PERIPHERAL
JURNAL ILMU KOMPUTER
Penerbit:
Universitas Cokroaminoto Palopo

**Peripheral: Jurnal Ilmu Komputer** **Vol. 1, No. 1, Tahun 2025**

# Analisis Perbandingan Keamanan Jaringan *Wireless Wpa-Psk* dan *Wpa2-Psk* pada Puskesmas Tomoni Timur

**Kadek Anjani**
Universitas Cokroaminoto Palopo
kadek@gmail.com

**Article Info**
**Kata Kunci:**



**Abstrak**

Tujuan penelitian ini adalah untuk menganalisa jarigan wireless dengan menggunakan metode kualitatif, *WPA* dan *WPA2-PSK serta m*embandingkan tingkat keamanan jaringan *WPA-PSK* dan *WPA2-PSK*. Penelitian ini menggunakan jenis penelitian kualitatif. Penelitian kualitatif adalah penelitian deskriptif dan biasanya menggunakan analisis. Dalam penelitian kualitatif, fokusnya adalah pada persentase dan kepentingan (perspektif subjektif). Hasil penelitian ini menunjukkan Sistem keamanan jaringan wpa/psk dan wpa2/psk Puskesmas Tomoni Timur dapat dibobol, terbukti saat peneliti melakukan pengujian keamanan jaringan menggunakan aplikasi Fluxion.

## PENDAHULUAN

*Wi-Fi Protected Access* 2-Per *Shared Key (WPA2-PSK)* merupakan tipe keamanan untuk jaringan *wireless, WPA2-PSK* menggunakan dua jenis enkripsi yaitu *Advanced Encryption Standard* (AES) dan *Temporal Key Integrity Protocol* (TKIP). Sedangkan *captive portal* adalah tipe keamanan jaringan *wireless* yang menggunkan halaman web, dan berfungsi untuk mengirim informasi login seperti *username* dan *password* ke *database.* Sistem keamanan *WPA2-PSK* dan *coptive portal* banyak digunakan oleh penyediaan jaringan publik *wireless* atau sering disebut *hospot,* dimana *hospot* merupakan area yang tersedia akses jarigan internet.

Dengan perkembangan teknologi informasi yang sangat cepat khususnya internet, interaksi dengan karyawan atau pekerja melalui jaringan komputer

memberikan dampak yang sangat besar terhadap jalannya suatu perusahaan atau instansi. Namun, proses ini sangat mengganggu dan berisiko ketika orang yang tidak berhak mendapatkan akses ke informasi yang sangat penting. Pertama-tama, perlu dicatat bahwa ada dua jenis alat transmisi untuk jaringan komputer, yaitu kabel dan nirkabel (WLAN).

Salah satu masalah keamanan jaringan terbesar saat ini adalah Internet, yang menghubungkan banyak jaringan, seperti jaringan nirkabel, di mana data dapat dikirim. Terkadang tidak aman, yang sering menunda keamanan jaringan dan membuka peluang bagi orang yang tidak bertanggung jawab. Menurut sebuah studi oleh East Tomon Health Center, stabil karena penggunanya melebihi kapasitasnya.

Saat ini, masalah keamanan jaringan sangat penting dan patut mendapat perhatian. Jaringan yang terhubung ke Internet pada dasarnya tidak aman dan *hecker* dapat mengeksploitasinya kapan saja, baik jaringan kabel maupun *wireless*. Ketika data dikirim, ia melewati beberapa terminal, yang berarti bahwa mereka memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menangkap atau memodifikasi data.

Saat mengembangkan desainnya, sistem keamanan jaringan yang terhubung ke Internet harus dipahami dan dipahami dengan baik untuk melindungi sumber daya jaringan secara efektif dan meminimalkan serangan peretas. Untuk mengamankan jaringan, harus terlebih dahulu menentukan tingkat ancaman yang harus diatasi dan risiko yang harus diambil atau dihindari.

Berikut ini akan dibahas mengenai ancaman, kelemahan, dan *policy* keamanan jaringan. *Issue* Keamanan jaringan sangat penting dan patut mendapat perhatian. Jaringan yang terhubung ke Internet pada dasarnya tidak aman dan dapat dieksploitasi oleh *hacker* kapan saja, baik di jaringan lokal maupun nirkabel. Ketika data dikirim, ia melewati beberapa terminal, yang berarti bahwa mereka memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menangkap atau memodifikasi data. Saat mengembangkan desain, sistem keamanan jaringan yang terhubung internet harus dirancang dan dipahami. Grup jaringan menerima paket yang dikirim oleh host. Karena sifat dari packet sniffing, cukup sulit untuk melindungi dari interferensi ini. Ini adalah metode pasif yang tidak mengharuskan penyerang melakukan apa pun, cukup dengarkan. (Nugroho, 2020).

*Institute of Electrical and Electronics Engineers* (IEEE) Ini mengharuskan grup 802.11i untuk mengimplementasikan metode keamanan yang kemudian dikenal sebagai WPA2. WPA2 sejauh ini berarti peningkatan tingkat keamanan WEP (*Wired Equivalent Privacy*). Enkripsi utama yang digunakan dalam WPA2 adalah enkripsi *Advanced Encryption System* (AES). [7]. Sistem keamanan jaringan WPA2-PSK untuk tipe ini memiliki dua pilihan enkripsi yaitu Temporal Key Integrity Protocol (TKIP) dan Advanced Encryption System (AES). TKIP menggunakan metode enkripsi yang lebih aman dan juga menggunakan kode MIC (Message Integrity Code) untuk melindungi jaringan dari serangan. .

*WPA* ini adalah kependekan dari *Wifi Protected Access*, suatu mode security yang menggantikan *WEP (Wired Equivalent Privacy)*. *WEP* perlu digantikan karena mengandung celah keamanan. WPA berevolusi menjadi WPA2 selama pekerjaan pengembangan, meskipun WPA2 tentu saja lebih aman karena alasan keamanan. Belakangan dalam pengenalannya, AES (*Advanced Encryption Standard*) menggantikan TKIP (*Temporal Key Integrity Protocol*) karena kelemahan keamanan pada TKIP. Jadi

AES lebih aman daripada TKIP. Untuk fungsi WPS (Wifi Protected Setup), WPS ini memiliki kelemahan keamanan. Oleh karena itu, fungsi WPS harus dinonaktifkan. Ada juga WPA/WPA2 Personal dan WPA/WPA2 Enterprise untuk WPA dan WPA2. Kami terutama menggunakan WPA Personal karena lebih sederhana, menggunakan password yang telah disepakati. Oleh karena itu *WPA/WPA2* Personal juga disebut *WPA/WPA2 PSK (Pre Shared Key)*.

*WPA* merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci *WEP*. Ada dua jenis yakni *WPA* personal (*WPA-PSK*), dan *WPA*-RADIUS. Saat ini yang sudah dapat di *crack* adalah *WPA-PSK*, yaitu dengan metode *offline brute force attack*. Kekerasan brutal dengan banyak kata dari kamus. Serangan ini berhasil jika kata sandi yang digunakan oleh jaringan nirkabel ditemukan dalam kamus kata yang digunakan oleh peretas. Anda dapat mencegah serangan terhadap keamanan nirkabel WPA-PSK dengan menggunakan frasa sandi satu frasa (Mulyanta, 2020).

## METODE

### Jenis Penelitian

Penelitian ini menggunakan jenis penelitian kualitatif. Penelitian kualitatif adalah penelitian deskriptif dan biasanya menggunakan analisis. Dalam penelitian kualitatif, fokusnya adalah pada persentase dan kepentingan (perspektif subjektif). Landasan teori berfungsi sebagai pedoman agar gagasan penelitian sesuai dengan fakta di lapangan.

### Teknik Pengumpulan Data

Pada Penelitian ini digunakan satu metode untuk pengumpulan data yang dijadikan sebagai acuan dalam analisis perbandingan keamanan jaringan *wireless WPA-PSK* dan *WPA2-PSK*, yaitu

a. Wawancara

Wawancara memungkinkan pewawancara analisis jaringan untuk mengumpulkan informasi yang akurat tentang keadaan jaringan Kesehatan Masyarakat tomoni timur secara langsung dengan responden..

b. Observasi

Observasi adalah metode pengumpulan data dengan cara mengamati secara langsung suatu objek dalam kurun waktu tertentu dan mencatat secara sistematis hal-hal tertentu yang diamati.

Banyaknya periode pengamatan yang akan dilakukan dan lamanya setiap periode pengamatan bergantung pada jenis data yang dikumpulkan.

c. Studi Pustaka

Langkah selanjutnya dalam pengumpulan data adalah mencari referensi yang relevan dengan penelitian ini. Referensi ini berasal dari jurnal penelitian, laporan penelitian, dan skripsi.

d. *Questioner* atau angket

Menurut Sugiyono (2018), Kuesioner adalah teknik survei di mana responden disajikan dengan serangkaian pertanyaan atau pernyataan tertulis. Menurut Sugiyono (2019), kuesioner adalah teknik pengumpulan data yang dilakukan dengan memberikan serangkaian pertanyaan atau pernyataan tertulis kepada responden. Jawaban untuk setiap pertanyaan memiliki skala.

