Analisis *Unauthorized Access Point* Menggunakan Teknik *Network Forensics*

Felicia Paramita[#1], Madeline[#2], Olga Alvina[#3], Rahel Esther Sentia[#4], Ade Kurniawan[#5]

[#]*Program Studi Teknik Informatika, Universitas Universal*

Kompleks Maha Vihara Duta Maitreya, Sungai Panas, Batam, Indonesia

[1]feliciaparamita1999@gmail.com

[2]30madeline18@gmail.com

[3]olgaalvina8@gmail.com

[4]rahelesther197@gmail.com

[5]ade.kurniawan@uvers.ac.id

Abstract— ***In this era, free access points are found available in various places. But this freedom comes with a price, and only a few users really understand the risk. In a recent survey, 70% of tablet owners and 53% of smartphone owners stated that they use public wifi hotspots. The biggest threat to public wifi security is how a hacker positions himself as a liaison between victims and Authorized Access Points. To do this the hacker creates an Unauthorized Access Point (Fake Access Point). We took a pen tester/attacker POV in this artikel for educational purposes, so that users may know the stages of Fake Access Point attack based on Kali Linux, Fluxion. For the digital evidence analysis stage, we used the customized OSCAR (Obtain information, Strategies, Collect Evidence, Analyze and Report) methods, where attacking is the stage for preparation, determining which wifi Access Points is going to be the target of the attack, and carrying out attacks. While, analysis is the stage of analyzing the steps of attack and how to distinguish between AAP and UAP. The results of our research are that after determining the target, the pen tester/attacker will use aircrack-ng on Fluxion to get a handshake, create a fake web interface, then launch a deauth all attack, also known as DoS, to AAP so that the victim / client cannot connect with the AAP and switch to Fake Access Point. The fake web interface will then ask the victim to enter the password, where after the password is found, the pen tester/attacker can see it through Fluxion. As a precautionary measure, the difference between a Fake Access Point and an Authorized Access Point is found in the presence or absence of the padlock symbol (Android) or an exclamation point (Windows 10).***

Keywords— ***Wireless network, Access Point, Unauthorized Access Point, fake access point attack, Fluxion.***

Abstrak— **Pada zaman ini, *free access point* telah tersedia di berbagai tempat. Namun, nyatanya kebebasan ini memiliki harga, dan hanya sedikit pengguna yang memahami benar risikonya. Ancaman terbesar terhadap kemanan *wifi* publik adalah bagaimana seorang *hacker* memposisikan dirinya sebagai penghubung antar korban dan *Authorized Access Point*. Untuk melakukan hal tersebut, *hacker* membuat *Unauthorized Access Point* (*Fake Access Point*). Dalam artikel ini *pen tester/attacker* diambil sudut pandang sebagai dengan tujuan edukasi, agar pengguna mengetahui tahapan serangan *Fake Access Point* dengan *tool Fluxion* berbasis OS Kali Linux. Tahapan analisis bukti digital menggunakan metode OSCAR (*Obtain Information*, *Strategies*, *Collect Evidence*, *Analyze and Report*) yang telah di kostumisasi, di mana *attacking* adalah tahapan untuk persiapan menentukan target *wifi Access Point* yang akan diserang serta menjalankan serangan. *Analysis* adalah tahapan menganalisa langkah penyerangan serta bagaimana cara membedakan *Authorized Access Point* dengan *Unauthorized Access Point*. Hasil penelitian yang dilakukan setelah menentukan target, *pen tester/attacker* akan menggunakan Aircrack-ng pada *Fluxion* untuk mendapatkan *handshake*, membuat *web interface* palsu, kemudian melancarkan serangan *Deauth all*, dikenal DoS ke AAP, sehingga korban/*client* tidak dapat terkoneksi dan masuk ke *Fake Access Point*. *Web interface* palsu kemudian akan meminta korban untuk memasukkan *password*. Setelah *password* ditemukan, maka *pen tester/attacker* dapat melihatnya melalui *Fluxion*. Sebagai langkah pencegahan, perbedaan antara *Fake Access Point* dan yang *Authorized Access Point* ditemukan pada ada tidaknya simbol gembok (Android) atau tanda seru (Windows 10).**

Kata Kunci— ***Wireless network, Access Point, Unauthorized Access Point,* serangan *Fake Access Point, Fluxion.***

I. PENDAHULUAN

Saat ini perangkat *wifi*, telah diintegrasikan ke dalam kehidupan kita sehari-hari karena memudahkan perangkat untuk saling terhubung ke jaringan Internet. Umumnya, terdapat dua jenis jaringan utama yaitu, *wired* dan *wireless* (Wireless Fidelity) [1]. *Internet traffic* saat ini berada dalam evolusi secara berkelanjutan. Sebagaimana dinyatakan oleh Cisco VNI IP *traffic forecast* 2017, lalu lintas IP global tahunan akan mencapai 3,3 Zettabytes (ZB) pada tahun 2021 [2]. Selain itu, jumlah perangkat yang terhubung ke Internet akan mencapai lebih dari tiga kali lipat, seperti: perangkat medis, mobil otonom, aset rumah, dan lain-lain [2].

Jumlah *wifi Access Point* telah berkembang dengan pesat. Namun, diikuti oleh kelemahan dari sisi keamanan *wifi* seperti: *Reconnaissance Attacks* [3], DoS *Attacks* [4], *Authentication Attacks* [5], WEP *Keystream and Plaintext Recovery* [6], *Attacks on* EAP *Protocols* [7], *Rogue Aps* [8]. Selanjutnya, menjamurnya *hotspot* (*public access point*) memberi kemudahan bagi perangkat *mobile*. Namun, banyak

ditemui penyalahgunaan *Fake Access Point* di tempat umum, di mana penyebaran *malware* dalam jaringan *wifi* menjadi ancaman utama [9]. Banyak korban (terutama para pengguna *smartphone*) dapat mengakses koneksi "*hotspot*" internet nirkabel *wifi* di tempat umum dengan lebih mudah. Mereka menjadi lebih rentan terhadap penipuan dan pencurian identitas, yang disebut sebagai serangan *Malicious*. *Fake Access Point* atau *Evil Twin* adalah istilah untuk *access point wifi* jahat, di mana ia meniru nama jaringan *wifi* asli yang ditawarkan dari tempat itu, tetapi ia sebenarnya telah dibuat oleh peretas untuk menyadap komunikasi nirkabel di antara peselancar internet.

