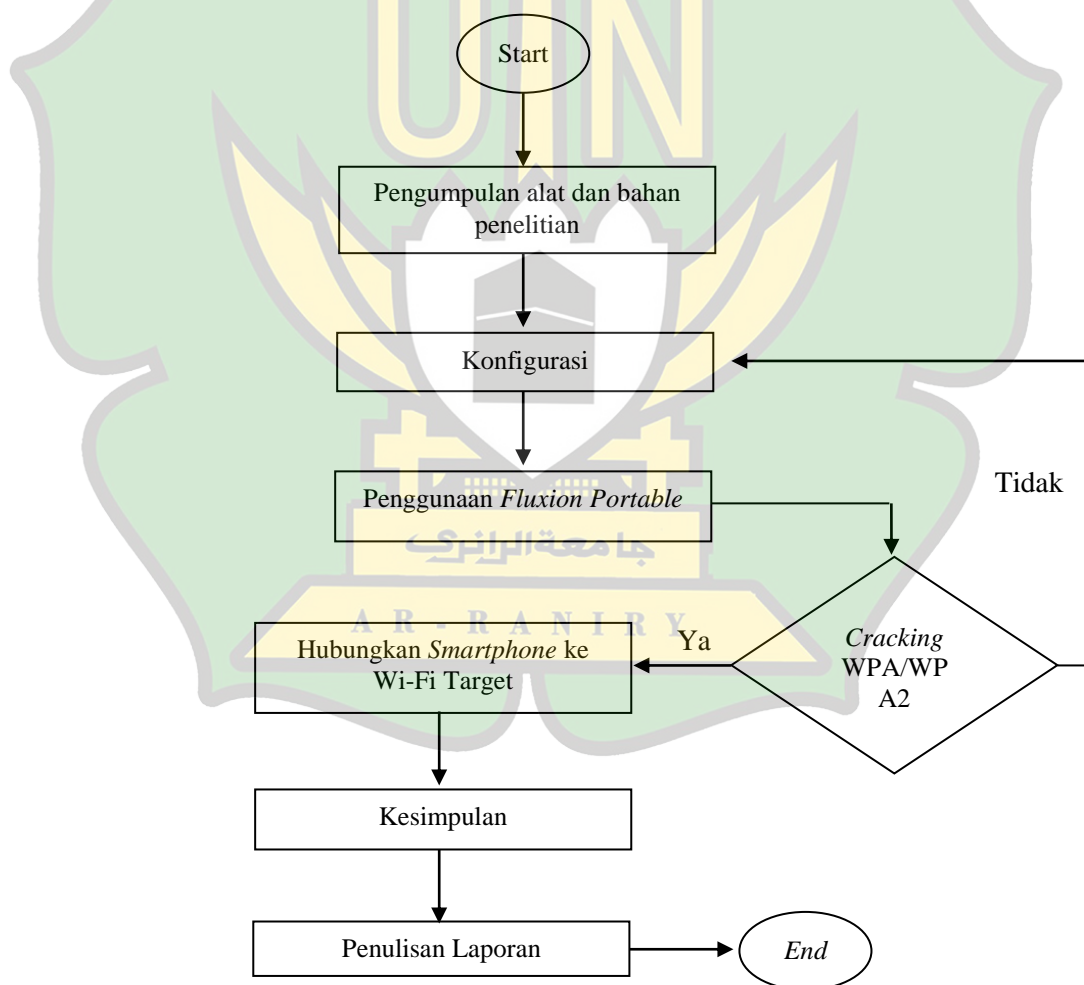
Kemudian datanglah satu pelanggan lain dan mencoba alat yang bernama *fluxion portable*, yang mana alat itu diuji cobakan di sudut warung tersebut. Setelah alat ini dihidupkan dengan menghubungkannya pada daya listrik, maka akan muncul SSID dan pelanggan tersebut menghubungkan perangkatnya pada SSID itu. Kemudian pelanggan itu melakukan penyettingan melalui google chrome yang ada pada ponselnya, dan memilih Wi-Fi dengan keamanan WPA/WPA2.

Selanjutnya, beberapa saat kemudian semua pelanggan lain yang menggunakan Wi-Fi yang sudah dipilih dan menjadi target dari pelanggan baru ini akan terputus. Kemudian saat itu juga SSID Wi-Fi pun sudah menjadi ganda, yang mana salah satu diantaranya adalah palsu. Dan setiap pelanggan akan menghubungkan kembali perangkat mereka dan beberapa diantaranya menghubungkan perangkat mereka pada SSID dan otomatis untuk memasukkan ulang kata sandi. Setelah memasukkan ulang kata sandi, maka otomatis kata sandi yang dimasukkan akan masuk dan tersimpan di *fluxion portable*. Adapun yang harus diperhatikan adalah sebagai berikut :

- Banyaknya SSID yang terlihat pada perangkat
- Metode *login* pada Wi-Fi yang sedikit berbeda

### 3.1.4 Alur Penelitian

Sebagaimana yang telah dijelaskan diatas, dengan rumusan masalah yang telah ditentukan dan juga penelitian terdahulu yang diambil dan dirangkum yang dimasukkan kedalam landasan teori dan tinjauan pustaka, maka penelitian ini pun dimulai. Kemudian dilakukan pengumpulan alat dan bahan yang digunakan dalam penelitian dan dilanjutkan dengan melakukan konfigurasi pada alat dan bahan tersebut. Berikutnya penggunaan *fluxion portable* dengan kemampuan *crackingnya* yang dilengkapi dengan dokumentasi dalam setiap kegiatan dari awal hingga akhir. Kemudian penarikan kesimpulan dan penulisan laporan. Untuk lebih jelasnya lihat gambar dibawah ini :

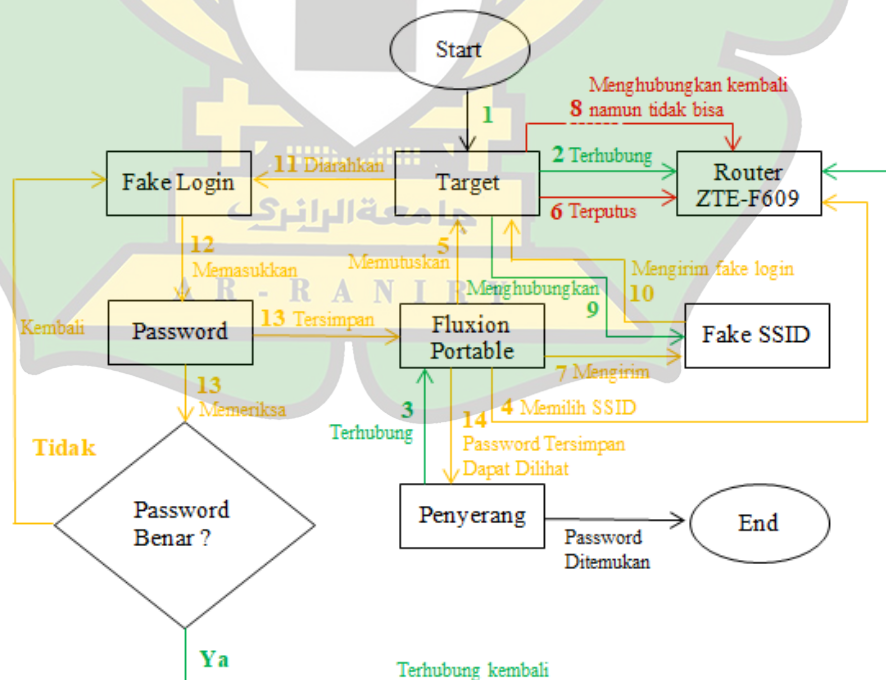


Gambar 3.1 Alur Penelitian

### 3.1.5 Flowchart Penelitian

Dalam menguji Wi-Fi dengan keamanan WPA/WPA2 menggunakan *fluxion portable* dimulai dengan menghubungkan *fluxion portable* dengan daya listrik kemudian penyediaan *smartphone* sebagai tempat konfigurasi dari *fluxion portable*. Kemudian hubungkan *smartphone* dengan *fluxion portable* melalui SSID milik *fluxion*.

Pertama buka chrome pada *smartphone* lalu masukkan *ip address* dari *fluxion portable* tersebut pada kolom pencarian kemudian cari. Selanjutnya akan muncul *interface* dari *fluxion portable*, untuk melihat *Access Point* yang aktif tekan menu *scan*, berikutnya untuk memutus semua *client* dari jaringan Wi-Fi maka pilih dulu *Access point* yang akan menjadi target dengan menekan pada nama SSIDnya lalu tekan *start deauth*, dan supaya *client* yang terputus dengan jaringan diminta untuk *login* ulang maka tekan *start evil twin*. Jika *client* melakukan *login* ulang dan menyetikkan kembali *passwordnya* maka akan muncul informasi yang berisikan nama SSID dan *password* yang sudah dimasukkan oleh *client*. Untuk lebih jelasnya lihat *flowchart* dibawah ini :

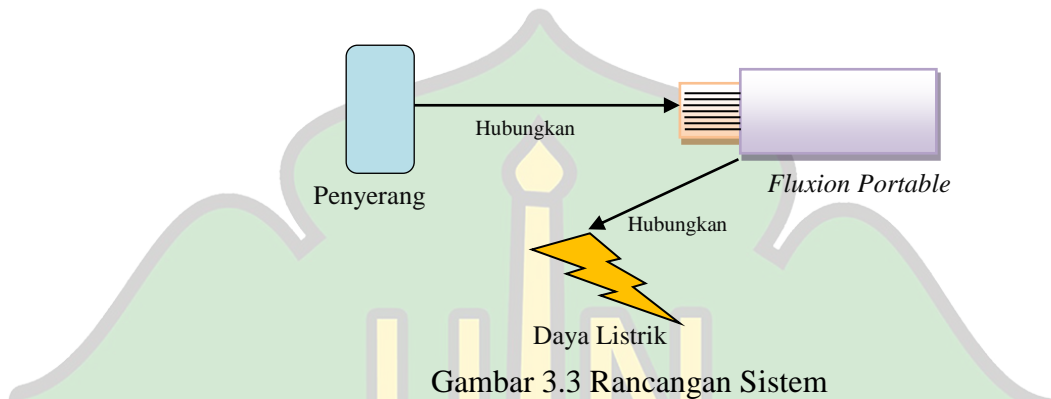


Gambar 3.2 Flowchart Penelitian

### 3.1.6 Rancangan Sistem Penelitian

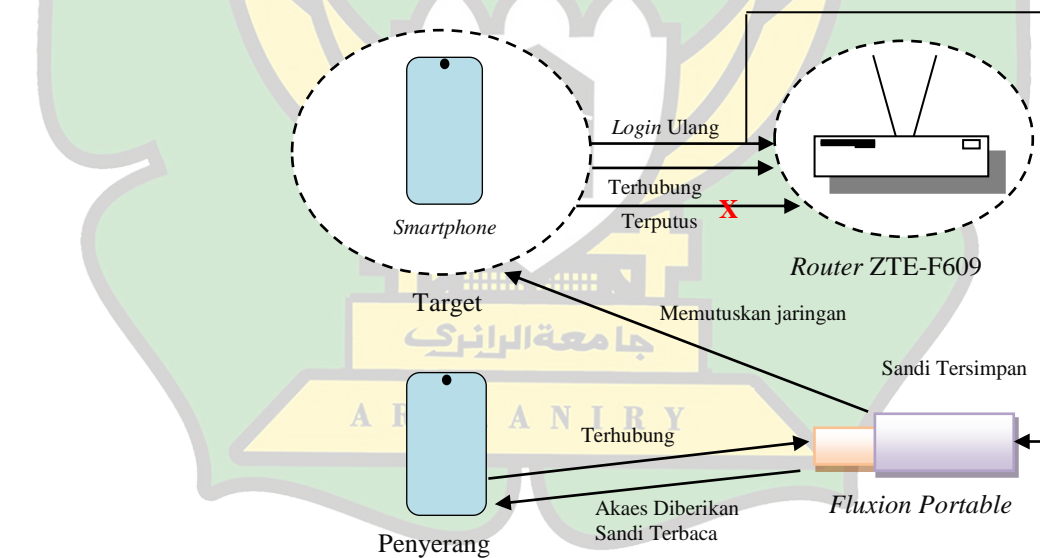
Untuk kelancaran penelitian, maka sangat diperlukan rancangan penelitian yang matang yang mana bertujuan untuk memudahkan dan mengatur alur dalam sebuah penelitian. Berikut ini adalah rancangan sistem penelitian yang digunakan :

- Setting perangkat dengan *fluxion*



Gambar 3.3 Rancangan Sistem

- Penyerangan pada Wi-Fi dengan keamanan WPA/WPA2



Gambar 3.4 Penyerangan Wi-Fi

## BAB IV HASIL DAN PEMBAHASAN

### 4.1 Konfigurasi *Router* ZTE-F609

Berikut ini adalah tahapan-tahapan yang harus diperhatikan sebelum melakukan konfigurasi pada *router* ZTE-F609.