Adapun beberapa pertanyaan yang diajukan, yaitu:

1) Jaringan apa yang digunakan di Puskesmas Tomoni Timur?
2) Seberapa cepat koneksi internet di Puskesmas Tomoni Timur?
3) Berapa jumlah pengguna online yang digunakan di Puskesmas Tomoni Timur?
4) Berapa jumlah komputer yang terkoneksi jaringan yang digunakan di Puskesmas Tomoni Timur?
5) Topologi apa yang digunakan di Pusat Kesehatan Tomoni Timur?

e. *Blackbox Testing*

Menurut Tri snadhika Jaya (2018), pengujian menggunakan *Blackbox Testing* adalah teknik pengujian perangkat lunak yang berfokus pada spesifikasi fungsional dari perangkat lunak. Teknik tes yang digunakan adalah teknik black box test. Teknik pengujian ini berfokus pada persyaratan fungsional sistem. Tes kotak hitam digunakan untuk menguji fungsi tertentu dari sistem. Proses pengujian menunjukkan bahwa fungsi bekerja dengan benar dalam arti input diterima dengan benar dan output benar serta integrasi data eksternal berjalan dengan baik.

**Analisis Data**

Analisis data adalah proses pengambilan atau penggabungan secara sistematis informasi yang dikumpulkan dari observasi, wawancara, dan tinjauan pustaka agar lebih mudah dipahami, dan dilakukan melalui pengorganisasian materi. Fase ini merupakan fase lanjutan dari fase pengumpulan data. Data yang diterima diproses atau dihitung untuk mendapatkan hasil. Kemudian kami menganalisis untuk menarik kesimpulan tentang permasalahan yang ada di Puskesmas Tomoni Timur.

## HASIL DAN PEMBAHASAN

**Analisis Sistem**

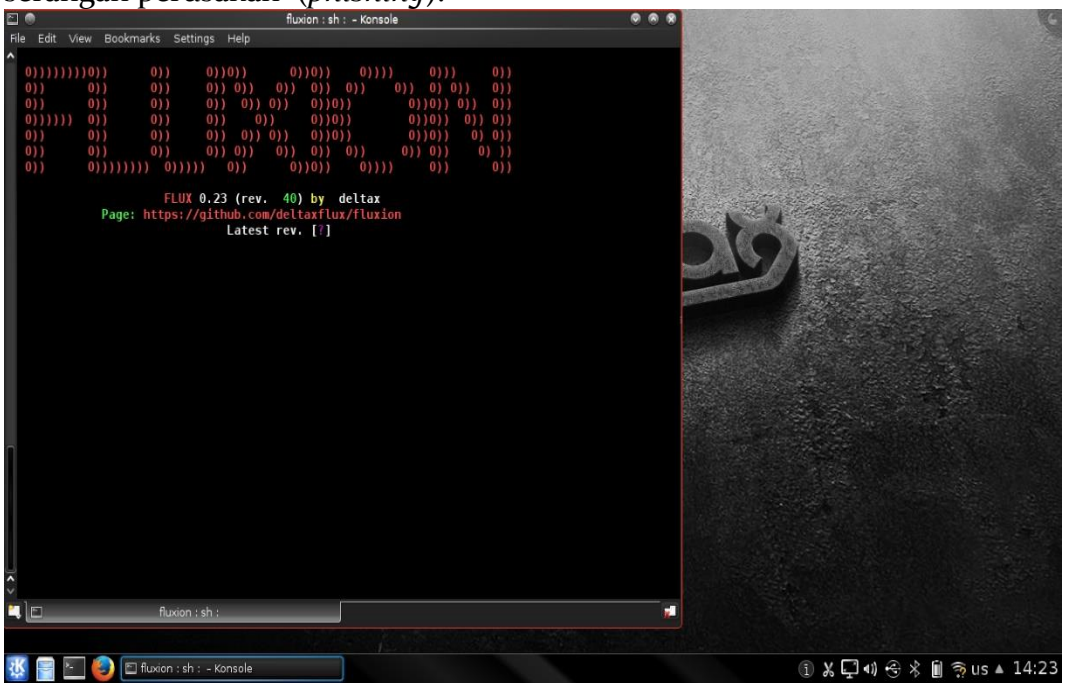
Berdasarkan arsitektur dan topologi yang diperoleh penulis, pada tahap ini penulis melakukan simulasi serangan terhadap jaringan *WPA2/PSK* dan *WPA/PSK* yang dirancang dengan Fluxion. Ini digunakan untuk mengetahui apakah sistem keamanan jaringan dapat ditembus dan kemudian mengusulkan solusi untuk masalah yang dianalisis terkait dengan pemrosesan keamanan jaringan .

1. Menjalankan *OS wifislax*


Gambar 20. Tampilan *desktop wifislax*

2. Membuka aplikasi *fluxion*

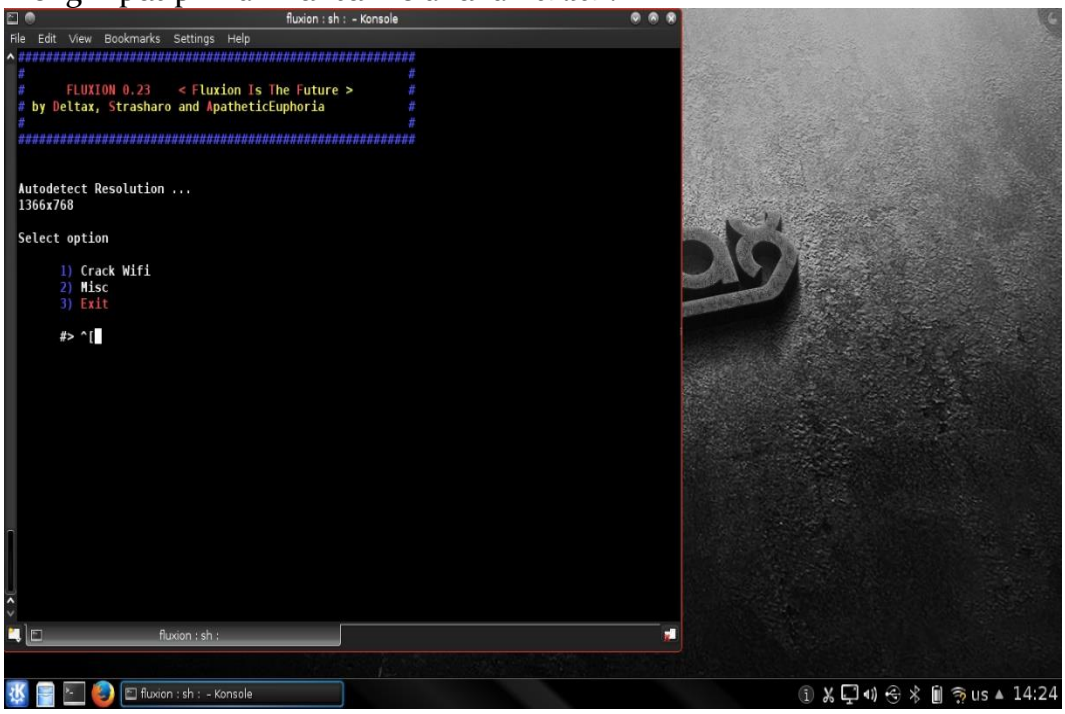
*Fluxion* adalah pemeriksaan keamanan jaringan. Program ini adalah pembuatan ulang alat Linset vk496 dengan lebih sedikit bug dan lebih banyak fungsi. Skrip aplikasi mencoba mendapatkan kunci *WPA*/*WPA2* pemancar target menggunakan serangan perusakan (*phishing*).




Gambar 21. Tampilan aplikasi *fluxion*

3. Melakukan *wifi crack*

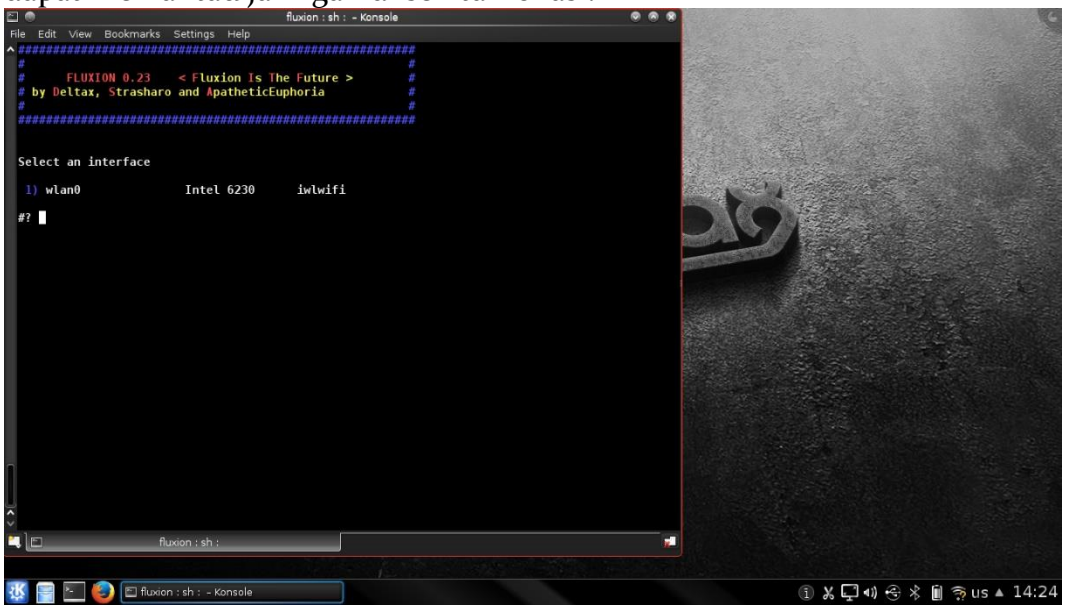
Pada tahap ini penulis melakukan *cracking wifi* pada aplikasi *fluxion* dengan mengimput pilihan 1 untu melakukan *crack*.