Sinyal *wifi* dapat dengan mudah dihubungkan ke jaringan dan mengendus informasi menggunakan *Fake Access Point*. *Fake AP* adalah jalur akses tidak sah yang terhubung ke jaringan perusahaan yang menimbulkan ancaman keamanan serius [1]. *Unauthorized access point* adalah ancaman keamanan paling signifikan untuk *wireless* LAN karena melibatkan pemasangan titik akses eksternal dan tidak sah [10]. Dari berbagai jenis, ada tiga gaya serangan yang umum yang mencakup titik akses ilegal adalah serangan *Man in the Middle*, *Ad Hoc Wireless Clients*, dan *Rogue Access Points*.

1. Man-in-The-Middle (MiTM). Ini adalah serangan yang melibatkan musuh dan dua pihak yang percaya bahwa mereka berkomunikasi secara langsung satu sama lain, tetapi dalam skenario nyata ini tidak benar.

2. Ad Hoc Wireless Network. Jaringan nirkabel yang dibentuk antara dua korban disebut jaringan *wireless* ad hoc. Ia juga dikenal sebagai IBSS (*Independent Basic Service Set*). Jaringan ini dapat dibentuk oleh musuh dengan korban tepercaya yang mengakibatkan kebocoran pesan pribadi.

3. Rogue Access Points. *Rogue Access Points* "*the silent killer*" adalah salah satu ancaman keamanan paling berbahaya yang kadang-kadang disebut sebagai *Fake Access Point*. Ini adalah *wireless access point*, pengaturan pada jaringan yang andal tanpa izin dari administrator jaringan dan memanfaatkan teknik pemilihan titik akses otomatis konvensional untuk menyulap korban nirkabel agar terhubung dengan *Rogue Access Point* ini [10].

Dalam makalah ini akan dibahas bagaimana *Unauthorized Access Point*, khususnya *Rogue Access Point* (*Fake Access Point*), bekerja dan dianalisis dengan pendekatan *Network Forensic* menggunakan metode OSCAR. *Network Forensics,* yang merupakan ilmu yang berhubungan dengan penangkapan, rekam, dan analisis lalu lintas jaringan [11]. Dalam artikel ini dianalisis bagaimana cara kerja *Fluxion* dalam membuat *Fake Access Point*. Metode yang dipilih adalah OSCAR karena metode ini sesuai dengan kebutuhan, yaitu jaringan dan metode dikustomisasi ini menjadi lebih sederhana sesuai dengan kebutuhan pengerjaan artikel ini. *Attacking* adalah tahapan untuk persiapan, menentukan target *wifi Access* Point yang akan diserang serta menjalankan serangan. *Analysis* adalah tahapan menganalisa langkah penyerangan serta bagaimana cara membedakan *Authorized Access Point* dengan *Unauthorized Access Point*.

Hasil dari penelitian ini, *Fluxion* memiliki atau merupakan kumpulan dari *tools* yang digunakan untuk membuat *Fake Access Point*. Setelah melakukan *monitoring* seluruh *channel* di sekitar dan menentukan *access point target* yang memiliki klien yang akan diserang, *pen tester/attacker* melakukan *handshaking* untuk mengenal *access point* yang akan ditiru. Dengan *deuth all*, *access point* yang asli akan *down* dan korban tidak dapat terhubung. *Pen tester/attacker* akan membuat *web interface* palsu dengan *Fluxion* untuk meyakinkan korban agar memasukkan *password* ke *Fake Access Point* sehingga *pen tester/attacker* mendapatkan *password* dari korban.

Untuk mempermudah khalayak umum memahami bagaimana proses berlangsungnya penelitian ini *literature review* dimuat dalam *section* II dan kemudian di *section* III akan dijelaskan mengenai perangkat keras dan lunak beserta metode yang akan digunakan. Selanjutnya, di *section* IV akan disampaikan secara mendalam hasil penelitian ini. Terakhir, di *section* V akan disimpulkan hasil penelitian beserta saran tentang *Fake Access Point*.

II. METODOLOGI

A. Previous Work

Baihaqi1, Yeni Yanti, dan Zulfan [12] dalam artikelnya membahas bahwa dewasa ini penggunaan perangkat teknologi jaringan Wifi sudah berkembang luas di seluruh dunia, baik digunakan untuk komunikasi suara maupun data. Jaringan Wifi memanfaatkan frekuensi tinggi untuk menghantarkan dan menghubungkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh *user* maupun oleh operator yang memberikan layanan komunikasi. Namun, dengan adanya *user* yang memanfaatkan teknologi jaringan Wifi, maka dapat memberikan sedikit celah keamanan yang dapat dimanfaatkan oleh penyerang. Penyerang dapat mengetahui *password* keamanan WPA2-PSK pada saat *user* terhubung ke jaringan Wifi tersebut. *Password* dihasilkan melalui beberapa teknik dan pengujian yang digunakan, di antaranya dengan memanfaatkan *user* yang terhubung ke jaringan Wifi, pengujian SSID palsu, dan pengujian WPS PIN. Namun, pada penelitian ini hanya dilakukan pengujian melalui *user* yang terhubung ke jaringan Wifi. Teknik dan pengujian ini semata-mata dilakukan untuk penetrasi terhadap keamanan jaringan *wifi* yang bertujuan untuk mengetahui *password* WPA2-PSK pada jaringan WiFi serta untuk menambah wawasan tentang keamanan jaringan WiFi. Dalam artikel tersebut, kelemahan yang ditemukan kurang dijelaskan secara detail mengenai istilah-istilah yang terdapat dalam *software Fluxion* tersebut. Selain itu, penelitian tersebut tidak menggunakan Wireshark untuk memantau perubahan jaringan serta tidak adanya perbedaan dari *Authorized Access Point* dengan *Unauthorized Access Point*.

Fabian Lanze, Andriy Panchenko, Ignacio Ponce-Alcaide, dan Thomas Engel [13] dalam artikelnya berbicara tentang penggunaan *hotspot wifi* publik telah menjadi rutinitas umum dalam kehidupan kita sehari-hari. Wifi publik menawarkan konektivitas cepat dan dengan anggaran yang ekonomis untuk