1. Pastikan *router* ZTE-F609 dalam keadaan sudah hidup

Andaikan *router* ZTE-F609 belum hidup silahkan untuk menghidupkannya terlebih dahulu dengan cara menghubungkan *router* dengan kabel *adaptor*.



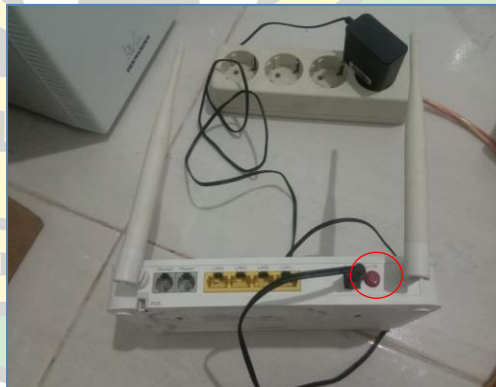
A R - Gambar 4.1 Menghubungkan  
*router* dengan *adaptor*

Kemudian langkah selanjutnya adalah menghubungkan kabel *adaptor* pada sumber daya listrik.



Gambar 4.2 Menghubungkan *adaptor* pada sumber listrik

Selanjutnya tekan tombol *power* untuk menghidupkan *routernya*. Biasanya tombol *power* dari ZTE-F609 terletak disamping *port* kabel *adaptor*.



Gambar 4.3 Tombol *power* untuk menghidupkan *router*

Setelah menekan tombol power maka lampu indikator pada router ZTE-F609 akan menyala dan router siap untuk digunakan.



Gambar 4.4 Router telah menyala

## 2. *Reset router ZTE-F609*

Agar memudahkan dalam konfigurasi peneliti melakukan *reset* pada *router* terlebih dahulu. *Reset* disini maksudnya mengembalikan *router* ini pada pengaturan awal. Tombol *reset* pada *router* ZTE-F609 ini terdapat pada sisi sebelah kanan *router*. Untuk mereset *router* bisa dilakukan dengan cara menekan tombol *reset* kira-kira 5-10 detik menggunakan jarum, atau tusuk gigi dan semacamnya.



Gambar 4.5 Reset router

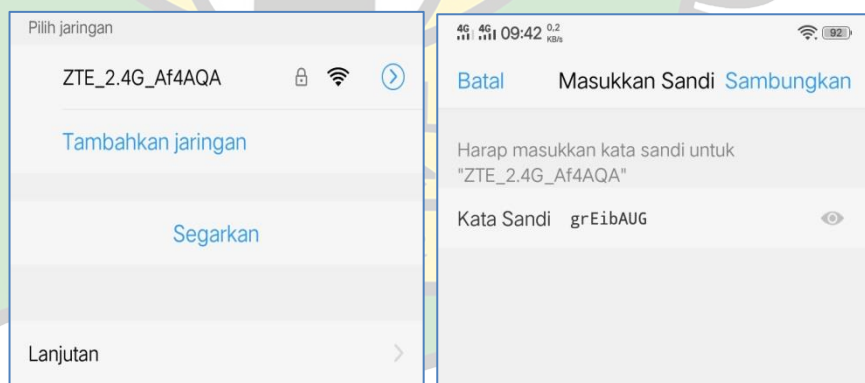
## 3. Menghubungkan *smartphone* pada SSID milik *router* ZTE-F609

Langkah pertama yang dilakukan adalah dengan menghidupkan Wi-Fi pada perangkat *smartphone*.



Gambar 4.6 Menghidupkan Wi-Fi pada *smartphone*

Selanjutnya pilih SSID milik *router* ZTE-F609 yang secara *default* diberi nama ZTE\_2.4G\_Af4AQA, lalu untuk kata sandi *defaultnya* adalah grEibAUG.



Gambar 4.7 Menghubungkan *smartphone* ke Wi-Fi

Jalan pintas untuk mengetahui SSID dan kata sandi *default* dari Wi-Fi ZTE-F609 ini bisa diketahui dengan melihat ke sisi belakang mesin *router* ZTE-F609.





Gambar 4.8 SSID dan *password* default ZTE-F609

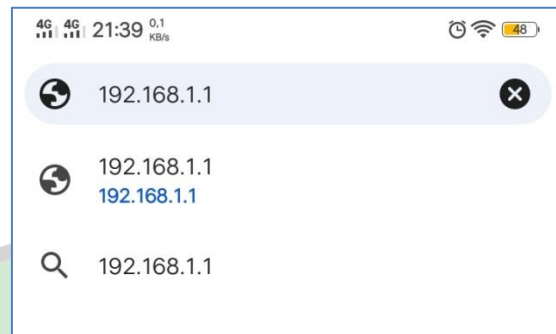
4. Melakukan konfigurasi pada *router* ZTE-F609

Untuk melakukan konfigurasi pada *router* ZTE-F609 ini caranya cukup mudah. Langkah pertama yang dilakukan adalah membuka *browser* chrome yang ada pada *smartphone*.



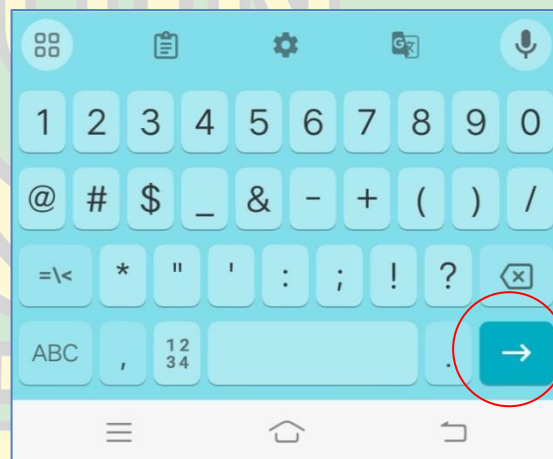
Gambar 4.9 Membuka *browser* Chrome

Selanjutnya pada kolom pencarian atau telusuri ketikkan alamat *ip address* dari *router ZTE-F609*, secara *default ip address* dari ZTE-F609 ini adalah 192.168.1.1.



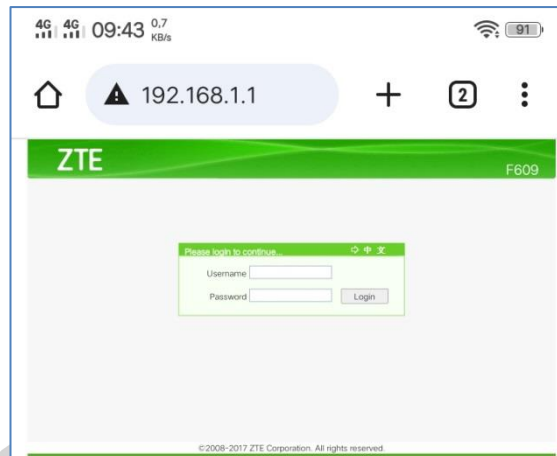
Gambar 4.10 *Default IP address*

Kemudian tekan *enter* atau tombol panah yang mengarah ke kanan pada *keyboard smartphone*.



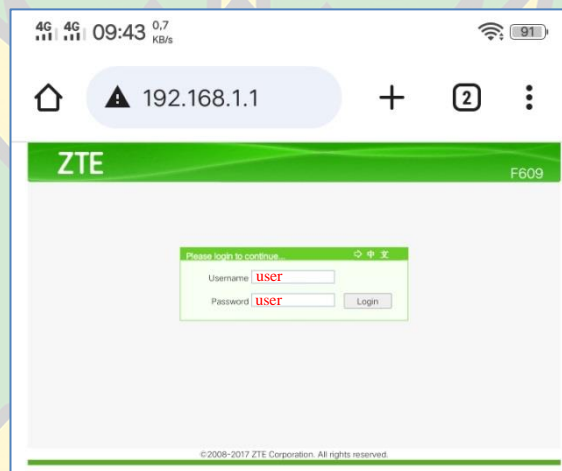
Gambar 4.11 *Enter / Tombol panah kanan*

Selanjutnya akan diarahkan ke halaman *login* dari *router ZTE-F609* tersebut. Berikut ini adalah tampilan halaman *login* ZTE-F609.



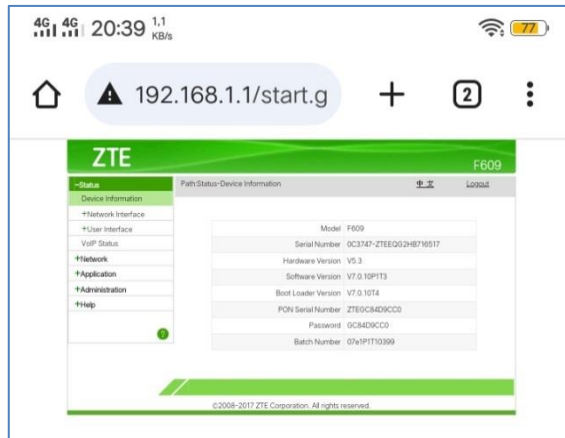
Gambar 4.12 Halaman *login router* ZTE-F609

Selanjutnya masukkan *username* dan *password* untuk *login router* ke ZTE-F609. Biasanya *username defaultnya* adalah *user* dan *password defaultnya* juga *user*. Setelah *username* dan *password* dimasukkan selanjutnya tekan tombol *login*.



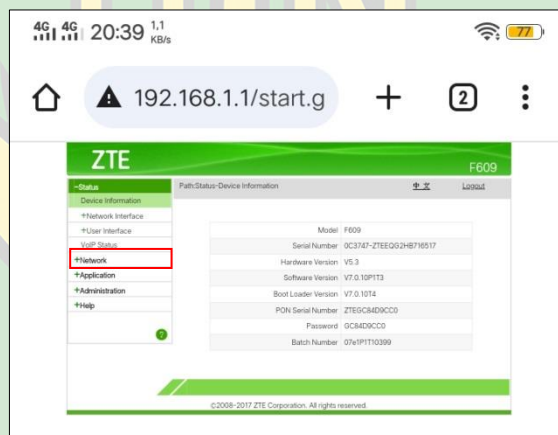
Gambar 4.13 *Username dan password login router*

Setelah berhasil *login*, maka akan dialihkan pada halaman konfigurasi dari *router* ZTE-F609, adapun tampilan awal konfigurasinya ialah seperti berikut :



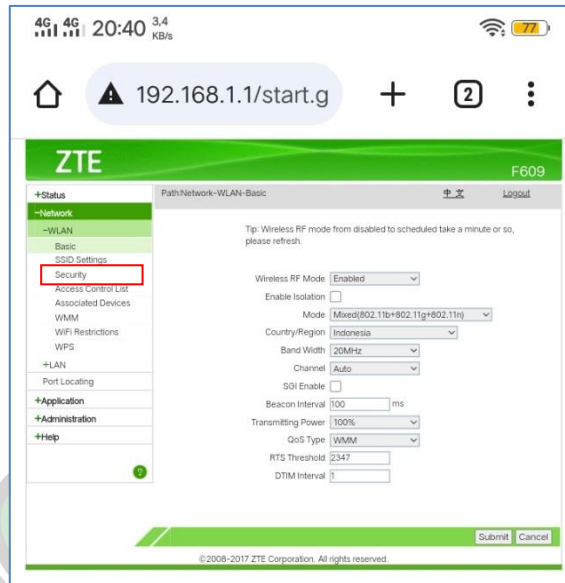
Gambar 4.14 Halaman utama setelah *login* ke *router*

Kemudian untuk melakukan konfigurasi pada *router* ZTE-F609, hal pertama yang harus dilakukan adalah dengan masuk ke menu *network* pada halaman utama *router* ZTE-F609.