Gambar 22. Tampilan menu *crack wifi*

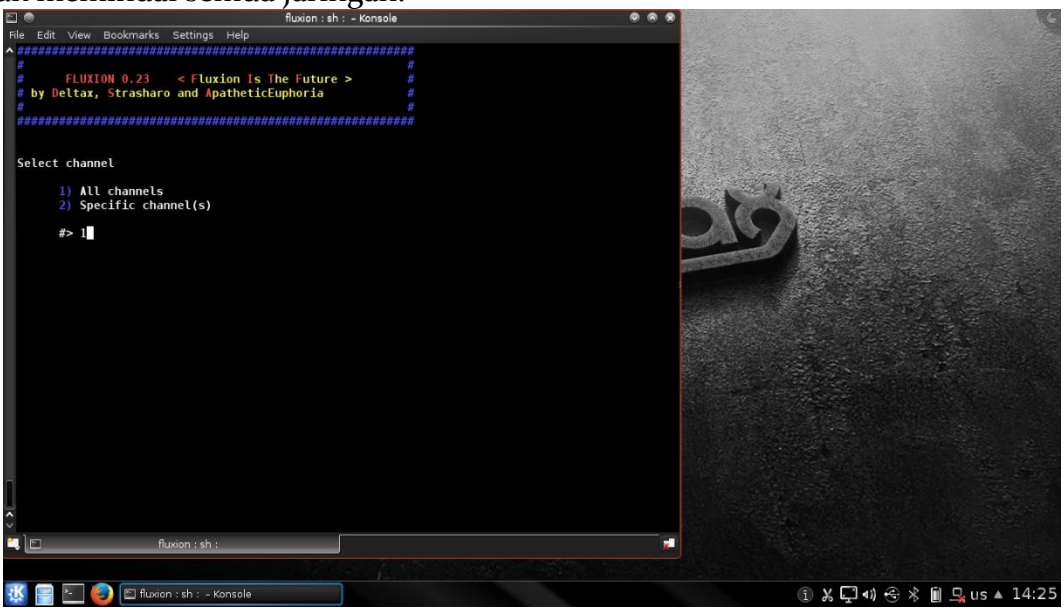
4. Melakukan *wifi crack* Jaringan *Wifi* yang Menggunakan Enkripsi *WPA/PSK*

Kemudian punulis masuk kembali ke opsi 1 untuk mengubah adaptor wifi dari status terkelola menjadi status terpantau. Hal ini dilakukan agar router wifi laptop dapat memantau jaringan di sekitar lokasi.



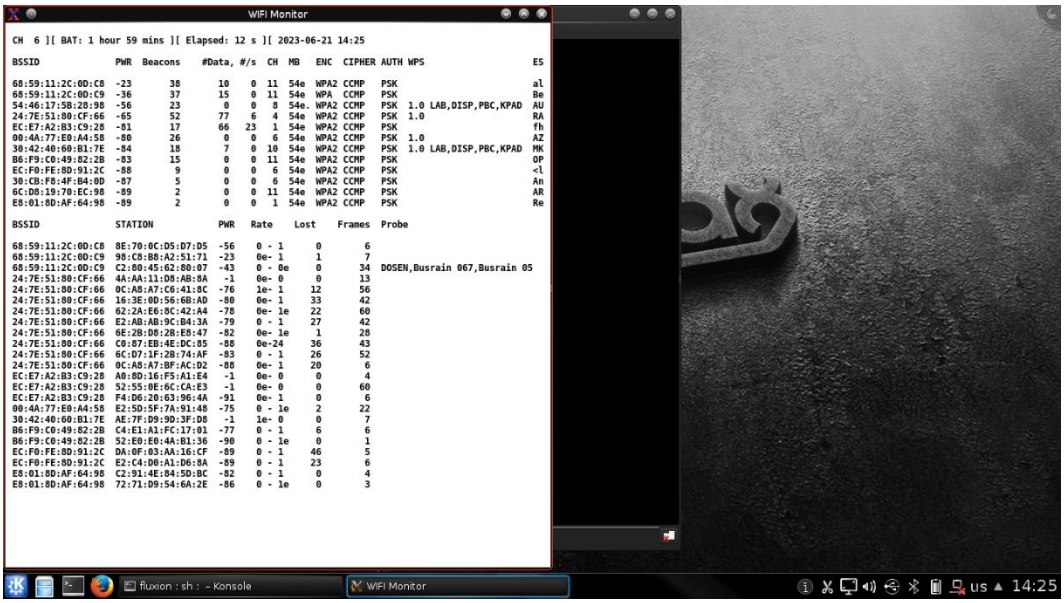

Gambar 23. Tampilan pemilihan adapter *wifi*

Kemudian fluxion akan menampilkan opsi pemindaian wifi. Penulis memilih opsi 1 untuk memindai semua jaringan.



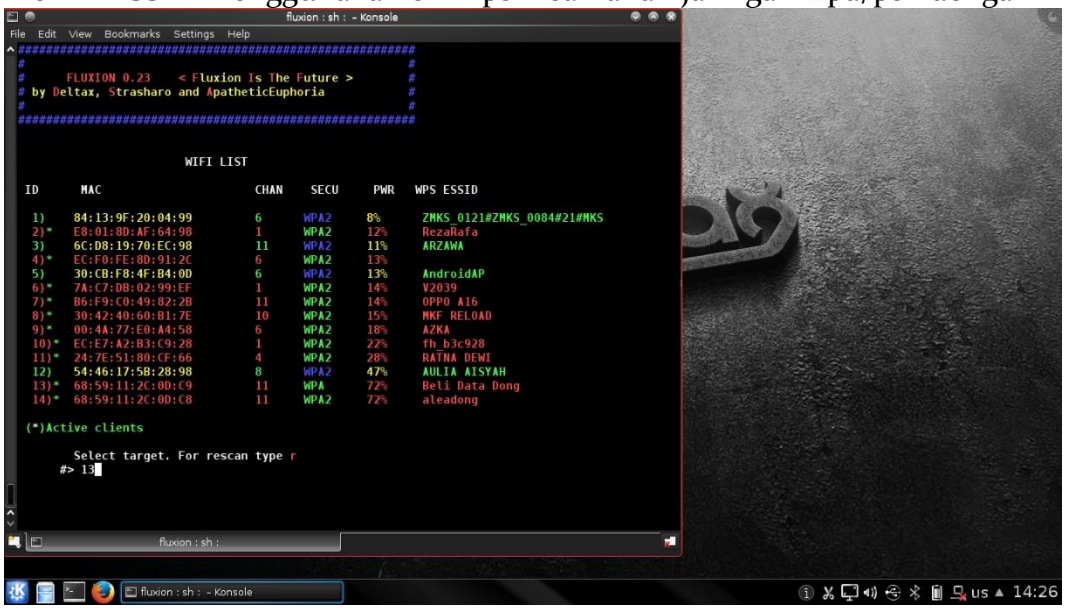

Gambar 24. Tampilan pemilihan *channel wifi*

Gambar di bawah menunjukkan beberapa jaringan *wifi* berserta client yang terhubung pada jaringan *wifi* berdasarkan hasil *scanning* aplikasi *fluxion*.



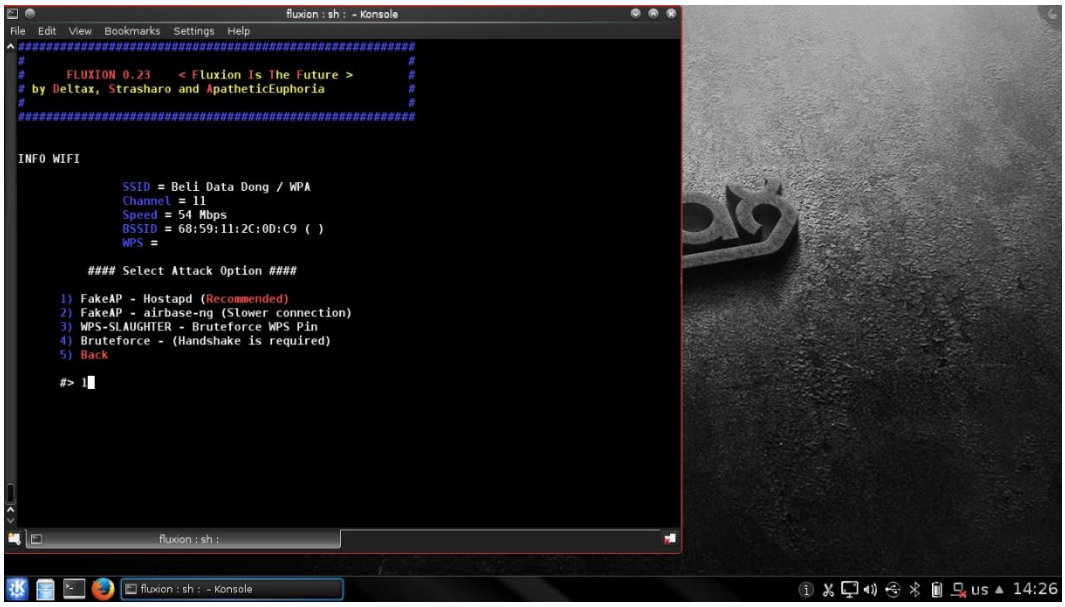

Gambar 25. Tampilan hasil *scanning* jaringan *wifi*

Setelah pemindaian selesai, aplikasi akan menampilkan beberapa SSID beserta pola enkripsi keamanan jaringan Wi-Fi, tanda bintang (*) di aplikasi menunjukkan bahwa SSID dapat ditipu untuk mendapatkan kata sandi di jaringan wifi. Peneliti memilih SSID menggunakan enkripsi keamanan jaringan wpa/psk dengan ID 13.