berbagai perangkat klien. Namun, *wifi* publik juga dapat menyebabkan ancaman keamanan yang parah karena pengidentifikasi 802.11 (SSID, BSSID) dapat dengan mudah dipalsukan. *Hacker* dapat membuat *Evil Twin*, yaitu *access point* (AP) pengguna sulit membedakan AP sah. Setelah pengguna terhubung ke Evil Twin, secara tidak sengaja membuat taman bermain untuk berbagai serangan, seperti pengumpulan data sensitif (misalnya informasi kartu kredit, kata sandi) atau serangan manusia di tengah, bahkan pada trafik yang dienkripsi. Celah keamanan ini sangat mengkhawatirkan dan menyebabkan pengembangan beberapa alat yang tersedia secara bebas, mudah digunakan, dan memungkinkan pemasangan serangan dari perangkat klien komoditas, seperti laptop, *smartphone*, atau tablet tanpa menarik perhatian. Dalam makalah ini diberikan ikhtisar terperinci dari alat yang telah dikembangkan (atau dapat disalahgunakan) untuk mengatur AP kembar. Pemeriksaan secara menyeluruh untuk mengidentifikasi karakteristik yang memungkinkan pembedaan dari AP berbasis perangkat keras yang sah. Dalam analisis ini ditemukan metode yang lebih tinggi untuk mendapatkan perangkat lunak berbasis perangkat lunak. Kesalahan ini mengeksploitasi kelemahan akibat persaingan perilaku perangkat keras atau kekhasan perangkat keras *wifi* klien yang dioperasikan. Evaluasi terhadap 60 AP perangkat keras dan berbagai alat pada *platform* yang berbeda mengungkapkan potensi besar untuk deteksi yang dapat diandalkan. Selanjutnya, metode yang digunakan dalam penelitian ini dapat membentuk perangkat keras klien yang khas dalam waktu singkat, tanpa menyambung ke jalur akses yang berpotensi tidak dapat dipercaya. Kelemahan dari penelitian ini ialah para pengguna perangkat tidak dapat membedakan *Authorized Access* Point, namun juga tidak memaparkan bagaimana cara membedakan Authorized *Access Point* dengan *Unauthorized Access Point* agar pengguna dapat menghindari jenis serangan ini.

HyunHo Kim, Young-Jin Kang, Ndibanje Bruce, SuHyun Park, dan HoonJae Lee [14] dalam artikelnya mengatakan bahwa perangkat *smartphone* generasi terkini dapat melakukan semua hal yang mungkin hanya dapat dilakukan dengan perangkat keras khusus. Dengan jaringan 3G dan 4G dapat terhubung ke jaringan data kapan saja dan di mana saja sesuai kebutuhan. Namun, ada batasan berapa banyak data jaringan yang diizinkan, sehingga sebagian besar pengguna perangkat *smartphone* cenderung terhubung ke jaringan *wifi* yang tidak mengkonsumsi paket data mereka. Meskipun *wifi* memiliki manfaat ekonomi, dibandingkan dengan jaringan kabel, masih ada banyak risiko keamanan, seperti menangkap atau mengubah data jaringan. Ada banyak kasus di mana penjahat pencurian identitas menggunakan jalur akses *wifi* yang tidak sah untuk memikat orang agar memberikan informasi pribadi mereka. Dalam makalah tersebut, *access point wifi* yang tidak sah digunakan untuk mensimulasikan kasus di atas dan membandingkan dengan kasus yang menggunakan *access point* resmi. Dalam kasus yang diangkat dalam penelitian ini, mengenai *Unauthorized wifi access* point, tidak ditemukan langkah-langkah terperinci dan jenis *software* yang digunakan untuk menyerang.

B. Forensik

Network forensics adalah ilmu yang berhubungan dengan penangkapan, rekam, dan analisis lalu lintas jaringan. Data lalu lintas jaringan ditangkap menggunakan *packet sniffers*, *alert*, dan *log* yang dikumpulkan dari alat keamanan jaringan yang ada. Data ini dianalisis untuk karakterisasi serangan dan diselidiki untuk melacak kembali pelanggarnya.

Network forensics mengurangi dan menyederhanakan waktu pemantauan, pelaporan, analisis, dan remediasi yang dibutuhkan untuk mempertahankan diri dari serangan. Ini membantu penuntutan melalui bukti yang secara forensik lengkap dan memberikan pemahaman tentang akar penyebab pelanggaran keamanan untuk memungkinkan respons yang cepat, cerdas, dan efektif untuk mencegah kejadian bencana dan risiko berkelanjutan. Hal ini memungkinkan untuk perbaikan setelah pelanggaran terjadi melalui kemampuan untuk memutar ulang serangan jaringan [11].

C. Konten Utama

Tahap persiapan dimulai dengan pengaturan perangkat keras dan perangkat lunak yang akan digunakan dalam penelitian ini. Pada tahap persiapan uji coba analisis *Unauthorized Access Point* terdapat lima perangkat keras yang digunakan, di mana perangkat keras tersebut dapat dilihat pada Tabel I. Spesifikasi dari perangkat keras yang digunakan saat uji coba berlangsung dapat dilihat pada Tabel II. Tabel III menunjukkan enam *software* yang digunakan dalam proses uji coba.

Analisis *Unauthorized Access Point* menggunakan metode OSCAR (*Obtain Information, Strategies, Collect Evidence, Analyze and Report*). Metode ini sesuai dengan yang dibutuhkan. Metode ini dikustomisasi menjadi lebih sederhana sesuai dengan kebutuhan pengerjaan artikel, seperti yang ditunjukkan pada Gambar 1 dengan penjelasan sebagai berikut:

1) Attacking

Ada beberapa jenis serangan dalam *Unauthorized Access Point*. Salah satunya adalah *Fake Access Point*. *Fake Access Point* digunakan untuk meniru *Authorized Wifi Access Point* dan menyebabkan *access point* tersebut menjadi *down*. Korban tidak akan dapat menggunakan *access point* tersebut dan beralih ke *Fake Access Point*.

TABEL I
PERANGKAT KERAS

Perangkat	Jenis Perangkat Keras	MAC Address	Peran
Client 1	laptop	-	*attacker*
Client 2	adapter	b0:4e:26:69:ac:f0	*attacker*
Client 3	*smartphone*	-	*victim*
Client 4	*router*	B0:4E:26:69:A0:F0	*victim*
Client 5	laptop	-	*victim*

Berdasarkan Gambar 2, persiapan pertama yang harus dilakukan adalah mencari lokasi yang memiliki banyak *wifi access point*. *Pen tester/attacker* akan menargetkan salah satu *access point* yang memiliki jarak jaringan yang dekat dan kuat. Selanjutnya, *pen tester/attacker* menggunakan *Fluxion* untuk membuat *Fake Access Point* dan memperoleh *password* dari korban.

2) Analysis

Analisis yang kami lakukan bertujuan untuk memberikan wawasan kepada *user* mengenai perbedaan *Fake Access Point* dengan *Authorized Access Point*. Dalam penelitian ini ditunjukkan tahapan penyerangan *Fake Access Point* dengan *Fluxion 2* untuk mendapatkan *password* dari korban yang pernah terhubung dengan *Wifi Authorized Access Point*.

