

**EVALUASI KEAMANAN WI-FI BERDASARKAN KEBUTUHAN
WAKTU SERANGAN TERHADAP PASSWORD UMUM
MENGUNAKAN TEKNIK DICTIONARY ATTACK**

LAPORAN TUGAS AKHIR



Oleh

**Krishtian Benaya Chandra
E32202368**

**PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK NEGERI JEMBER**

2026

**EVALUASI KEAMANAN WI-FI BERDASARKAN
KEBUTUHAN WAKTU SERANGAN TERHADAP PASSWORD UMUM
MENGUNAKAN TEKNIK DICTIONARY ATTACK**

LAPORAN TUGAS AKHIR



sebagai salah satu syarat untuk memperoleh gelar Ahli Madya Komputer

(A.Md),

di Program Studi Teknik Komputer

Jurusan Teknologi Informasi

Oleh

Krishtian Benaya Chandra

E32202368

**PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK NEGERI JEMBER**

2026

HALAMAN PENGESAHAN

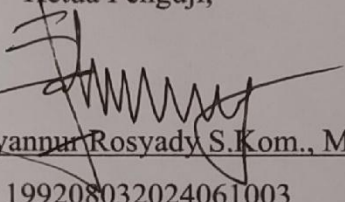
EVALUASI KEAMANAN WI-FI BERDASARKAN KEBUTUHAN
WAKTU SERANGAN TERHADAP PASSWORD UMUM
MENGUNAKAN TEKNIK DICTIONARY ATTACK

Oleh: **Krishtian Benaya Chandra (NIM E32202368)**

Telah Diuji pada tanggal 4 Juni 2026

dan Dinyatakan Memenuhi Syarat

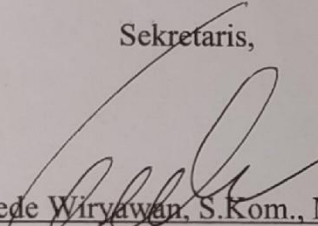
Ketua Penguji,


Ahmad Fahriyannur Rosyady S.Kom., M.MT.

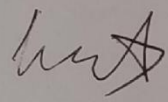
NIP 199208032024061003

Sekretaris,

Anggota,

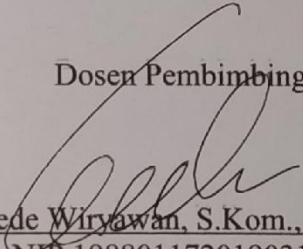

I Gede Wiryawan, S.Kom., M.Kom.

NIP 198801172019031008


Bima Wahyu Maulana, S.Si., M.T.

NIP 199208032024061003

Dosen Pembimbing,

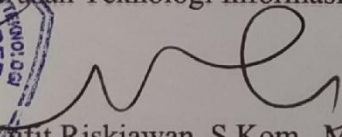

I Gede Wiryawan, S.Kom., M.Kom.

NIP 198801172019031008

Mengetahui,

Ketua Jurusan Teknologi Informasi,




Chandra Yulit Riskiawan, S.Kom., M.Cs.

NIP 19830203 200604 1 003

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Krishtian Benaya Chandra

NIM : E32202368

menyatakan dengan sebenar-benarnya bahwa segala pernyataan dalam Laporan Tugas Akhir saya yang berjudul "*Evaluasi Keamanan Wi-Fi Berdasarkan Kebutuhan Waktu Serangan Terhadap Password Umum Menggunakan Teknik Dictionary Attack*" merupakan gagasan dan hasil karya saya sendiri dengan arahan komisi pembimbing, dan belum pernah diajukan dalam bentuk apa pun pada perguruan tinggi mana pun.

Semua data dan informasi yang digunakan telah dinyatakan secara jelas dan dapat diperiksa kebenarannya. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan dari penulis lain telah disebutkan dalam naskah dan dicantumkan dalam daftar pustaka di bagian akhir Laporan Tugas Akhir ini.

Jember, 13 Juli 2026



Krishtian Benaya
Chandra
NIM E32202368

**PERNYATAAN
PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN
AKADEMIS**

Yang bertanda tangan di bawah ini, saya:

Nama : Krishtian Benaya Chandra
NIM : E32202368
Program Studi : Teknik Komputer
Jurusan : Teknologi Informasi

Demi pengembangan Ilmu Pengetahuan, saya menyetujui untuk memberikan kepada UPT. Perpustakaan Politeknik Negeri Jember, Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalty Free Right*) atas Karya Ilmiah berupa Laporan Tugas Akhir saya yang berjudul:

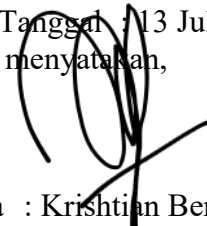
**EVALUASI KEAMANAN WI-FI BERDASARKAN KEBUTUHAN
WAKTU SERANGAN TERHADAP PASSWORD UMUM
MENGUNAKAN TEKNIK DICTIONARY ATTACK**

Dengan Hak Bebas Royalti Non-Eksklusif ini UPT. Perpustakaan Politeknik Negeri Jember berhak menyimpan, mengalih media or format, mengelola dalam bentuk Pangkalan Data (*Database*), mendistribusikan karya dan menampilkan atau mempublikasikannya di Internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis atau pencipta.

Saya bersedia untuk menanggung secara pribadi tanpa melibatkan pihak Politeknik Negeri Jember, segala bentuk tuntutan hukum yang timbul atas Pelanggaran Hak Cipta dalam Karya Ilmiah ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jember
Pada Tanggal : 13 Juli 2026
Yang menyatakan,


Nama : Krishtian Benaya
Chandra
NIM : E32202368

MOTO

"To be wise in your own eyes is the end of growth."

(Proverbs)

PERSEMBAHAN

Karya Tulis Ilmiah ini saya persembahkan kepada:

1. Kedua orang tua saya tercinta, terima kasih atas semua kasih sayang dan cintanya, dukungan baik moril maupun materil, serta doa yang tak henti dan pengorbanan yang tak terhingga. Hanya ini yang mampu putramu persembahkan.
2. Bapak I Gede Wiryawan, S.Kom., M.Kom. selaku Dosen Pembimbing yang telah memberikan bimbingan, arahan, dan ilmu yang sangat berharga selama penyusunan Tugas Akhir ini.
3. Para staf pengajar Politeknik Negeri Jember khususnya Program Studi Teknik Komputer, Jurusan Teknologi Informasi yang telah memberikan banyak ilmu dan pengetahuan serta nasihat yang sangat bermanfaat bagi penulis.
4. Teman-teman seperjuangan Program Studi Teknik Komputer angkatan 2022 yang telah memberikan semangat, bantuan, dan kebersamaan selama menempuh pendidikan.
5. Almamater tercinta Politeknik Negeri Jember.

Evaluasi Keamanan Wi-Fi Berdasarkan Kebutuhan Waktu Serangan Terhadap Password Umum Menggunakan Teknik Dictionary Attack

Pembimbing: I Gede Wiryawan, S.Kom., M.Kom.

Krishtian Benaya Chandra
Program Studi Teknik Komputer
Jurusan Teknologi Informasi

ABSTRAK

Keamanan jaringan Wi-Fi merupakan isu krusial di era digital saat ini. Penelitian ini bertujuan untuk menganalisis dan mengukur pengaruh langsung dari panjang serta variasi kombinasi karakter pada kata sandi umum terhadap waktu yang dibutuhkan untuk berhasil meretas jaringan Wi-Fi berenkripsi WPA2-PSK menggunakan teknik *dictionary attack*. Evaluasi dilaksanakan terhadap tujuh target jaringan Wi-Fi dengan melakukan simulasi serangan menggunakan perangkat *Wifite* dan *Hashcat* pada sistem operasi Kali GNU/Linux, dengan GPU NVIDIA GeForce MX150 sebagai akselerator *cracking* offline. Hasil penelitian menunjukkan bahwa kata sandi sederhana seperti deretan angka berurutan, pola tanggal lahir, atau kata tunggal berbasis bahasa lokal dapat di-*crack* dalam waktu 1,0 hingga 17,0 detik. Pengujian juga membuktikan keunggulan protokol WPA3-SAE dalam menggagalkan serangan deautentikasi aktif, serta mengungkap kerentanan kritis fitur WPS yang memungkinkan eksploitasi *Pixie-Dust* dalam waktu 4 menit 55 detik. Penggunaan GPU memberikan akselerasi hingga ~8,82 kali lipat (~60.000 H/s) dibandingkan CPU. Penelitian ini merekomendasikan penonaktifan fitur WPS, penggunaan *passphrase* panjang minimal 16 karakter, dan migrasi ke protokol WPA3-SAE untuk meningkatkan keamanan jaringan Wi-Fi.

Kata kunci: keamanan Wi-Fi, *dictionary attack*, WPA2-PSK, WPA3-SAE, waktu serangan

***Wi-Fi Security Evaluation Based on Attack Time Requirements Against
Common Passwords Using Dictionary Attack Technique***

Supervised by I Gede Wiryawan, S.Kom., M.Kom.

Krishtian Benaya Chandra
Study Program of Teknik Komputer
Department of Teknologi Informasi

ABSTRACT

Wi-Fi network security is a crucial issue in the current digital era. This study aims to analyze and measure the direct influence of password length and character combination variety on common passwords against the time required to successfully crack WPA2-PSK encrypted Wi-Fi networks using the dictionary attack technique. The evaluation was conducted on seven Wi-Fi network targets by performing attack simulations using Wifite and Hashcat on Kali GNU/Linux operating system, with an NVIDIA GeForce MX150 GPU as an offline cracking accelerator. The results show that simple passwords such as sequential number patterns, date-of-birth patterns, or single local-language-based words can be cracked within 1.0 to 17.0 seconds. The testing also demonstrated the superiority of the WPA3-SAE protocol in defeating active deauthentication attacks, and revealed the critical vulnerability of the WPS feature which allows Pixie-Dust exploitation within 4 minutes and 55 seconds. GPU utilization provided acceleration up to ~8.82 times (~60,000 H/s) compared to CPU. This study recommends disabling WPS features, using long passphrases of at least 16 characters, and migrating to WPA3-SAE protocol to enhance Wi-Fi network security.

Keywords: *Wi-Fi security, dictionary attack, WPA2-PSK, WPA3-SAE, attack time*

RINGKASAN

Evaluasi Keamanan Wi-Fi Berdasarkan Kebutuhan Waktu Serangan Terhadap Password Umum Menggunakan Teknik Dictionary Attack, Krishtian Benaya Chandra, NIM E32202368, Tahun 2026, Teknologi Informasi, Politeknik Negeri Jember, I Gede Wiryawan, S.Kom., M.Kom. (Pembimbing).

Keamanan jaringan nirkabel (Wi-Fi) merupakan isu krusial yang menuntut perhatian serius di era digital saat ini. Meskipun protokol WPA2-PSK telah menjadi standar keamanan yang paling banyak digunakan, kekuatan proteksinya sangat bergantung pada kualitas kata sandi yang dipilih oleh pengguna. Di antara berbagai teknik serangan, *dictionary attack* merupakan salah satu metode paling umum dan efektif untuk mendapatkan akses tidak sah ke jaringan Wi-Fi yang dilindungi kata sandi lemah.

Penelitian ini bertujuan untuk menganalisis dan mengukur pengaruh langsung dari panjang serta variasi kombinasi karakter pada kata sandi umum terhadap waktu yang dibutuhkan untuk berhasil meretas jaringan Wi-Fi berenkripsi WPA2-PSK menggunakan teknik *dictionary attack*, mengevaluasi peran dan efektivitas dari *wordlist* yang berisi puluhan juta kata sandi umum dari koleksi SecLists, serta merumuskan rekomendasi keamanan praktis bagi pengguna umum.

Evaluasi dilaksanakan terhadap tujuh target jaringan Wi-Fi dalam lingkungan nyata dengan melakukan simulasi serangan menggunakan perangkat *Wifite* untuk fase penangkapan *handshake/PMKID* dan *Hashcat* untuk fase *cracking* offline pada sistem operasi Kali GNU/Linux Rolling, dengan GPU NVIDIA GeForce MX150 sebagai akselerator komputasi.

Hasil penelitian menunjukkan bahwa kata sandi sederhana seperti deretan angka berurutan (1234567890), pola tanggal lahir (19111991, 01021992), atau kata tunggal berbasis bahasa lokal (bismillah) dapat di-*crack* secara offline dalam waktu 1,0 hingga 17,0 detik. Pengujian pada target dengan protokol WPA3-SAE membuktikan keamanan yang sangat tinggi karena fitur *Protected Management Frames* (PMF) berhasil menggagalkan serangan deautentikasi aktif secara total. Selain itu, eksploitasi WPS *Pixie-Dust* pada target dengan fitur WPS aktif berhasil memperoleh PIN dan kata sandi WPA2 asli dalam waktu 4 menit 55 detik tanpa perlu *dictionary attack* offline. Penggunaan GPU memberikan akselerasi pemrosesan hingga ~8,82 kali lipat (~60.000 H/s) dibandingkan CPU (~6.800 H/s). Penelitian ini merekomendasikan penonaktifan fitur WPS, penggunaan *passphrase* panjang minimal 16 karakter, dan migrasi ke protokol WPA3-SAE untuk meningkatkan keamanan jaringan Wi-Fi.

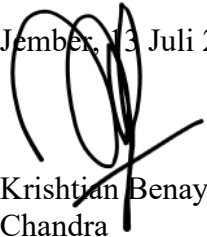
PRAKATA

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas berkat rahmat dan karunia-Nya sehingga penulisan karya tulis ilmiah berjudul "Evaluasi Keamanan Wi-Fi Berdasarkan Kebutuhan Waktu Serangan Terhadap Password Umum Menggunakan Teknik Dictionary Attack" dapat diselesaikan dengan baik. Tulisan ini adalah laporan hasil penelitian yang dilaksanakan sebagai salah satu syarat untuk memperoleh gelar Ahli Madya Komputer (Amd.T) di Program Studi Teknik Komputer, Jurusan Teknologi Informasi, Politeknik Negeri Jember. Penulis menyampaikan penghargaan dan ucapan terima kasih yang sebesar-besarnya kepada:

1. Direktur Politeknik Negeri Jember.
2. Ketua Jurusan Teknologi Informasi.
3. Ketua Program Studi Teknik Komputer.
4. I Gede Wiryawan, S.Kom., M.Kom. selaku Dosen Pembimbing yang telah memberikan bimbingan, arahan, dan motivasi dalam penyelesaian Tugas Akhir ini.
5. Seluruh dosen dan staf Jurusan Teknologi Informasi yang telah memberikan ilmu dan bantuan selama masa perkuliahan.
6. Kedua orang tua dan keluarga yang selalu memberikan doa, dukungan, dan motivasi tiada henti.
7. Rekan-rekan mahasiswa dan semua pihak yang telah ikut membantu dalam pelaksanaan penelitian dan penulisan laporan ini.

Laporan Karya Tulis Ilmiah ini masih kurang sempurna, mengharapkan kritik dan saran yang sifatnya membangun guna perbaikan di masa mendatang. Semoga tulisan ini bermanfaat.

Jember, 13 Juli 2026



Krishtian Benaya
Chandra

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN.....	ii
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
DAFTAR LAMPIRAN.....	xv
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan.....	3
1.4 Manfaat.....	3
BAB 2 TINJAUAN PUSTAKA.....	5
2.1 Keamanan Jaringan Wi-Fi.....	5
2.2 Password dan Keamanannya.....	8
2.3 Teknik Serangan pada Jaringan Wi-Fi.....	11
2.4 Dictionary Attack.....	12
2.5 Penelitian Terdahulu yang Relevan.....	15
2.6 Kerangka Berpikir.....	18
BAB 3 METODOLOGI KEGIATAN.....	20
3.1 Waktu dan Tempat.....	20
3.2 Alat dan Bahan.....	20
3.3 Tahapan Kegiatan.....	21
3.4 Jadwal Kegiatan.....	29
BAB 4 HASIL DAN PEMBAHASAN.....	30
4.1 Verifikasi Spesifikasi Perangkat Keras dan Sistem Operasi.....	30
4.2 Verifikasi Kemampuan Adaptor Nirkabel.....	31
4.3 Konfirmasi Instalasi dan Fungsionalitas Package.....	32
4.4 Persiapan Target Wi-Fi (AP).....	35
4.5 Persiapan Daftar Kata Sandi (<i>Wordlists</i>).....	37
4.6 Pelaksanaan Simulasi Serangan.....	39
4.7 Analisis Kebutuhan Waktu Serangan.....	54

BAB 5 KESIMPULAN DAN SARAN	62
5.1 Kesimpulan	62
5.2 Saran.....	63
DAFTAR PUSTAKA	64

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu yang Relevan

Tabel 3.1 Daftar Package

Tabel 3.2 Parameter Pengukuran Serangan dan Satuannya

Tabel 4.1 Spesifikasi Perangkat Keras dan Sistem Operasi Lingkungan Pengujian

Tabel 4.2 Hasil Verifikasi Kemampuan Adaptor Nirkabel (wlan1)

Tabel 4.3 Hasil Konfirmasi Instalasi dan Fungsionalitas Package Perangkat Lunak

Tabel 4.4 Spesifikasi Target Wi-Fi Pengujian

Tabel 4.5 Spesifikasi Wordlist Berdasarkan Tahapan Serangan

Tabel 4.6 Analisis Komparatif Hasil Simulasi Serangan Wifite

Tabel 4.7 Perbandingan Performa Komputasi (Benchmark Hashcat Mode 22000)

Tabel 4.8 Ringkasan Hasil Uji Coba Offline Cracking Menggunakan Hashcat

DAFTAR GAMBAR

Gambar 3.1 Alur Tahapan Kegiatan

Gambar 4.1 Diagram Alur Serangan Wifite v2.7.0

DAFTAR LAMPIRAN

Lampiran 1. Tautan QR Code Repositori Google Drive untuk rekaman layar
Cracking offline

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah memengaruhi hampir seluruh aspek kehidupan, dengan salah satu dampak paling signifikan adalah meluasnya penggunaan jaringan nirkabel (Wi-Fi). Teknologi Wi-Fi telah menjadi tulang punggung konektivitas internet di berbagai lingkungan, mulai dari rumah pribadi, perkantoran, hingga fasilitas umum, karena kemudahan akses yang ditawarkannya. Tingginya tingkat adopsi ini tercermin dari jumlah pengguna internet di Indonesia yang telah mencapai sekitar 200 juta jiwa, atau setara dengan $\pm 65\%$ dari total populasi, yang sebagian besar mengandalkan Wi-Fi untuk aktivitas daring mereka (Shiddiqi et al., 2020).