Gambar 4.15 Menu *Network*

Setelah halaman *network* terbuka, maka klik atau tekan menu *security* untuk melakukan perubahan *password* pada Wi-Fi yang nantinya akan digunakan.



Gambar 4.16 Menu *security*

Berikutnya, setelah menu *security* ini terbuka maka *password* dari Wi-Fi yang saat ini kita gunakan juga akan terlihat.



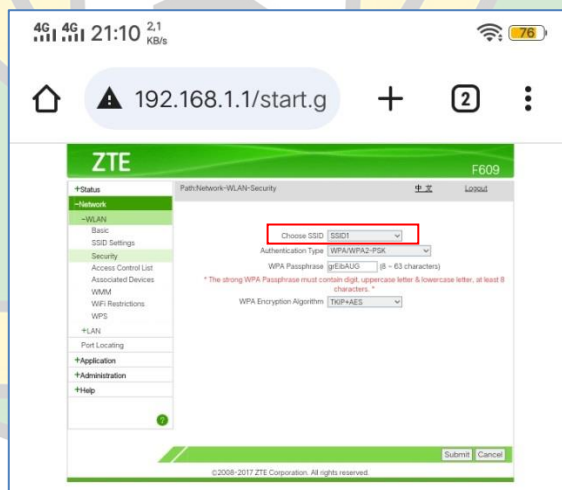
Gambar 4.17 Halaman menu *Security*

Kemudian hal yang harus dilakukan selanjutnya adalah mengubah *password default* Wi-Fi sesuai dengan kehendak sendiri. Untuk mengubah *password* Wi-Finya langsung dengan menekan ke menu *WPA Passphrase* dan ketikkan *password* sesuai dengan keinginan.



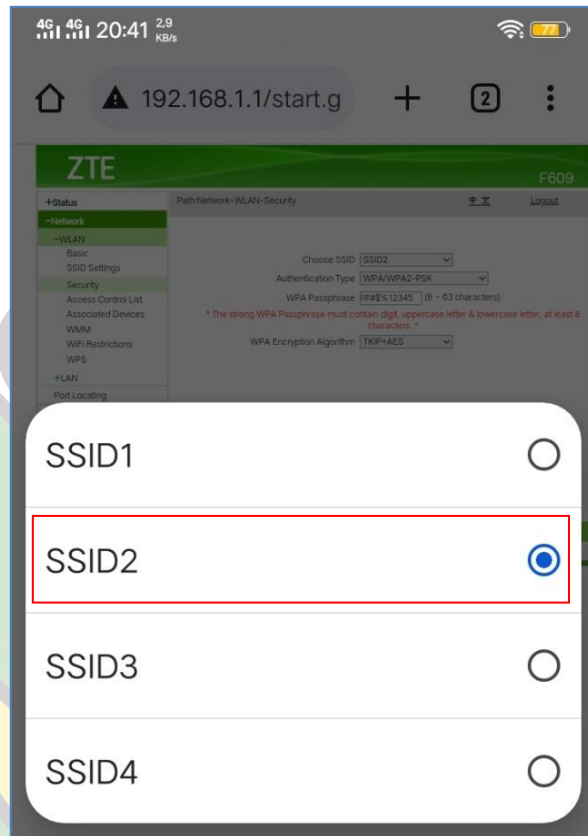
Gambar 4.18 Halaman mengubah *password* Wi-Fi

Pada penelitian ini, peneliti memilih untuk mengaktifkan sebuah SSID baru yakni SSID 2, yang mana pada *router* ZTE-F609 ini, terdapat 4 SSID yang dapat di aktifkan secara bersamaan. Hal ini peneliti lakukan untukantisipasi lupa *password* yang nantinya bisa saja terjadi. Adapun langkahnya yakni dengan menekan menu *Choose SSID*



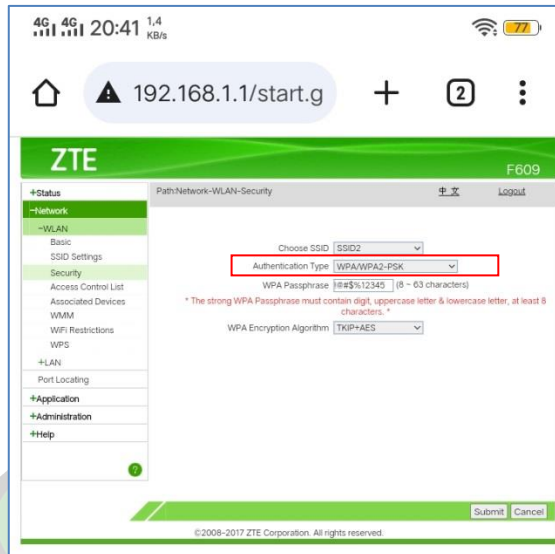
Gambar 4.19 Menu *Choose SSID*

Setelah menekan menu *Choose SSID* maka akan keluar tampilan pilihan SSID1 sampai dengan 4, lalu pilih SSID2.



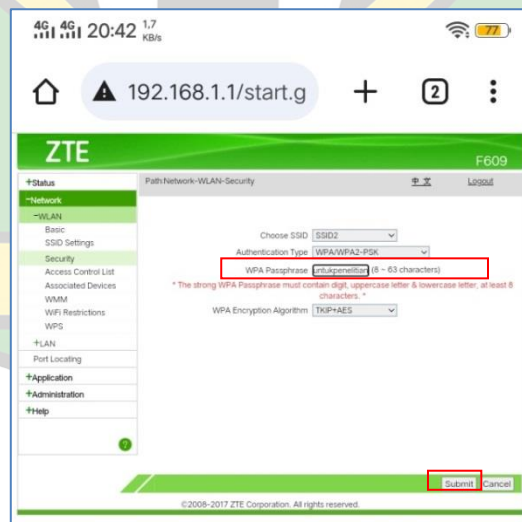
Gambar 4.20 Menu memilih SSID2

Setelah SSID2 dipilih, maka otomatis halaman yang berisikan *password* dari SSID2 akan terbuka dan *password* dapat yang kemudian dapat diubah. Sebelum mengubah *password* pastikan pada menu *authentication type* terpilih WPA/WPA2-PSK agar memenuhi standar dari penelitian ini.



Gambar 4.21 Menu mengubah *Authentication Type*

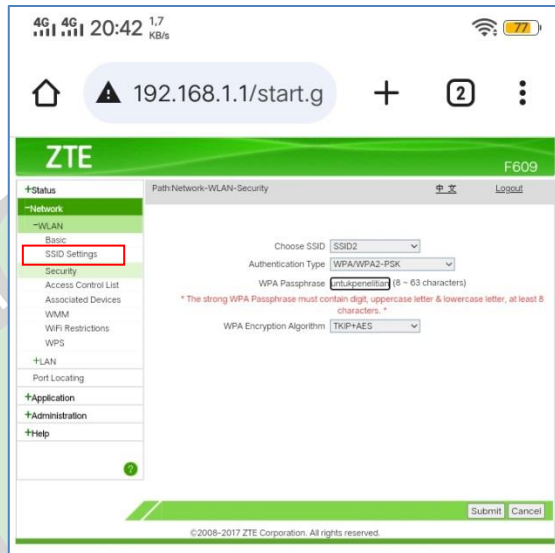
Untuk mengubah *passwordnya* juga sama dengan yang dijelaskan sebelumnya yakni dengan menekan menu *WPA Passphrase* kemudian ketikkan *password* yang diinginkan dan klik tombol *submit* untuk menyimpan perubahan *password* yang dilakukan. Disini peneliti mengubah *passwordnya* menjadi “untukpenelitian”.



Gambar 4.22 Mengubah *password SSID2*

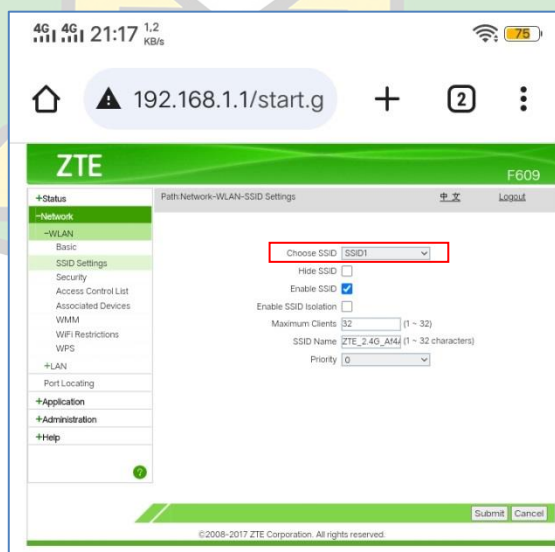


Sampai disini *password* dari SSID2 sudah berhasil diubah. Selanjutnya agar SSID2 ini dapat terlihat pada Wi-Fi di *Smartphone* dan bisa digunakan. Maka SSID2 ini perlu diaktifkan terlebih dahulu. Adapun caranya yakni dengan masuk ke menu *SSID Setting*.



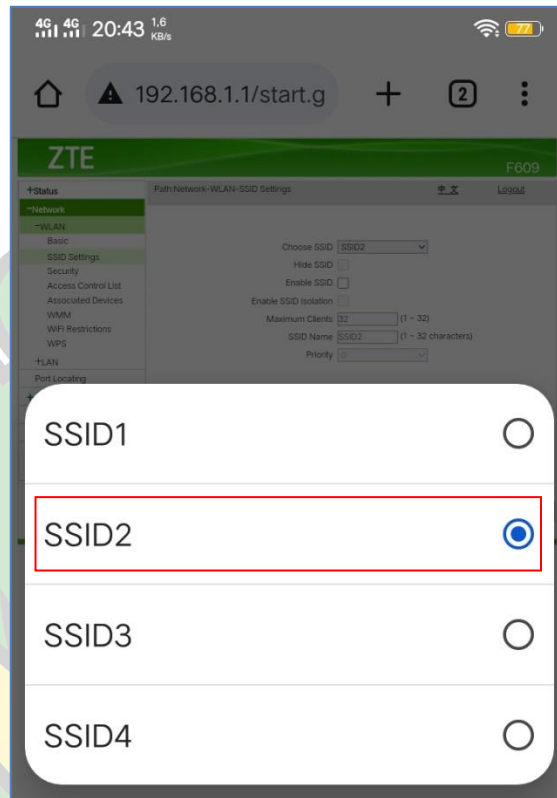
Gambar 4.23 Menu *SSID Setting*

Setelah masuk ke halaman menu *setting*, langkah selanjutnya untuk mengaktifkan SSID2 ini adalah dengan menekan menu *Choose SSID*.