TABEL II
SPESIFIKASI PERANGKAT KERAS

Perangkat	Jenis Perangkat Keras	Spesifikasi
Client 1	laptop	Intel (R) Core (TM) i7-7700HQ CPU @2.80GHz ~2.81GHz, 16GB RAM, 128GB SSD, Intel (R) HD Graphics 630 Card.
Client 2	adapter	TP-LINK TL-WN7200ND, 150 Mbps data transfer rate, 16 QAM, 64 QAM, CCK, OFDM Line Coding Format, DSSS, FHSS Spread Spectrum Method, Ad-Hoc Mode, *wifi* Protected Setup (WPS) Features, TP-Link Technologies Manufacturer.
Client 3	*smartphone*	POCOPHONE F1, M1805E10A model, Octa-core Max 2.8GHz, 6GB RAM, 128GB internal memory.
Client 4	*router*	AC1350 High Power Wireless Dual Band Router Archer C58HP, 450Mbps on the 2.4GHz *wifi* band and 867Mbps on the 5GHz band, high gain external antennas, increased output power of up to 1000mw*1, coverage – Up to 10,000 Square Feet*2.
Client 5	laptop	Intel (R) Core (TM) i7-7700HQ CPU @2.80GHz ~2.81GHz, 16GB RAM, 128GB SSD, Intel (R) HD Graphics 630 Card.

TABEL III
PERANGKAT LUNAK

Perangkat	Jenis Perangkat Lunak	Peran
Client 1	Kali Linux 2019.3	*attacker*
Client 2	*Fluxion* 2	*attacker*
Client 3	VMware Workstation 15 Player	*attacker*
Client 4	Android versi 6.0.1	*victim*
Client 5	Windows 10	*victim*
Client 6	Wireshark	*attacker*

III. HASIL DAN PEMBAHASAN

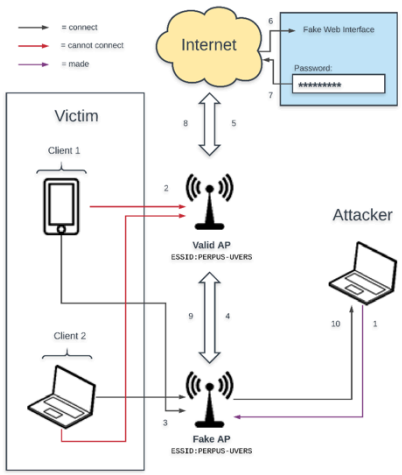
Penelitian ini berfokus pada langkah-langkah dalam penyerangan menggunakan *Fake Access Point* dengan perangkat lunak *Fluxion 2*.

A. Langkah Penyerangan

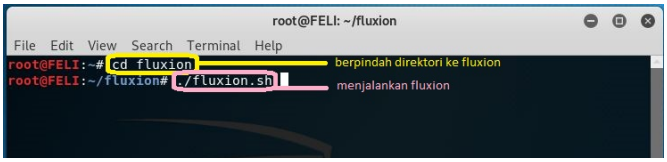
Langkah pertama dimulai dengan menjalankan sistem operasi *Kali Linux*. Dalam penelitian ini digunakan *VMware* untuk menjalankan *Kali Linux* tersebut. Selanjutnya, membuka terminal untuk memberi perintah berpindah ke direktori (*cd*) *Fluxion*. Perintah tersebut memberi tahu *shell* untuk menjalankan *file Fluxion*.sh yang terletak di direktori saat ini. Setelah berhasil menjalankan *Fluxion*, langkah selanjutnya adalah memilih bahasa yang dikehendaki (Gambar 4).

Setelah memilih bahasa, terlihat pada Gambar 3, dengan perintah (cd) *Fluxion*.sh memilih *channel*. *Channel* adalah saluran khusus untuk menyiarkan masing-masing *access point*, sehingga tidak terjadi gangguan antar *access point* yang berada pada jarak dekat. *All channels* akan menunjukkan seluruh *channel* yang ada di sekitar, seperti yang terlihat pada Gambar 5. Di sisi yang lain, menu *Specific Channel(s)* akan memberikan pilihan kepada *pen tester/attacker* untuk memilih satu spesifik *channel*. Dalam hal ini, diambil perintah 1 (*all channel*), seperti terlihat pada Gambar 6.

Gambar 1 Metodologi OSCAR



Gambar 2 Serangan *Fake Access Point*



Gambar 3 Terminal *Kali Linux*

Pada Gambar 6, target *access point* dengan ESSID: perpus-uvers, Auth: PSK, Cipher: CCMP, ENC: WPA2, MB: 405, Ch: 11, #/s: 0, #Data: 0, *Beacons*: 4, Pwr: -54, BSSID: B0:4E:26:69:A0:F0. Contohnya, apabila *pen tester/attacker* memilih *channel* nomor 1, maka *Fluxion* akan menampilkan seluruh *access point* dengan *channel* 1 saja. Setelah memilih *all channel*, maka *Fluxion* akan menampilkan jendela *wifi* monitor. Masing-masing keterangan dari setiap *access point* akan ditunjukkan per barisnya, dengan penjelasan sebagai berikut:

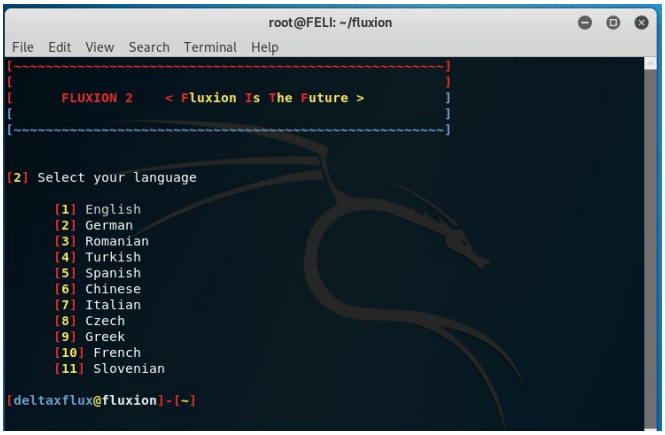
1) BSSID (*Basic Service Set IDentifier*) menunjukkan MAC *address* untuk setiap *access point*. Setiap perangkat jaringan memiliki MAC *address*-nya masing-masing.

2) Pwr atau *power* menunjukkan seberapa jauh access point tersebut dari adapter kita. Semakin besar angka negatifnya maka access point tersebut semakin jauh jaraknya.

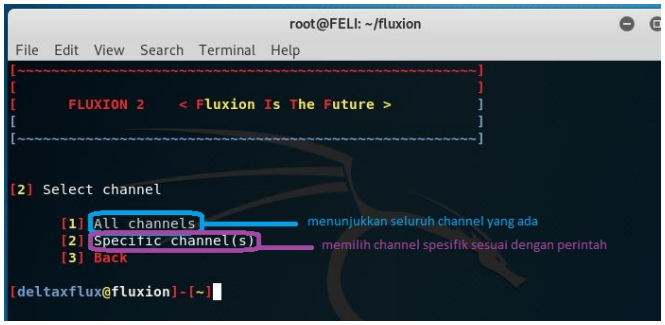
3) *Beacons* menunjukkan sinyal yang dikirim oleh *access point* untuk memberitahu keberadaannya kepada setiap perangkat.