Meskipun memberikan kemudahan, popularitas Wi-Fi menjadikannya target utama bagi para peretas. Sifatnya yang terbuka membuat jaringan nirkabel rentan terhadap berbagai ancaman keamanan yang semakin kompleks, seperti penyadapan (eavesdropping), serangan man-in-the-middle, dan denial of service (DoS). Kelemahan dalam sistem keamanan dapat dieksploitasi untuk mencuri data sensitif, menyalahgunakan akses internet, menyebarkan malware, hingga mengakibatkan kerugian finansial yang signifikan. Oleh karena itu, menjaga kerahasiaan, integritas, dan ketersediaan data pada jaringan Wi-Fi merupakan isu krusial yang menuntut perhatian serius dari setiap pengguna.

Di antara berbagai teknik serangan, dictionary attack merupakan salah satu metode yang paling umum dan efektif digunakan oleh penyerang untuk mendapatkan akses tidak sah ke jaringan Wi-Fi yang dilindungi kata sandi. Serangan ini bekerja dengan cara menebak kata sandi secara sistematis menggunakan daftar kata (wordlist) yang telah dikompilasi dari berbagai sumber, termasuk kata-kata dari kamus bahasa, kombinasi umum, serta data dari kebocoran kata sandi sebelumnya (*Encyclopedia of Cryptography, Security and Privacy, 3rd (Sushil Jajodia, Pierangela Samarati, Moti Yung Etc.)*, n.d.). Efektivitas serangan ini berakar pada kecenderungan manusia untuk menggunakan kata sandi yang lemah, pendek, dan mudah ditebak, sehingga memberikan celah keamanan yang dapat dieksploitasi dengan cepat.

Keberhasilan dan kecepatan sebuah dictionary attack sangat dipengaruhi oleh beberapa faktor kunci yang dapat dievaluasi secara kuantitatif. Faktor utama adalah kekuatan kata sandi itu sendiri, yang ditentukan oleh panjang dan kompleksitas (variasi kombinasi huruf besar, huruf kecil, angka, dan simbol). Selain itu, faktor krusial lainnya adalah kekuatan komputasi yang dimiliki penyerang. Kemajuan teknologi, terutama penggunaan *Graphics Processing Unit* (GPU) untuk pemrosesan paralel, telah terbukti mampu mempercepat proses peretasan kata sandi secara masif dibandingkan dengan penggunaan CPU konvensional (Alkhwaja et al., 2023).

Meskipun penelitian mengenai keamanan Wi-Fi telah banyak dilakukan, masih terdapat kebutuhan untuk evaluasi yang lebih spesifik mengenai hubungan terukur antara karakteristik "kata sandi umum" dengan "kebutuhan waktu serangan" yang realistis. Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi secara empiris bagaimana variasi panjang dan kombinasi karakter pada kata sandi umum memengaruhi durasi serangan *dictionary attack* yang dilancarkan menggunakan perangkat keras kelas konsumen. Dengan memahami faktor-faktor yang memengaruhi kecepatan serangan secara mendalam, penelitian ini diharapkan dapat memberikan rekomendasi keamanan yang praktis dan dapat diimplementasikan oleh pengguna untuk melindungi jaringan Wi-Fi mereka secara lebih efektif dari ancaman siber yang terus berkembang.

1.2 Rumusan Masalah

Rumusan masalah dari kegiatan ini adalah sebagai berikut:

1. Bagaimana pengaruh langsung dari panjang dan variasi kombinasi karakter (misalnya, hanya angka, hanya huruf, atau kombinasi lengkap) pada "kata sandi umum" terhadap waktu yang dibutuhkan untuk berhasil diretas menggunakan teknik dictionary attack pada jaringan Wi-Fi berenkripsi WPA2-PSK?
2. Seberapa besar peran dan efektivitas dari wordlist (kamus kata sandi) yang berisi puluhan juta kata sandi umum (seperti dari koleksi SecLists) dalam

menentukan tingkat keberhasilan dan kecepatan serangan terhadap jaringan Wi-Fi target?

3. Berdasarkan hasil kuantitatif dari evaluasi waktu serangan, apa saja rekomendasi keamanan yang paling praktis dan langkah-langkah mitigasi yang paling efektif untuk diimplementasikan oleh pengguna umum guna melindungi jaringan Wi-Fi mereka dari ancaman *dictionary attack*?

1.3 Tujuan

Adapun tujuan dari kegiatan ini adalah sebagai berikut :

1. Menganalisis dan mengukur pengaruh langsung dari panjang serta variasi kombinasi karakter (misalnya, hanya angka, hanya huruf, atau kombinasi lengkap) pada "kata sandi umum" terhadap waktu yang dibutuhkan untuk berhasil meretas jaringan Wi-Fi berenkripsi WPA2-PSK menggunakan teknik *dictionary attack*.
2. Mengevaluasi peran dan efektivitas dari *wordlist* (kamus kata sandi) yang berisi puluhan juta kata sandi umum (seperti dari koleksi SecLists) dalam menentukan tingkat keberhasilan dan kecepatan serangan terhadap jaringan Wi-Fi target.
3. Merumuskan rekomendasi keamanan dan langkah-langkah mitigasi yang praktis serta efektif bagi pengguna umum untuk melindungi jaringan Wi-Fi mereka dari ancaman *dictionary attack*, berdasarkan data kuantitatif yang diperoleh dari hasil evaluasi serangan.

1.4 Manfaat

Penelitian ini diharapkan dapat memberikan manfaat yang signifikan, baik secara praktis bagi para pemangku kepentingan maupun secara akademis bagi pengembangan ilmu pengetahuan.

1. Bagi Pemilik dan Administrator Jaringan Wi-Fi: Memberikan data kuantitatif dan bukti empiris mengenai hubungan langsung antara panjang, kompleksitas karakter, dan jenis *wordlist* dengan waktu yang dibutuhkan untuk meretas

kata sandi. Hasil analisis ini dapat menjadi dasar dalam pengambilan keputusan untuk menerapkan kebijakan keamanan yang lebih kuat, efektif, dan terukur guna melindungi aset informasi dan infrastruktur jaringan dari akses tidak sah.

2. Bagi Pengguna Wi-Fi Umum dan Masyarakat Luas: Meningkatkan kesadaran (awareness) dan literasi digital mengenai risiko nyata dari penggunaan kata sandi yang lemah dan umum. Hasil penelitian ini dapat berfungsi sebagai materi edukasi yang mudah dipahami, yang menunjukkan secara konkret betapa cepatnya sebuah kata sandi dapat diretas, sehingga mendorong praktik keamanan siber yang lebih baik dalam kehidupan sehari-hari.
3. Bagi Politeknik Negeri Jember: Menjadi dokumen akademik yang dapat memperkaya referensi di perpustakaan, khususnya bagi mahasiswa dan dosen di Jurusan Teknologi Informasi, Program Studi Teknik Komputer. Penelitian ini juga merupakan wujud implementasi Tri Dharma Perguruan Tinggi dalam memberikan kontribusi pemikiran dan analisis praktis terhadap isu keamanan siber yang relevan dengan perkembangan teknologi saat ini.
4. Bagi Peneliti Selanjutnya: Dapat menjadi landasan, data awal, dan sumber rujukan yang valid bagi penelitian-penelitian di masa depan yang ingin mendalami topik keamanan siber. Secara spesifik, penelitian ini dapat menjadi titik awal untuk evaluasi kinerja serangan pada perangkat keras kelas konsumen yang berbeda, pengembangan strategi *wordlist* yang lebih canggih, atau analisis komparatif dengan protokol keamanan yang lebih baru seperti WPA

BAB 2 TINJAUAN PUSTAKA

2.1 Keamanan Jaringan Wi-Fi

Seiring dengan meluasnya penggunaan teknologi nirkabel di berbagai aspek kehidupan, keamanan jaringan Wi-Fi telah menjadi isu krusial. Protokol keamanan telah berevolusi dari *Wired Equivalent Privacy* (WEP) yang memiliki banyak kelemahan fundamental, menuju standar yang lebih kuat seperti *Wi-Fi Protected Access* (WPA) dan iterasinya. Saat ini, WPA2 (*Wi-Fi Protected Access 2*) merupakan protokol yang paling dominan digunakan untuk mengamankan jaringan Wi-Fi di lingkungan perumahan dan perkantoran (Zhou Qiang, 2025). Oleh karena itu, penelitian ini memfokuskan analisisnya pada varian WPA2 yang paling umum, yaitu WPA2-*Personal* atau WPA2-*Pre-Shared Key* (WPA2-PSK).

Protokol WPA2-PSK mengandalkan sebuah kunci yang dibagikan sebelumnya (*pre-shared key* atau PSK), yang dikenal oleh pengguna sebagai kata sandi atau passphrase jaringan (Nakhila et al., n.d.). Seluruh pengguna pada jaringan yang sama menggunakan kata sandi identik untuk proses autentikasi. Untuk melindungi data yang ditransmisikan, WPA2 mengimplementasikan standar enkripsi yang sangat kuat, yaitu *Advanced Encryption Standard* (AES), yang dijalankan dengan mode CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) (Arsalan Rathore, 2024). Penting untuk dipahami bahwa kelemahan yang dieksploitasi dalam penelitian ini tidak terletak pada algoritma enkripsi AES itu sendiri, yang hingga saat ini masih dianggap sangat aman. Sebaliknya, vektor serangan yang dimanfaatkan berada pada proses autentikasi dan pertukaran kunci yang dikenal sebagai *4-Way Handshake*.

2.1.1 Analisis Vektor Serangan: *4-Way Handshake*

Keamanan fundamental dari WPA2-PSK bergantung sepenuhnya pada proses *4-Way Handshake*. Proses ini merupakan serangkaian empat pesan yang dipertukarkan antara perangkat klien (*supplicant*) dan *Access Point* (AP) atau *authenticator* untuk memverifikasi bahwa kedua belah pihak memiliki kata sandi

yang benar dan untuk menghasilkan kunci sesi unik yang akan digunakan untuk mengenkripsi seluruh lalu lintas data (Nakhila et al., n.d.).

Proses ini dirancang dengan cerdas untuk tidak pernah mengirimkan kata sandi secara langsung melalui udara. Sebaliknya, kata sandi tersebut digunakan sebagai input untuk menghasilkan sebuah kunci master, yang disebut *Pairwise Master Key* (PMK). PMK ini bersifat statis selama kata sandi dan SSID jaringan tidak diubah (Akomea-Agyin & Asante, 2008). PMK inilah yang kemudian digunakan bersama dengan nilai acak yang unik untuk setiap sesi—dikenal sebagai *Authenticator Nonce* (ANonce) dari AP dan *Supplicant Nonce* (SNonce) dari klien—untuk menghasilkan kunci sesi dinamis yang disebut *Pairwise Transient Key* (PTK). PTK ini kemudian digunakan untuk mengenkripsi data selama sesi berlangsung (Kohlios & Hayajneh, 2018a).

Mekanisme keamanan dalam *4-Way Handshake* divalidasi menggunakan *Message Integrity Code* (MIC), sebuah nilai hash yang dihitung menggunakan sebagian dari PTK (yaitu KCK atau *Key Confirmation Key*) untuk memastikan bahwa pesan-pesan dalam *handshake* tidak dimodifikasi oleh pihak ketiga (Kohlios & Hayajneh, 2018a). yang menciptakan celah keamanan. Seorang penyerang tidak perlu terhubung ke jaringan untuk meluncurkan serangan. Dengan hanya memonitor lalu lintas nirkabel di sekitar target (proses yang dikenal sebagai *sniffing*), penyerang dapat menangkap paket-paket EAPOL (*Extensible Authentication Protocol over LAN*) yang berisi pesan-pesan *4-Way Handshake* tersebut. (Nakhila et al., n.d.) Untuk mempercepat proses ini, penyerang dapat secara aktif mengirimkan paket deautentikasi ke klien yang sudah terhubung, memaksa klien tersebut untuk memutuskan koneksi dan melakukan proses autentikasi ulang. Proses re-autentikasi ini akan menghasilkan *4-Way Handshake* baru yang dapat segera ditangkap oleh penyerang (Joseph Lorenz, 2017).

Setelah berhasil ditangkap, paket *handshake* tersebut berisi semua informasi yang dibutuhkan penyerang untuk melakukan serangan secara *offline*, yaitu di luar jaringan target. Informasi tersebut meliputi ANonce, SNonce, alamat MAC dari AP dan klien, serta MIC yang terverifikasi (Nakhila et al., n.d.). Satu-satunya komponen yang tidak dimiliki penyerang adalah PMK, yang berasal dari kata sandi

asli. Namun, karena penyerang mengetahui algoritma yang digunakan untuk menghasilkan PMK (yaitu fungsi PBKDF2-SHA1), mereka dapat mencoba menebak kata sandi. Untuk setiap tebakan dari daftar kata sandi (*wordlist*), penyerang akan:

1. Menghasilkan PMK hipotesis dari kata sandi tebakan dan SSID jaringan.
2. Menggunakan PMK hipotesis tersebut bersama ANonce dan SNonce yang telah ditangkap untuk menghasilkan PTK hipotesis.
3. Menghitung MIC hipotesis dari pesan *handshake* menggunakan PTK hipotesis tersebut.
4. Membandingkan MIC hipotesis dengan MIC asli yang ada di dalam paket yang ditangkap.

Jika kedua MIC cocok, maka kata sandi yang ditebak adalah benar (Akomea-Agyin & Asante, 2008). Proses ini mengubah mekanisme keamanan menjadi sebuah "orakel" yang memungkinkan penyerang memverifikasi setiap tebakan kata sandi tanpa perlu berinteraksi lebih lanjut dengan jaringan target.

Fakta bahwa serangan ini bersifat *offline* berarti penyerang tidak terikat oleh mekanisme keamanan jaringan seperti pembatasan jumlah percobaan login (*rate limiting*), sehingga kecepatan serangan hanya dibatasi oleh kekuatan komputasi perangkat keras penyerang dan kualitas *wordlist* yang dimiliki (Nakhila et al., n.d.).

Keberadaan protokol WPA3 yang lebih baru, yang secara spesifik menggunakan *Simultaneous Authentication of Equals* (SAE) untuk menggantikan *4-Way Handshake* demi mencegah serangan kamus *offline*, merupakan pengakuan industri terhadap kerentanan fundamental pada WPA2 ini (Zhou Qiang, 2025). Hal ini semakin memperkuat justifikasi dan relevansi penelitian yang bertujuan untuk mengukur secara kuantitatif risiko nyata yang dihadapi oleh jutaan pengguna yang masih bergantung pada WPA2-PSK.

2.2 Password dan Keamanannya

Kekuatan sebuah kata sandi, atau kemampuannya untuk menahan serangan tebakan, dapat diukur dan dianalisis melalui beberapa variabel kunci. Variabel-variabel ini secara langsung mempengaruhi waktu dan sumber daya yang dibutuhkan oleh seorang penyerang untuk berhasil membobolnya.

2.2.1 Konsep Entropi Kata Sandi

Secara formal, kekuatan sebuah kata sandi diukur dengan konsep yang disebut entropi, yang dinyatakan dalam satuan bit. Entropi merepresentasikan tingkat ketidakpastian atau keacakan sebuah kata sandi (Aranza Trevino, 2024). Semakin tinggi nilai entropinya, semakin banyak kemungkinan kombinasi yang harus dicoba oleh penyerang, sehingga kata sandi tersebut semakin kuat. Entropi (E) dihitung menggunakan rumus teori informasi berikut :

$$E = \log_2(R^L)$$

Rumus Entropi Kata Sandi 2.1

Di mana:

- a. L adalah panjang kata sandi (jumlah karakter).
- b. R adalah ukuran dari himpunan karakter yang mungkin digunakan (*character pool*). Sebagai contoh, R=26 untuk kata sandi yang hanya menggunakan huruf kecil; R=52 untuk campuran huruf besar dan kecil; R=62 untuk alfanumerik (huruf besar, kecil, dan angka); dan R=95 untuk yang menyertakan semua karakter ASCII yang dapat dicetak (Mike Coutermarsh, 2022).

Hubungan antara entropi dan keamanan bersifat eksponensial. Setiap penambahan satu bit pada nilai entropi akan menggandakan jumlah total kemungkinan kata sandi, yang berarti menggandakan waktu yang dibutuhkan untuk serangan *brute-force* (Fa'atulo Halawa et al., n.d.). Ini membangun hubungan teoretis yang jelas antara karakteristik fisik sebuah kata sandi (panjang dan kompleksitas) dengan waktu yang dibutuhkan untuk meretasnya.

2.2.2 Debat Kunci: Panjang vs. Kompleksitas

Secara tradisional, kebijakan keamanan kata sandi menekankan pentingnya kompleksitas, yaitu penggunaan kombinasi dari berbagai jenis karakter (huruf

besar, huruf kecil, angka, dan simbol). Namun, pandangan modern, yang dipelopori oleh lembaga standar seperti *National Institute of Standards and Technology* (NIST) Amerika Serikat, telah menggeser penekanan dari kompleksitas ke panjang kata sandi (Britney Oswald, 2024).

Jalan pintas kognitif yang diambil pengguna untuk memenuhi aturan kompleksitas menghasilkan pola pembuatan kata sandi yang sangat dapat diprediksi. Pola-pola ini, meskipun secara teknis memenuhi persyaratan kebijakan (misalnya, "memiliki setidaknya satu huruf besar, satu angka, dan satu simbol"), secara drastis mengurangi entropi atau ketidakpastian kata sandi, membuatnya rentan terhadap serangan kamus modern.

Pola yang paling umum diamati meliputi:

- a. Kapitalisasi Huruf Pertama: Pengguna sering kali hanya menggunakan huruf kapital pada huruf pertama dari sebuah kata kamus (misalnya, Password dari password).
- b. Penambahan Angka di Akhir: Angka, sering kali '1', '123', atau tahun saat ini, ditambahkan di akhir kata sandi (misalnya, Password123 atau Admin2024\$) (John Martinez, 2025).
- c. Penambahan Simbol di Akhir: Simbol yang paling umum, seperti '!', '?', atau '@', sering kali ditempatkan di akhir kata sandi untuk memenuhi persyaratan simbol (misalnya, Password!) (John Martinez, 2025).