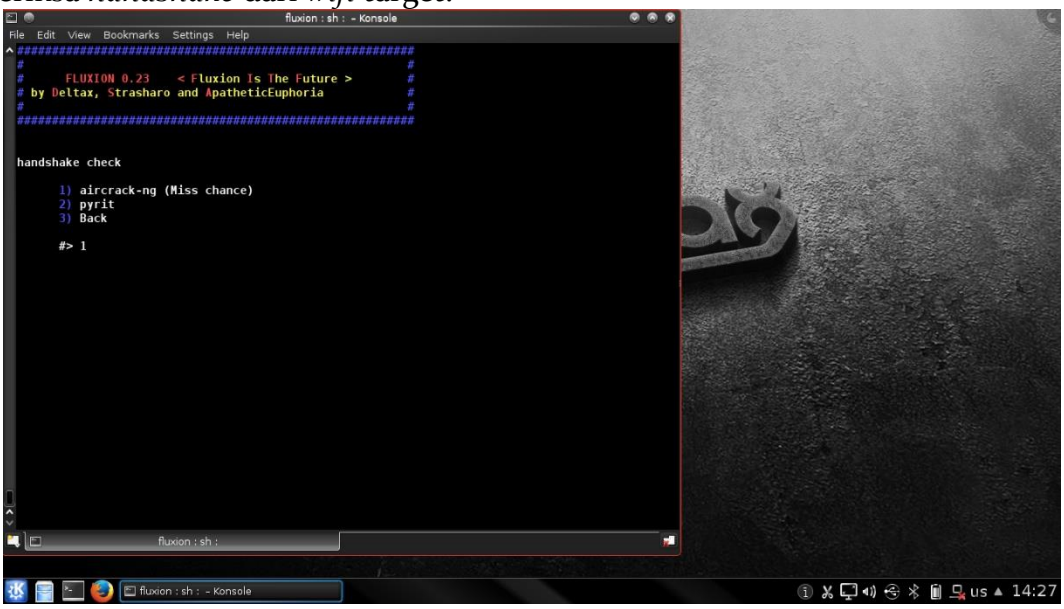

Gambar 26. Tampilan SSID setelah proses *scanning*

Selanjutnya, aplikasi akan memberikan informasi Wi-Fi target, termasuk: Nama SSID, saluran yang digunakan, kecepatan jaringan, alamat MAC wifi, dan jenis enkripsi kata sandi wifi. Penulis memilih opsi 1 sebagai serangan dengan *fake-AP-Hotspat* sesuai yang direkomendasikan oleh aplikasi *fluxion*.



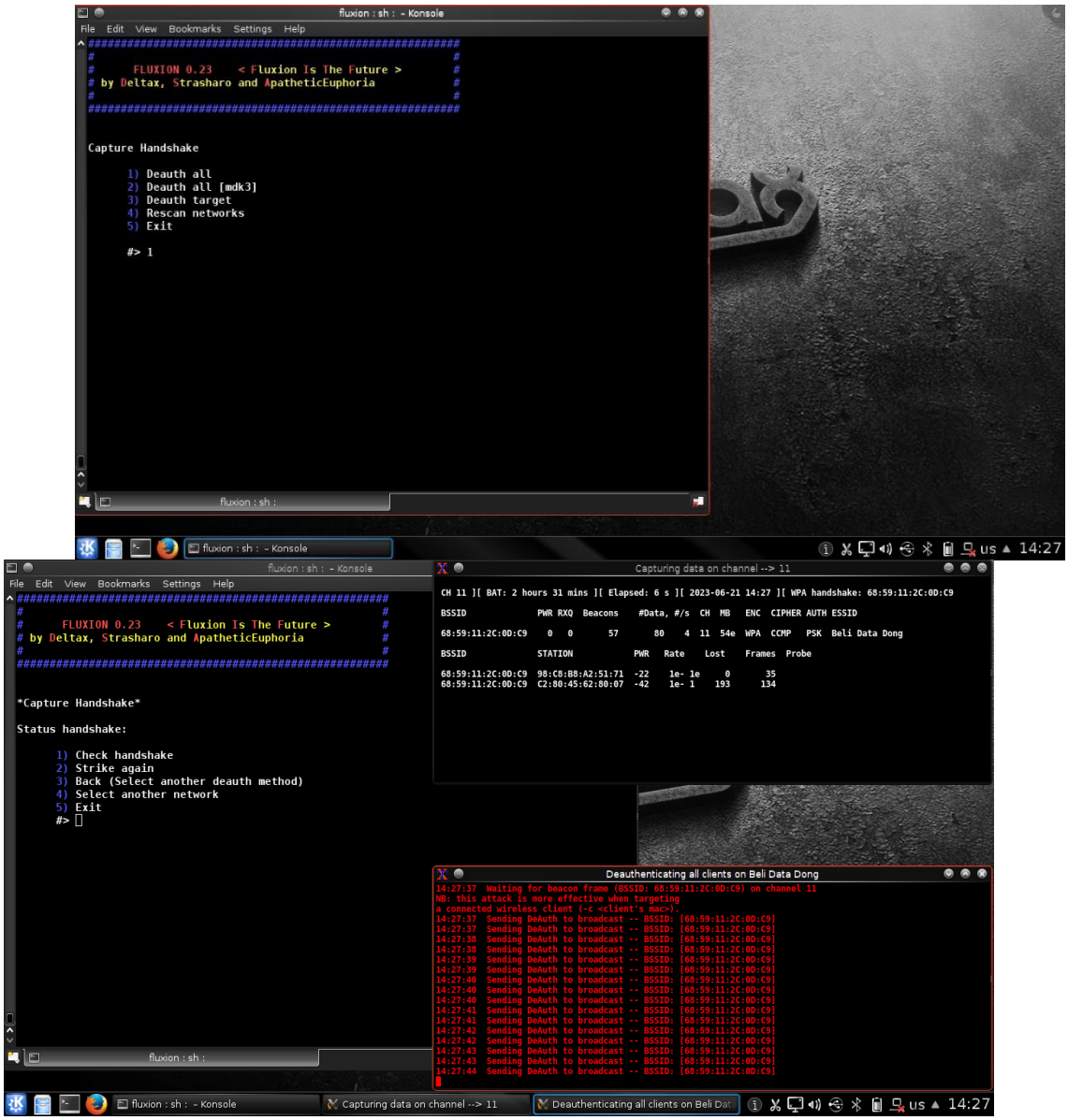

Gambar 27. Tampilan tipe penyerangan

Tahap selanjutnya aplikasi akan memeriksa *handshake* pada jaringan target dengan menggunakan *aircack-ng* atau *pyrit*. Disini penulis memilih pilihan 1 untuk memeriksa *handshake* dari *wifi* target.



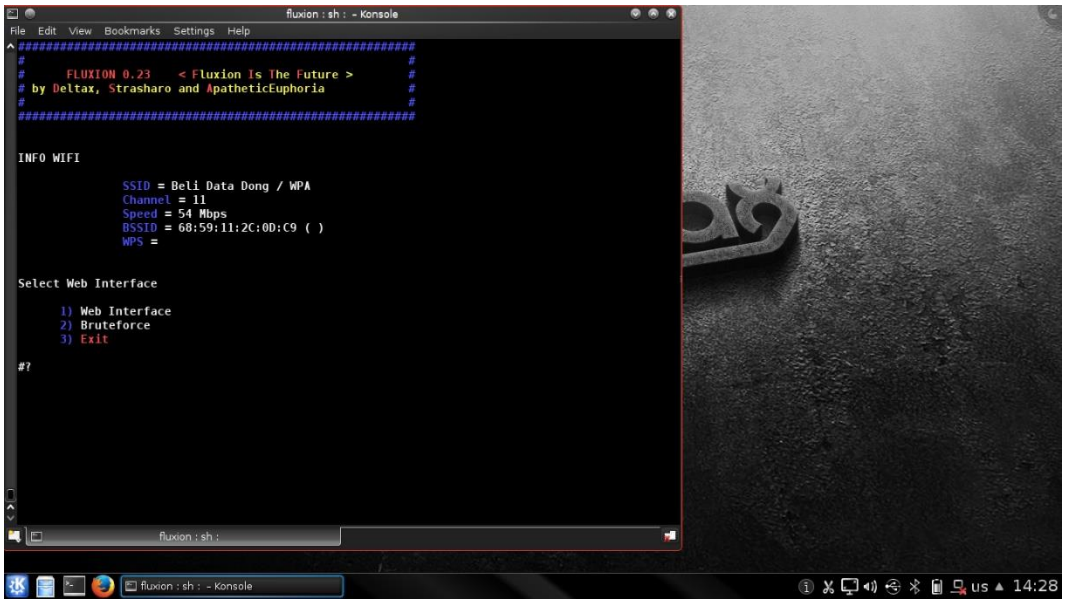

Gambar 28. Tampilan pemeriksaan *handshake*

Selain itu, aplikasi akan menampilkan opsi untuk merekam jabat tangan pada SSID *client* target dengan melakukan serangan mematikan. *Deauthentication (denial of service)* serangan dapat menyerang titik akses dan *client*. Tujuannya adalah untuk mencegah koneksi antara klien dan jalur akses. Pelaku memilih opsi pertama dengan melakukan serangan yang menghancurkan semua client yang terhubung dengan SSID target.