4) #Data menunjukkan jumlah dari paket-paket berguna yang telah di sadap.

5) *#/s* menunjukkan jumlah dari paket data yang telah dikumpulkan selama 10 detik terakhir.



Gambar 4 *Fluxion 2* (pemilihan bahasa)



Gambar 5 *Fluxion 2* (*channel*)

6) Ch atau *channel* menunjukkan jumlah dari *channel* yang disiarkan oleh *access point* tersebut.

7) MB menunjukkan kecepatan maksimum yang didukung oleh *access point* tersebut.

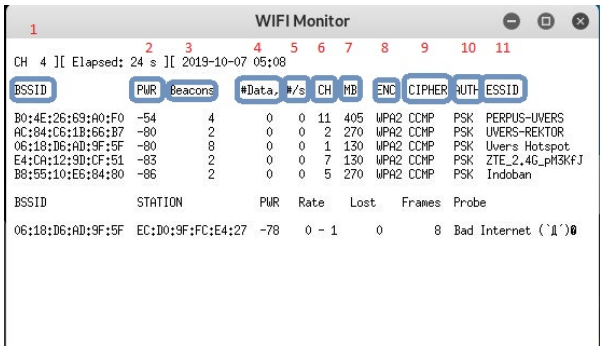
8) ENC atau *encryption* menunjukkan jenis enkripsi yang digunakan oleh *access point* tersebut.

9) Cipher menunjukkan jenis sandi yang digunakan untuk mendekripsi paket-paket tersebut.

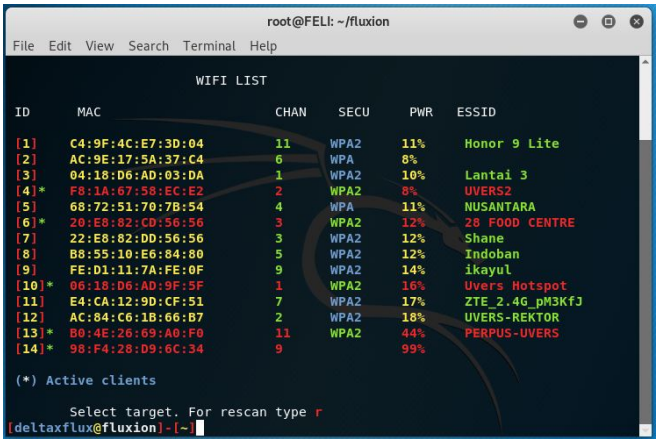
10) Auth atau *authentication* menunjukkan tipe autentikasi yang dibutuhkan untuk *access point*.

11) ESSID (*Extended Service Set IDentifier*) menunjukkan nama dari *access point* tersebut.

Setelah mendapatkan data yang diberikan *wifi monitor* dan menargetkan sebuah *access point*, maka *pen tester/attacker* mengakhiri *monitoring* dengan `ctrl+c`. Setelah *Fluxion* menampilkan *wifi list*, *pen tester/attacker* akan memilih target *Fake Access Point*. *Pen tester/attacker* sebaiknya memilih *access point* yang memiliki presentase *power* yang lebih tinggi dan memiliki korban yang aktif. Pada Gambar 7 dapat dilihat bahwa *access point* yang memiliki korban aktif ditandai dengan simbol bintang di samping ID-nya. Apabila tidak ada *access point* yang sesuai dengan kehendak, maka *pen tester/attacker* dapat me-*rescan* ulang *wifi* list dengan mengetik '`r`' lalu `enter`.



Gambar 6 *Wifi* monitor

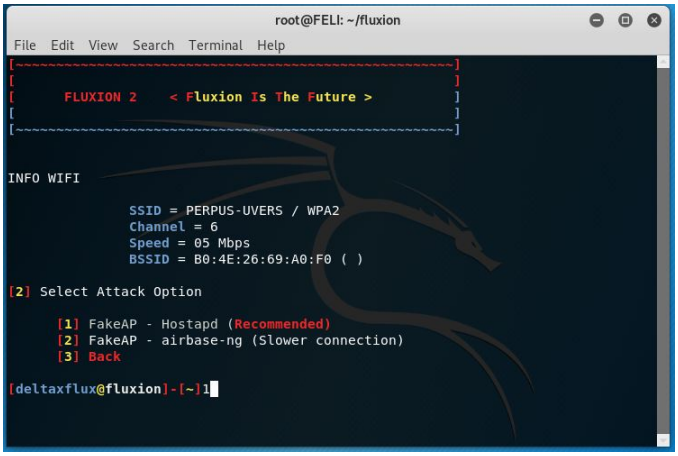


Gambar 7 *Access Point list*

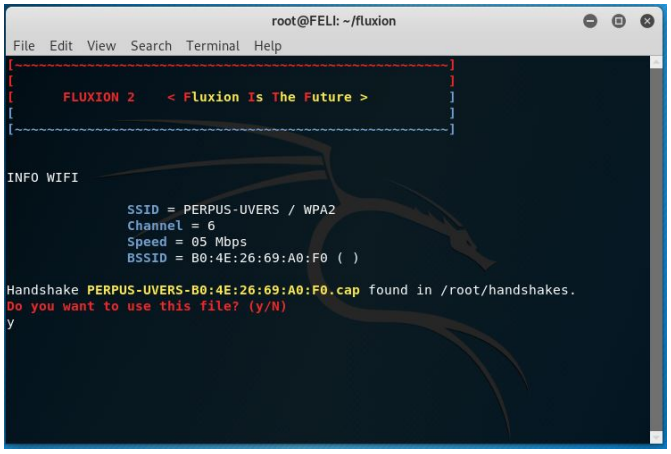
Gambar 8 menunjukkan *pen tester/attacker* memilih opsi serangan dengan *FakeAP–hostapd* atau *host access point daemon* yang merupakan *access point software pen tester/attacker* yang mampu mengubah *network interface card* menjadi *access point* dan server autentikasi. Untuk opsi yang kedua, *FakeAP–airbase-ng* adalah sarana yang ditujukan untuk menyerang korban sebagai lawan dari *access point*.

Berdasarkan Gambar 9, setelah memilih tipe serangan nomor 1, *pen tester/attacker* melakukan *handshake*. *Handshake* merupakan sistem perkenalan yang terjadi antara satu perangkat dengan perangkat lainnya, sehingga memungkinkan perangkat tersebut terkoneksi dan dapat bertukar data.