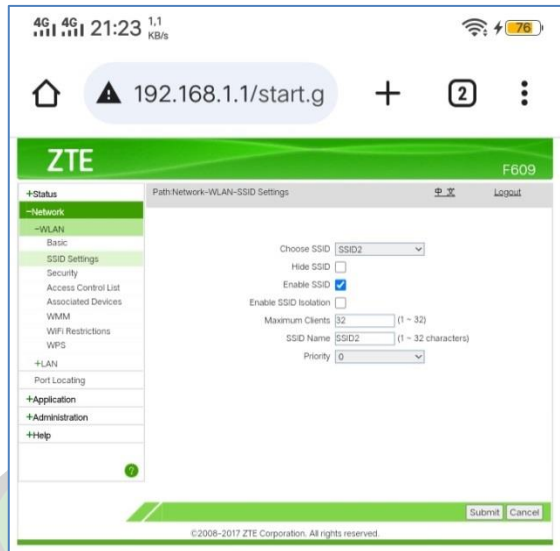
Gambar 4.24 Halaman menu *SSID Setting*

Kemudian, setelah menekan menu *Choose SSID* maka halaman yang berisikan nama SSID1 sampai dengan SSID4 otomatis akan ditampilkan. Setelah daftar nama SSID ini muncul, selanjutnya pilih SSID2.



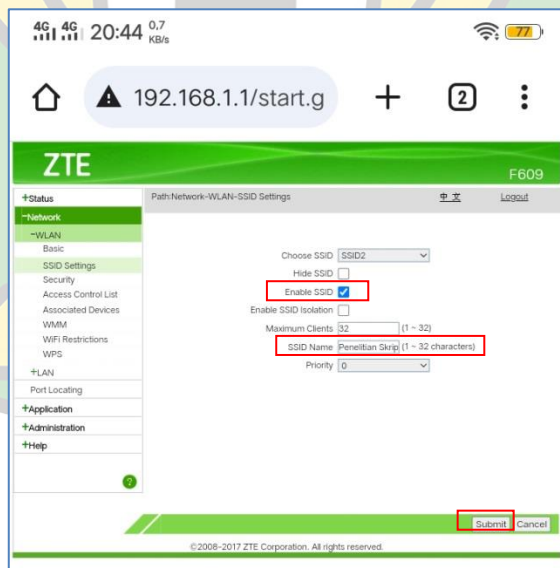
Gambar 4.25 Menu *Choose SSID*

Setelah memilih SSID2, selanjutnya yang harus dilakukan adalah menekan atau memberi tanda centang pada kolom *Enable SSID* supaya SSID2 ini nantinya aktif dan dapat digunakan.



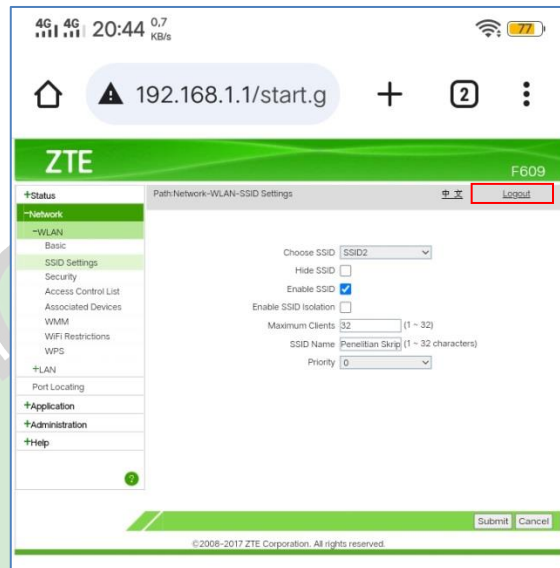
Gambar 4.26 Halaman *enable SSID*

Langkah selanjutnya ubah nama SSID2 ini pada kolom *SSID Name* dengan nama baru sesuai keinginan. Disini peneliti mengubah nama SSID2 menjadi “ Penelitian Skripsi “. Selanjutnya klik *submit* untuk menyimpan nama SSID2 yang sudah diubah.



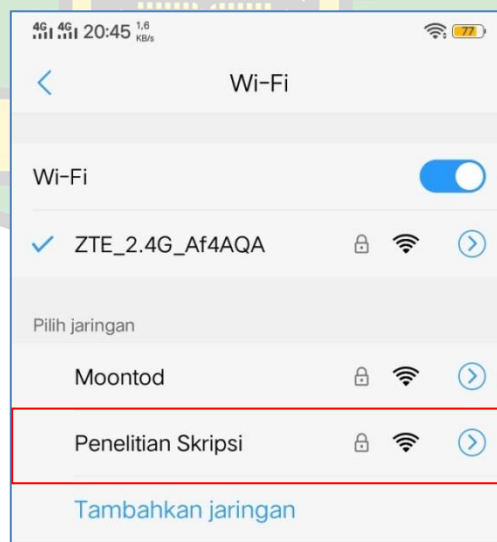
Gambar 4.27 Mengubah nama SSID2

Dan sebagai langkah terakhir setelah berhasil mengubah nama SSID2, yang harus dilakukan selanjutnya adalah keluar dari halaman konfigurasi *router* ZTE-F609 dengan menekan tombol *Logout*.



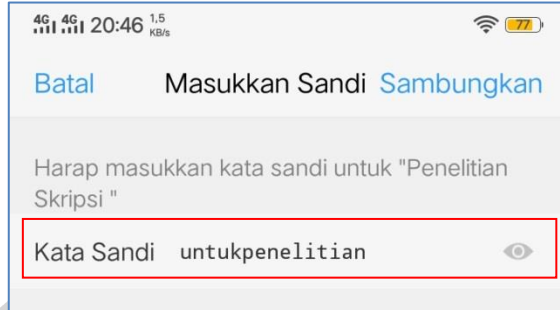
Gambar 4.28 Tombol *Logout*

Sampai tahap ini konfigurasi *router* ZTE-F609 telah selesai dilakukan dan sebuah Wi-Fi baru berhasil dibuat. Untuk memastikan keberhasilan dalam melakukan *setting* ataupun konfigurasi dari ZTE-F609, hidupkan Wi-Fi pada perangkat *smartphone* dan cari nama Wi-Fi yang telah dibuat sebelumnya.



Gambar 4.29 Mencari Wi-Fi yang sudah dibuat

Disini peneliti menghubungkan perangkat *smartphone* pada Wi-Fi yang sudah dibuat sebelumnya dengan nama “Penelitian Skripsi” dan *passwordnya* “untukpenelitian”.



Gambar 4.30 Menghubungkan *smartphone* pada Wi-Fi yang sudah dibuat

Jika Wi-Fi yang dipilih sesuai dengan yang sudah dibuat dan *password* yang dimasukkan juga sudah benar maka *smartphone* akan otomatis terhubung.



Gambar 4.31 Berhasil terhubung pada Wi-Fi yang sudah dibuat

#### 4.2 Hasil Pengujian Wi-Fi Dengan Keamanan WPA/WPA2 Menggunakan *Fluxion Portable*

Penelitian ini membahas tentang pengujian Wi-Fi dengan keamanan WPA/WPA2 menggunakan *fluxion portable* dan juga menggunakan alat-alat pendukung lainnya yakni :

- *Smartphone* 2 buah (1 sebagai target dan untuk melakukan konfigurasi *router*. Kemudian 1 lagi sebagai pelaku yang berusaha mencuri *password* Wi-Fi atau penyerang).
- Sebuah *charger smartphone micro USB* sebagai pemasok daya listrik untuk *fluxion portable*.
- *Fluxion Portable* sebagai alat untuk mencuri *password* Wi-Fi target.

Adapun tahapan pengujian yang dilakukan adalah sebagai berikut :

- 1) Menghubungkan *fluxion portable* pada listrik

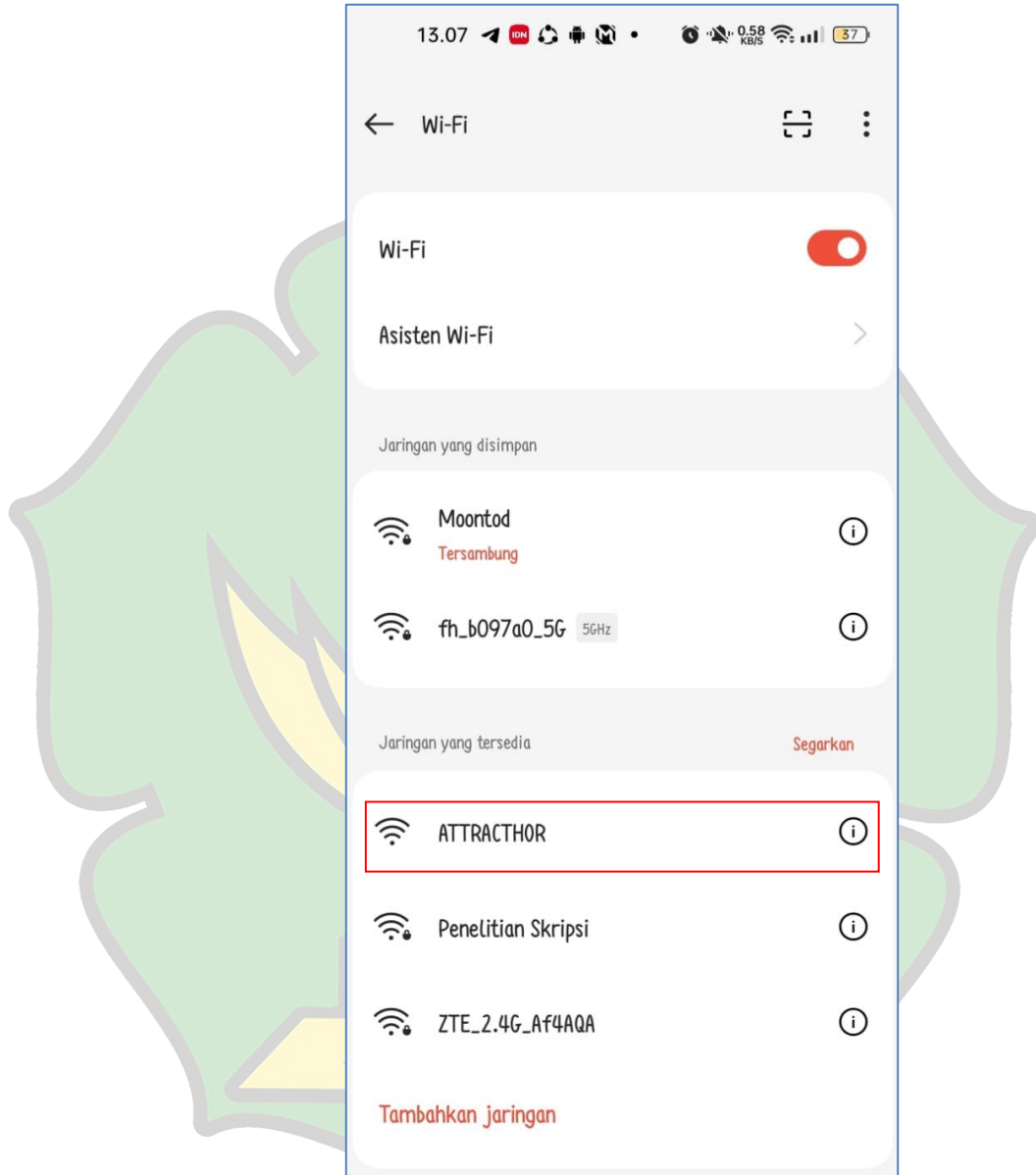
Langkah pertama yang dilakukan adalah mengaktifkan *fluxion portable* dengan menghubungkannya pada listrik menggunakan *charger smartphone micro USB*.