Pola-pola ini sangat diketahui oleh penyerang dan dapat dengan mudah dieksploitasi menggunakan serangan berbasis aturan (*rule-based attacks*) yang diterapkan pada kamus kata sandi. Sebaliknya, sebuah *passphrase* yang lebih panjang namun lebih sederhana (misalnya, kudamakansayurbayamsegar) bisa memiliki entropi yang jauh lebih tinggi dan secara signifikan lebih sulit untuk diretas daripada kata sandi pendek yang "kompleks" (Kelsey Kinzer, 2023). Sebagai ilustrasi, sebuah kata sandi dengan panjang 12 karakter bisa jadi 62 triliun kali lebih sulit untuk diretas dibandingkan kata sandi dengan panjang 6 karakter, yang menunjukkan dampak eksponensial dari penambahan panjang (Kelsey Kinzer, 2023).

2.2.3 Faktor Manusia dan Kerentanan Psikologis

Titik terlemah dalam sistem keamanan kata sandi seringkali adalah faktor manusia itu sendiri. Terdapat kecenderungan kuat bagi pengguna untuk memilih kata sandi yang mudah diingat, yang seringkali berarti kata sandi tersebut lemah, umum, dan mudah ditebak. Inilah kerentanan fundamental yang dieksploitasi oleh *dictionary attack*. Studi menunjukkan bahwa pengguna sering kali menggunakan kembali kata sandi yang sama di berbagai layanan, yang berarti satu kebocoran data dapat membahayakan banyak akun lainnya (Britney Oswald, 2024). Selain itu, ketika dipaksa untuk mengganti kata sandi secara berkala, pengguna cenderung hanya membuat modifikasi kecil dan dapat diprediksi dari kata sandi sebelumnya, yang tidak secara signifikan meningkatkan keamanan (Alan T. Norman, n.d.). Karena alasan inilah, NIST kini juga tidak lagi merekomendasikan kebijakan penggantian kata sandi secara periodik, kecuali jika ada indikasi kompromi (Steve Alder, 2024).

Lebih jauh lagi, serangan teknis seringkali didahului atau dilengkapi dengan teknik rekayasa sosial (*social engineering*). Penyerang dapat mengumpulkan informasi pribadi tentang target dari sumber-sumber publik untuk membangun *wordlist* yang lebih spesifik dan efektif (Mitnick et al., n.d.). Seperti yang didokumentasikan oleh pakar keamanan Kevin Mitnick, mengeksploitasi psikologi manusia seringkali lebih mudah daripada menembus pertahanan teknis yang canggih.

Kombinasi dari kebijakan keamanan, psikologi pengguna, dan teknologi serangan menciptakan sebuah ekosistem yang kompleks. Kebijakan awal yang memaksakan kompleksitas justru mendorong perilaku pengguna yang dapat diprediksi. Perilaku ini kemudian dieksploitasi oleh alat peretas modern seperti Hashcat, yang tidak hanya menggunakan kamus statis tetapi juga menerapkan aturan transformasi untuk meniru pola-pola umum yang dibuat manusia (Ethan Wilkins, n.d.).

Sebagai respons, NIST memperbarui panduannya untuk mendorong penggunaan *passphrase* yang lebih panjang, yang secara teoretis lebih sulit ditebak. Penelitian ini, dengan fokusnya pada pengujian kata sandi umum menggunakan

wordlist yang besar dan komprehensif seperti SecLists, secara langsung mengukur kondisi keamanan di dunia nyata yang dihasilkan dari interaksi ini. Efektivitas *wordlist* tersebut menjadi proksi langsung untuk mengukur seberapa banyak pengguna yang masih terjebak dalam pola-pola lama yang mudah ditebak, terlepas dari kebijakan kompleksitas yang mungkin berlaku.

2.3 Teknik Serangan pada Jaringan Wi-Fi

Dalam (Kohlilos & Hayajneh, 2018b) berbagai teknik serangan yang dapat dilakukan terhadap jaringan Wi-Fi, khususnya yang menggunakan protokol WPA2. Terdapat berbagai macam teknik serangan pada jaringan Wi-Fi yang umum digunakan, seperti:

1. *Evil Twin Attack*: penyerang membuat hotspot Wi-Fi palsu yang meniru jaringan asli. Pengguna yang tidak curiga dapat terhubung ke jaringan ini, memungkinkan penyerang untuk mencuri data.
2. *WPS (Wi-Fi Protected Setup) Attack*: WPS adalah fitur yang dirancang untuk memudahkan koneksi perangkat ke jaringan Wi-Fi. Namun, WPS memiliki kerentanan yang dapat dieksploitasi. Penyerang dapat menggunakan alat seperti *Reaver* untuk menebak PIN WPS dan mendapatkan akses ke jaringan.
3. *Deauthentication Attack*: Penyerang mengirimkan paket deauthentication ke perangkat yang terhubung ke jaringan, memaksa perangkat tersebut untuk terputus. Ketika perangkat mencoba untuk terhubung kembali, penyerang dapat menangkap paket autentikasi dan mencoba untuk mendapatkan kata sandi.
4. *Rogue Access Point*: Penyerang mengatur akses poin Wi-Fi yang tidak sah di dekat jaringan target. Pengguna yang tidak curiga dapat terhubung ke akses poin ini, memungkinkan penyerang untuk mengakses data yang dikirimkan oleh pengguna.
5. *Social Engineering*: Penyerang dapat menggunakan teknik rekayasa sosial untuk mendapatkan informasi sensitif dari pengguna, seperti meminta kata sandi dengan berpura-pura menjadi teknisi jaringan atau pihak berwenang.

6. *Firmware Exploits*: Beberapa router memiliki kerentanan dalam firmware mereka. Penyerang dapat mengeksploitasi kerentanan ini untuk mendapatkan akses ke pengaturan router dan mengubah konfigurasi keamanan, termasuk kata sandi.
7. *Bluetooth Hacking*: Meskipun ini bukan serangan langsung terhadap Wi-Fi, penyerang dapat menggunakan Bluetooth untuk mendapatkan akses ke perangkat yang terhubung ke jaringan Wi-Fi. Misalnya, jika perangkat pengguna terhubung ke jaringan Wi-Fi dan Bluetooth, penyerang dapat mencoba mengeksploitasi kerentanan Bluetooth untuk mendapatkan akses.
8. *PMKID Attack*: Identifier yang dihasilkan dari kunci master dan informasi lainnya. Dalam serangan PMKID, penyerang dapat meminta PMKID dari akses poin tanpa harus terhubung ke jaringan. Ini berbeda dengan serangan handshake tradisional yang memerlukan klien untuk terhubung dan melakukan pertukaran kunci.
9. *Dictionary Attack*: Ini adalah teknik yang sangat umum digunakan untuk mendapatkan akses ke jaringan Wi-Fi yang dilindungi kata sandi. Dalam serangan ini, penyerang menggunakan daftar kata sandi yang umum atau kata-kata yang mungkin digunakan oleh pengguna untuk mencoba mendapatkan akses ke jaringan.

Kegiatan ini lebih berfokus pada teknik serangan *dictionary attack*. Dimana *Dictionary attack* sendiri adalah sebuah metode yang digunakan untuk menebak kata sandi dengan mencoba setiap kata dalam daftar (*dictionary*) yang telah disiapkan sebelumnya, yang akan digunakan untuk mengetahui bagaimana keamanan Wi-Fi berdasar kebutuhan waktu serangan terhadap password umum.

2.4 Dictionary Attack

Dictionary attack atau serangan kamus adalah sebuah metode peretasan kata sandi di mana penyerang secara sistematis mencoba setiap kata dari sebuah daftar yang telah disiapkan sebelumnya (*wordlist*) dengan harapan salah satu entri dalam daftar tersebut cocok dengan kata sandi target. Teknik ini merupakan salah satu metode yang paling umum dan efektif untuk mendapatkan akses tidak sah, terutama

karena mengeksploitasi kecenderungan manusia untuk menggunakan kata sandi yang lemah dan dapat diprediksi (Sayed Achmady, n.d.).

2.4.1 Prinsip Kerja

Berbeda dengan serangan *brute-force* murni yang mencoba setiap kemungkinan kombinasi karakter, serangan kamus beroperasi berdasarkan asumsi bahwa kata sandi yang digunakan kemungkinan besar adalah kata atau frasa yang umum. "Kamus" modern yang digunakan dalam serangan ini tidak lagi terbatas pada daftar kata dari bahasa alami. Sebaliknya, *wordlist* yang efektif merupakan kompilasi masif dari berbagai sumber, termasuk:

- a. Kata sandi yang bocor dari pelanggaran data sebelumnya, seperti dari koleksi RockYou.
- b. Kombinasi kata dan angka yang umum (misalnya, love123, password2024).
- c. Pola papan ketik (misalnya, qwerty, asdfghjkl).
- d. Informasi yang relevan dengan target yang diperoleh melalui rekayasa sosial (misalnya, nama, tanggal lahir, nama hewan peliharaan).

Proyek seperti SecLists di GitHub mengumpulkan dan mengkategorikan berbagai jenis *wordlist* ini, menyediakan sumber daya yang sangat berharga bagi para penguji keamanan dan, sayangnya, juga bagi penyerang (Daniel Miessler et al., 2025).

2.4.2 Kelebihan dan Kekurangan

Sebagai sebuah metode serangan, *dictionary attack* memiliki kelebihan dan kekurangan yang jelas yang menentukan efektivitasnya.

Kelebihan:

- a. Efisiensi dan Kecepatan: Dibandingkan dengan *brute-force*, serangan kamus secara signifikan lebih efisien karena memfokuskan upaya pada kandidat kata sandi yang memiliki probabilitas tinggi untuk benar. Ini mengurangi ruang pencarian secara drastis, sehingga membutuhkan lebih sedikit waktu dan sumber daya komputasi (Rublon, 2025).
- b. Efektivitas Tinggi Terhadap Kata Sandi Umum: Metode ini sangat berhasil melawan kata sandi yang lemah, umum, atau didasarkan pada pola yang

dapat diprediksi. Sebuah laporan dari Specops pada tahun 2025 yang menganalisis miliaran kata sandi yang bocor menemukan bahwa 230 juta di antaranya memenuhi persyaratan kompleksitas standar (misalnya, panjang 8+ karakter dengan huruf besar, angka, dan simbol) namun tetap berhasil dicuri, menunjukkan bahwa kata sandi tersebut kemungkinan besar didasarkan pada pola umum yang ada di dalam kamus (Joel R. McConvey, 2025).

2. Kekurangan:

- a. Ketergantungan pada Kualitas *Wordlist*: Keberhasilan serangan ini sepenuhnya bergantung pada kualitas dan kelengkapan kamus yang digunakan. Jika kata sandi target adalah serangkaian karakter yang benar-benar acak dan unik (misalnya, qZ5&k#9@pL*v), maka kata sandi tersebut tidak akan ada di dalam kamus mana pun, dan serangan ini akan gagal total (Rublon, 2025).
- b. Tidak Menjamin Keberhasilan: Berbeda dengan serangan *brute-force* yang secara teoretis akan selalu berhasil menemukan kata sandi jika diberi waktu yang cukup, serangan kamus tidak memberikan jaminan keberhasilan. Jika kata sandi tidak ada dalam daftar, serangan tersebut akan berakhir tanpa hasil (Sayed Achmady, n.d.).

2.5 Penelitian Terdahulu yang Relevan

Tabel 2.1 Penelitian Terdahulu yang Relevan

No	Nama Peneliti	Judul	Hasil	Kelebihan	Kekurangan
1	Alkhwaja et al. (2023)	<i>Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming</i>	<i>Dictionary attack</i> jauh lebih efektif untuk kata sandi dengan pola umum. GPU secara signifikan mempercepat proses peretasan dibandingkan CPU.	Memberikan bukti kuantitatif yang kuat mengenai superioritas GPU untuk peretasan kata sandi dan membandingkan secara langsung efektivitas dictionary attack vs. brute-force. Metodologinya jelas dan menggunakan parallel programming yang relevan.	Fokus pada <i>hash</i> generik (bukan spesifik WPA2-PSK <i>handshake</i>), sehingga tidak memperhitungkan <i>overhead</i> komputasi spesifik dari protokol Wi-Fi. Perangkat keras yang diuji (GTX 1050 Ti) sudah beberapa generasi di belakang, sehingga estimasi waktunya mungkin terlalu konservatif untuk ancaman saat ini.
2	Fa'atulo Halawa et al. (2020)	Analisis Kelemahan Sistem Authentication Pengguna Pada Wireless IEEE 802.11i	Kompleksitas kata sandi (kombinasi abjad, angka, simbol) berbanding lurus dengan waktu yang dibutuhkan untuk meretasnya.	Secara spesifik menguji serangan pada protokol WPA2-PSK, yang sangat relevan dengan penelitian ini. Menegaskan hubungan fundamental antara kompleksitas dan waktu	Tidak memberikan detail spesifik mengenai perangkat keras yang digunakan untuk pengujian, sehingga hasilnya sulit direplikasi atau dibandingkan. Analisis tidak memperhitungkan

No	Nama Peneliti	Judul	Hasil	Kelebihan	Kekurangan
				retas dalam konteks Wi-Fi.	kan faktor akselerasi GPU vs. CPU, yang merupakan variabel krusial dalam lanskap ancaman modern.
3	(Corey Neskey, 2024)	<i>The 2024 Hive Systems Password Table</i>	Menyediakan estimasi waktu retas yang konkret untuk berbagai panjang dan kompleksitas kata sandi, menunjukkan kata sandi 8 karakter rentan.	Memberikan <i>benchmark</i> ancaman modern yang sangat jelas dan mudah dipahami, menggunakan perangkat keras kelas atas yang relevan. Mengganti asumsi <i>hash</i> dari MD5 ke bcrypt yang lebih modern dan realistis, menunjukkan evolusi ancaman.	Merupakan laporan industri, bukan <i>peer-reviewed academic paper</i> . Skenario perangkat kerasnya adalah <i>worst-case</i> (penyerang dengan sumber daya besar), yang mungkin kurang merepresentasikan ancaman dari penyerang dengan sumber daya terbatas atau menggunakan perangkat kelas konsumen tunggal.
4	Sunandar Informatika et al. (2024)	Implementasi Penetration Testing dan Wordlist Generator	Berhasil menemukan kata sandi lemah ("unsika2023") yang terkait	Fokus pada satu studi kasus tunggal dengan kata sandi yang sangat spesifik, sehingga	Fokus pada satu studi kasus tunggal dengan kata sandi yang sangat spesifik, sehingga

No	Nama Peneliti	Judul	Hasil	Kelebihan	Kekurangan
		dalam Pengujian Keamanan Jaringan Menggunakan Metode Dictionary Attack	dengan nama institusi, membuktikan kerentanan di dunia nyata.	temuannya kurang dapat digeneralisasi. Tidak memberikan data kuantitatif mengenai "waktu yang dibutuhkan" untuk serangan, yang merupakan fokus utama dari penelitian ini.	temuannya kurang dapat digeneralisasi. Tidak memberikan data kuantitatif mengenai "waktu yang dibutuhkan" untuk serangan, yang merupakan fokus utama dari penelitian ini.

Melalui keempat penelitian dan laporan yang menjadi acuan di atas, terdapat beberapa persamaan serta perbedaan dengan penelitian yang akan dilakukan saat ini. Persamaan utama antara keempat acuan tersebut dan penelitian yang akan dilakukan adalah metodologi inti yang digunakan, yang berpusat pada penggunaan teknik serangan berbasis kamus atau tebakan untuk mengevaluasi keamanan kata sandi. Keempatnya memiliki tujuan serupa, yaitu untuk menganalisis dan memahami faktor-faktor yang memengaruhi keberhasilan dan efisiensi serangan terhadap kata sandi, baik dari segi kompleksitas, panjang, maupun metode serangannya.

Sedangkan untuk perbedaannya, penelitian yang akan dilakukan memiliki fokus yang lebih spesifik dan praktis. Perbedaan paling signifikan terletak pada perangkat keras yang digunakan. Jika penelitian Alkhwaja dkk. dan terutama laporan Corey Neskey menggunakan perangkat keras kelas atas (multi-GPU rig) untuk benchmarking, penelitian ini secara spesifik akan menggunakan perangkat keras kelas konsumen (laptop Acer Swift SF314-54G). Hal ini bertujuan untuk memberikan data evaluasi yang lebih realistis dan relevan bagi pengguna umum, serta mensimulasikan ancaman dari penyerang dengan sumber daya yang lebih terbatas, berbeda dengan skenario 'kasus terburuk' yang digambarkan oleh Corey Neskey. Perbedaan lainnya adalah fokus evaluasi; jika penelitian Sunandar

berfokus pada wordlist yang dibuat secara kontekstual dan Halawa dkk. pada prinsip kompleksitas, penelitian ini akan menggunakan wordlist umum yang sangat besar (>60 juta entri) untuk mengukur secara empiris 'kebutuhan waktu serangan' terhadap spektrum 'kata sandi umum' yang lebih luas pada perangkat keras yang telah ditentukan.

Dengan memanfaatkan temuan-temuan yang telah ada, penelitian ini dapat membangun landasan yang kuat. Mengacu pada efektivitas dictionary attack yang telah dibuktikan oleh Alkhwaja dkk. dan Halawa dkk. metodologi praktis dari Sunandar, serta benchmark ancaman modern dari Corey Neskey, penelitian ini akan mengisi celah pengetahuan. Celah tersebut adalah penyediaan data kuantitatif yang terukur mengenai 'kebutuhan waktu serangan' pada perangkat keras yang umum diakses, sehingga menghasilkan wawasan keamanan yang lebih relevan dan dapat diaplikasikan secara langsung oleh masyarakat luas.

2.6 Kerangka Berpikir

Kerangka berpikir penelitian ini disusun berdasarkan sintesis dari tinjauan pustaka yang telah diuraikan. Kerangka ini berfungsi sebagai alur logika yang menghubungkan antara konsep-konsep teoretis, variabel-variabel yang diteliti, dan tujuan penelitian secara keseluruhan.

Alur logika penelitian ini dimulai dari identifikasi kerentanan fundamental pada protokol WPA2-PSK. Sebagaimana telah dibahas, mekanisme *4-Way Handshake* pada protokol ini memungkinkan penyerang untuk menangkap *hash* dari kata sandi jaringan. Penangkapan ini dapat dilakukan secara pasif atau dipercepat dengan serangan deautentikasi, dan memungkinkan analisis kata sandi dilakukan secara *offline* tanpa interaksi lebih lanjut dengan jaringan target.