Pada Gambar 10a dapat dilihat hasil dari *Wireshark pen tester/attacker*. Gambar 10c merupakan hasil dari *Wireshark Analyzer* 2, namun perubahan keduanya tidak ter-*capture*. Gambar 10b merupakan hasil dari *Wireshark Analyzer* 1 yang menunjukkan informasi ketika *handshake* dilakukan. Proses *handshake* tersebut yaitu:



Gambar 8 Info *wifi*



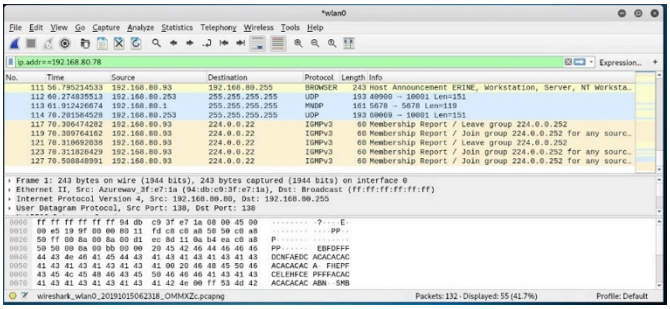
Gambar 9 Info *wifi* (*handshake*)

1) Certificate Status, Server Key Exchange, Server Hello Done.

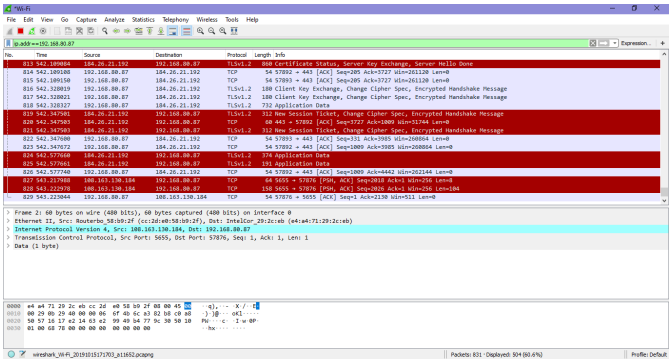
Certificate Status memvalidasi apakah sertifikat digital X.509 server ditiadakan atau tidak, dan dipastikan dengan menghubungi OCSP *Server* (*Online Certificate Status Protocol*) yang ditunjuk.

Server Key Exchange membawa parameter algoritme pertukaran kunci yang dibutuhkan klien dari server untuk mendapatkan enkripsi simetris yang bekerja setelahnya. Format parameter tersebut bergantung secara eksklusif pada *Cipher Suite* yang dipilih, yang sebelumnya telah ditetapkan oleh server melalui pesan *Server Hello*.

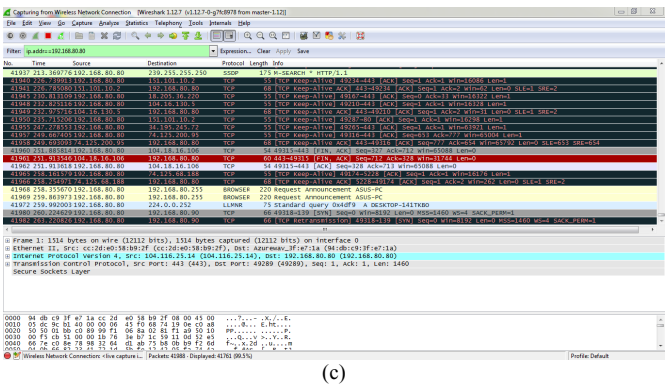
Server Hello menyelesaikan bagian *server* dari *handshake negotiation* tapi tidak membawa informasi tambahan.



(a)



(b)



(c)

Gambar 10 *Wireshark* (*handshake*)

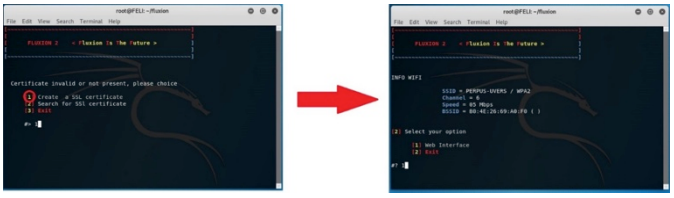
2) New Session Ticket, Change Cipher Spec, Encrypted Handshake Message.

New Session Ticket adalah teknik untuk melanjutkan sesi TLS dengan menyimpan materi kunci yang dienkripsi pada klien. Dalam TLS 1.2 *handshake* dipercepat menjadi dua hingga satu perjalanan. *Change Cipher Spec* adalah pesan yang dikirim oleh klien dan server untuk memberi tahu pihak penerima bahwa catatan selanjutnya akan dilindungi di bawah *CipherSpec* dan kunci yang baru saja ditukar. Pada *Encrypted Handshake Message*, klien dan server akan saling mengirim pesan terenkripsi yang mengatakan bahwa informasi utama sudah benar. Klien (*web browser*) akan melihat kunci hijau di bilah alamat. Klien dan server akan mengenkripsi HTTP *traffic* dengan *session key*.

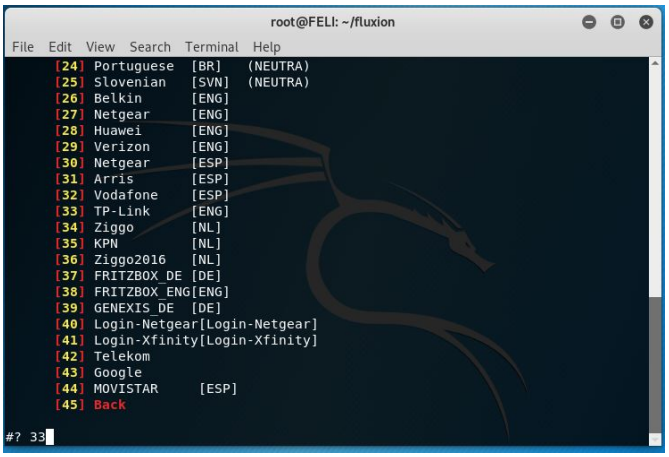
3) Application Data

Pada titik ini, klien dan server telah selesai melakukan *handshake*. Komunikasi terenkripsi telah tersedia dan data aplikasi dapat dikirim dengan aman.

Setelah *pen tester/attacker* melakukan *handshake*, seperti pada Gambar 11, *pen tester/attacker* akan memilih antara membuat atau mencari *SSL certificate* palsu. SSL *certificate* (*Secure Sockets Layer*) adalah sertifikat digital yang mengautentikasi identitas situs web dan mengenkripsi informasi yang dikirim ke server dengan menggunakan teknologi SSL. Dalam penelitian ini dipilih untuk membuat SSL *certificate* palsu dengan *web interface*. Pada Gambar 12 *pen tester/attacker* akan memilih bentuk dari halaman *login* yang palsu. *Template* halaman *login* yang dipilih sesuai dengan yang umum digunakan oleh masyarakat.