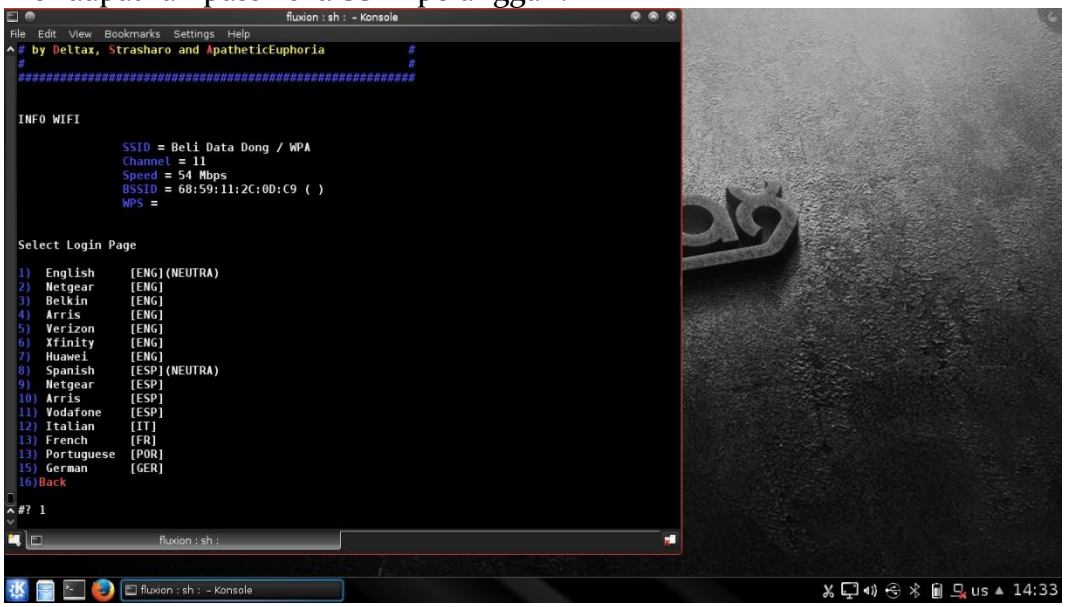

Gambar 29. Tampilan melakukan *capture handshake*

Setelah aplikasi *Fluxion* menerima handshake dari klien pada *SSID* target, maka aplikasi akan menampilkan antarmuka web untuk memilih jenis serangan untuk mendapatkan password SSID target, aplikasi menampilkan 2 jenis serangan, yaitu antarmuka *web* dan *brute force*. Penulis memilih cara 1 untuk mendapatkan *password SSID* dari *client*.



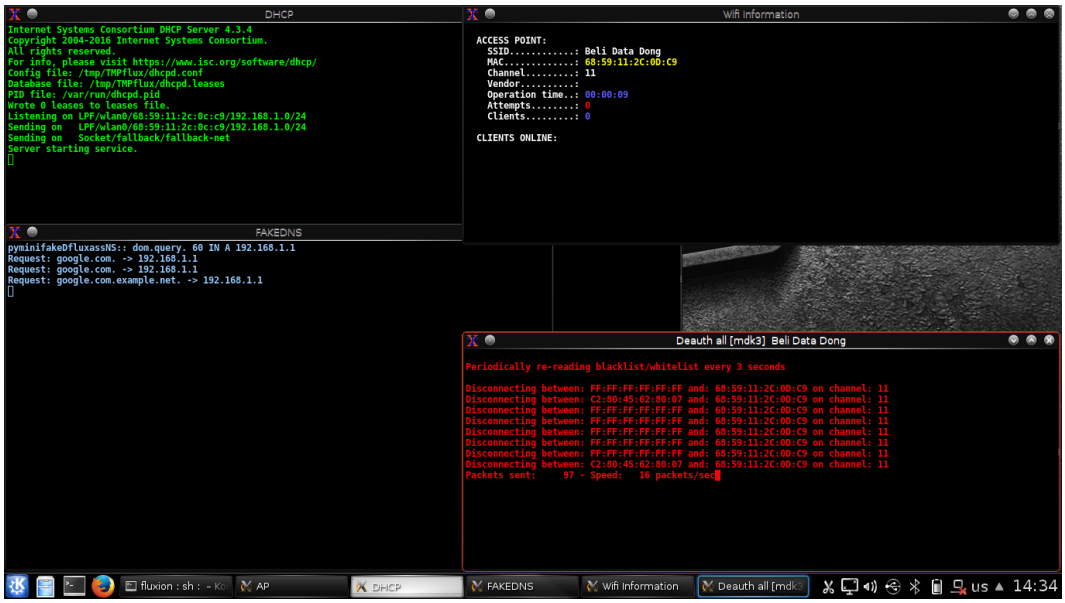

Gambar 30. Tampilan *web interface*

Selanjutnya, *Fluxion* akan menampilkan pilihan bahasa untuk halaman login palsu pada SSID target. Penulis memilih opsi bahasa 1, *Fluxion App* menyerang SSID pelanggan dengan cara phishing dengan menunjukkan *form login* palsu untuk mendapatkan password SSID pelanggan.

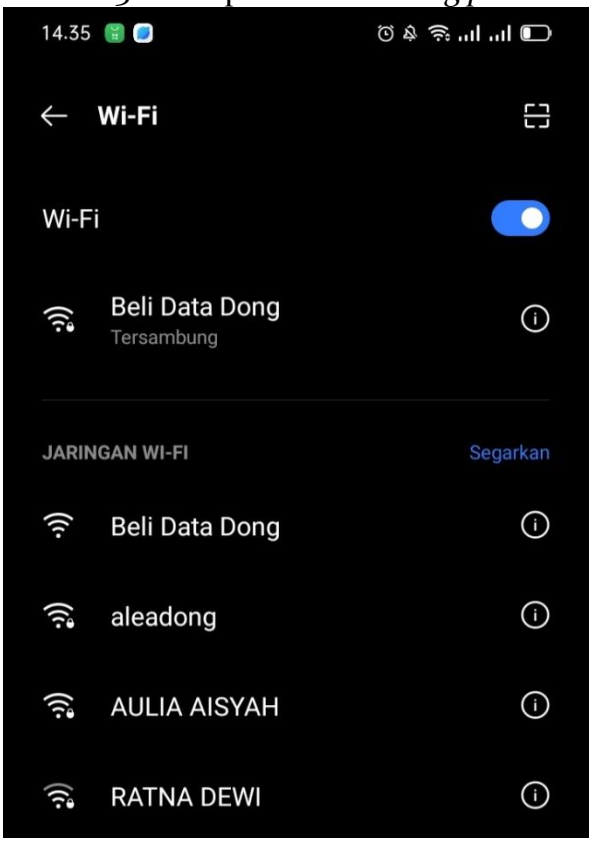



Gambar 31. Tampilan pemilihan Bahasa

Setelah memilih bahasa, aplikasi Fluxion menyerang klien dengan memutuskan sambungan dari SSID dan kemudian membuat SSID palsu dengan nama yang sama untuk mengelabui *Client*. *Client* tidak bisa connect padahal masih connect ke SSID asli, sehingga client terpaksa menggunakan SSID palsu untuk connect ke jaringan.

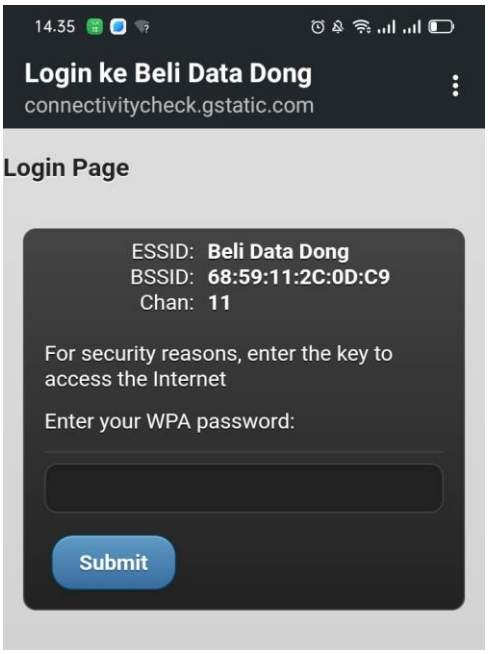



Gambar 32. Tampilan monitoring *password*



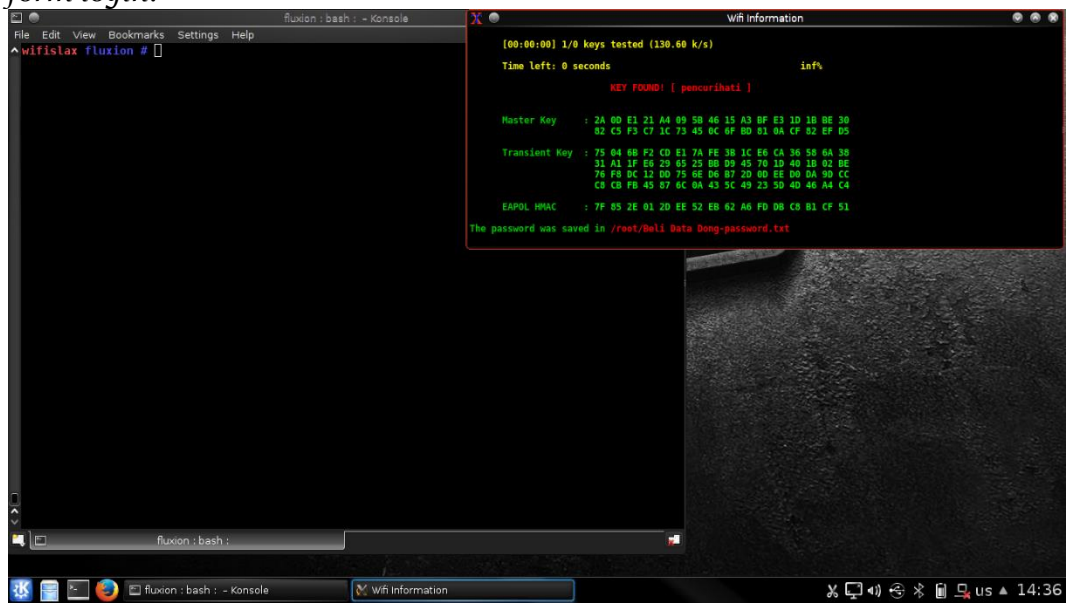

Gambar 33. Tampilan SSID palsu

Setelah *client* terhubung dengan SSID palsu smartphone client akan langsung diarahkan ke *browser* untuk melakukan login.