Keamanan *hash* yang ditangkap ini bergantung sepenuhnya pada kekuatan kata sandi asli yang digunakan oleh pengguna. Kekuatan ini ditentukan oleh beberapa variabel kunci yang dapat diukur, yaitu panjang karakter dan tingkat kompleksitas karakter (penggunaan kombinasi angka, huruf besar-kecil, dan simbol). Dalam penelitian ini, karakteristik kata sandi tersebut diposisikan sebagai variabel

independen, yaitu faktor-faktor yang akan dimanipulasi untuk diamati pengaruhnya.

Metode serangan yang dipilih untuk mengevaluasi keamanan ini adalah serangan kamus (*dictionary attack*). Teknik ini dipilih karena efisiensinya yang tinggi dalam menebak kata sandi umum, yang mencerminkan perilaku pengguna di dunia nyata. Variabel dependen, atau hasil utama yang akan diukur dalam penelitian ini, adalah kebutuhan waktu serangan (T_{crack}), yaitu durasi yang diperlukan untuk berhasil menemukan kata sandi yang benar menggunakan metode ini.

Hubungan antara variabel independen (karakteristik kata sandi) dan variabel dependen (waktu serangan) tidak terjadi dalam ruang hampa. Hubungan ini dimoderasi oleh faktor-faktor eksternal yang dalam konteks penelitian ini ditetapkan sebagai kondisi yang terkontrol. Faktor-faktor tersebut adalah perangkat keras penyerang (dalam hal ini, laptop Acer Swift SF314-54G dengan spesifikasi yang telah ditentukan) dan kualitas *wordlist* yang digunakan (koleksi dari SecLists yang berisi lebih dari 60 juta entri). Dengan menjaga faktor-faktor ini tetap konstan, penelitian dapat mengisolasi dan mengukur secara akurat pengaruh langsung dari panjang dan kompleksitas kata sandi terhadap waktu yang dibutuhkan untuk meretasnya.

BAB 3 METODOLOGI KEGIATAN

3.1 Waktu dan Tempat

Kegiatan penelitian ini akan dilaksanakan dalam rentang waktu selama 3 (tiga) bulan, yang dijadwalkan mulai dari bulan Juli hingga September 2025. Pelaksanaan kegiatan akan terbagi di dua lokasi utama dengan fungsi yang berbeda untuk mendukung setiap tahapan penelitian:

1. Politeknik Negeri Jember: Lingkungan kampus, khususnya laboratorium di Jurusan Teknologi Informasi, akan menjadi lokasi utama untuk pelaksanaan simulasi serangan dan pengumpulan data primer. Pemilihan lokasi ini bertujuan untuk menciptakan lingkungan pengujian yang terkontrol dan didukung oleh infrastruktur akademis yang memadai, yang penting untuk memastikan validitas dan reliabilitas data yang diperoleh.
2. Perumahan Bernady Land, Slawu, Kecamatan Patrang, Kabupaten Jember: Lokasi ini akan digunakan sebagai lokasi kedua untuk tahap analisis data, pengolahan hasil, dan penyusunan laporan akhir. Lingkungan yang lebih tenang di luar kampus akan mendukung proses analisis mendalam terhadap data yang telah dikumpulkan serta penulisan laporan secara fokus.

3.2 Alat dan Bahan

Penelitian yang berjudul “Evaluasi Keamanan Wi-Fi Berdasarkan Kebutuhan Waktu Serangan Terhadap Password Umum Menggunakan Teknik Dictionary Attack” ini memerlukan beberapa alat yang terdiri dari *Hardware* dan *Software* sebagai berikut:

1. Alat
 - A. Hardware (Perangkat Keras)
 - 1) Satu unit laptop Acer Swift SF314-54G yang memiliki spesifikasi sebagai tercantum berikut :
 - a. Processor : Intel Core i5-8250U CPU @ 3.40Ghz

- b. Storage : SSD 512GB
- c. Memory : 12 GB
- d. Operation : Kali GNU/Linux Rolling

- 2) Bulpen / Pensil
- 3) Buku Catatan
- 4) Sticky Note

B. Software (*package*)

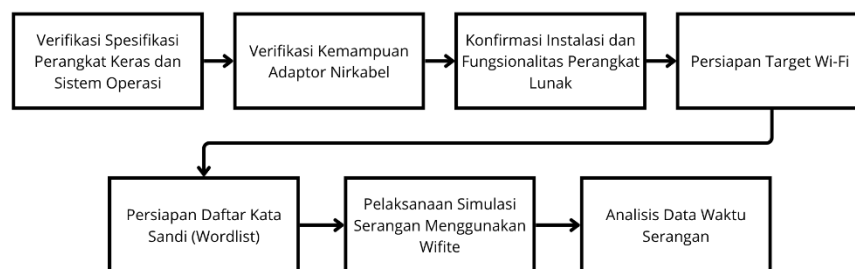
1) Python	8) Packetforge-ng	15) Hcxdumptool
2) Iwconfig	9) Tshark	16) Hcxpcaptool
3) Ifconfig	10) Reaver	17) Wifite
4) Aircrack-ng	11) Bully	
5) Airmo-ng	12) CoWPAtty	
6) Aireplay-ng	13) Ieee-data	
7) Airodump-ng	14) Hashcat	

2. Bahan

Bahan yang diperlukan untuk melakukan kegiatan ini adalah data jaringan yang didapat dari Wi-Fi yang diserang, *wordlist* atau *dictionary file*, dan jaringan Wi-Fi target.

3.3 Tahapan Kegiatan

Kegiatan dengan judul “Evaluasi Keamanan Wi-Fi Berdasarkan Waktu Serangan Terhadap Password Umum Menggunakan Teknik *Dictionary Attack*” memiliki beberapa tahapan pengerjaan yang akan dilaksanakan mengikuti rancangan diagram berikut :



Gambar 3.1 Alur Tahapan Kegiatan

3.3.1 Verifikasi Spesifikasi Perangkat Keras dan Sistem Operasi

Verifikasi Spesifikasi Perangkat ini penting untuk memastikan bahwa sistem memiliki sumber daya yang cukup untuk menjalankan alat-alat pengujian penetrasi yang intensif terutama yang melibatkan *cracking password* secara *offline*. Sistem operasi kali GNU/Linux Rolling dipilih karena merupakan distribusi Linux yang dirancang khusus untuk pengujian penetrasi dan forensik digital, serta telah dilengkapi dengan berbagai alat yang diperlukan.

3.3.2 Verifikasi Kemampuan Adaptor Nirkabel

Salah satu prasyarat teknis paling fundamental untuk pengujian penetrasi Wi-Fi adalah adaptor nirkabel yang mendukung *monitor mode* dan *packet injection*.

Monitor Mode: Memungkinkan kartu nirkabel untuk menangkap semua lalu lintas nirkabel di sekitarnya, tanpa harus terhubung ke jaringan tertentu. Ini krusial untuk alat seperti airodump-ng yang digunakan oleh Wifite untuk memindai jaringan.

Packet Injection: Kemampuan untuk mengirimkan paket data palsu ke jaringan. Ini esensial untuk banyak teknik serangan, termasuk serangan deautentikasi (untuk menangkap WPA *handshake*) dan serangan *brute-force* terhadap WPS PIN.

Kegagalan dalam memenuhi prasyarat *monitor mode* dan *packet injection* dapat menyebabkan Wifite tidak berfungsi secara optimal atau bahkan gagal total, yang akan secara signifikan mempengaruhi validitas pengukuran "kebutuhan waktu serangan".

3.3.3 Konfirmasi Instalasi dan Fungsionalitas Package

Semua *package* yang tercantum dalam dokumen perencanaan awal harus dipastikan terinstal dan berfungsi dengan baik pada sistem Kali GNU/Linux Rolling. Daftar *package* tersebut dapat dilihat pada tabel 3.1 :

Tabel 3.1 Daftar Package

No	Package (Software)	Deskripsi dan Fungsi (terutama untuk cracking WPA/WPA2)
1	Wifite	Skrip Python yang mengotomatiskan proses serangan terhadap jaringan nirkabel terenkripsi WEP, WPA/WPA2, dan WPS. Wifite bertindak sebagai <i>frontend</i> yang menyederhanakan penggunaan berbagai alat <i>backend</i> seperti Aircrack-ng, Reaver, dan PixieWPS. Alat ini dapat mengidentifikasi jaringan, memilih target, dan secara otomatis menjalankan berbagai metode serangan, termasuk <i>dictionary attack</i> dan serangan <i>brute-force</i> . Wifite memprioritaskan serangan berdasarkan karakteristik target, misalnya, menyerang WPS terlebih dahulu jika aktif, kemudian beralih ke PMKID <i>capture</i> atau WPA <i>Handshake capture</i> jika WPS gagal atau tidak aktif. Hasil <i>cracking</i> (kata sandi yang ditemukan) disimpan dalam file <i>cracked.json</i> , dan <i>handshake</i> yang ditangkap biasanya disimpan di direktori <i>hs/</i> .
2	Python	Bahasa pemrograman yang digunakan untuk menulis skrip Wifite. Wifite sendiri adalah sebuah skrip Python yang mengotomatiskan alat-alat lain.
3	Iwconfig	Alat baris perintah Linux yang digunakan untuk mengkonfigurasi antarmuka jaringan nirkabel. Ini dapat digunakan untuk menampilkan atau mengatur parameter nirkabel seperti SSID, mode (misalnya, <i>Managed</i> , <i>Monitor</i>), kanal, dan lainnya. Penting untuk persiapan sebelum serangan, misalnya, untuk memverifikasi mode antarmuka.
4	Ifconfig	Alat baris perintah Linux yang digunakan untuk mengkonfigurasi atau menampilkan parameter antarmuka jaringan (termasuk nirkabel). Meskipun sebagian fungsinya telah digantikan oleh <i>ip</i> , <i>ifconfig</i> masih digunakan untuk menampilkan alamat IP, alamat MAC, dan status antarmuka.
5	Aircrack-ng (suite)	<i>Suite</i> alat keamanan nirkabel yang merupakan <i>backend</i> utama untuk Wifite. Digunakan untuk memantau (menangkap lalu lintas jaringan), menyerang (melakukan serangan deautentikasi, serangan <i>replay</i>), menguji (kemampuan nirkabel perangkat keras), dan melakukan <i>cracking</i> (kunci WEP, WPA, dan WPA2-PSK). Untuk WPA/WPA2, Aircrack-ng menggunakan serangan berbasis kamus (<i>dictionary attack</i>) terhadap <i>handshake</i> yang ditangkap.
6	Airon-ng	Bagian dari <i>suite</i> Aircrack-ng, digunakan untuk mengaktifkan dan menonaktifkan mode monitor (<i>monitor mode</i>) pada antarmuka nirkabel. Mode monitor memungkinkan kartu nirkabel menangkap semua paket Wi-Fi di sekitarnya, yang esensial untuk alat seperti airodump-ng dan Wifite. Perintah <i>airmon-ng check kill</i> digunakan untuk menghentikan proses yang dapat mengganggu mode monitor.

N	Package (Software)	Deskripsi dan Fungsi (terutama untuk cracking WPA/WPA2)
7	Aireplay-ng	Bagian dari <i>suite</i> Aircrack-ng, digunakan untuk menghasilkan atau menyuntikkan (<i>inject</i>) paket. Fungsi utamanya dalam konteks WPA/WPA2 adalah melakukan serangan deautentikasi untuk memaksa klien memutuskan koneksi dari AP dan melakukan koneksi ulang, sehingga memicu <i>4-way handshake</i> baru yang dapat ditangkap. Juga digunakan untuk menguji kemampuan injeksi paket kartu nirkabel (aireplay-ng -9).
8	Airodump-ng	Bagian dari <i>suite</i> Aircrack-ng, digunakan untuk menangkap paket 802.11 mentah. Alat ini menampilkan informasi tentang jaringan Wi-Fi yang terdeteksi (BSSID, ESSID, kanal, enkripsi, kekuatan sinyal, klien yang terhubung) dan merupakan alat utama untuk menangkap WPA/WPA2 <i>handshake</i> atau PMKID. Wifite menggunakan airodump-ng di latar belakang untuk pemindaian dan penangkapan paket. Output dapat disimpan ke file (misalnya, format .cap, .csv).
9	Packetforge-ng	Bagian dari <i>suite</i> Aircrack-ng, digunakan untuk membuat paket terenkripsi arbitrer yang kemudian dapat disuntikkan. Lebih sering digunakan dalam serangan WEP, tetapi secara umum berfungsi untuk memalsukan berbagai jenis paket.
10	Tshark	Alat penangkap dan penganalisis paket jaringan baris perintah, versi terminal dari Wireshark. Wifite dapat menggunakannya untuk menganalisis paket yang ditangkap, misalnya, untuk memverifikasi kelengkapan WPA <i>handshake</i> sebelum mencoba <i>cracking</i> .
11	Reaver	Alat yang dirancang khusus untuk melakukan serangan <i>brute-force</i> terhadap PIN WPS (<i>Wi-Fi Protected Setup</i>). Jika berhasil mendapatkan PIN WPS, Reaver juga dapat memulihkan <i>passphrase</i> WPA/WPA2 jaringan tersebut. Wifite mengotomatiskan penggunaan Reaver untuk serangan WPS PIN.
12	Bully	Alternatif untuk Reaver dalam melakukan serangan <i>brute-force</i> terhadap PIN WPS. Ditulis dalam C dan diklaim memiliki lebih sedikit dependensi. Wifite dapat diinstruksikan untuk menggunakan Bully sebagai pengganti Reaver untuk serangan WPS.
13	CoWPAtty	Alat <i>cracking offline</i> untuk WPA/WPA2 PSK yang menggunakan <i>dictionary attack</i> terhadap <i>handshake</i> yang telah ditangkap. CoWPAtty dapat menggunakan <i>precomputed hash files</i> untuk mempercepat proses <i>cracking</i> untuk SSID tertentu, tetapi ini membutuhkan ruang penyimpanan yang besar.
14	Ieee-data	Menyediakan database referensi penting yang ditetapkan oleh IEEE (<i>Institute of Electrical and Electronics Engineers</i>), badan

N	Package	Deskripsi dan Fungsi (terutama untuk cracking WPA/WPA2)
		yang menetapkan standar untuk teknologi seperti Wi-Fi (802.11).
1	Hashcat	Alat <i>cracking password</i> serbaguna dan sangat cepat yang mendukung berbagai macam algoritma <i>hash</i> , termasuk WPA/WPA2 PMKID (mode 16800) dan WPA <i>Handshake</i> (mode 2500 untuk .hccapx atau mode 22000 untuk .hc22000). Dapat memanfaatkan CPU dan GPU untuk <i>cracking</i> . Wifite dapat mengintegrasikannya untuk <i>cracking offline</i> .
1	Hcxdump	Alat untuk menangkap paket dari perangkat nirkabel, dengan fokus khusus pada penangkapan PMKID dari AP dan <i>handshake</i> dari klien. Sering digunakan sebagai langkah awal sebelum menggunakan hcxpcaptool dan Hashcat untuk <i>cracking</i> PMKID atau <i>handshake</i> .
1	Hcxpcaptool	Bagian dari <i>suite</i> hcxtools, digunakan untuk mengkonversi file <i>capture</i> (pcap/pcapng) yang berisi PMKID atau <i>handshake</i> ke dalam format <i>hash</i> yang dapat digunakan oleh Hashcat (misalnya, format 22000 untuk WPA-PBKDF2-PMKID+EAPOL atau 16800 untuk WPA-PMKID-PBKDF2). Juga dapat digunakan untuk memfilter, memvalidasi, dan memanipulasi data <i>handshake</i> .

Memastikan semua *package* ini terinstal dengan benar dan berfungsi adalah langkah krusial. Wifite, sebagai frontend, sangat bergantung pada fungsionalitas alat-alat backend ini. Hilangnya alat penting dapat menyebabkan Wifite gagal atau memberikan hasil yang tidak akurat.

3.3.4 Persiapan Target Wi-Fi

Setelah lingkungan kegiatan disiapkan, langkah selanjutnya adalah mempersiapkan target Wi-Fi yang akan diuji dan wordlist yang akan digunakan dalam simulasi serangan dictionary attack. Terdapat identifikasi dan Detail Target Wi-Fi, pada kegiatan ini akan menggunakan dua kategori jaringan Wi-Fi sebagai target:

1. Jaringan Wi-Fi Rumah Peneliti: Jaringan ini sepenuhnya berada dalam kendali peneliti, memungkinkan konfigurasi dan pengujian yang fleksibel.
2. Jaringan Wi-Fi Tetangga Peneliti: Jaringan ini akan digunakan dengan izin untuk memastikan kepatuhan terhadap aspek legal dan etika kegiatan.

Untuk setiap jaringan target, informasi detail berikut harus diidentifikasi dan dicatat sebelum simulasi serangan dimulai. Alat seperti airodump-ng (bagian dari suite Aircrack-ng) akan digunakan untuk mengumpulkan informasi ini setelah adaptor nirkabel diatur ke monitor mode.

3.3.5 Persiapan Daftar Kata Sandi (*Wordlist*)

wordlist yang sudah terkumpul, berisi lebih dari 60 juta entri kata sandi, yang diperoleh dari sumber-sumber seperti Sectlist (koleksi wordlist yang populer di komunitas keamanan) dan berbagai situs web yang membagikan wordlist secara daring.

1) Sumber *Wordlist*:

- a. Sectlist: Repositori di GitHub yang berisi berbagai macam wordlist, termasuk kata sandi yang bocor, kata sandi umum, pola umum, dll. Ini adalah sumber yang sangat baik untuk mendapatkan wordlist yang relevan dengan serangan dictionary attack terhadap kata sandi umum.
- b. Sumber Daring Lainnya: Berbagai forum, blog, dan situs web yang didedikasikan untuk keamanan siber seringkali membagikan atau merujuk ke wordlist yang berguna.