Gambar 11 Membuat sertifikat dan *web interface* palsu



Gambar 12 Halaman *login*

Setelah memilih halaman *login*, *Fluxion* akan menunjukkan jendela DHCP, *Deauth All*, dan *Fake*DNS, seperti pada Gambar 13.

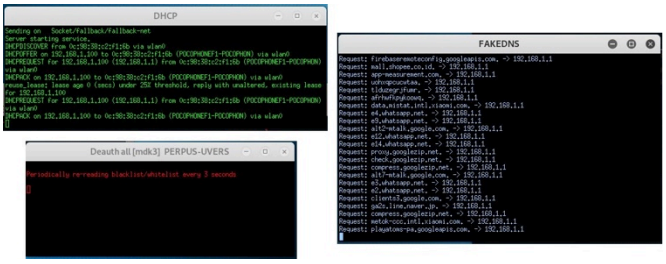
1) *DHCP* atau *Dynamic Host Configuration Protocol* adalah layanan yang secara otomatis memberikan nomor IP kepada komputer yang memintanya. Komputer yang memberikan nomor IP disebut sebagai DHCP *Server*, sedangkan komputer yang meminta nomor IP disebut sebagai DHCP *Client*.

2) *Deauth All* [mdk3] adalah serangan yang akan memutuskan koneksi korban berbasis *wireless*.

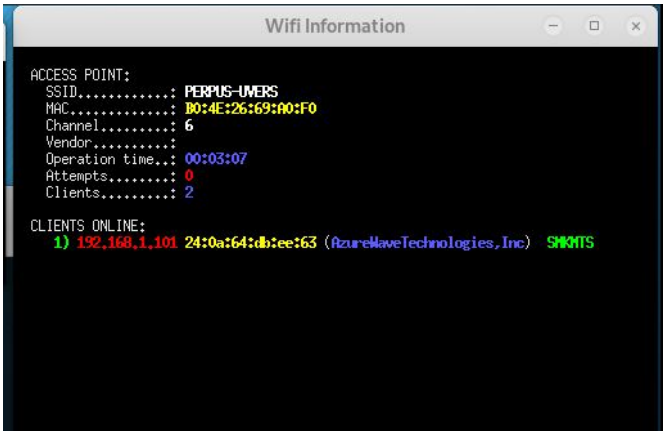
3) *Fake*DNS, menanggapi pertanyaan DNS A (pertanyaan *host address*) dan merespon dengan IP yang sama berulang-ulang.

Setelah menjalankan *Deauth All*, proses *Wireshark capture* berhenti beroperasi.

Gambar 14 menunjukkan informasi korban yang mengakses *Fake Access Point pen tester/attacker*. Gambar 15 menunjukkan tampilan bahwa *Authorized Wifi Access Point* tidak dapat diakses lagi. Korban akan mencoba untuk mengakses *Fake Access Point* yang memiliki SSID yang sama. Jika korban terhubung dengan *Fake Access Point*, maka korban akan dialihkan secara otomatis ke *login page* yang palsu dan diminta untuk mengisi *password.*



Gambar 13 DHCP, *Fake*DNS, Deauth All [mdk3]



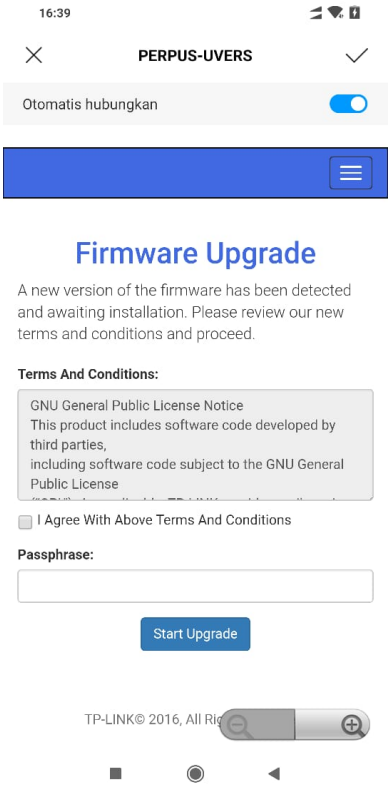
Gambar 14 Informasi *wifi*

Gambar 16 menunjukkan keadaan setelah korban memasukkan *password*, maka pada jendela informasi *wifi* akan tertera '*key found*'. *Password* yang dimasukkan akan berada dalam kurung siku. *Password* kemudian akan tersimpan dalam *file* dalam bentuk .txt.

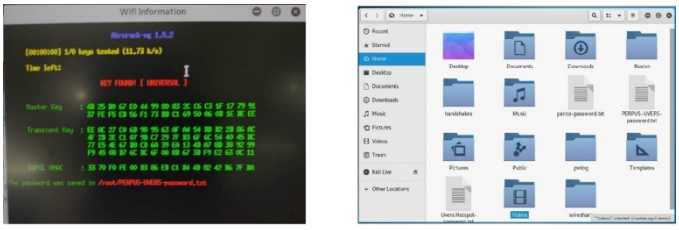
B. Cara Membedakan Fake Access Point

Permasalahan dalam penelitian ini adalah khalayak umum seringkali tidak dapat mengenali perbedaan antara *Authorized Access Point* dengan *Fake Access Point*. Oleh karena itu, dicari cara yang lebih mudah dimengerti bagi korban yang tidak memiliki *basic* teknologi dengan baik sekalipun, yaitu dengan membedakan ESSID-nya.

Pada Gambar 17 dapat dilihat bahwa pada komputer, khususnya Windows 10, tampilan *Fake Access Point* ditandai dengan tanda seru, sedangkan *Authorized Access Point* tidak memiliki tanda seru. Selain itu, jaringan *Fake Access Point* terbuka atau '*open*', berbeda dengan *Authorized Access Point* dimana jaringannya diamankan atau '*secured*'.



Gambar 15 Halaman *mobilephone login* palsu



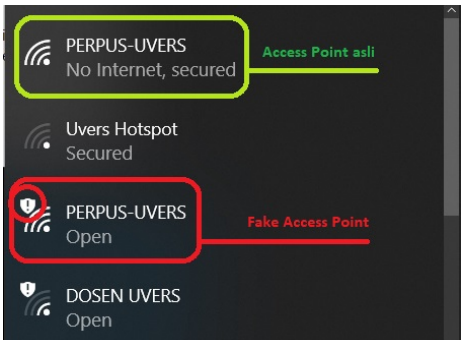
Gambar 16 Informasi *wifi* (*key found*)

Seperti yang dapat dilihat pada Gambar 18, ESSID pada *smartphone*, khususnya *Android*, menunjukkan perbedaan tampilan *Fake Access Point* dengan *Authorized Access Point* dengan ada atau tidaknya simbol gembok. *Fake Access Point* tidak memiliki simbol gembok, sedangkan *Authorized Access Point* memiliki simbol gembok.