Gambar 34. Tampilan *form login* SSID palsu

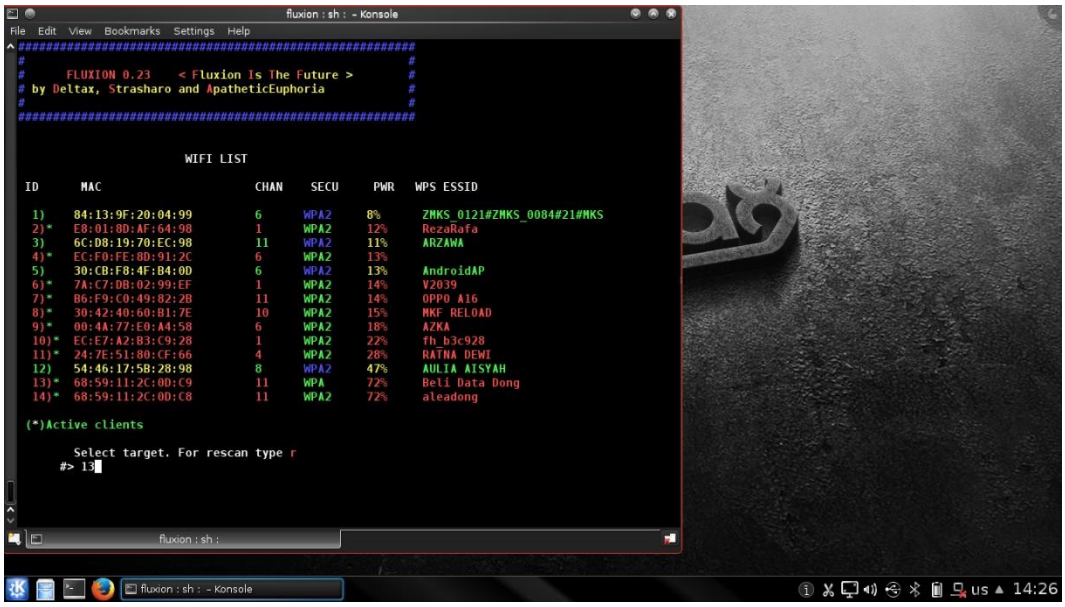
Setelah *client* memasukkan *password* aplikasi *fluxion* akan melakukan dekripsi pada wpa/psk untuk menampilkan *password* yang di isi oleh *client* sebelumnya pada *form login*.




Gambar 35. Tampilan *password* yang berhasil di dapatkan

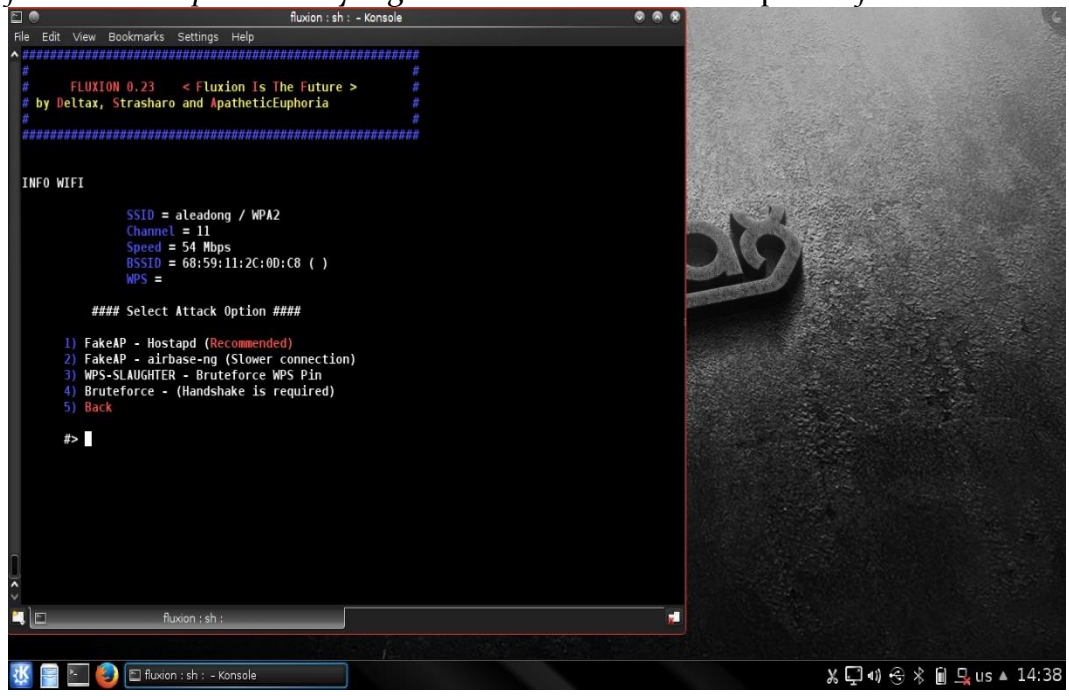
5. Melakukan *wifi crack* Jaringan *Wifi* yang Menggunakan Enkripsi *WPA2/PSK*

Setelah melakukan analisis pada enkripsi *password WPA/PSK,* kemudian penulis melakukan *cracking password* pada enkripsi *WPA2/PSK*. Langkah-langkahnya masih sama seperti sebelumnya, bedanya hanya SSID yang di-hack. Peneliti memilih SSID menggunakan enkripsi keamanan jaringan wpa2/psk dengan ID 14.



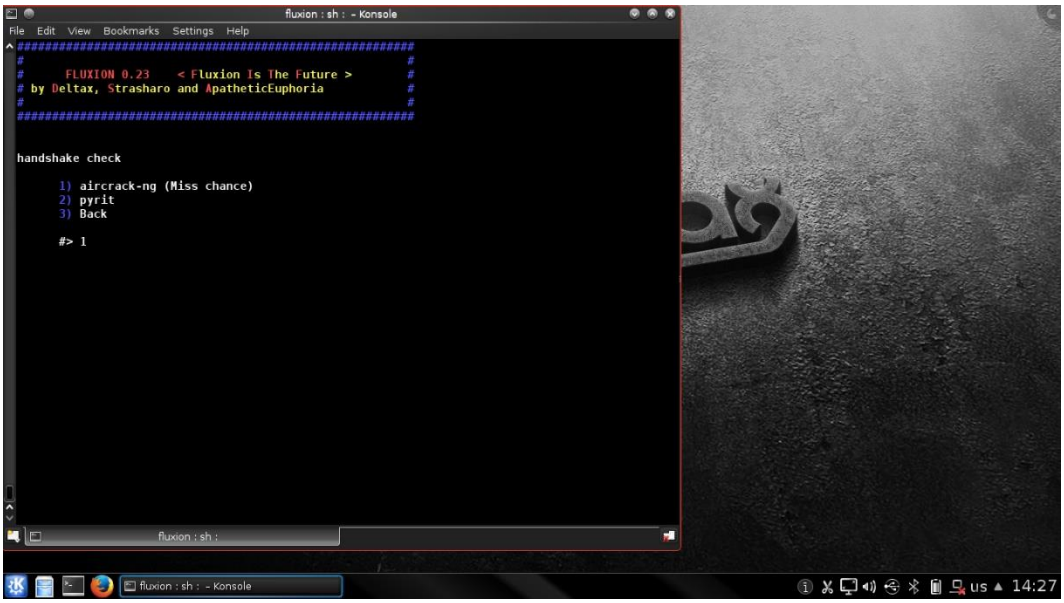

Gambar 36. Tampilan SSID setelah proses *scanning*

Kemudian aplikasi akan memberikan info *wifi* yang menjadi target antara lain: nama SSID, *channel* yang digunakan, kecepatan jaringan, *MAC address wifi* dan tipe eknripsi *password wifi*. Penulis memilih pilihan 1 sebagai tipe penyerangan dengan *fake-AP-Hotspat* sesuai yang direkomendasikan oleh aplikasi *fluxion*.