Gambar 4.32 Menghubungkan *fluxion portable* pada listrik

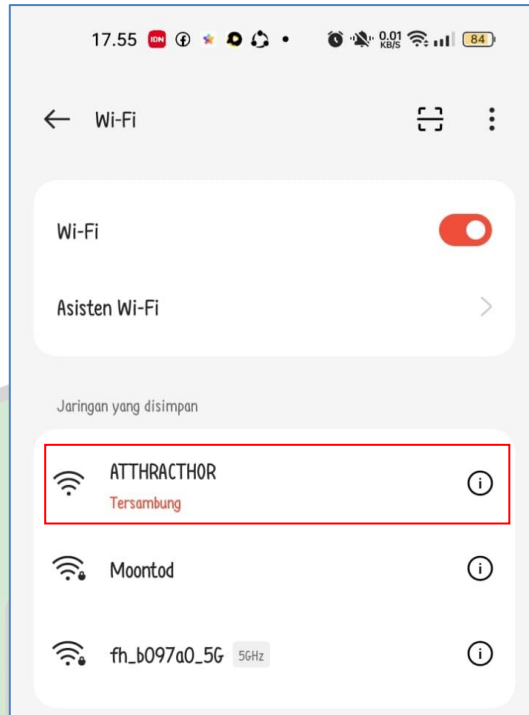
2) Konfigurasi *fluxion portable* dan penyerangan

Setelah *fluxion portable* dihidupkan maka akan memunculkan sebuah Wi-Fi yang bernama “ATTRACTHOR” dan tidak memiliki keamanan apapun.



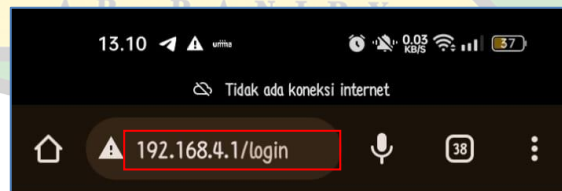
Gambar 4.33 Munculnya Wi-Fi ATTRACTHOR

Selanjutnya hubungkan *smartphone* (penyerang) pada Wi-Fi ATTRACTHOR lalu buka aplikasi chrome sebagai media untuk melakukan konfigurasi *fluxion portable*.



Gambar 4.34 Menghubungkan *smartphone* (penyerang) ke Wi-Fi ATTRACTHOR

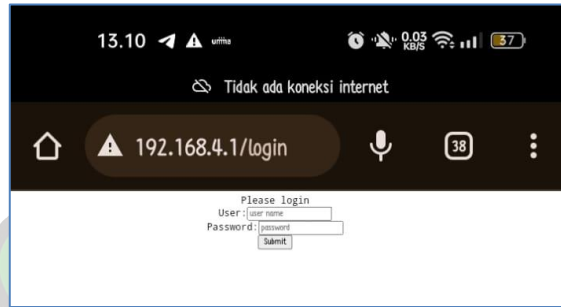
Setelah *smartphone* penyerang terhubung ke Wi-Fi ATTRACTHOR, selanjutnya buka aplikasi chrome di *smartphone* (penyerang) dan ketikkan nomor alamat untuk masuk ke halaman konfigurasi *fluxion portable* yakni 192.168.4.1/setup pada kolom pencarian dan tekan *enter* atau *search* untuk masuk ke halaman konfigurasi.



Gambar 4.35 Alamat halaman untuk konfigurasi *fluxion portable*

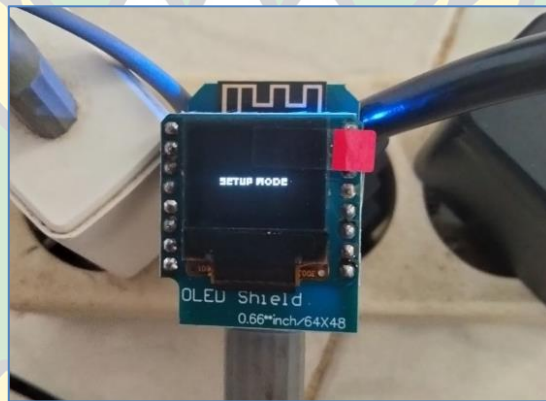


Setelah melakukan pencarian alamat halaman konfigurasi *fluxion portable* melalui chrome maka akan terbuka sebuah halaman yang meminta untuk melakukan *login*. Untuk melakukan *login*, pada *user* ketikkan “razor” dan *password* “admin” kemudian tekan tombol *submit* untuk *login*.



Gambar 4.36 *Login* ke halaman konfigurasi *fluxion portable*

Selanjutnya, setelah berhasil *login* ke halaman konfigurasi *fluxion portable*, maka secara bersamaan pada layar *fluxion portable* akan muncul keterangan “*SETUP MODE*”.



Gambar 4.37 *SETUP MODE* pada layar *fluxion portable*

Sampai tahap ini *fluxion portable* siap untuk dikonfigurasi. Langkah selanjutnya yang harus dilakukan adalah memilih Wi-Fi yang ingin dijadikan korban untuk dicuri *password*nya dengan cara pada sub menu *target* pilih *network* dan tekan *select*.

```
13.13 192.168.4.1/setup
Tidak ada koneksi internet

This is Attractor 083a8dccd962 version 1.9
Evetka Razorhacktheplanet 2022

Device ID...: 083a8dccd962
ChipID.....: 13424994
Free Space..: 2878.66 KB
Version....: [1.9]
Reboot.....: [now]
Reset.....: [now]
JSON Status: [open]
Password...: [admin]
My SSID....: [ATTRACTHOR]

[TARGET]-
-----
Captive.....: [preview] /captive.htm
File Manager: [open]
Network.....: [select]

[OPTIONS]-----
-----
Death Attack...: [no]
Beacon Mist....: [no]
Broadcast.....: [no]
HearbeatBlink..: [no]
InputValidation: [no]
BootValidation.: [no]
AutoReboot.....: [no]

[STATUS]-----
-----
RSSI.....: 0
Channel.....: 0
Data packets...: 0
STA Known.....: 0
DNS Queries....: 0
Clients seen...: 0
Passwords.....: [5/3] [clear all]
```

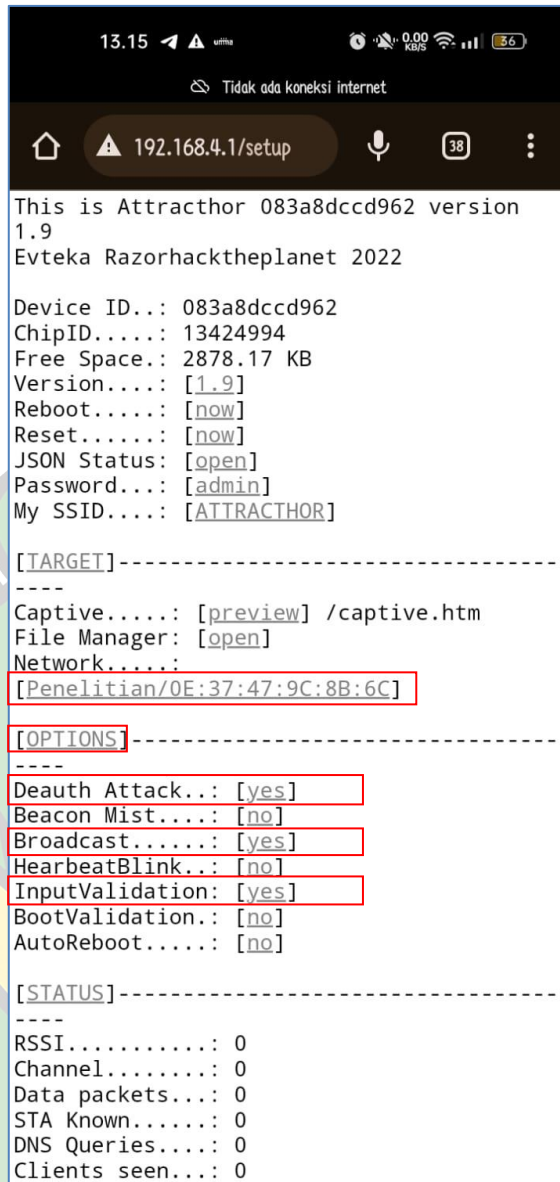
Gambar 4.38 Halaman konfigurasi *fluxion portable*

Setelah menekan tombol *select* maka akan diarahkan pada halaman baru yang berisi daftar Wi-Fi yang ada disekitar area tersebut. Untuk memilih Wi-Fi yang akan dijadikan target, tekan tombol *select* disebelah kiri dari nama Wi-Fi tersebut.

Select SSID	BSSID	Channel	RSSI	Encryption	Chance
<a href="#">select</a> Moontod	EC:E7:A2:B0:97:A0	1	-62	WPA2 / PSK	76%
<a href="#">select</a> ZTE_2_4G_Af4AQA	0C:37:47:8C:8B:6C	6	-10	WPA / WPA2 / PSK	100%
<a href="#">select</a> Penelitian Skripsi	0E:37:47:9C:8B:6C	6	-10	WPA / WPA2 / PSK	100%
<a href="#">select</a> Lalaa	0E:A8:A7:EF:39:1E	11	-86	WPA2 / PSK	28%

Gambar 4.39 Daftar nama Wi-Fi di area sekitar

Dalam penelitian ini, peneliti memilih Wi-Fi “ Penelitian Skripsi “ yang sudah dibuat sebelumnya untuk di jadikan bahan uji coba. Setelah memilih Wi-Fi yang akan menjadi target maka akan dialihkan kembali ke halaman konfigurasi awal *fluxion portable*. Selanjutnya pada sub menu *options* tekan tombol *NO* untuk mengubahnya menjadi *YES*. Adapun pilihan yang harus diubah dari *NO* menjadi *YES* di sub menu *options* ini adalah *death attack* ( memulai serangan dengan memutus semua perangkat yang terhubung pada Wi-Fi yang sudah dipilih menjadi target ), *broadcast* ( mengirim SSID atau Wi-Fi tiruan yang hampir sama persis dengan aslinya ), dan *input validation* ( untuk memberikan perintah pada *fluxion portable* jika ada *password* yang dimasukkan akan dilakukan pengecekan langsung pada *router ZTE-F609* ). Untuk memulai serangan ini, selanjutnya pada *smartphone* (penyerang) agar Wi-Finya di matikan.



Gambar 4.40 Memulai penyerangan

Setelah Wi-Fi pada *smartphone* (penyerang) dimatikan maka beberapa saat kemudian pada layar *fluxion portable* akan berubah menjadi terdapat nama Wi-Fi yang sudah dipilih.



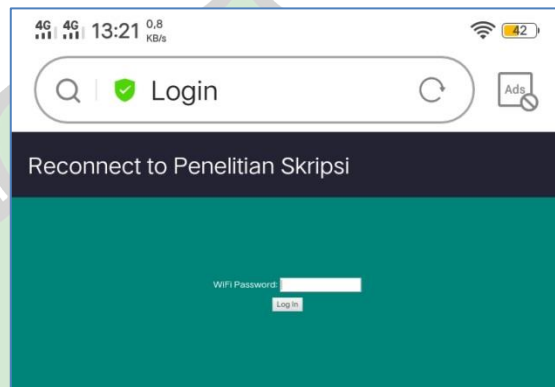
Gambar 4.41 Keterangan pada layar *fluxion portable* berubah

Di sisi lain setelah penyerangan dimulai maka pada *smartphone* target akan terputus dari Wi-Fi “Penelitian Skripsi” yang telah dihubungkan pada konfigurasi *router* sebelumnya. Kemudian akan muncul dua Wi-Fi dengan nama yang sama tapi jenis keamanan berbeda. Wi-Fi satu akan ada *icon* gemboknya sedangkan Wi-Fi yang satunya lagi tidak.