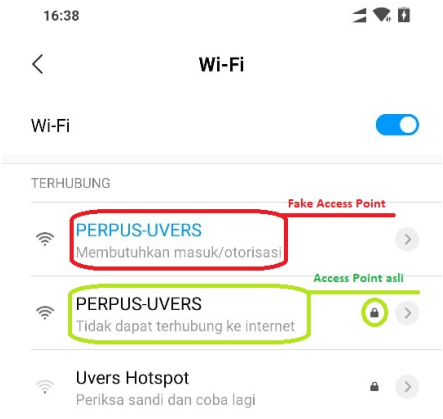
IV. KESIMPULAN

Dari penelitian ini disimpulkan bahwa *public wifi access point* memiliki banyak resiko, seperti mudah diretas. Salah satu contohnya adalah dengan menggunakan *Fake Access Point*. Melalui perangkat lunak *Fluxion 2*, serangan ini menggunakan *Deauth All* (DoS) untuk membanjiri lalu lintas jaringan dengan banyak data, sehingga lalu lintas jaringan yang datang dari *pen tester/attacker* terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan.

Seiring dengan langkah penyerangan yang dilakukan dengan *Fluxion 2*, kondisi jaringan dipantau dengan menggunakan perangkat lunak *Wireshark*. Dalam proses pemantauan yang dilakukan, setiap langkah serangan yang diambil berdampak pada keadaan jaringan. Hal ini ditandai dengan warna merah dan hitam pada *Wireshark* sebagai indikator *bad TCP, TTL low or unexpected*, dan *checksum errors.* Perubahan terlihat saat proses *handshake* dijalankan. *Wireshark Analyzer* 1 ditandai dengan baris berwarna merah



Gambar 17 ESSID Windows 10



Gambar 18 ESSID Android

dengan teks putih. Selain itu, hasil *pen tester/attacker Wireshark* yang dijalankan pada OS Kali Linux, proses *Capture* berhenti di nomor 127, atau saat *Fluxion* dijalankan. Sementara itu, proses *capture* yang dilakukan oleh *Wireshark Analyzer* 1 dan 2 berhenti dan kehilangan koneksi ketika *Fluxion* menjalankan *Deauth All*. Bagi khalayak umum yang kurang memahami serangan tersebut akan beralih ke *Fake Access Point*. Terlebih lagi, akibat dari *Fake Access Point* tidak hanya sekedar mencuri *password*, tetapi *Fake Access Point* sangat berbahaya bagi korban karena dengan meng-input *password* atau meng-klik tombol di *web interfac*e yang palsu, korban secara tidak sadar atau tanpa sepengetahuannya memperbolehkan *malware* untuk menyerang perangkat dan data pribadinya.

Untuk mengidentifikasi serangan *Fake Access Point* dengan mudah ialah dengan melihat SSID dari public *wifi*, selain itu kita juga dapat melihat lalu lintas serangan yang terjadi secara spesifik melalui software *wireshark*.

DAFTAR REFERENSI

[1] S. Ayare, S. Das, V. Sayanekar, dan P. R. Patkar, "Fake access point detection in network," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 3, no. 3, hlm. 5727–5729, 2014.

[2] O. Salman, I. H. Elhajj, A. Chehab, dan A. Kayssi, "A multi-level internet traffic classifier using deep learning," dalam *2018 9th International Conference on the Network of the Future (NOF)*, 2018, hlm. 68–75.

[3] H. Mustafa dan W. Xu, "CETAD: Detecting evil twin access point attacks in wireless hotspots," dalam *2014 IEEE Conference on Communications and Network Security*, 2014, hlm. 238–246.

[4] D. Kim dan S. An, "PKC-based DoS attacks-resistant scheme in wireless sensor networks," *IEEE Sens. J.*, vol. 16, no. 8, hlm. 2217–2218, Apr. 2016.

[5] D. Wang dan P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle and solutions," *Comput. Networks*, vol. 73, hlm. 41–57, Nov. 2014.

[6] T. Mekhaznia dan A. Zidani, "*Wifi* security analysis," *Procedia Comput. Sci.*, vol. 73, hlm. 172–178, 2015.

[7] Y. Ma dan H. Ning, "Improvement of EAP authentication method based on radius server," dalam *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, 2018, hlm. 1324–1328.

[8] T. Zhou, Z. Cai, B. Xiao, Y. Chen, dan M. Xu, "Detecting rogue AP with the crowd wisdom," dalam *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, 2017, hlm. 2327–2332.

[9] B. Shan, "The spread of malware on the WiFi network: epidemiology model and behaviour evaluation," dalam *2009 1st International Conference on Information Science and Engineering, ICISE 2009*, 2009, hlm. 1916–1918.

[10] A. Kumar dan P. Paul, "Security analysis and implementation of a simple method for prevention and detection against evil twin attack in IEEE 802.11 wireless LAN," dalam *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, 2016, hlm. 176–181.

[11] I. Riadi dan A. Kurniawan, *Forensik Jaringan & Cloud*. yogyakarta: Diandra Kreatif, 2019.

[12] Y. Yanti, dkk.., "Implementasi sistem keamanan WPA2-PSK pada jaringan *wifi*," *J. Serambi Eng.*, vol. 3, no. 1, hlm. 248–254, Jan. 2018.

[13] F. Lanze, A. Panchenko, I. Ponce-Alcaide, dan T. Engel, "Hacker's toolbox: detecting software-based 802.11 evil twin access points," dalam *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 2015, hlm. 225–232.

[14] H. Kim, Y.-J. Kang, N. Bruce, S. Park, dan H. Lee, "Smartphone-based secure access control in wireless network analysis," dalam *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, 2015, hlm. 344–347.

Felicia Paramita, kelahiran kota Dumai, mahasiswi program sarjana komputer yang saat ini sedang menjalani pendidikan di Universitas Universal.

Madeline, kelahiran kota Batam, mahasiswi program sarjana komputer yang saat ini sedang menjalani pendidikan di Universitas Universal.

Olga Alvina, kelahiran kota Batam, mahasiswi program sarjana komputer yang saat ini sedang menjalani pendidikan di Universitas Universal.

Rahel Esther Sentia, kelahiran kota Jakarta, mahasiswi program sarjana komputer yang saat ini sedang menjalani pendidikan di Universitas Universal.

Ade Kurniawan, menerima gelar Magister Digital Forensik pada 2014 dari Universitas Islam Indonesia. Saat ini ia adalah dosen Departemen Teknik Informatika Universitas Universal. Minat penelitiannya meliputi komputer, keamanan jaringan, dan digital forensik.

Halaman kosong