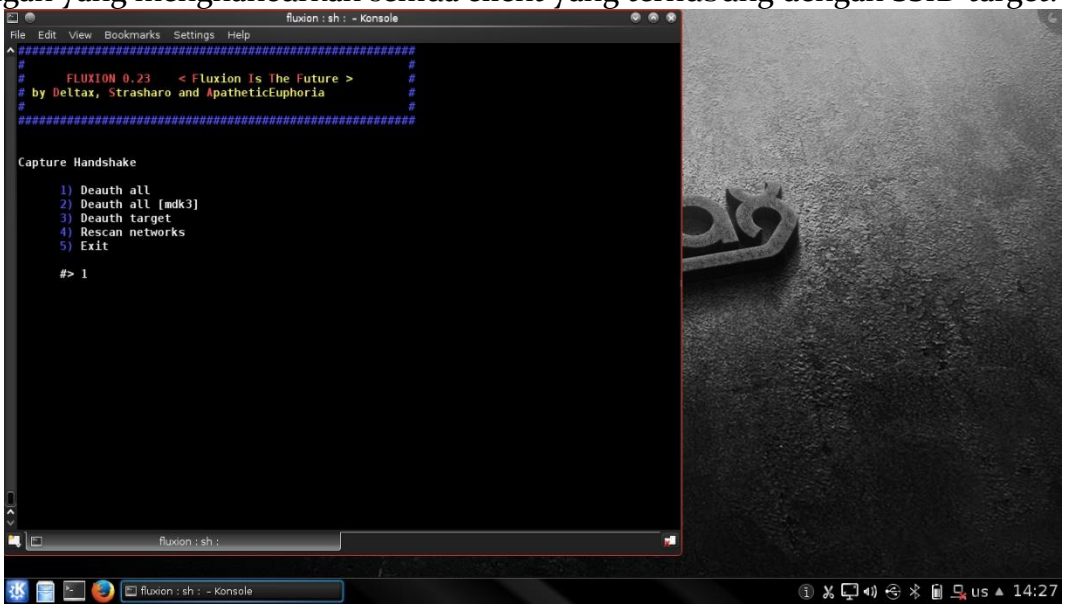

Gambar 37. Tampilan tipe penyerangan

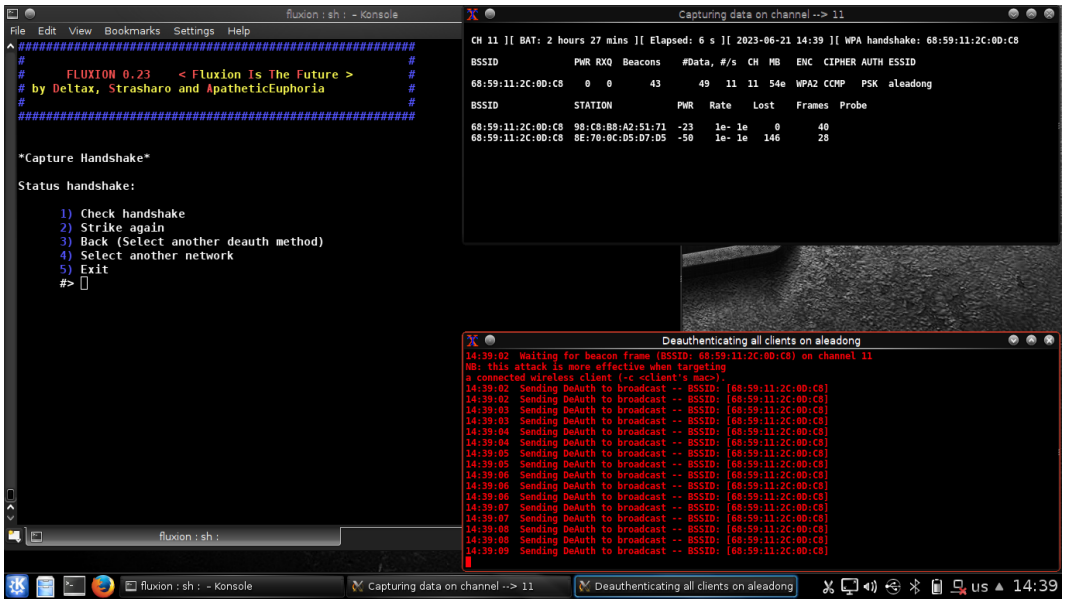
Tahap selanjutnya aplikasi akan memeriksa *handshake* pada jaringan target dengan menggunakan *aircack-ng* atau *pyrit*. Disini penulis memilih pilihan 1 untuk memeriksa *handshake* dari *wifi* target.




Gambar 38. Tampilan pemeriksaan *handshake*

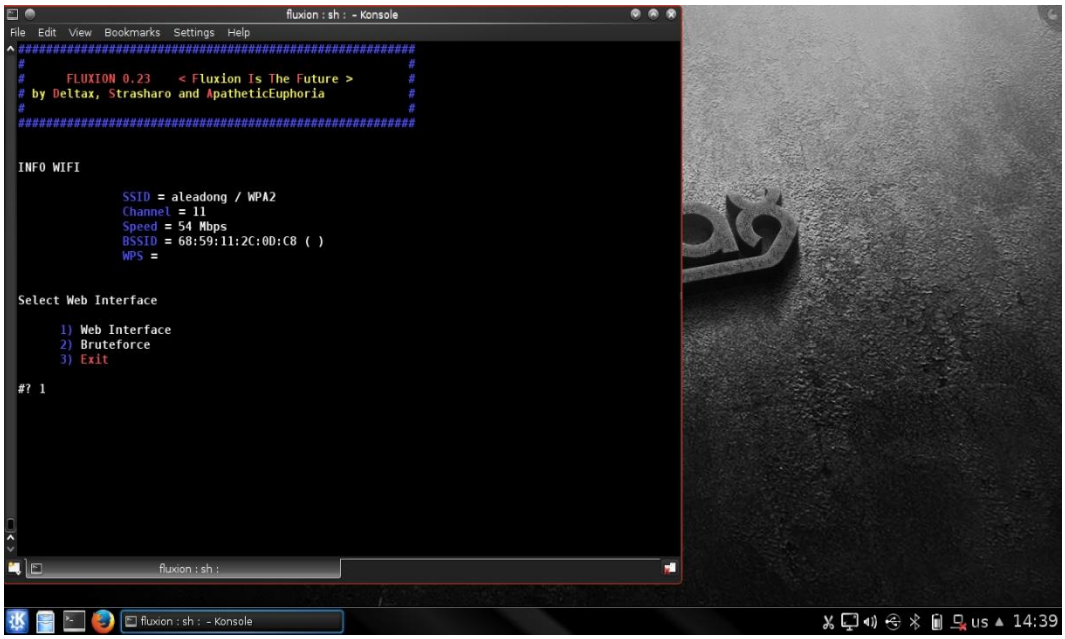
Selanjutnya aplikasi akan menampilkan pilihan menangkap *handshaske* pada *client* SSID target dengan melakukan *deauth attack*. *Deauthentication Attack* (*Denial of Service*) dapat menyerang titik akses dan klien. Tujuannya adalah untuk mencegah koneksi antara klien dan jalur akses. Pelaku memilih opsi pertama dengan melakukan serangan yang menghancurkan semua client yang terhubung dengan SSID target.





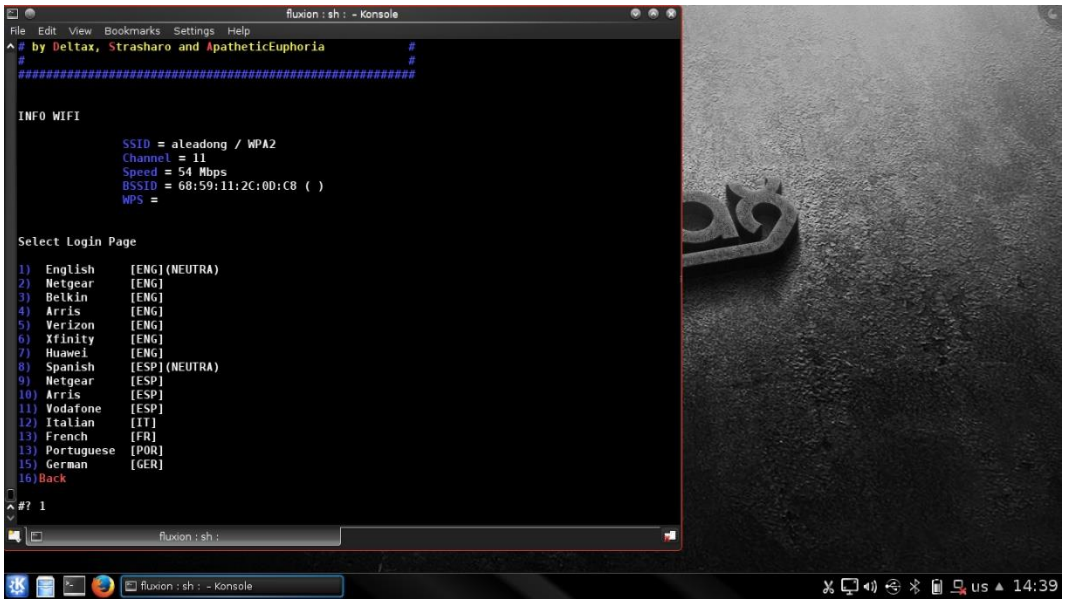

Gambar 39. Tampilan melakukan *capture handshake*

Setelah aplikasi *Fluxion* menerima handshake dari klien pada SSID target, maka aplikasi akan menampilkan antarmuka web untuk memilih jenis serangan untuk mendapatkan password SSID target, aplikasi menampilkan 2 jenis serangan, yaitu antarmuka *web* dan *brute force*. Penulis memilih cara 1 untuk mendapatkan *password* SSID dari *client*.



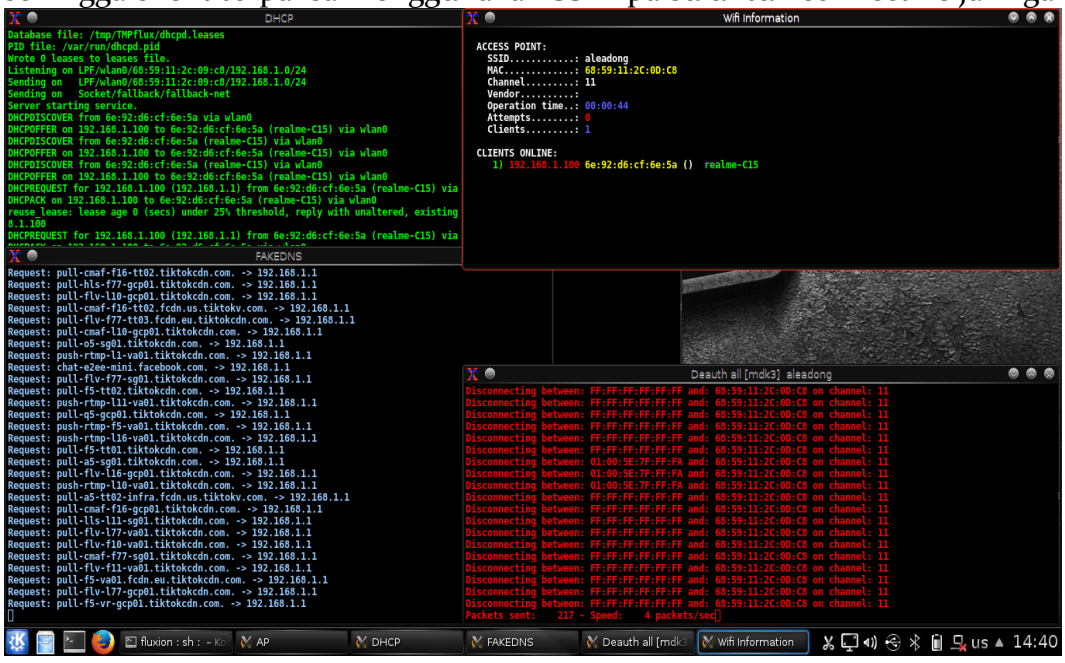

Gambar 40. Tampilan *web interface*

Selanjutnya, Fluxion akan menampilkan pilihan bahasa untuk halaman login palsu pada SSID target. Penulis memilih opsi bahasa 1, Fluxion App menyerang SSID pelanggan dengan cara phishing dengan menunjukkan form login palsu untuk mendapatkan password SSID pelanggan.