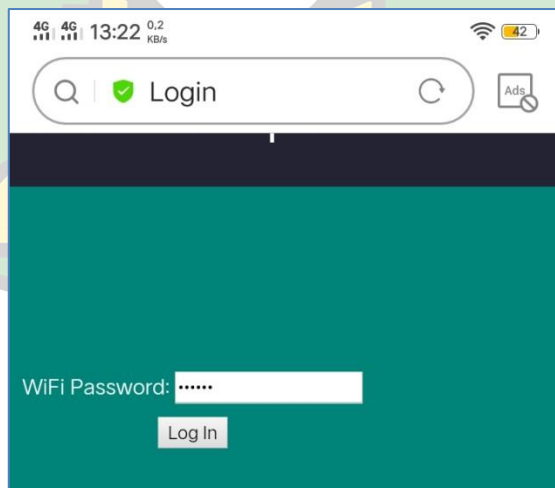
Gambar 4.42 Wi-Fi target menjadi dua

Wi-Fi yang memiliki icon gembok adalah Wi-Fi asli, sedangkan Wi-Fi tanpa *icon* gembok adalah Wi-Fi tiruan. Pada saat seperti ini Wi-Fi asli tidak akan bisa digunakan oleh siapapun meski dilakukan beberapa kali percobaan menghubungkan ulang. Selanjutnya dalam kepanikan dan tanda tanya pengguna memilih untuk menghubungkan *smartphonenya* pada Wi-Fi tiruan. Alhasil setelah *smartphone* target terhubung pada Wi-Fi tiruan maka *smartphone* target tersebut akan diarahkan pada halaman *login*.

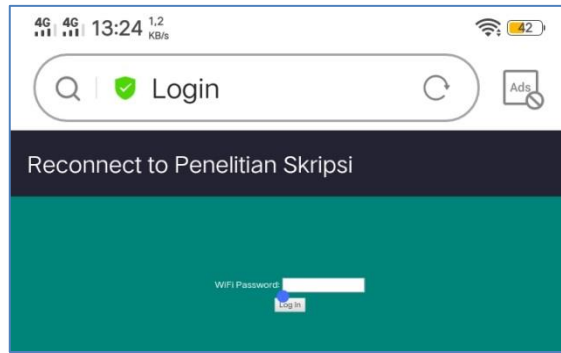


Gambar 4.43 Halaman *login* Wi-Fi tiruan

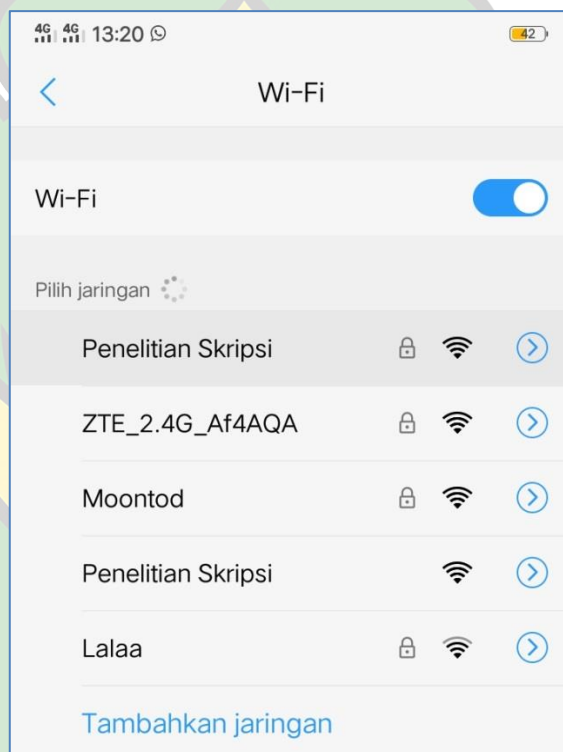
Adapun *password* dari Wi-Fi “Penelitian Skripsi” ialah “untukpenelitian”. Pada halaman *login* Wi-Fi pada *smartphone* target terlebih dahulu dicoba dengan *password* yang salah yakni “123456” maka *smartphone* target tersebut tidak bisa terhubung dan diminta untuk *login* kembali.



Gambar 4.44 *Input password* yang salah



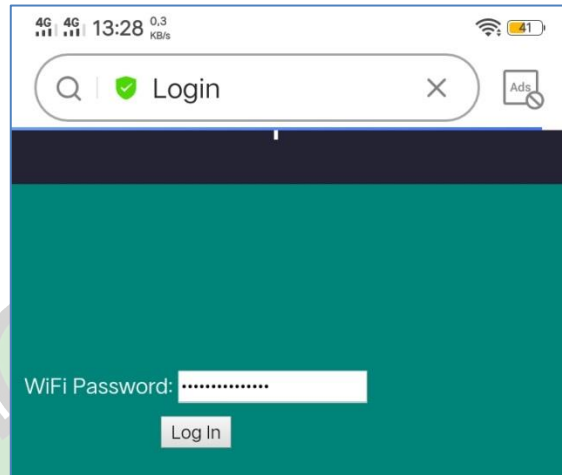
Gambar 4.45 *Login* ulang jika *password* yang dimasukkan salah



Gambar 4.46 *Smartphone* target tetap tidak bisa terhubung pada Wi-Fi asli

*Smartphone* target akan terus menerus diminta untuk memasukkan *password* pada halaman *login* sampai *password* yang dimasukkan benar. Selama proses ini tidak ada pilihan lain kecuali memasukkan *password* yang benar atau menunggu penyerang menghentikan *fluxion portable* miliknya.

Selanjutnya, saat memasukkan *password* yang benar, maka *smartphone* target akan terhubung pada Wi-Fi asli dan Wi-Fi tiruan akan berubah nama menjadi “ATTRACTHOR”.



Gambar 4.47 *Input password* yang benar



Gambar 4.48 Terhubung pada Wi-Fi asli dan Wi-Fi tiruan berubah nama



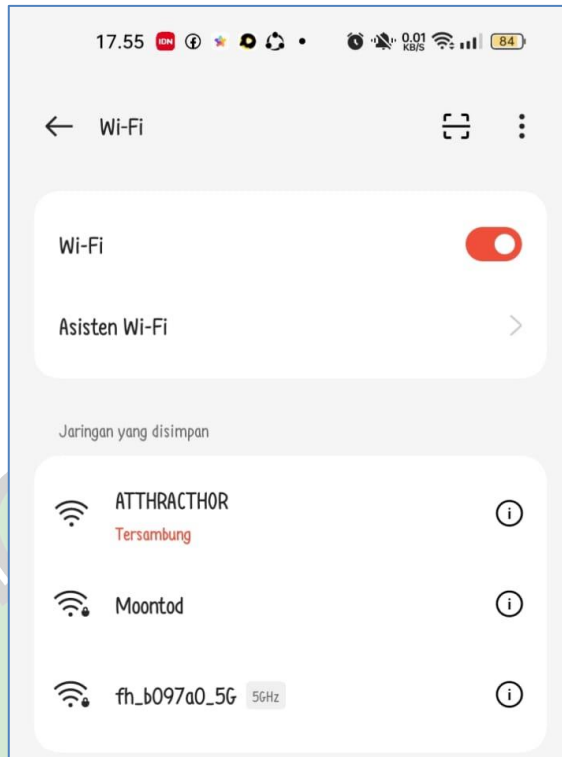
Setelah *password* yang benar dimasukkan pada halaman *login* dan *smartphone* target juga sudah berhasil terhubung pada Wi-Fi asli maka pada layar *fluxion portable* juga akan berubah keterangan menjadi “*SETUP MODE password valid*”.



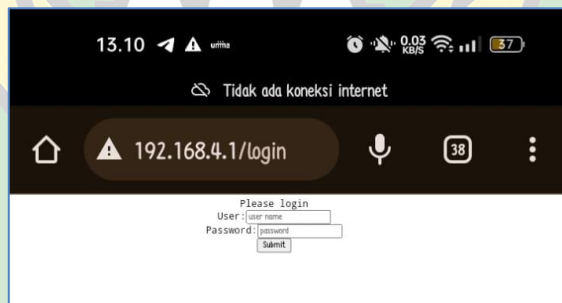
Gambar 4.49 *SETUP MODE password valid*

### 3) Hasil Penyerangan

Setelah tahapan konfigurasi dan penyerangan diatas selesai dilakukan sehingga pada layar *fluxion portable* juga sudah muncul keterangan *SETUP MODE password valid*, maka pencurian *password* Wi-Fi sudah berhasil dilakukan. Tahapan selanjutnya untuk melihat *password* Wi-Fi yang telah dicuri oleh *fluxion portable* maka *smartphone* (penyerang) harus dihubungkan kembali ke Wi-Fi *fluxion portable* yang bernama “ATTRACTHOR”. Kemudian *login* kembali pada halaman konfigurasi *fluxion portable* tersebut.



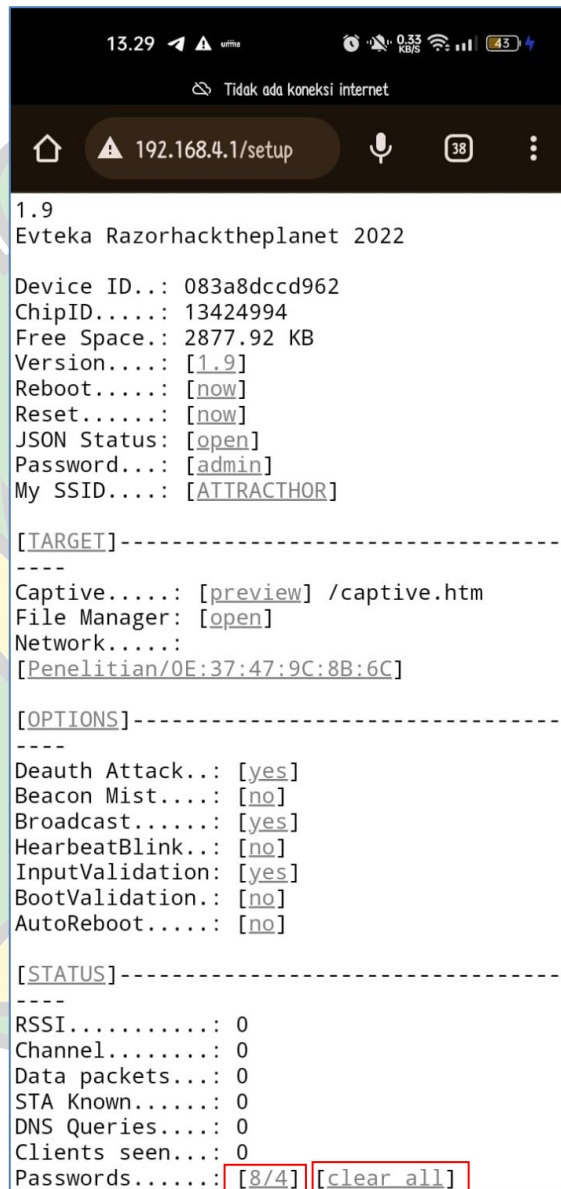
Gambar 4.50 Menghubungkan kembali *smartphone* penyerang pada Wi-Fi ATTRACTHOR



Gambar 4.51 *Login* kembali pada halaman konfigurasi *fluxion portable*

Selanjutnya, setelah *login* kembali pada halaman konfigurasi *fluxion portable*, yang harus dilakukan berikutnya adalah melihat *password* yang sudah dimasukkan oleh *smartphone* target pada halaman *login*.