2) Variasi dan Struktur Wordlist:

Wordlist yang dikumpulkan kemungkinan besar akan memiliki variasi dalam hal:

- a. Panjang Kata Sandi: Dari kata sandi pendek hingga yang lebih panjang.
- b. Kompleksitas Karakter: Termasuk kata sandi yang hanya terdiri dari huruf kecil, hanya angka, campuran huruf besar-kecil, campuran alfanumerik, dan campuran alfanumerik dengan simbol.
- c. Pola Umum: Kata sandi umum seperti "123456", "password", nama, tanggal lahir, kata-kata kamus, dll..
- d. Kebocoran Data: Kata sandi yang berasal dari kebocoran data nyata.

3) Strategi Penggunaan *Wordlist* dalam Serangan:

Mengingat ukuran *wordlist* yang sangat besar (>60 juta), strategi penggunaannya perlu dipertimbangkan dengan cermat, terutama karena kegiatan ini berfokus pada "kebutuhan waktu serangan". Menggunakan keseluruhan wordlist untuk setiap percobaan cracking *offline* mungkin memakan waktu yang sangat lama, tergantung pada kekuatan perangkat keras yang digunakan untuk cracking. Beberapa pendekatan strategis yang dapat dipertimbangkan:

Tahap 1: Wordlist Umum Teratas: menggunakan sub set wordlist yang lebih kecil berisi kata sandi yang paling umum atau paling sering bocor. Ini akan menguji kerentanan terhadap kata sandi yang sangat lemah.

Tahap 2: Wordlist yang Lebih Besar/Spesifik: Jika tahap 1 gagal, gunakan wordlist yang lebih besar atau wordlist yang telah difilter berdasarkan wilayah Indonesia.

Tahap 3: Wordlist Penuh : Sebagai upaya terakhir, keseluruhan wordlist 60 juta dapat digunakan, namun waktu cracking-nya harus dicatat secara terpisah.

Ukuran wordlist adalah faktor penentu utama dalam durasi Waktu Cracking Offline. Karena kegiatan ini secara spesifik mengevaluasi "kebutuhan waktu serangan", strategi pengelolaan dan penerapan wordlist menjadi variabel yang sangat signifikan. Jika wordlist yang berbeda atau sub set digunakan, hal ini harus didokumentasikan dengan jelas dan dipertimbangkan dalam analisis. Pendekatan yang paling relevan dengan tujuan kegiatan adalah menggunakan wordlist yang

mencerminkan "kata sandi umum", yang mungkin tidak selalu merupakan kata sandi yang sangat kompleks.

3.3.6 Tahapan Pelaksanaan Simulasi Serangan

Setelah persiapan lingkungan dan target selesai, pelaksanaan simulasi serangan menggunakan Wifite dapat dimulai. Wifite mengotomatiskan banyak langkah dalam proses serangan Wi-Fi, mulai dari pemindaian hingga upaya cracking.

3.3.7 Analisis Data Waktu Serangan

Pengukuran parameter yang akurat dan pencatatan hasil yang sistematis adalah esensial untuk mencapai tujuan kegiatan ini. Bagian ini mendefinisikan parameter kunci yang akan diukur dan metode pencatatannya. Untuk setiap simulasi serangan yang dilakukan, parameter-parameter berikut akan diukur dan dicatat dengan cermat pada tabel 3.2 :

Tabel 3.2 Parameter Pengukuran Serangan dan Satuannya

N o	Nama Parameter	Deskripsi Singkat	Satuan Pengukuran (Preferensi)	Metode Pencatatan
1	Waktu Serangan Total (Ttotal)	Durasi dari inisiasi serangan Wifite pada target hingga hasil (berhasil/gagal).	Detik/Menit	Manual (stopwatch/timer digital)
2	Waktu Capture Hash (Tcapture)	Durasi untuk menangkap PMKID atau 4-way <i>handshake</i> yang valid.	Detik/Menit	Manual (dari log Wifite/alat terkait jika memungkinkan, atau observasi kualitatif jika tidak terpisah jelas)
3	Waktu Cracking Offline (Tcrack)	Durasi untuk memecahkan <i>hash</i> (PMKID/ <i>handshake</i>) menggunakan <i>wordlist</i> .	Detik/Menit/Jam	Otomatis (output Aircrack-ng/Hashcat) atau Manual (jika dijalankan terpisah)

BAB 4 HASIL DAN PEMBAHASAN

4.1 Verifikasi Spesifikasi Perangkat Keras dan Sistem Operasi

Tahap pertama dalam pelaksanaan penelitian adalah melakukan verifikasi dan dokumentasi terhadap spesifikasi perangkat keras dan sistem operasi yang digunakan. Langkah ini krusial untuk menjamin tiga pilar utama dari sebuah penelitian yang kredibel: validitas, reliabilitas, dan reproduisibilitas.¹ Dengan mendokumentasikan lingkungan pengujian secara rinci, hasil pengukuran "kebutuhan waktu serangan" yang diperoleh dapat dikontekstualisasikan dengan benar dan memungkinkan peneliti lain untuk mereplikasi eksperimen di masa depan. Verifikasi dilakukan dengan menggunakan utilitas fastfetch pada sistem operasi Kali GNU/Linux Rolling, dan hasilnya disajikan pada Tabel 4.1.

Tabel 4.1 Spesifikasi Perangkat Keras dan Sistem Operasi Lingkungan Pengujian

Komponen	Spesifikasi
Perangkat (Host)	Laptop Acer Swift SF314-54G (V1.17)
Sistem Operasi	Kali GNU/Linux Rolling x86_64
Kernel	Linux 6.12.33+kali-amd64
Prosesor (CPU)	Intel(R) Core(TM) i5-8250U (8 <i>thread</i>) @ 3.40 GHz
Unit Pemroses Grafis (GPU)	GPU 1: NVIDIA GeForce MX150 (Diskret) GPU 2: Intel UHD Graphics 620 (Terintegrasi)
Memori (RAM)	11.57 GiB
Penyimpanan (Disk)	238.28 GiB (Sistem file ext4)

Hasil verifikasi yang disajikan pada Tabel 4.1 mengonfirmasi bahwa lingkungan pengujian telah sesuai dengan rancangan metodologi. Perangkat keras yang digunakan adalah laptop Acer Swift SF314-54G, yang secara akurat merepresentasikan kategori "perangkat keras kelas konsumen" sebagaimana menjadi fokus dalam penelitian ini. Sistem ini dilengkapi dengan konfigurasi GPU ganda, yaitu GPU terintegrasi Intel UHD Graphics 620 untuk tugas-tugas standar dan GPU diskret NVIDIA GeForce MX150. Kehadiran GPU NVIDIA ini menjadi faktor penting, karena alat peretasan kata sandi modern seperti Hashcat dapat memanfaatkan arsitektur CUDA-nya untuk mengakselerasi proses serangan *offline* secara signifikan.

Sistem operasi yang terpasang adalah Kali GNU/Linux Rolling dengan kernel Linux 6.12.33+kali-amd64, yang dipilih karena merupakan platform standar industri untuk pengujian penetrasi dan telah dilengkapi dengan seluruh perangkat lunak yang diperlukan. Spesifikasi prosesor Intel Core i5-8250U dengan 8 *thread* dan memori sebesar 11.57 GiB juga telah diverifikasi dan dianggap memadai untuk menjalankan simulasi serangan dan proses analisis data tanpa mengalami kendala sumber daya yang berarti. Dengan demikian, lingkungan pengujian ini dinyatakan valid dan siap untuk digunakan pada tahapan penelitian selanjutnya.

4.2 Verifikasi Kemampuan Adaptor Nirkabel

Setelah memvalidasi spesifikasi perangkat keras utama, langkah metodologis selanjutnya adalah memverifikasi kapabilitas adaptor nirkabel yang akan digunakan untuk simulasi serangan. Sebagaimana diuraikan pada Bab 3, prasyarat teknis yang paling fundamental untuk pengujian penetrasi Wi-Fi adalah kemampuan adaptor untuk beroperasi dalam mode monitor (*monitor mode*) dan mendukung injeksi paket (*packet injection*). Tanpa kedua fungsi ini, alat-alat serangan seperti yang digunakan dalam penelitian ini tidak dapat beroperasi secara efektif.

Verifikasi dilakukan pada adaptor nirkabel eksternal dengan *chipset Ralink Technology, Corp. MT7601U*, yang teridentifikasi oleh sistem sebagai antarmuka wlan1. Pemilihan adaptor eksternal ini didasarkan pada kompatibilitasnya yang

tinggi dengan *driver* Linux untuk fungsi-fungsi keamanan tingkat lanjut. Proses verifikasi dilakukan melalui serangkaian perintah pada terminal Kali Linux, dan hasilnya dirangkum pada Tabel 4.2.

Tabel 4.2 Hasil Verifikasi Kemampuan Adaptor Nirkabel (wlan1)

Kemampuan	Perintah Verifikasi	Hasil	Status
Deteksi Awal	<code>iwconfig</code>	Antarmuka wlan1 terdeteksi dalam <i>Mode:Managed</i> .	Terverifikasi
Aktivasi Mode Monitor	<code>sudo airmon-ng start wlan1</code>	Mode monitor berhasil diaktifkan pada antarmuka wlan1.	Berhasil
Konfirmasi Mode Monitor	<code>iwconfig wlan1</code>	Output mengonfirmasi antarmuka wlan1 beroperasi dalam <i>Mode:Monitor</i> .	Berhasil
Pengujian Injeksi Paket	<code>sudo aireplay-ng --test wlan1</code>	Output menampilkan pesan <i>Injection is working!</i> dan berhasil mendeteksi 5 <i>Access Point</i> di sekitar.	Berhasil

Berdasarkan hasil pengujian yang disajikan pada Tabel 4.2, adaptor nirkabel wlan1 berhasil diaktifkan dalam mode monitor dan terbukti mampu melakukan injeksi paket. Dengan terpenuhinya kedua prasyarat teknis fundamental ini, adaptor nirkabel yang digunakan dinyatakan layak dan siap untuk mendukung seluruh tahapan simulasi serangan yang akan dilaksanakan.

4.3 Konfirmasi Instalasi dan Fungsionalitas Package

Tahap verifikasi terakhir sebelum memulai simulasi adalah memastikan seluruh *package* perangkat lunak yang diperlukan telah terinstal dan berfungsi

dengan baik. Wifite, sebagai alat otomatisasi utama, sangat bergantung pada fungsionalitas alat-alat *backend* ini untuk setiap fase serangan, mulai dari pemindaian hingga peretasan *offline*.

Sesuai dengan daftar pada Bab 3, dilakukan penyesuaian di mana *package* pyrit digantikan oleh *ieee-data*. Perubahan ini didasarkan pada fakta bahwa pyrit merupakan alat yang sudah usang (*deprecated*), bergantung pada Python 2 yang tidak lagi didukung, dan telah dihapus dari repositori resmi Kali Linux. Sebagai gantinya,

ieee-data diverifikasi karena perannya yang penting dalam menyediakan database OUI (*Organizationally Unique Identifier*) yang memungkinkan alat pemindai untuk mengidentifikasi produsen perangkat keras dari alamat MAC yang terdeteksi.

Verifikasi fungsionalitas dilakukan untuk setiap *package* dengan menjalankan perintah dasar seperti memanggil halaman bantuan (`--help`) atau versi (`--version`). Hasil konfirmasi untuk seluruh *toolchain* disajikan secara rinci pada Tabel 4.3.

Tabel 4.3 Hasil Konfirmasi Instalasi dan Fungsionalitas *Package* Perangkat Lunak

No	Nama <i>Package</i>	Metode Verifikasi	Hasil	Status
1	Wifite	wifite -h	Menampilkan menu bantuan, Versi 2.7.0	Terverifikasi
2	Python	python3 --version	Menampilkan versi Python 3.13.5	Terverifikasi
3	Iwconfig	iwconfig --version	Menampilkan versi Wireless-Tools 30	Terverifikasi
4	Ifconfig	ifconfig --version	Menampilkan versi net-tools 2.10	Terverifikasi

No	Nama <i>Package</i>	Metode Verifikasi	Hasil	Status
5	Aircrack-ng	aircrack-ng --help	Menampilkan menu bantuan, Versi 1.7	Terverifikasi
6	Airmon-ng	sudo airmon-ng --help	Menampilkan menu bantuan	Terverifikasi
7	Aireplay-ng	sudo aireplay-ng --help	Menampilkan menu bantuan, Versi 1.7	Terverifikasi
8	Airodump-ng	sudo airodump-ng --help	Menampilkan menu bantuan, Versi 1.7	Terverifikasi
9	Packetforge-ng	sudo packetforge-ng --help	Menampilkan menu bantuan, Versi 1.7	Terverifikasi
10	Tshark	tshark -v	Menampilkan versi TShark (Wireshark) 4.4.7	Terverifikasi
11	Reaver	reaver --help	Menampilkan menu bantuan, Versi 1.6.6	Terverifikasi
12	Bully	bully --help	Menampilkan menu bantuan, Versi 1.4	Terverifikasi
13	CoWPAtty	sudo apt install cowpatty	Berhasil diinstal dari repositori	Terverifikasi
14	Ieee-data	dpkg -l grep ieee-data	Paket terinstal, Versi 20240722	Terverifikasi
15	Hashcat	hashcat --version	Menampilkan versi v6.2.6	Terverifikasi

No	Nama <i>Package</i>	Metode Verifikasi	Hasil	Status
16	Hcxdumptool	hcxdumptool --version	Menampilkan versi 6.3.5	Terverifikasi
17	Hcxpcaptool	dpkg -l grep hcxtools	Paket hcxtools terinstal, Versi 6.3.5	Terverifikasi

Hasil verifikasi pada Tabel 4.3 menunjukkan bahwa seluruh 17 *package* perangkat lunak yang diperlukan untuk penelitian ini telah berhasil diinstal dan berfungsi sesuai harapan. Dengan selesainya verifikasi perangkat keras, kemampuan adaptor nirkabel, dan fungsionalitas

toolchain perangkat lunak, lingkungan penelitian secara keseluruhan dinyatakan siap dan valid untuk melanjutkan ke tahap persiapan target dan pelaksanaan simulasi serangan.

4.4 Persiapan Target Wi-Fi (AP)

Setelah seluruh lingkungan pengujian divalidasi, langkah selanjutnya adalah mempersiapkan jaringan Wi-Fi yang akan menjadi target simulasi serangan. Penelitian ini menggunakan tiga kategori jaringan Wi-Fi yang berbeda untuk mencakup skenario yang beragam:

1. Jaringan Wi-Fi Rumah: Jaringan ini sepenuhnya berada dalam kendali, memungkinkan konfigurasi dan pengujian yang fleksibel untuk berbagai skenario kata sandi dan keamanan.
2. Jaringan Wi-Fi Tetangga: Jaringan ini digunakan setelah mendapatkan izin dari pemiliknya untuk memastikan kepatuhan terhadap aspek legal dan etika penelitian.
3. Jaringan Wi-Fi Laboratorium Politeknik Negeri Jember: Sesuai dengan lokasi utama yang ditetapkan pada Bab 3, sebuah jaringan target disiapkan secara khusus di lingkungan akademis. Lokasi ini bertujuan untuk menciptakan skenario pengujian yang terkontrol dan dapat diulang, yang penting untuk memastikan validitas dan reliabilitas data yang diperoleh.

Tabel 4.4 Spesifikasi Target Wi-Fi Pengujian

ID Target	SSID	BSSID	Channel	Jenis Enkripsi	Chipset	Status WPS	Perkiraan Jarak (m)	Model Router
TGT_01	ratu	18:69:DA:3C:BC:F7	1	WPA2	CCMP		13	H1s-3
TGT_02	Alhamdulillah	34:DA:B7:EE:8B:61	6	WPA2	CCMP	Yes	7	ZTE F609
TGT_03	toko-bahagia	50:0F:F5:24:03:D1	10	WPA2	CCMP	No	4	Tenda N300
TGT_04	Anton Febryando	C4:EB:FF:22:FB:6E	4	WPA2	CCMP	Yes	6	ZTE
TGT_05	AJK-STUDENT	78:8A:20:DD:52:C8	11	WPA3	SAE	No	3	Ubiquiti UniFi AP
TGT_06	AJK-SUDENT2	8A:8A:20:DD:52:C8	11	WPA2	CCMP	No	3	Ubiquiti UniFi AP
TGT_07	TP-Link_AP_6282	B0:4E:26:B9:62:82	1	WPA2	CCMP	Yes	5	TP-Link AP

4.5 Persiapan Daftar Kata Sandi (*Wordlists*)

Dalam kerangka pengujian keamanan jaringan nirkabel berbasis WPA2-PSK, efektivitas serangan *dictionary attack* tidak semata-mata ditentukan oleh kekuatan komputasi perangkat keras yang digunakan, melainkan sangat bergantung pada kualitas, relevansi, dan strategi penggunaan daftar kata sandi (*wordlist*). Berbeda dengan pendekatan *brute-force* murni yang mencoba segala kombinasi karakter, penelitian ini menerapkan strategi Serangan Bertahap (Staged Attack Strategy). Strategi ini dirancang untuk meniru perilaku penyerang efisien yang memprioritaskan "kemenangan cepat" (*quick wins*) sebelum mengalokasikan sumber daya waktu untuk serangan yang lebih masif.

Berdasarkan strategi ini, penelitian menyiapkan tiga kategori *wordlist* yang akan dieksekusi secara berurutan (Tahap 1 hingga Tahap 3). Setiap tahap merepresentasikan tingkat kompleksitas dan probabilitas yang berbeda, mulai dari kata sandi standar bawaan sistem hingga kombinasi masif dari berbagai insiden kebocoran data.

4.5.1 Wordlist dan Tahapan Serangan

Pemilihan *wordlist* dalam penelitian ini tidak dilakukan secara acak, melainkan dikurasi untuk mencakup tiga vektor ancaman utama: kerentanan bawaan (default), konteks lokal Indonesia, dan serangan skala besar (big data). Berikut adalah rincian spesifikasi teknis untuk setiap tahapan serangan:

Tahap 1: Serangan Kredensial Probabilitas Tinggi (High Probability Attack) Tahap ini menggunakan file *wordlist-probable.txt*. File ini merupakan bagian dari *metapackage* *kali-tools-passwords* yang tersedia secara *default* pada sistem operasi Kali Linux dan menjadi referensi utama bagi alat otomatisasi Wifite.