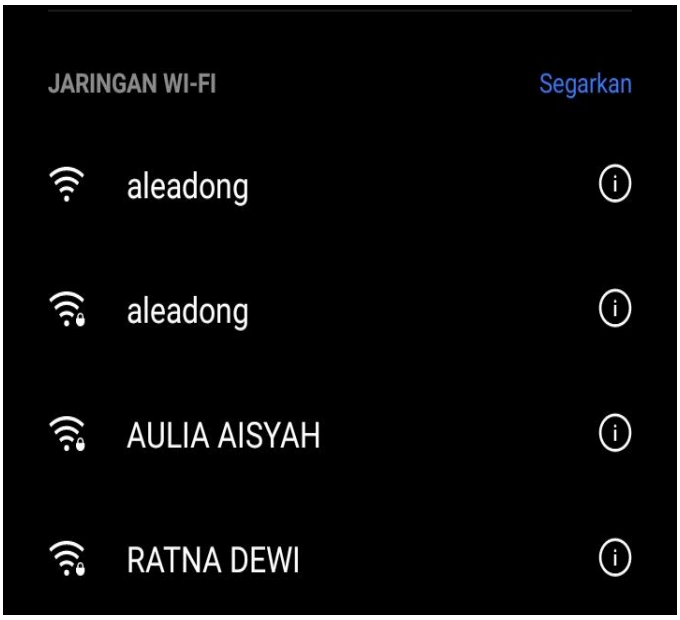



Gambar 41. Tampilan pemilihan Bahasa

Setelah memilih bahasa, aplikasi Fluxion menyerang klien dengan memutuskan sambungan dari SSID dan kemudian membuat SSID palsu dengan nama yang sama untuk mengelabui klien. Client tidak bisa connect padahal masih connect ke SSID asli, sehingga client terpaksa menggunakan SSID palsu untuk connect ke jaringan.

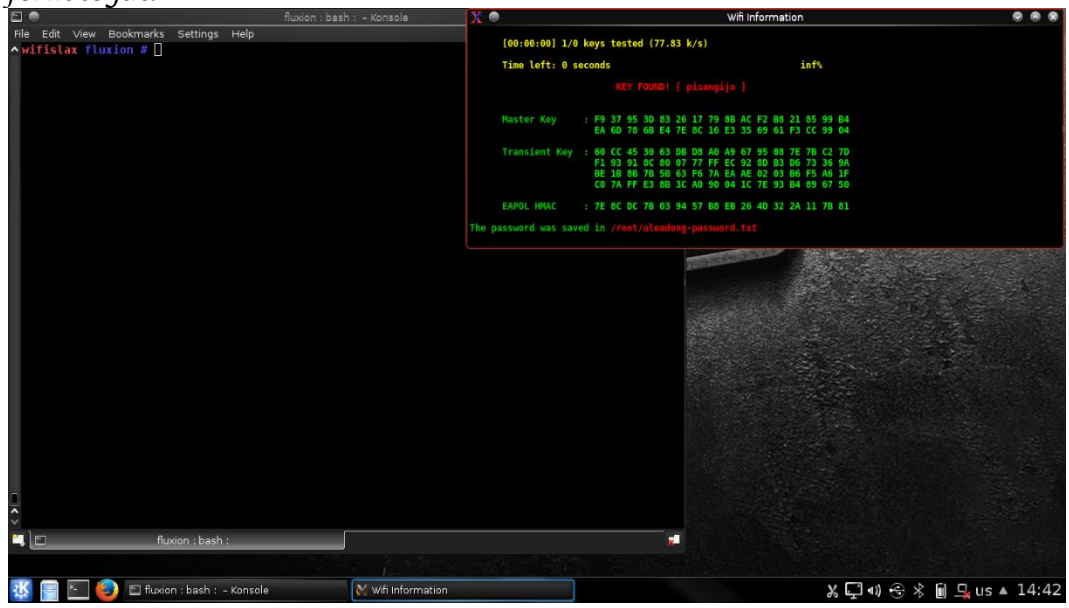



Gambar 42. Tampilan monitoring *password*




Gambar 43. Tampilan SSID palsu

Setelah *client* memasukkan *password* aplikasi *fluxion* akan melakukan dekripsi pada wpa/psk untuk menampilkan *password* yang di isi oleh *client* sebelumnya pada *form login*.




Gambar 44. Tampilan *password* yang berhasil di dapatkan

**SIMPULAN**

Berdasarkan hasil serangkaian kajian, analisis perbandingan keamanan jaringan wireless *WPA/PSK* dan *WPA2/PSK* di Puskesmas Tomoni Timur, terhadap pembentukan dan batasan masalah yang ada : Sistem keamanan jaringan wpa/psk dan wpa2/psk Puskesmas Tomoni Timur dapat dibobol, terbukti saat peneliti melakukan pengujian keamanan jaringan menggunakan aplikasi Fluxion. Pengujian sistem keamanan jaringan wpa/psk dan wpa2/psk di Puskesmas Tomoni Timur tidak dapat password karena human error tidak memahami dan tidak mengetahui jenis serangan yang ada pada *wireless*. Fungsi pengujian *black box* sistem yang diuji dapat berjalan

sesuai dengan yang diharapkan, validator dan pengguna. Peringkat validator anggota sangat baik.

## DAFTAR PUSTAKA

Alfaridzi,dkk. (2021). *Penerapan Arsitektur Industrial Pada Perancangan Showroom Dan Bengkel Mobil Toyota Di B Aceh*. Universitas Syiah Kuala. VOLUME 5, No.4, November 2021, hal 1719

Arkandiantika, I. dkk. 2019. Pengembangan Media Pembelajaran Virtual Reality pada Materi Pengenalan Termination dan Splicing Fiber Optic. Jurnal Dimensi Pendidikan dan Pembelajaran. Hal 29-36

Deanka (2021). Perancangan Ulang Interior Showroom Astra Internasional Daihatsu Kota Batam Dengan Pendekatan Brand Design Laporan Pengantar Karya Tugas Akhir. Universitas Telkom Bandung

Devansa, 2019. Analisi User Experience dan User *Interface* Menggunakan Metode Goms Analysis dengan Membandingkan Dua *Website ECommerce*. Yogyakarta

Dharma,dkk. (2022). *Penerapan ECommerce Terhadap Kinerja dan Pelaku Bisnis dalam Meningkatkan Penjualan Online*. Universitas Islam Negeri Sumatera Utara. Vol. 2 No. 2, Year [2022] Page 40554061

Kurniawan,dkk. (2022). *Pengaruh Pencahayaan pada* Showroom *Terhadap Kenyamanan Visual (Studi Kasus* Showroom *Harley Davidson, Bandung)*. , Universitas Kristen Maranatha, Bandung, Jawa Barat Indonesia. Volume 8 Nomor 1 (2022) halaman 612

Miarso. 2004. Menyemai Benih Teknologi Pendidikan. Jakarta: Prenadamedia Group.

Puspa, C dan Sudibya (2016). Analisis Preferensi Masyarakat dalam Pengelolaan Ekosistem Mangrove di Pesisir Pantai Kecamatan Loloda Kabupaten Halmahera Barat. Jurnal. Spasial Vol 6.No. 2,2019

Putri,dkk. (2023). *Rancang Bangun Sistem informasiToko KUD TaniJaya Kabupaten Madiun Berbasis Website*. Universitas PGRI Madiun. Vol.2, No.1Maret2023

Rahman, H. A., & Saputra, A. (2020). Perancangan Sistem Persediaan Barang Berbasis Java untuk Sistem Informasi Showroom dan Bengkel. *Jurnal Riset dan Aplikasi Mahasiswa Informatika (JRAMI)*, *1*(03), 430437.

Robani, A. M., Hadi, S., Nurdiawan, O., Dwilestari, G., & Suarna, N. (2021). Sistem Informasi Penjualan Motor Bekas Berbasis Android Untuk Meningkatkan Penjualan di Mokascirebon. Com. *JURIKOM (Jurnal Riset Komputer)*, *8*(6), 205212.

Safitri,dkk. (2021). *Pengaruh Penggunaan Aplikasi* Android *Berbantuan Appsgeyser.Com terhadap Hasil Belajar Siswa Pada Mata Pelajaran Ilmu Pengetahuan Sosial*. 2 IAIN Bengkulu, Indonesia. Volume 1, Nomor 1 (2021): Juni

Sugianto, L., Kriswinarso, T.B., Bachri S., Lihu, I. 2021. Pengembangan Perangkat Pembelajaran Matematika Berbasis Masalah Berorientasi pada Hasil Belajar Peserta Didik. Pedagogy. Volume 6 No. 2. (149-162)

Suwarti dan Catriwati (2022). *Aplikasi Pengingat Jadwal Dan Tugas Kuliah Berbasis* Android. Vol 6, No.1, April 2022