Untuk melihat *password* tersebut, maka pada sub menu *STATUS* tekan angka pada bagian sebelah kanan *passwords*, yang mana pada bagian *password* pada *fluxion portable* ini tertera 8/4. Adapun maksud dari 8/4 adalah 8 merupakan total *password* yang didapatkan dan 4 adalah total *password* yang benar. Kemudian untuk menghapus *password* yang tersimpan pada *fluxion portable* ini, tekan tombol *clear all* yang terdapat disebelah kanan 8/4.



```
13.29 192.168.4.1/setup 0.33 KB/s 43%
Tidak ada koneksi internet
1.9
Evteka Razorhacktheplanet 2022
Device ID..: 083a8dccc962
ChipID.....: 13424994
Free Space.: 2877.92 KB
Version....: [1.9]
Reboot.....: [now]
Reset.....: [now]
JSON Status: [open]
Password...: [admin]
My SSID....: [ATTRACTHOR]

[TARGET]-----
----
Captive.....: [preview] /captive.htm
File Manager: [open]
Network.....:
[Penelitian/0E:37:47:9C:8B:6C]

[OPTIONS]-----
----
Death Attack..: [yes]
Beacon Mist....: [no]
Broadcast.....: [yes]
HearbeatBlink..: [no]
InputValidation: [yes]
BootValidation.: [no]
AutoReboot.....: [no]

[STATUS]-----
----
RSSI.....: 0
Channel.....: 0
Data packets...: 0
STA Known.....: 0
DNS Queries....: 0
Clients seen...: 0
Passwords.....: [8/4] [clear all]
```

Gambar 4.52 Sub menu *STATUS*

Setelah menekan tombol 8/4 maka akan diarahkan pada halaman yang berisi daftar *passwords* yang sudah didapatkan. Untuk mengetahui *password* tersebut benar maka disamping *password* itu terdapat keterangan “ *valid* “. Jika tidak ada keterangan *valid* maka *password* tersebut dipastikan salah.



Gambar 4.53 Daftar *password* yang sudah didapat

### 4.3 Mengidentifikasi SSID Wi-Fi Asli dengan SSID Wi-Fi yang Palsu

Berdasarkan tahapan konfigurasi dan penyerangan menggunakan *fluxion portable* yang telah dijelaskan diatas, informasi yang dapat diperoleh mengenai bagaimana cara mengidentifikasi Wi-Fi asli dengan Wi-Fi yang palsu antara lain :

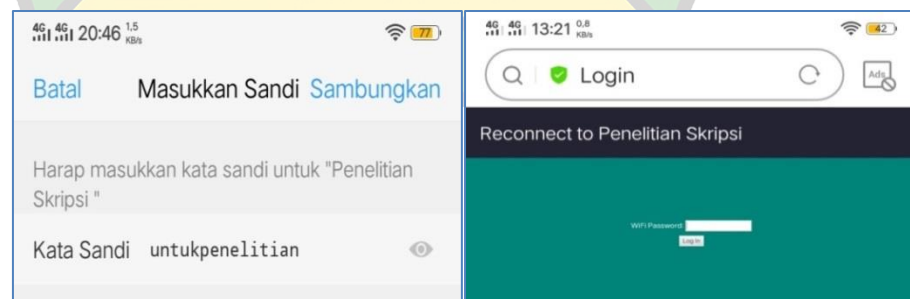
- 1) Wi-Fi asli memiliki ikon gembok sedangkan Wi-Fi tiruan tidak



Gambar 4.54 Wi-Fi asli memiliki ikon gembok sedangkan yang palsu tidak

- 2) Wi-Fi asli dengan yang palsu memiliki cara menghubungkan yang berbeda

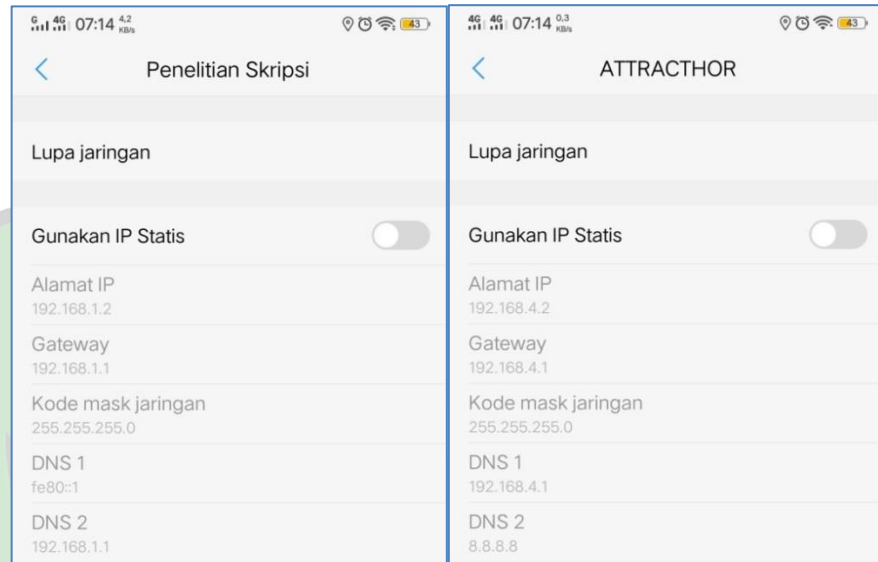
Pada Wi-Fi asli cara menghubungkannya tidak menggunakan halaman *login*. Sementara pada Wi-Fi palsu untuk menghubungkannya menggunakan halaman *login*.



Gambar 4.55 Perbedaan cara menghubungkan pada kedua Wi-Fi

3) Informasi mengenai alamat ip dan *gateway* pada Wi-Fi asli berbeda dengan Wi-Fi yang palsu.

Pada Wi-Fi asli alamat IP *default* nya adalah 192.168.1.2 dan *gateway*nya 192.168.1.1 sedangkan pada Wi-Fi tiruan alamat ip dan *gateway* nya berbeda dengan yang asli.

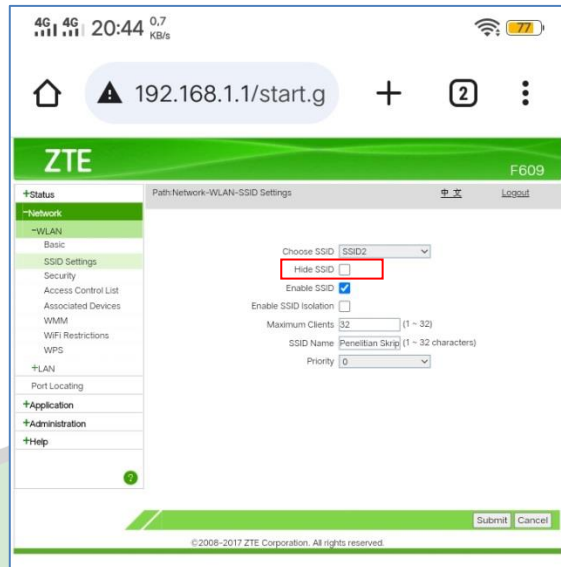


Gambar 4.56 Perbedaan alamat ip dan *gateway* pada kedua Wi-Fi

Adapun langkah yang dapat diterapkan untuk mengantisipasi terjadinya pencurian *password* Wi-Fi ini ialah sebagai berikut :

- Menyembunyikan Wi-Fi

Berdasarkan penyerangan yang telah diuraikan diatas, peneliti menemukan bahwa Wi-Fi yang disembunyikan tidak terdapat di dalam daftar Wi-Fi sekitar yang di cari oleh *fluxion portable*. Hal ini menandakan bahwa Wi-Fi yang disembunyikan tidak dapat terdeteksi oleh *fluxion portable*. Dengan tidak dapat terdeteksi maka Wi-Fi tersebut akan terhindar dari menjadi korban *fluxion portable*. Adapun cara menyembunyikan Wi-Fi ialah pada saat mengganti nama SSID atau nama Wi-Fi pastikan tombol “ *Hide SSID* “ dicentang. Maka dengan begitu Wi-Fi akan disembunyikan dari *public*.



Gambar 4.57 Centang pada kolom *Hide SSID*

- Mengganti *router* atau menggunakan mikrotik

Adapun alternatif lain yang dapat dilakukan ialah dengan mengganti *router* ZTE-F609 menjadi *router* yang *support whitelist user* atau menggunakan mikrotik dan terapkan fitur *whitelist user*, dimana fitur ini membuat Wi-Fi tersebut hanya dapat diakses oleh perangkat yang terdaftar saja.

## BAB V

### KESIMPULAN DAN SARAN

#### 5.1 Kesimpulan

Berdasarkan uraian pembahasan yang telah dipaparkan diatas maka dapat diambil kesimpulan sebagai berikut :

- 1) *Fluxion portable* membuat semua perangkat yang terhubung pada Wi-Fi target terputus setelah dilakukan konfigurasi seperti pada gambar 4.38 sampai 4.40 halaman 46-48. Setelah terputus maka tidak akan ada perangkat yang dapat terhubung pada Wi-Fi target meskipun dilakukan percobaan menghubungkan ulang berulang kali. Dalam keadaan panik dan tanda tanya maka pengguna akan menghubungkan perangkat mereka pada Wi-Fi tiruan yang kemudian akan dialihkan pada halaman *login* untuk melakukan *login* ulang. Jika pengguna memasukkan *password* Wi-Fi yang benar maka perangkat akan langsung terhubung pada Wi-Fi asli. Akan tetapi, jika pengguna memasukkan *password* Wi-Fi yang salah maka akan diminta untuk memasukkan *password* Wi-Fi kembali, sampai *password* yang dimasukkan benar.
- 2) WPA/WPA2 merupakan protokol keamanan tertinggi yang digunakan untuk melindungi jaringan Wi-Fi. Keefektifan dari *fluxion portable* tergantung pada situasi dan lingkungan jaringan yang diuji. *Fluxion portable* akan sangat efektif untuk menguji Wi-Fi dengan keamanan WPA/WPA2 jika dilakukan di lingkungan yang mayoritas penduduknya berasal dari kalangan non-IT dan terdapat banyak pengguna aktif pada Wi-Fi tersebut.
- 3) Pada penelitian ini SSID Wi-Fi asli dan yang palsu masih dapat dibedakan dengan jelas melalui *icon* gembok yang terdapat di sebelah kanan SSID Wi-Fi asli. Sedangkan pada SSID Wi-Fi tiruan tidak terdapat *icon* apapun seperti pada gambar 4.54 halaman 57. Perbedaan yang mencolok juga sangat terlihat melalui metode menghubungkan yang sedikit berbeda antara Wi-Fi asli dengan yang palsu dan juga



pada alamat ip serta gateway yang digunakan juga berbeda seperti pada gambar 4.55 dan 4.56 halaman 57 dan 58 .

## 5.2 Saran

Adapun saran yang dapat peneliti berikan melalui penelitian yang telah dilakukan ialah sebagai berikut :

- Perlu adanya edukasi terhadap pengguna jasa layanan terkait pencurian *password* Wi-Fi yang dapat merugikan pengguna jasa layanan dan memberikan *update* informasi terkait teknologi baru yang berpotensi merugikan pihak pengguna jasa layanan *internet* yang dilakukan oleh *provider*.
- Perlu adanya pengembangan lanjutan pada *fluxion portable* menjadi lebih baik lagi pada bagian metode menghubungkan yang awalnya masih menggunakan halaman *login* dikembangkan menjadi tidak menggunakan halaman *login*. Dan seandainya jika memang menggunakan halaman *login* setidaknya halaman *login* tersebut dapat di modifikasi sendiri oleh pengguna, serta alamat ip dan *gateway* yang digunakan agar di *setting* seperti *default router* pada umumnya.