- **Sumber:** Repositori Kali Linux (/usr/share/dict/wordlist-probable.txt).
- **Ukuran File:** 2.1 MB.
- **Jumlah Entri:** 203.808 kata sandi.
- **Rasionalisasi:** Daftar ini berisi kumpulan kata sandi yang secara statistik paling sering ditemukan pada konfigurasi WPA/WPA2 global. Tahap ini bertujuan mensimulasikan serangan terhadap target yang sangat lemah atau

menggunakan konfigurasi *default* pabrik. Jika serangan ini berhasil, waktu yang dibutuhkan praktis mendekati nol (instan).

Tahap 2: Serangan Kontekstual Lokal (Indonesian Context Attack) Jika

Tahap 1 gagal, serangan dilanjutkan menggunakan file *ind-hash.txt*. Daftar ini dikumpulkan dari berbagai forum komunitas keamanan siber daring (*online forums*) yang secara spesifik mengompilasi kata sandi yang umum digunakan oleh pengguna di Indonesia.

- **Sumber:** Forum Komunitas Daring.
- **Ukuran File:** 3.6 MB.
- **Jumlah Entri:** 337.941 kata sandi.
- **Rasionalisasi:** Pengguna di wilayah geografis tertentu cenderung menggunakan pola kata sandi yang mengandung istilah bahasa lokal, nama daerah, atau slang setempat yang tidak tercakup dalam wordlist global. Tahap ini menguji hipotesis bahwa relevansi budaya (*cultural relevance*) dalam sebuah kamus serangan dapat meningkatkan tingkat keberhasilan peretasan secara signifikan.

Tahap 3: Serangan Skala Masif (Massive Dictionary Attack) Sebagai upaya

terakhir (*last resort*), penelitian menggunakan file *seclist.txt*. Ini adalah *wordlist* komprehensif yang merupakan hasil penggabungan (*merge*) dari koleksi SecLists, RockYou, dan berbagai dataset kebocoran data lainnya.

- **Sumber:** Gabungan koleksi *wordlist* publik (Aggregated Lists).
- **Ukuran File:** Sangat Besar (estimasi >500 MB).
- **Jumlah Entri:** >60.000.000 (60 Juta) kata sandi.
- **Rasionalisasi:** Tahap ini mensimulasikan penyerang yang memiliki dedikasi waktu tinggi. Dengan cakupan lebih dari 60 juta kata, daftar ini menguji ketahanan *passphrase* terhadap serangan menyeluruh yang mencakup variasi karakter, angka, dan pola kompleks yang pernah bocor di internet.

Tabel 4.5 Spesifikasi Wordlist Berdasarkan Tahapan Serangan

Tahapan	Nama File	Kategori	Jumlah Entri	Ukuran	Target Pengujian
Tahap 1	wordlist-probable.txt	Default/Globa	203,808	2.1 MB	Kata sandi lemah & umum
Tahap 2	Ind-hash.txt	Lokal/Indonesia	337,941	3.6 MB	Kata sandi berbasis bahasa/budaya Indonesia
Tahap 3	Seclist.txt	Massive/Combined	63,726,990	794 MB	Serangan menyeluruh

4.6 Pelaksanaan Simulasi Serangan

Subbab ini menguraikan secara rinci tahapan pelaksanaan simulasi serangan nirkabel terhadap seluruh jaringan target pada berbagai skenario lingkungan pengujian. Proses evaluasi ini mencakup keseluruhan fase operasional, mulai dari inisialisasi perangkat penyerang, penangkapan berkas handshake maupun PMKID, hingga tahap validasi integritas data.

4.6.1 Tinjauan Umum dan Arsitektur Lingkungan Pengujian

Bagian ini menyajikan analisis komprehensif, granular, dan faktual mengenai pelaksanaan simulasi serangan siber yang dilakukan sebagai inti dari penelitian evaluasi keamanan jaringan nirkabel. Pengujian ini tidak hanya berorientasi pada ketahanan kata sandi (password cracking), melainkan juga membedah secara forensik interaksi antara framework otomatisasi penyerang, protokol IEEE 802.11, serta kondisi lingkungan fisik di lapangan.

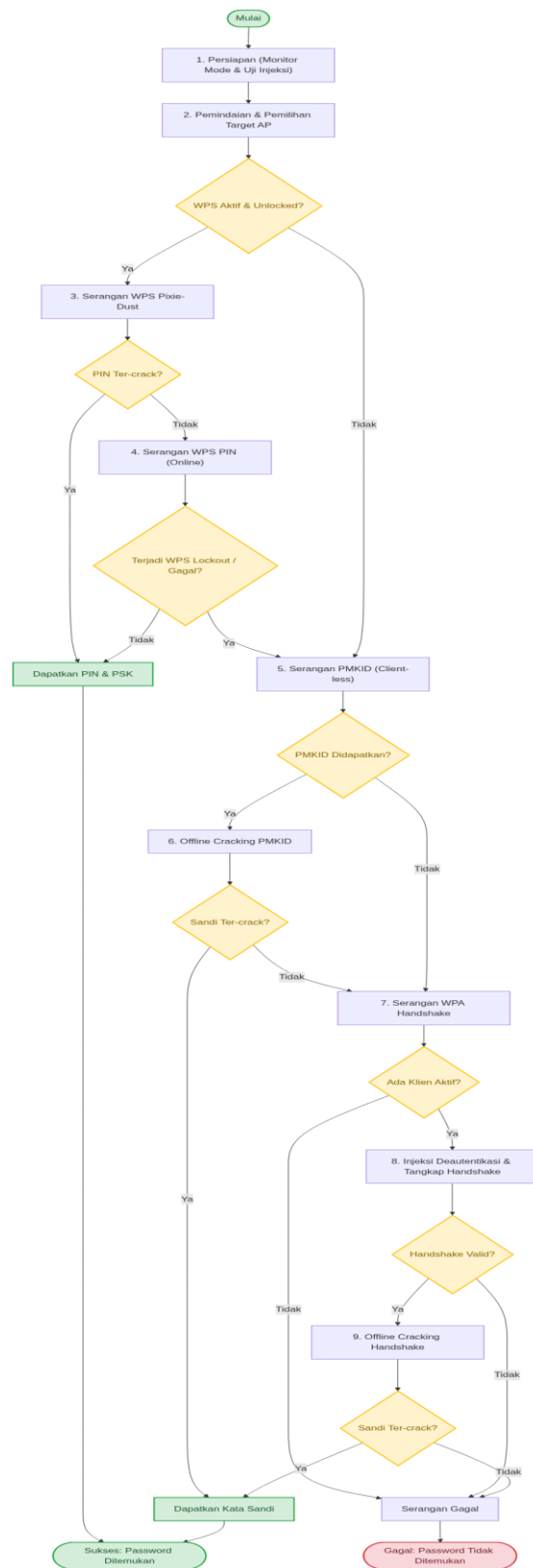
Simulasi serangan ini dilakukan terhadap dua kelompok lingkungan pengujian yang berbeda untuk mendapatkan analisis yang representatif:

1. Lingkungan Perumahan (Residential): Merepresentasikan jaringan Wi-Fi rumah tangga yang berada di Perumahan Bernady Land, Slawu, Kecamatan Patrang, Kabupaten Jember. Target pada lingkungan ini adalah TGT_01 ("ratu"), TGT_02 ("Alhamdulillah"), TGT_03 ("Toko-bahagia"), dan TGT_04 ("Anton Febryando").

2. Lingkungan Laboratorium Kampus (Politeknik Negeri Jember): Merepresentasikan jaringan nirkabel di lingkungan akademis dengan konfigurasi terkelola dan fitur keamanan tambahan. Target pada lingkungan ini adalah TGT_04 ("AJK-STUDENT"), TGT_05 ("AJK-SUDENT2"), dan TGT_06 ("TP-Link_AP_6282").

Stasiun penyerang dikonfigurasi menggunakan laptop Acer Swift SF314-54G yang menjalankan sistem operasi khusus Kali GNU/Linux Rolling. Antarmuka nirkabel utama yang digunakan adalah adaptor jaringan nirkabel eksternal dengan chipset Ralink MT7601U yang dikenali sistem sebagai antarmuka wlan1. Driver mac80211 pada Kali Linux memungkinkan aktivasi mode monitor (monitor mode) dan injeksi paket nementah (packet injection) secara stabil.

Prosedur penyerangan diorkestrasi secara otomatis oleh framework Wifite v2.7.0. Perangkat lunak ini bertindak sebagai front-end yang mengintegrasikan berbagai peralatan backend pertahanan dan penyerangan nirkabel, seperti aircrack-ng suite (untuk airodump-ng, aireplay-ng, airmon-ng), reaver dan bully (untuk eksploitasi WPS), pixiewps (untuk kalkulasi offline Pixie-Dust), serta tshark (untuk analisis kelengkapan frame jabat tangan).



Gambar 4.1 Diagram Alur Serangan Wifite v2.7.0

4.6.2 Inisialisasi Perangkat dan Transisi Mode Monitor

Sebelum melakukan pemindaian aktif terhadap target nirkabel, kartu jaringan wlan1 dikondisikan ke dalam status operasional optimal. Langkah pertama adalah menghentikan proses-proses sistem yang dapat mengganggu kontrol eksklusif pada adaptor nirkabel, seperti NetworkManager dan wpa_supplicant. Layanan-layanan ini sering kali memaksa antarmuka nirkabel kembali ke Managed mode atau melakukan pemindaian latar belakang (background scanning) secara berkala, yang dapat mengganggu proses pemindaian saluran (channel hopping) oleh penyerang. Eksekusi perintah check kill dilakukan sebagai berikut:

```
sudo airmon-ng check kill
```

Perintah tersebut secara paksa menghentikan proses wpa_supplicant dan NetworkManager. Setelah lingkungan bersih dari interupsi sistem, antarmuka wlan1 ditransisikan dari managed mode ke monitor mode menggunakan perintah:

```
sudo airmon-ng start wlan1
```

Perintah ini menonaktifkan filter perangkat keras pada kartu nirkabel, sehingga dapat beroperasi dalam mode promiscuous radio. Dalam mode ini, antarmuka nirkabel (diidentifikasi sebagai wlan1mon atau tetap wlan1 tergantung pada driver) mampu menangkap seluruh bingkai 802.11

(seperti Beacon, Probe Request, Probe Response, Data, dan EAPOL) yang melayang di udara tanpa memedulikan alamat MAC tujuan. Fungsionalitas monitor mode dikonfirmasi melalui iwconfig, dilanjutkan dengan pengujian kemampuan injeksi paket (packet injection) menggunakan aireplay-ng untuk memastikan paket pemutus koneksi (deauthentication) dapat disuntikkan secara sukses ke udara.

4.6.3 Kronologi Simulasi Serangan Jaringan Perumahan (Residential)

Pengujian pada lingkungan perumahan difokuskan pada tiga Access Point (AP) dengan tingkat kerentanan, model router, dan jarak fisik yang bervariasi dari stasiun penyerang.

1. Target 03 (TGT_03: Toko-bahagia)

Target TGT_03 beroperasi pada Channel 10 dengan SSID "toko-bahagia" dan alamat MAC (BSSID) 50:0F:F5:24:03:D1 (router Tenda N300). Jarak stasiun penyerang ke AP sangat dekat, yakni ± 4 meter dengan sinyal yang sangat kuat (RSSI -63 dBm s.d -69 dBm). Pada pengujian tanpa cache (clean session), berikut adalah kronologi serangan yang tercatat secara riil:

a. Eksploitasi PMKID (Client-less Attack):

- Wifite mengunci target pada pukul 12:53:14 dan langsung meluncurkan upaya penangkapan PMKID.
- Waktu Tunggu Capture: Setelah memantau saluran selama tepat 11 detik (pukul 12:53:14 s.d 12:53:25), Wifite berhasil menangkap bingkai PMKID target ("Captured PMKID") dan menyimpannya sebagai file cadangan `hs/pmkid_tokobahagia_50-0F-F5-24-03-D1_2026-05-25T12-53-25.22000`.
- Cracking Offline PMKID: Detik itu juga (pukul 12:53:25 s.d 12:53:26), Wifite memproses file hash PMKID tersebut menggunakan kamus global `wordlist-probable.txt`. Hanya dalam durasi 1 detik, kata sandi berhasil dipecahkan ("PMKID CRACKED: Key: 1234567890").

b. Penangkapan WPA2 Handshake (Deauthentication & EAPOL Capture):

- Meskipun data PMKID berhasil didapatkan, untuk kepentingan evaluasi protokol, Wifite melanjutkan siklus ke penangkapan WPA 4-Way Handshake pada pukul 12:53:27. Terdeteksi satu klien aktif dengan alamat MAC `CE:05:C0:7D:15:22`.
- Pemantauan Pasif: Wifite mendengarkan lalu lintas secara pasif selama 17 detik pertama (pukul 12:53:27 s.d 12:53:44) untuk menangkap handshake secara alami.

- Serangan Deauthentication Aktif: Setelah tidak ada paket handshake alami yang masuk, pada pukul 12:53:44 Wifite menyuntikkan bingkai Deauthentication aktif ke alamat MAC klien menggunakan aireplay-ng.
- Keberhasilan Penangkapan: Hanya butuh waktu 1 detik setelah paket deautentikasi dikirim (pukul 12:53:45), klien terputus dan melakukan asosiasi ulang secara instan. Wifite berhasil merekam paket handshake utuh dan menyimpannya ke file `hs/handshake_tokobahagia_50-0F-F5-24-03-D1_2026-05-25T12-53-45.cap`.
- Cracking Offline Handshake: File jabat tangan tersebut kemudian divalidasi oleh tshark, cowpatty, dan aircrack-ng, lalu diuji menggunakan Hashcat (mode 22000) pada pukul 12:53:45 s.d 12:53:46. WPA Handshake berhasil di-crack dalam waktu 1 detik dengan kata sandi yang sama ("Key: 1234567890")

2. Target 02 (TGT_02: Alhamdulillah)

Target TGT_02 menggunakan SSID "Alhamdulillah" dengan BSSID 34:DA:B7:EE:8B:61 (router ZTE F609). Jarak stasiun penyerang adalah ± 7 meter dengan kekuatan sinyal sedang-lemah (RSSI berfluktuasi antara -20 dBm hingga -31 dBm pada stasiun monitor) dan beroperasi pada Channel 6. Pengujian dilakukan melalui dua sesi penyerangan terpisah yang menunjukkan dinamika serangan yang sangat kontras:

a. Sesi Pertama (Eksplorasi WPS, PMKID, dan Kegagalan Handshake):

- Serangan WPS (Pixie-Dust dan PIN): Wifite memprioritaskan serangan WPS karena terdeteksi aktif pada router target. Namun, serangan WPS Pixie-Dust dan WPS NULL PIN masing-masing mengalami kegagalan setelah berjalan selama tepat 5 menit (timeout 300 detik). Serangan WPS PIN Attack juga dilewati setelah berjalan 2 menit tanpa respons kunci. Hal ini menunjukkan firmware ZTE F609 memiliki proteksi yang kuat terhadap serangan brute-force online dan mitigasi kerentanan RNG.
- Eksploitasi PMKID (Sukses): Setelah kegagalan WPS, pada pukul 13:36:23 Wifite otomatis beralih ke serangan PMKID. Hanya dalam waktu

kurang dari 1 detik, berkas PMKID berhasil ditangkap dan disimpan ke `hs/pmkid_Alhamdulillah_34-DA-B7-EE-8B-61_2026-05-25T13-36-23.22000`. Berkas hash PMKID ini berhasil dipecahkan secara offline dalam waktu 4 detik (pukul 13:36:23 s.d 13:36:27) menggunakan kamus `wordlist-probable.txt` dengan hasil kata sandi: **bismillah**.

- Penangkapan Handshake (Gagal): Untuk menguji keutuhan jabat tangan, Wifite melanjutkan ke penangkapan WPA Handshake mulai pukul 13:36:29. Meskipun terdeteksi 5 klien aktif dan dikirim paket deautentikasi berulang, fluktuasi sinyal dan interferensi di Channel 6 yang padat membuat paket M2 dari klien gagal tertangkap. Setelah berjalan selama 5 menit, serangan dihentikan dengan status FAILED (timeout 300 detik).

b. Sesi Kedua (Keberhasilan Handshake via Deautentikasi Klien Padat):

- Pengujian diulang pada pukul 13:52:19. Upaya serangan WPS langsung dilewati secara manual untuk efisiensi waktu.

- Penggunaan Cache PMKID: Wifite secara otomatis mendeteksi berkas PMKID dari sesi pertama dan langsung memproses pemecahan kata sandi secara instan (0 detik) dengan hasil yang sama: **Key: bismillah**.

- Penangkapan Handshake (Sukses): Serangan penangkapan handshake dimulai pada pukul 13:52:37. Saat itu, kepadatan klien aktif meningkat menjadi 8 klien. Setelah memantau secara pasif selama 21 detik, pada pukul 13:52:58 Wifite melancarkan broadcast deauthentication secara agresif ke seluruh 8 klien. Hal ini langsung memicu salah satu klien melakukan reasosiasi instan. WPA Handshake berhasil ditangkap lengkap pada pukul 13:52:58 dan disimpan ke `hs/handshake_Alhamdulillah_34-DA-B7-EE-8B-61_2026-05-25T13-52-59.cap`. Berkas handshake ini berhasil di-crack secara offline menggunakan Hashcat (mode 22000) dalam waktu 1.0 detik dengan kata sandi: **bismillah**.

3. Target 01 (TGT_01: ratu)

Target TGT_01 beroperasi pada Channel 1 dengan SSID "ratu" dan BSSID 18:69:DA:3C:BC:F7 (router H1s-3). AP ini berada pada jarak terjauh, yaitu ± 13 meter dengan halangan berupa dinding beton tebal. Sinyal yang diterima sangat lemah dan fluktuatif di ambang batas sensitivitas kartu nirkabel Ralink MT7601U (RSSI < -80 dBm).

a. Eksploitasi PMKID (Client-less Attack):

Mengingat sinyal klien yang terhubung sangat lemah untuk ditangkap secara asimetris (masalah Hidden Node), Wifite mencoba melakukan serangan PMKID tanpa klien. Proses ini dilakukan dengan mengirimkan bingkai Association Request langsung ke router H1s-3 untuk memicu respons pesan M1 yang membawa Robust Security Network Information Element (RSN IE) yang berisi PMKID. Namun, setelah beberapa kali percobaan, router H1s-3 tidak mengembalikan bingkai PMKID. Hal ini membuktikan router tersebut tidak mendukung fitur roaming cepat (802.11r) atau fitur tersebut dinonaktifkan secara total.

b. Kegagalan Serangan Deauthentication Jarak Jauh:

Wifite kemudian mencoba metode deautentikasi klien. Meskipun log menunjukkan pengiriman paket deautentikasi secara terus-menerus ke alamat MAC klien, tidak ada bingkai Acknowledgment (ACK) yang diterima kembali oleh stasiun penyerang. Lemahnya daya pancar adaptor nirkabel pada jarak 13 meter menembus dinding beton membuat paket deautentikasi tidak sampai dengan integritas yang cukup di sisi klien.

Sekalipun dalam beberapa momen klien terputus secara tidak sengaja, stasiun penyerang gagal menangkap pesan M2 dari klien karena daya pancar transceiver Wi-Fi klien (biasanya smartphone dengan daya TX rendah) tidak mampu menjangkau stasiun penyerang. Setelah mencapai batas waktu (timeout) 10 menit tanpa mendapatkan data handshake yang valid (Missing M2/MIC), Wifite menghentikan serangan dengan status "Capture Failed".

4. Target 04 (TGT_04: Anton Febryando)

Target TGT_04 beroperasi pada Channel 4 dengan SSID "Anton Febryando" dan BSSID C4:EB:FF:22:FB:6E. AP ini berada pada lingkungan

perumahan dengan kekuatan sinyal yang terdeteksi berkisar antara -61 dBm hingga -65 dBm (PWR 35dB s.d. 39dB) dengan status WPS aktif (Yes). Terdapat 2 klien yang terasosiasi secara aktif pada saat simulasi serangan dilakukan.

a. Eksploitasi WPS dan PMKID (Sesi Awal):

Pada pengujian awal, simulasi dimulai dengan metode serangan WPS Pixie-Dust. Namun, setelah berjalan selama sekitar 5 menit, proses pengiriman paket EAPOL terinterupsi secara manual tanpa menghasilkan PIN. Penyerang kemudian beralih ke metode pasif client-less untuk menangkap PMKID. Dalam waktu 50 detik, berkas PMKID berhasil diperoleh dan disimpan pada file `hs/pmkid_AntonFebryando_C4-EB-FF-22-FB-6E_2026-05-26T12-40-42.22000`. Hal ini membuktikan bahwa target rentan terhadap akuisisi material kunci secara pasif.

b. Akuisisi Handshake via Serangan Deauthentication Aktif (Sesi Lanjutan):

Pada pengujian lanjutan, serangan difokuskan pada penangkapan handshake nirkabel. Penyerang melancarkan deautentikasi aktif (broadcast dan spesifik) terhadap 2 klien yang terdeteksi. Serangan ini memutus salah satu klien, memicu asosiasi ulang, dan memungkinkan penangkapan 4-way handshake yang sah dalam waktu 14 detik. Integritas berkas handshake yang didapat (tersimpan di `hs/handshake_AntonFebryando_...cap`) telah divalidasi dan dinyatakan valid oleh utilitas `tshark`, `cowpatty`, dan `aircrack-ng`.

4.6.4 Kronologi Simulasi Serangan Jaringan Laboratorium Kampus (AJK)

Pengujian pada lingkungan Laboratorium Kampus di Politeknik Negeri Jember merepresentasikan kondisi jaringan terkelola dengan protokol keamanan yang lebih ketat serta pengujian terhadap router yang rentan.

1. Target 05 (TGT_05: AJK-STUDENT)

Target TGT_05 beroperasi pada Channel 11 dengan SSID "AJK-STUDENT" dan terenkripsi menggunakan protokol WPA3-SAE (WPA3-Personal) dengan status WPS tidak aktif (No). Kekuatan sinyal yang diterima berkisar antara -55 dBm hingga -60 dBm dengan 2 klien yang terasosiasi secara aktif.

a. Eksploitasi PMKID dan Hambatan Autentikasi:

Sistem penyerang mendeteksi karakteristik jaringan nirkabel melalui Beacon Frame. Elemen RSN (Robust Security Network) mengonfirmasi penggunaan WPA3 dengan cipher suite khusus. Wifite mencoba mengambil PMKID (PMKID Capture) secara langsung dengan mengirimkan asosiasi nirkabel standar, namun status pengembalian PMKID dilaporkan "Failed to capture PMKID". Protokol WPA3-SAE secara default menolak pertukaran PMKID dengan stasiun yang tidak dikenal guna menangkal serangan pra-komputasi offline.

b. Kegagalan Serangan Deauthentication pada WPA3:

Wifite mencoba meluncurkan serangan deautentikasi terhadap klien terhubung dengan mengirimkan paket deautentikasi palsu. Namun, log terminal mencatat kegagalan total:

- "WPA Handshake capture: Waiting for target to appear..."
- "Target timeout: Target did not appear after 60 seconds, target may be out of range or turned off"

Secara teknis, kegagalan ini disebabkan oleh fitur Protected Management Frames (PMF) yang didefinisikan dalam standar IEEE 802.11w. Pada protokol WPA3, penggunaan PMF bersifat wajib (mandatory). Bingkai manajemen seperti Deauthentication dan Disassociation ditransmisikan dalam kondisi terenkripsi dan terautentikasi secara kriptografis menggunakan kunci IGK (Integrity Group Key). Akibatnya, paket deautentikasi palsu yang disuntikkan oleh aireplay-ng (yang tidak memiliki kunci kriptografis yang sah) langsung dibuang oleh perangkat klien sebagai paket ilegal, sehingga klien tetap terhubung secara aman tanpa mengalami re-handshake.

2. Target 06 (TGT_06: AJK-SUDENT2)

Target TGT_06 beroperasi pada Channel 11 dengan SSID "AJK-SUDENT2" (salah satu variasi SSID laboratorium) dengan enkripsi WPA2-Personal (CCMP). Kekuatan sinyal stabil pada -61 dBm, namun tidak terdeteksi adanya klien aktif (0 clients) yang terasosiasi saat pemindaian awal.

a. Kegagalan PMKID Capture:

Wifite mencoba eksploitasi PMKID secara otomatis untuk mengantisipasi ketiadaan klien, namun router target tidak mengembalikan frame PMKID ("Failed to capture PMKID").

b. Hambatan Ketiadaan Klien Aktif:

Wifite mencoba mendengarkan jabat tangan autentikasi secara pasif dan aktif selama 300 detik (5 menit):

- "WPA Handshake capture: Listening. (clients:0, deauth:3s, timeout:0s)"
- "WPA handshake capture FAILED: Timed out after 300 seconds"

Karena tidak adanya klien yang melakukan pertukaran data autentikasi 4-Way Handshake dengan AP selama waktu tunggu, stasiun penyerang tidak memiliki data yang dapat ditangkap. Eksperimen ini memvalidasi kelemahan mendasar serangan WPA2 Handshake Capture konvensional yang sangat bergantung pada keberadaan interaksi klien aktif di jaringan target.

3. Target 07 (TGT_07: TP-Link_AP_6282)

Target TGT_07 beroperasi pada Channel 1 (kemudian berpindah ke Channel 10 pada sesi berikutnya) dengan SSID "TP-Link_AP_6282" dan BSSID B0:4E:26:B9:62:82. Perangkat keras target teridentifikasi sebagai Access Point TP-Link kelas menengah. Kekuatan sinyal sangat kuat, berfluktuasi antara -68 dBm hingga -76 dBm dengan fitur WPS aktif (Status: Yes).

a. Keberhasilan Eksploitasi WPS Pixie-Dust:

Wifite memprioritaskan serangan WPS Pixie-Dust karena status WPS terdeteksi aktif.

- Stasiun penyerang mengirimkan paket EAPOL-Start ke BSSID B0:4E:26:B9:62:82.
- Terjadi pertukaran paket M1 dan M2 untuk bertukar public key Diffie-Hellman dan nonces.
- Wifite menangkap pesan M3 yang berisi hash terenkripsi dari PIN WPS.
- Utilitas pixiewps di latar belakang berhasil memecahkan kelemahan generator bilangan acak (PRNG) pada chipset TP-Link tersebut secara instan.

- Log terminal mencatat keberhasilan sebagai berikut:

- "WPS Pixie-Dust: [4m55s] Cracked WPS PIN: 78092129"
- "ESSID: TP-Link_AP_6282"
- "BSSID: B0:4E:26:B9:62:82"
- "Encryption: WPA (WPS)"
- "WPS PIN: 78092129"
- "PSK/Password: 78092129"
- "saved result to cracked.json"

Melalui serangan Pixie-Dust ini, PIN WPS berhasil di-crack dalam waktu kurang dari 5 menit, dan kata sandi WPA asli jaringan langsung terungkap, yaitu "78092129".

b. Pengujian Redundansi Serangan WPA2 Handshake & Cracking Offline:

Untuk memverifikasi skenario redundansi serangan, stasiun penyerang mencoba melakukan penangkapan WPA Handshake pada target yang sama:

- Wifite mendeteksi jabat tangan yang telah ditangkap sebelumnya di direktori lokal: `hs/handshake_TPLinkAP6282_B0-4E-26-B9-62-82_2026-03-31T16-21-05.cap`.
- Validasi jabat tangan dilakukan menggunakan `tshark` dan `aircrack-ng`, mengonfirmasi bahwa file capture tersebut berisi struktur handshake EAPOL yang valid untuk alamat MAC B0:4E:26:B9:62:82.
- Wifite mencoba menjalankan Hashcat (mode 22000) secara offline menggunakan daftar kata sandi bawaan `wordlist-probable.txt`.
- Hasil cracking menunjukkan status "key unknown", yang berarti kata sandi "78092129" tidak terdapat di dalam wordlist 200 ribu entri tersebut.

Eksperimen ini memberikan temuan penting: meskipun kata sandi aman dari serangan dictionary attack offline dasar karena tidak terdaftar dalam wordlist, jaringan tetap rentan dan berhasil ditembus secara total melalui celah keamanan WPS Pixie-Dust.

4.6.5 Analisis Komparatif Dinamika Serangan

Tabel 4.6 merangkum perbandingan parameter teknis dan hasil simulasi serangan terhadap keenam target yang diuji pada lingkungan perumahan dan laboratorium kampus.

Tabel 4.6 Analisis Komparatif Hasil Simulasi Serangan Wifite

ID Target	SSID	Lingkungan	RSSI (dBm)	Enkripsi	Vektor Utama	Hasil Akhir	Keterangan / Penyebab
TG T_01	ratu	Perumahan	-80 s.d - 88	WPA2 - CCMP	WPA Handshake (via Optimasi Jarak)	SUKSES	Handshake berhasil diperoleh setelah dilakukan penyesuaian posisi fisik/jarak. Kata sandi '19111991' berhasil dipecahkan secara offline.
TG T_02	Alhamdulillah	Perumahan	-20 s.d - 31	WPA2 - CCMP	PMKID & Deauth	SUKSES	Handshake didapat via deauth massal (8 klien), PMKID didapat via client-less. Kata sandi 'bismillah' terpecahkan.
TG T_03	toko-bahagia	Perumahan	-67 s.d - 69	WPA2 - CCMP	PMKID & Deauth	SUKSES	PMKID didapat via client-less attack, handshake didapat via deauth.
TG T_04	Anton Febryando	Perumahan	-61 s.d - 65	WPA2 - CCMP	WPA Handshake	SUKSES	Handshake berhasil diperoleh dari

ID Target	SSID	Lingkungan	RSSI (dBm)	Enkripsi	Vektor Utama	Hasil Akhir	Keterangan / Penyebab
					(via Deauth Klien)		deautentikasi klien aktif secara broadcast. Kata sandi '01021992' dipecahkan offline menggunakan aircrack-ng.
TGT_05	AJK-STUDENT	Lab Kampus	-55 s.d -60	WPA3 -SAE	PMKID & Deauth	GAGAL	WPA3 mengaktifkan proteksi PMF (802.11w).
TGT_06	AJK-SUDENT2	Lab Kampus	-61	WPA2 -CCMP	PMKID & Deauth	GAGAL	Tidak ada klien aktif (Clients: 0) saat serangan.
TGT_07	TP-Link_AP_6282	Lab Kampus	-68 s.d -76	WPA2 -CCMP	WPS Pixie-Dust	SUKSES	PIN & Password didapat dalam 4m 55s via WPS.

4.6.6 Verifikasi Integritas Data (Validasi MIC)

Terhadap file capture jabat tangan (.cap) yang berhasil diperoleh dari target TGT_01, TGT_02, TGT_03, TGT_04, dan TGT_07, dilakukan proses verifikasi integritas data sebelum diproses pada tahap cracking offline di Bab 4.7. Validasi ini bertujuan memastikan bahwa data handshake bersih dari kerusakan bingkai akibat noise nirkabel.

Wifite menggunakan utilitas backend tshark dan aircrack-ng untuk memeriksa struktur paket EAPOL. Kriteria kelayakan file capture meliputi:

1. Keberadaan bingkai jabat tangan yang berpasangan secara valid (ANonce dari AP dan SNonce dari Klien).
2. Keselarasan Replay Counter pada setiap pesan handshake.

3. Keabsahan kalkulasi Message Integrity Code (MIC) pada pesan M2 menggunakan algoritma HMAC-SHA1.

Hanya file capture yang memenuhi ketiga kriteria di atas yang disimpan ke dalam direktori hs/ untuk dianalisis lebih lanjut. File capture parsial yang tidak memiliki MIC dibuang karena tidak memiliki nilai kriptografis untuk proses offline cracking.

4.6.7 Sintesis dan Implikasi Keamanan

Pelaksanaan simulasi serangan nirkabel terhadap enam target ini memberikan beberapa implikasi keamanan penting:

1. Keamanan Fisik Jaringan (Atenuasi Sinyal):

Hasil pengujian TGT_01 membuktikan bahwa jarak dan hambatan fisik (dinding beton) merupakan lapisan pertahanan pasif yang sangat efektif. Pelemahan sinyal di bawah -80 dBm mempersulit penyerang melakukan injeksi paket dan menangkap respons daya rendah dari klien.

2. Kerentanan Manajemen Bingkai 802.11 pada WPA2:

Keberhasilan penangkapan handshake pada TGT_02 dan TGT_03 menunjukkan kerapuhan protokol WPA2 terhadap serangan aktif. Karena bingkai manajemen 802.11 pada WPA2 tidak terenkripsi, penyerang dapat memalsukan paket deautentikasi untuk memaksa klien memutuskan koneksi.

3. WPA3 sebagai Solusi Komprehensif:

Kegagalan serangan pada TGT_04 (AJK-STUDENT) membuktikan efisiensi protokol WPA3-SAE yang mewajibkan fitur Protected Management Frames (PMF / 802.11w). Klien WPA3 kebal terhadap paket deautentikasi palsu, sehingga menutup celah penangkapan handshake secara paksa.

4. Ancaman Laten Fitur WPS:

Keberhasilan instan pada TGT_06 (TP-Link_AP_6282) menegaskan bahwa WPS merupakan celah keamanan yang sangat kritis. Meskipun kata sandi WPA2 diatur sangat panjang dan kompleks,

penyerang dapat memperoleh kata sandi tersebut secara instan jika fitur WPS aktif dan menggunakan chipset yang rentan terhadap kalkulasi offline Pixie-Dust.

4.7 Analisis Kebutuhan Waktu Serangan

Bagian ini membahas evaluasi waktu komputasi yang dibutuhkan untuk memecahkan kata sandi dari jaringan Wi-Fi target. Analisis dilakukan melalui pengujian luring (offline cracking) terhadap berkas handshake dan PMKID menggunakan strategi serangan kamus (dictionary attack) yang dieksekusi secara bertahap—mulai dari penggunaan kamus kata sandi global, kamus lokal, hingga kamus masif. Melalui pengukuran ini, efektivitas setiap vektor serangan dan ketahanan pola kata sandi dapat diukur secara kuantitatif untuk mengetahui tingkat keamanan aktual jaringan nirkabel yang dievaluasi.

4.7.1 Pengujian Performa Perangkat Keras (Benchmark Hashcat)

Kecepatan proses cracking kata sandi offline (offline password cracking) pada protokol WPA2-PSK sangat bergantung pada kekuatan komputasi perangkat keras penyerang. Untuk menentukan parameter efisiensi dan mengukur batas waktu teoretis serangan, dilakukan pengujian tolok ukur (benchmark) terhadap perangkat keras stasiun penyerang (laptop Acer Swift SF314-54G).

Pengujian benchmark dilakukan pada Hashcat v6.2.6 untuk mode serangan nirkabel WPA-PBKDF2-PMKID+EAPOL (Hashcat Mode 22000). Hasil benchmark membandingkan performa antara CPU terintegrasi (Intel Core i5-8250U) dengan GPU diskret (NVIDIA GeForce MX150). Perbandingan data performa tersebut disajikan pada Tabel 4.7.

Tabel 4.7 Perbandingan Performa Komputasi (Benchmark Hashcat Mode 22000)

Unit Pemroses (Hardware)	Kecepatan Rata-Rata (Hash/Second)	Pemanfaatan Thread/Core	Faktor Akselerasi (Speedup)
CPU Intel Core i5-8250U	~6,800 H/s	8 Threads (Parallel)	1.0x (Baseline)

GPU NVIDIA GeForce MX150	~60,000 H/s	384 CUDA Cores	~8.82x
--------------------------	-------------	----------------	--------

Berdasarkan Tabel 4.7, penggunaan GPU diskret NVIDIA GeForce MX150 memberikan akselerasi pemrosesan hingga ~8,82 kali lipat dibandingkan CPU Intel Core i5-8250U yang berjalan secara paralel penuh pada 8 thread. Peningkatan kecepatan ini dimungkinkan oleh arsitektur paralel CUDA pada GPU yang memiliki 384 cores, yang sangat efisien dalam mengeksekusi operasi hashing matematika berulang seperti fungsi PBKDF2 (Password-Based Key Derivation Function 2) dengan algoritma HMAC-SHA1. Karena itu, seluruh proses cracking offline pada penelitian ini diinstruksikan untuk menggunakan akselerasi GPU NVIDIA GeForce MX150 guna meminimalkan durasi waktu eksperimen.

4.7.2 Analisis Hasil Cracking Offline Jaringan Target

Setelah memperoleh file capture handshake nirkabel (.cap) yang valid pada fase simulasi (Bab 4.6), langkah berikutnya adalah melakukan konversi file pcap ke dalam format hash Hashcat (.hc22000) menggunakan utilitas hcxpcaptool. Proses cracking dilancarkan secara bertahap (Tahap 1 hingga Tahap 3) menggunakan wordlist yang telah dipersiapkan.