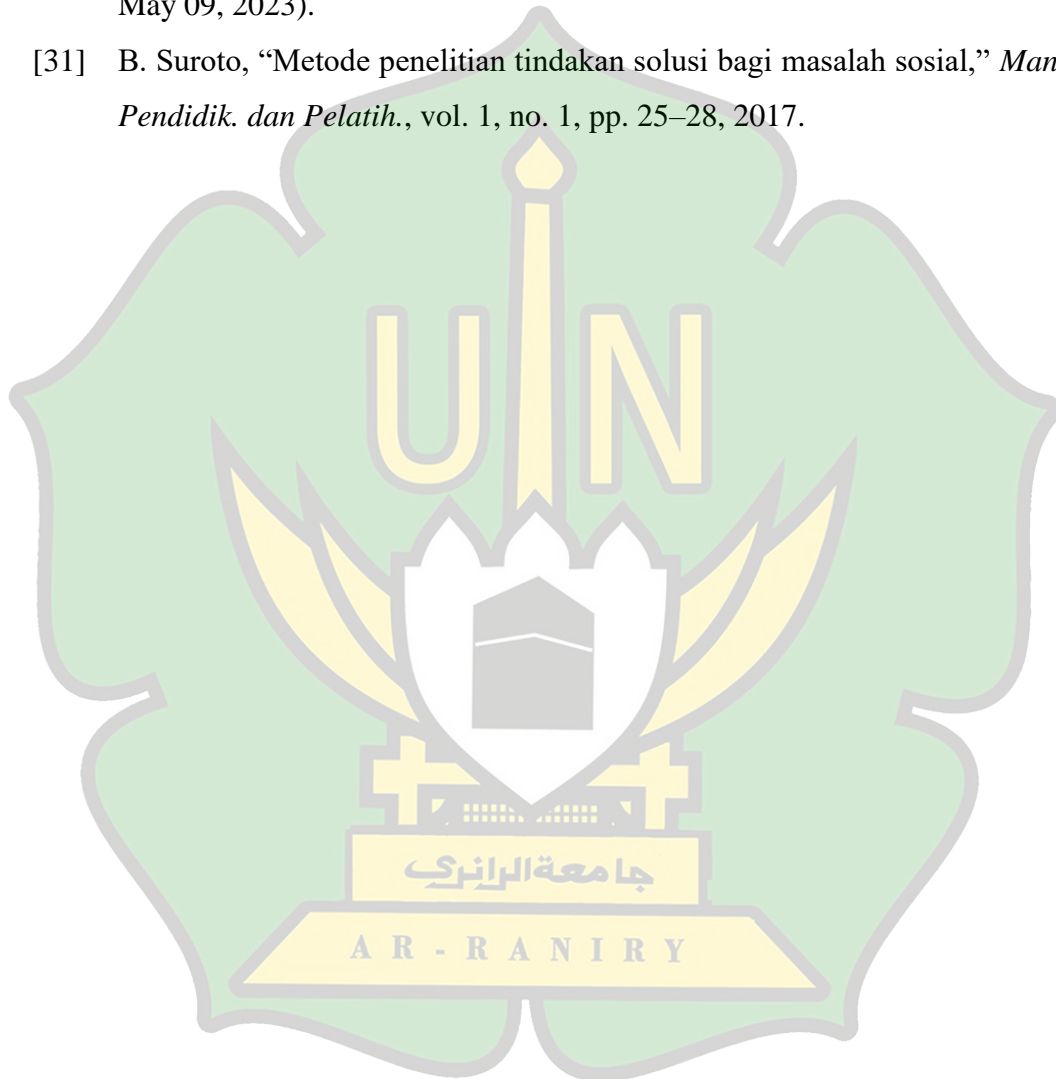
## DAFTAR PUSTAKA

- [1] D. Bayu, "Ada 611 Perusahaan Penyedia *Internet* di Indonesia pada 2021," *DataIndonesia.id*, 2022. <https://dataindonesia.id/internet/detail/ada-611-perusahaan-penyedia-internet-di-indonesia-pada-2021> (accessed Mar. 14, 2023).
- [2] R. Hanif, "DIPSTATISTIK *INTERNET SERVICE PROVIDER (FIXED BROADBAND)* YANG PALING BANYAK DIGUNAKAN DI INDONESIA," *Blog Disprategy*, 2022. <https://dipstrategy.co.id/blog/dipstatistik-internet-service-provider-fixed-broadband-yang-paling-banyak-digunakan-di-indonesia/> (accessed Mar. 14, 2023).
- [3] S. Sahat, M. Pasaribu, and R. Hidayat, "ANALISIS PERSONAL *SELLING* PRODUK INDIHOME PADA PT . TELKOM CABANG BANDA ACEH TAHUN 2021," vol. 7, no. 5, pp. 1039–1043, 2021.
- [4] O. Situngkir, "Apa alasan orang memasang Wi-Fi?," *Quora.com*, 2020. <https://id.quora.com/Apa-alasan-orang-memasang-Wi-Fi> (accessed Mar. 14, 2023).
- [5] Pemerintah Indonesia, "Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik", Jakarta : Lembaran Negara RI, No.115, Jakarta, 2008.
- [6] D. N. Widiatama, "ANALISA UJI KEAMANAN WPA2 MENGGUNAKAN *FLUXION* PADA PT. ANDAGLOS GLOBAL TEKNOLOGI," Institut Informatika Dan Bisnis Darmajaya, 2019
- [7] F. Paramita, O. Alvina, R. E. Sentia, and A. Kurniawan, "Menggunakan Teknik *Network Forensics*," vol. 14, no. 2, pp. 63–72, 2021.
- [8] R. Mandasari, "ANALISIS METODE *FLUXION* MENGGUNAKAN WI-FI *DEAUTHER* UNTUK UJI KEAMANAN WPA2 PADA PERANGKAT *ROUTER WIRELESS* TOTOLINK N300RT", Universitas Islam Riau, 2021.

- [9] K. Wahana, *Tips Jitu Optimasi Jaringan Wi-Fi*. Semarang: Penerbit Andi, 2010.
- [10] N. Bestari, “Wi-Fi: Pengertian, Fungsi, dan Cara Kerja, Materi Informatika Dasar,” *Bobo.id*, 2022. <https://bobo.grid.id/read/083490264/Wi-Fi-pengertian-fungsi-dan-cara-kerja-materi-informatika-dasar?page=all> (accessed May 09, 2023).
- [11] J. Gondohanindijo, “Sistem Keamanan Jaringan NIRKABEL,” *Maj. Ilm. Inform.*, vol. 3, no. 2, 2012.
- [12] I. S. Hidayat, “Pilihan Wi-Fi Security Mana Yang Paling Aman Untuk Kita?,” *Murdockcruz*, 2017. <https://www.murdockcruz.com/2017/12/29/pilihan-wi-fi-security-mana-yang-paling-aman-untuk-kita/> (accessed May 06, 2023).
- [13] W. Kurniawan, *Computer Starter Guide : Jaringan Komputer*. Semarang: Penerbit Andi, 2007.
- [14] Y. J. Waloea, *Computer Networking*. Yogyakarta: Penerbit Andi, 2012.
- [15] E. Santi, “Apa Itu Router? Ini Pengertian, Fungsi, Jenis, Cara Kerja, dan Bedanya dengan Modem!,” *Idwebhost.com*, 2022. <https://idwebhost.com/blog/apa-itu-router/> (accessed May 09, 2023).
- [16] K. Amira, “Pengertian IP Address: Fungsi, Cara Kerja, dan Versi IP Address,” *Gramedia.com*. 2021. Available: [https://www.gramedia.com/literasi/pengertian-ip-address/#Pengertian\\_IP\\_Address](https://www.gramedia.com/literasi/pengertian-ip-address/#Pengertian_IP_Address) (accessed Nov 16, 2023).
- [17] A. Faradilla, “Apa Itu IP Address? Pengertian, Jenis, dan Fungsinya,” *Hostinger*. 2022. Available: <https://www.hostinger.co.id/tutorial/apa-itu-ip-address> (accessed Nov 16, 2023).
- [18] Cloudmatika, “Memahami Apa itu Gateway serta Jenis-jenisnya pada Sebuah Jaringan,” *Cloudmatika*. 2022. Available: <https://cloudmatika.co.id/blog-detail/apa-itu-gateway> (accessed Nov 16, 2023).

- [19] Haryono, “IMPLEMENTASI MODEM SISCO LINKSYS WAG 120N SEBAGAI *GATEWAY* DAN *HOTSPOT AREA*,” *PIKSEL*, vol. 1, no. 1, pp. 7–17, 2013.
- [20] F. N. Dihan, “*SMARTPHONE*: ANTARA KEBUTUHAN DAN *LIFE STYLE*,” vol. 2010, no. semnasIF, pp. 312–321, 2010.
- [21] V. Kumar, “*Fluxion* di Kali Linux digunakan untuk peretasan WPA WPA2 dalam hitungan menit Panduan Pemula,” CyberPratibha. 2023. Available: <https://www.cyberpratibha.com/blog/fluxion-wpa-wpa2-hacking/>
- [22] A. Kristanto, *Keamanan Data Pada Jaringan Komputer*, 1st ed. Yogyakarta: Gava Media, 2003.
- [23] Z. M. Luthfansa and U. D. Rosiani, “Pemanfaatan Wireshark untuk *Sniffing* Komunikasi Data Berprotokol HTTP pada Jaringan *Internet*,” *Inf. Eng. Educ. Technol.*, vol. 05, no. 1, 2021.
- [24] M. Akbar, “PERANCANGAN *SOFTWARE IDS SNORT* UNTUK PENDETEKSIAN SERANGAN *INTERRUPTION ( Netcut )* PADA JARINGAN *WIRELESS*,” *INSTEK*, vol. 03, no. 01, 2018.
- [25] B. W. Santoso, F. Sundawa, and M. Azhari, “Implementasi Algoritma *Brute Force* Sebagai Mesin Pencari ( *Search Engine* ) Berbasis Web Pada *Database*,” *SISFOTEK Glob.*, vol. 6, no. 1, 2016.
- [26] D. I. Junaedi, “Antisipasi Dampak *Social Engineering* Pada Bisnis Perbankan,” *Infoman’s*, vol. 11, no. 1, pp. 1–10, 2017, doi: 10.33481/infomans.v11i1.13.
- [27] D. Firmansyah, “PENERAPAN TEKNOLOGI *BLOCKCHAIN* UNTUK MENGATASI SERANGAN *MAN IN THE MIDDLE*”, *Journal Science Informatica and Robotics* , vol. 1, no. 1, pp. 73–80, 2023.
- [28] M. Napizahmi, “*Man in the Middle Attack*: Pengertian, Jenis dan Cara Menghindarinya,” DewaWeb. Available: <https://www.dewaweb.com/blog/pengertian-man-in-the-middle-attack/>. (accessed Nov 16, 2023).

- [29] Lina, I. M. Fernandes, and G. Ryan, “ANALISIS POLA SOSIAL *ENGINEERING* MENGGUNAKAN TEKNIK WI-FI DEAUTHER DAN EVIL TWIN,” *Rekayasa Komputasi Terap.*, vol. 02, no. 04, 2022.
- [30] Idwebhost, “Keamanan Wi-Fi – 10 Cara Dasar Untuk Mengamankan *Wireless Network*,” *Idwebhost.com*, 2020.  
<https://idwebhost.com/blog/mengamankan-wireless-network/> (*accessed* May 09, 2023).
- [31] B. Suroto, “Metode penelitian tindakan solusi bagi masalah sosial,” *Manaj. Pendidik. dan Pelatih.*, vol. 1, no. 1, pp. 25–28, 2017.



## **RIWAYAT HIDUP PENULIS**

Nama : Reja Anggara Selian  
Tempat/Tanggal lahir : Batumbulan / 17 Agustus 2000  
Jenis Kelamin : Laki-Laki  
Alamat Rumah : Desa Batumbulan I, Kec. Babussalam, Kab.  
Aceh Tenggara  
Telp/HP : +62 812 6945 3190  
E-Mail institusi : 180212023@student.ar-raniry.ac.id

### **RIWAYAT PENDIDIKAN**

Sekolah Dasar (SD)/Sederajat : MIN Terutung Padi  
Sekolah Menengah Pertama (SMP) /Sederajat : SMPN 4 Kutacane  
Sekolah Menengah Atas (SMA) /Sederajat : MAN 1 Aceh Tenggara  
Perguruan Tinggi : UIN Ar-Raniry  
Banda Aceh  
Fakultas/Program Studi : Fakultas Tarbiyah dan  
Keguruan / Pendidikan  
Teknologi Informasi

### **RIWAYAT KELUARGA**

Nama Ayah : Mateli  
Pekerjaan Ayah : Petani  
Nama Ibu : Saidah  
Pekerjaan Ibu : Petani  
Alamat Lengkap : Desa Batumbulan I, Kec. Babussalam, Kab.  
Aceh Tenggara