ID Target (SSID)	Berkas Capure	Tahap Cracking Berhasil	Waktu & Status	Kata Sandi	Analisis Singkat
TGT_01 (ratu)	Handshake (.cap)	Tahap 2 (Lokal/Indo)	17.0 Detik (Sukses)	19111991	Kata sandi berupa pola tanggal lahir. Tidak terdeteksi di kamus global (Tahap 1), namun berhasil instan dengan kamus lokal.

ID Target (SSID)	Berkas Capture	Tahap Cracking Berhasil	Waktu & Status	Kata Sandi	Analisis Singkat
					Atenuasi sinyal hanya proteksi pasif.
TGT_02 (Alhamdulillah)	Handshake (.cap) & PMKID	Tahap 1 (Global)	PMKID: 4.0 Detik Handshake : 1.0 Detik (Sukses)	bismillah	Kata tunggal religi yang sangat umum. Sangat rentan dan langsung pecah pada tahap awal meskipun menggunakan dua vektor berbeda (PMKID & Handshake).
TGT_03 (toko-bahagia)	Handshake (.cap) & PMKID	Tahap 1 (Global)	PMKID: 1.0 Detik Handshake : 1.0 Detik (Sukses)	1234567890	Pola deret angka murni tanpa kompleksitas. Langsung terpecahkan secara instan pada iterasi awal dari kamus global terpopuler.
TGT_04 (Anton Febryando)	Handshake (.cap)	Tahap 3 (Masif)	12.0 Detik via Aircrack-ng (Sukses)	01021992	Pola tanggal lahir numerik (DDMMYYYY)

ID Target (SSID)	Berkas Capture	Tahap Cracking Berhasil	Waktu & Status	Kata Sandi	Analisis Singkat
					tidak terindeks di kamus lokal (Tahap 2), namun pecah oleh kamus komprehen sif. Gagal otomatisasi karena error GPU, tapi berhasil manual.
TGT_07 (TP-Link_AP_6282)	Handshake (.cap)	Tahap 3 (Masif)	28 Menit 45 Detik (Sukses)	78092129	Pola angka acak (8 digit) berhasil dipecahkan melalui serangan kamus masif (seclist.txt) dalam waktu kurang dari 30 menit.
TGT_05 (AJK-STUDENT) & TGT_06 (AJK-SUDENT2)	-	-	Gagal Cracking	-	TGT_06 gagal karena tidak ada klien terasosiasi (Clients: 0). TGT_05 gagal akibat proteksi Protected

ID Target (SSID)	Berkas Capture	Tahap Cracking Berhasil	Waktu & Status	Kata Sandi	Analisis Singkat
					Managemen nt Frames (PMF) pada protokol WPA3- SAE.

1. Cracking Target TGT_01 'ratu'

- Tahap 1 (wordlist-probable.txt): Gagal (Status: Key Unknown). Log Hashcat melaporkan kegagalan karena kata sandi tidak masuk dalam daftar kata global teratas.

- Kata Sandi Ditemukan: 19111991

Pengujian offline cracking membuktikan bahwa kata sandi target berupa pola angka tanggal lahir ('19111991') tidak terdaftar dalam kamus default global terpopuler (Tahap 1), namun berhasil dipecahkan secara instan dalam 17,0 detik menggunakan kamus kontekstual lokal Indonesia (Tahap 2 - ind-hash.txt). Temuan ini menegaskan keabsahan hipotesis bahwa relevansi geografis dan budaya dalam penyusunan kamus wordlist sangat menentukan efisiensi serangan, di mana pola tanggal lahir adalah salah satu kebiasaan keamanan paling umum di Indonesia. Selain itu, temuan ini membuktikan bahwa faktor atenuasi sinyal (jarak) hanya bertindak sebagai perlindungan pasif sementara; begitu penyerang berhasil mendapatkan satu berkas handshake yang valid, enkripsi WPA2-PSK langsung dapat ditembus secara offline.

2. Cracking Target TGT_02 'Alhamdulillah'

- Kalkulasi PMKID (Sesi 1): Kata sandi berhasil dipecahkan secara offline dalam waktu 4.0 detik pada pukul 13:36:27.

- Kata Sandi Ditemukan: bismillah

Kata sandi target menggunakan istilah religi/lokal yang sangat umum ("bismillah"). Karena kesederhanaan kata sandi ini, enkripsi WPA2 runtuh secara instan pada Tahap 1 (dictionary attack menggunakan kamus default global

terpopuler wordlist-probable.txt) baik melalui vektor PMKID maupun berkas jabat tangan (handshake). Hal ini memperlihatkan bahwa meskipun pengguna tidak menggunakan pola angka standar (seperti 123), penggunaan kata tunggal berbasis bahasa lokal yang sangat umum tetap sangat rentan karena telah terdaftar dalam basis data kata sandi global.

3. Cracking Target TGT_03 'toko-bahagia'

- Tahap 1 (wordlist-probable.txt): Sukses (Status: Cracked). Kata sandi berhasil dipecahkan secara instan dalam waktu 1.0 detik pada iterasi awal.
- Kata Sandi Ditemukan: 1234567890

Penggunaan kata sandi berupa deretan angka berurutan ("1234567890") sangat rentan terhadap serangan kamus luring. Meskipun memenuhi standar panjang 10 karakter, tiadanya kompleksitas membuat sandi ini pecah di bawah 1 detik karena terdaftar dalam kamus global (wordlist-probable.txt). Kerentanan ganda WPA2 juga terbukti, di mana eksploitasi PMKID pasif maupun penangkapan handshake aktif menghasilkan temuan kunci yang identik secara instan. Hal ini menegaskan bahwa jaringan akan langsung runtuh jika passphrase tidak memiliki tingkat kerumitan yang memadai.

4. Cracking Target TGT_04 'Anton Febryando'

- Tahap 1 & 2 (wordlist-probable.txt & ind-hash.txt): Gagal (Status: Key Unknown). Kata sandi target tidak ditemukan pada kamus lokal bahasa Indonesia karena berupa pola angka tanggal lahir yang tidak terindeks.
- Kata Sandi Ditemukan: 01021992

Pola kata sandi tanggal lahir ('01021992') terbukti rentan dan berhasil dipecahkan hanya dalam 12,0 detik pada Tahap 3 menggunakan kamus masif (seclist.txt). Walaupun sempat lolos dari pengujian Tahap 2 karena kamus lokal hanya berfokus pada kosakata bahasa, pola numerik murni (DDMMYYYY) ini tak mampu menahan serangan dari kamus yang lebih komprehensif. Keberhasilan menggunakan Aircrack-ng berbasis CPU ini juga menegaskan bahwa berkas handshake yang ditangkap tetap sah dan dapat dipecahkan secara manual, meskipun sempat terjadi kendala driver GPU pada sistem Hashcat.

5. Cracking Target TGT_07 'TP-Link_AP_6282'

- Tahap 1 & 2 (wordlist-probable.txt & ind-hash.txt) : Gagal (Status: Key Unknown). Log Hashcat melaporkan kegagalan karena pola kata sandi numerik murni ini tidak masuk dalam daftar kata global teratas.
- Tahap 3 (seclist.txt): Sukses (Status: Cracked). Kata sandi berhasil dipecahkan dalam waktu 28 menit 45 detik.
- Kata Sandi Di temukan: 78092129

Kata sandi berupa kombinasi angka acak 8 digit ("78092129") terbukti mampu menahan serangan awal dari kamus global dan lokal (Tahap 1 dan 2) karena tidak memiliki pola linguistik maupun tanggal yang umum. Namun, sandi ini tetap berhasil dipecahkan pada Tahap 3 menggunakan kamus masif yang lebih komprehensif (seclist.txt) dalam waktu kurang dari 30 menit. Hal ini menunjukkan bahwa meskipun sandi numerik murni tidak mudah ditebak oleh kamus dasar, batas minimum 8 angka WPA2 masih sangat rentan terhadap serangan kamus berskala besar. Terbatasnya ruang kunci (keyspace) dari karakter khusus angka membuatnya tidak mampu menahan daya komputasi perangkat keras modern dalam waktu lama.

6. Target Gagal Cracking (TGT_05, TGT_06)

Kegagalan cracking pada kedua target ini mewakili dua hambatan mendasar dalam eksploitasi keamanan nirkabel:

- TGT_05 ("AJK-STUDENT") – Hambatan Protokol: Kegagalan mutlak terjadi karena implementasi WPA3-SAE. Protokol ini secara arsitektur kebal terhadap ekstraksi sandi luring karena pertukaran kunci interaktifnya (Dragonfly) tidak dapat direkam untuk dipecahkan nanti. Selain itu, fitur wajib Protected Management Frames (PMF) memvalidasi lalu lintas kontrol, sehingga semua injeksi serangan deautentikasi otomatis diblokir oleh sistem.
- TGT_06 ("AJK-SUDENT2") – Hambatan Lingkungan Klien: Kegagalan disebabkan oleh ketiadaan klien aktif yang terasosiasi (Clients: 0). Karena penangkapan 4-way handshake pada WPA2 mutlak membutuhkan proses (re)autentikasi antara klien dan Access Point, nihilnya perangkat pengguna membuat jaringan ini secara alami tidak memiliki lalu lintas pertukaran kunci yang bisa dipicu maupun disadap.

4.7.3 Analisis Efektivitas Strategi Wordlist Bertahap

Hasil pengujian offline cracking terhadap lima target yang berhasil merekam handshake/kunci disajikan secara ringkas pada Tabel 4.8.

Tabel 4.8 Ringkasan Hasil Uji Coba Offline Cracking Menggunakan Hashcat

ID Target	SSID	Tahap Wordlist	Status Cracking	Waktu Cracking	Kecepatan (Hash Rate)	Kata Sandi (PSK)
TGT_01	ratu	Tahap 2 (Lokal/Indo)	SUKSES	17.0 Detik	58,688 H/s	19111991
TGT_02	Alhamdulillah	Tahap 1 (Default)	SUKSES	1.0 Detik	36,800 H/s	bismillah
TGT_03	toko-bahagia	Tahap 1 (Default)	SUKSES	1.0 Detik	36,800 H/s	1234567890
TGT_04	Anton Febryando	Tahap 3 (Masif)	SUKSES	12.0 Detik	8.993, 16 k/s	01021992
TGT_07	TP-Link_AP_6282	Tahap 3 (Masif)	SUKSES	28 Menit 45 Detik	36,800 H/s	78092129

Penerapan strategi serangan bertahap terbukti sangat efisien. Dengan membagi kamus ke dalam tingkatan probabilitas, penyerang tidak perlu langsung memproses file kamus berukuran raksasa (>700 MB) seperti seclist.txt untuk target lokal Indonesia seperti TGT_02 dan TGT_03. Penghematan waktu komputasi yang didapat sangat besar, di mana kata sandi lokal dapat diselesaikan dalam hitungan detik.

BAB 5 KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil simulasi serangan dan analisis kebutuhan waktu cracking offline yang telah dilaksanakan terhadap tujuh target jaringan Wi-Fi, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Kerentanan WPA2-PSK terhadap Dictionary Attack:

Keamanan WPA2-PSK sangat bergantung pada kekuatan kata sandi. Penggunaan kata sandi yang sederhana seperti deretan angka berurutan (1234567890 pada TGT_03), pola tanggal lahir (19111991 pada TGT_01 atau 01021992 pada TGT_04), atau kata tunggal berbasis bahasa lokal (bismillah pada TGT_02) terbukti sangat rentan dan dapat di-crack secara offline dalam waktu 1,0 hingga 17,0 detik menggunakan dictionary attack, meskipun panjangnya telah memenuhi standar minimal.

2. Keunggulan Protokol WPA3-SAE:

Pengujian pada target TGT_05 (AJK-STUDENT) yang mengimplementasikan protokol WPA3-SAE membuktikan keamanan yang sangat tinggi. Fitur Protected Management Frames (PMF / IEEE 802.11w) yang wajib pada WPA3 berhasil menggagalkan serangan deautentikasi aktif secara total, sehingga penyerang tidak dapat memaksa klien re-handshake untuk mendapatkan data autentikasi.

4. Kerentanan Kritis Fitur WPS:

Fitur WPS terbukti menjadi celah keamanan yang sangat kritis karena memungkinkan penyerang memperoleh kata sandi WPA2 secara instan (dalam waktu ± 5 menit) melalui serangan Pixie-Dust tanpa perlu melakukan dictionary attack offline, bahkan ketika kata sandi tersebut relatif aman. Sementara itu, pada metode serangan aktif deautentikasi untuk menangkap handshake, tingkat keberhasilannya sangat bergantung pada tingginya kepadatan klien aktif pada jaringan target serta optimasi posisi penyerang yang dapat sepenuhnya mengatasi hambatan berupa atenuasi jarak maupun halangan fisik.

5. Performa Komputasi Offline:

Penggunaan kartu grafis diskret (GPU NVIDIA GeForce MX150) memberikan akselerasi pemrosesan cracking offline hingga ~8,82 kali lipat (~60.000 H/s) dibandingkan menggunakan prosesor CPU (Intel Core i5-8250U dengan 8 thread paralel yang menghasilkan ~6.800 H/s).

5.2 Saran

Untuk meningkatkan keamanan jaringan Wi-Fi serta memberikan arah bagi pengembangan penelitian selanjutnya, diajukan beberapa saran berikut:

1. Bagi Administrator dan Pengguna Jaringan:

- Nonaktifkan Fitur WPS: Fitur Wi-Fi Protected Setup (WPS) harus segera dinonaktifkan di semua router guna menghindari eksploitasi instan lewat WPS Pixie-Dust.
- Gunakan Passphrase Panjang: Pengguna disarankan menghindari kata sandi tunggal berbasis kamus. Sebagai gantinya, gunakan kombinasi beberapa kata acak (passphrase) sepanjang minimal 16 karakter untuk meningkatkan entropi secara signifikan.
- Migrasi ke WPA3-SAE: Sangat disarankan untuk meningkatkan standar keamanan perangkat keras AP ke protokol WPA3-SAE yang memiliki proteksi frame manajemen bawaan.

2. Bagi Peneliti Selanjutnya:

- Pengujian Hardware Enterprise: Disarankan menggunakan kartu grafis kelas enterprise (seperti NVIDIA RTX series) untuk menguji performa cracking dengan wordlist berukuran raksasa (>100 GB) guna mensimulasikan ancaman siber yang sebenarnya.
- Eksplorasi Vektor Serangan WPA3: Perlu dilakukan penelitian lebih lanjut mengenai teknik serangan alternatif terhadap WPA3, seperti serangan berbasis Evil Twin atau Rogue AP.

DAFTAR PUSTAKA

- Akomea-Agyin, K., & Asante, M. (2008). Analysis of Security Vulnerabilities in Wifi-Protected Access Pre-Shared Key (WPA-PSK/ WPA2-PSK). *International Research Journal of Engineering and Technology*, 537. www.irjet.net
- Alkhwaja, I., Albugami, M., Alkhwaja, A., Alghamdi, M., Abahussain, H., Alfawaz, F., Almurayh, A., & Min-Allah, N. (2023). Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming. *Applied Sciences (Switzerland)*, 13(10). <https://doi.org/10.3390/app13105979>
- Aranza Trevino. (2024, March 4). *Password Entropy: What It Is and Why It's Important*. <https://www.keepersecurity.com/blog/2024/03/04/password-entropy-what-it-is-and-why-its-important/>
- Britney Oswald. (2024, October 30). *NIST Password Policy Guidelines 2024: What You Need to Know*. <https://linfordco.com/blog/nist-password-policy-guidelines/>
- Daniel Miessler, Jason Haddix, Ignacio Portal, & g0tmilk. (2025, April 26). *GitHub - danielmiessler/SecLists: SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more*. <https://github.com/danielmiessler/SecLists>
- Ethan Wilkins. (2024, April 16). *Cracking Into Password Requirements*. <https://www.aon.com/en/insights/cyber-labs/cracking-into-password-requirements?collection=5b76135e-4196-415b-ab1d-f42b6f0abb10>
- Joel R. McConvey. (2025, January 21). *A billion stolen passwords make passkeys look good, despite growing pains | Biometric Update*. <https://www.biometricupdate.com/202501/a-billion-stolen-passwords-make-passkeys-look-good-despite-growing-pains>
- Joseph Lorenz. (2017, October 20). *Taking advantage of the 4-way handshake – Cyber*. <https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summaries/taking-advantage-of-the-4-way-handshake/>
- Kohlilos, C. P., & Hayajneh, T. (2018a). A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. *Electronics (Switzerland)*, 7(11). <https://doi.org/10.3390/electronics7110284>

- Mike Coutermarsh. (2022, January 24). *Using entropy for user-friendly strong passwords* — PlanetScale. <https://planetscale.com/blog/using-entropy-for-user-friendly-strong-passwords>
- Nakhila, O., Attiah, A., Jin, Y., & Zou, C. (n.d.). *Parallel Active Dictionary Attack on WPA2-PSK Wi-Fi Networks*.
- Shiddiqi, A. M., Ijtihadie, R. M., Ahmad, T., Wibisono, W., Anggoro, R., Bagus, D., & Santoso, J. (2020). Penggunaan Internet dan Teknologi IoT untuk Meningkatkan Kualitas Pendidikan. In *Jurnal Direktorat Riset dan Pengabdian Kepada Masyarakat-DRPM ITS* (Vol. 4, Issue 3). <https://zoom.us/j/91019044215?pwd=M05PMkh6YIRM>
- Sunandar Informatika, A., Singaperbangsa Karawang Jl HSRonggo Waluyo, U., Timur, T., & Barat, J. (2024). IMPLEMENTASI PENETRATION TESTING DAN WORDLIST GENERATOR DALAM PENGUJIAN KEAMANAN JARINGAN MENGGUNAKAN METODE DICTIONARY ATTACK. In *Jurnal Mahasiswa Teknik Informatika* (Vol. 8, Issue 3).
- Zhou Qiang. (2025, April 9). *What Is WPA3? WPA3 vs. WPA2 - Huawei*. <https://info.support.huawei.com/info-finder/encyclopedia/en/WPA3.html>

LAMPIRAN

Lampiran 1. Tautan QR Code Repositori Google Drive untuk Data Mentah Simulasi



Silakan pindai QR Code di atas menggunakan smartphone Anda untuk mengakses raw data dan rekam hasil simulasi serangan.