Model Inspeksi Keamanan Jaringan Nirkabel dengan Teknik Wardriving Berbasis ChatBot

Mei Purweni[1], Dedy Hariyadi [2*], Faulinda Ely Nastiti, Fazlurrahman [3]
[1]Universitas Duta Bangsa Surakarta
[2]Universitas Jenderal Achmad Yani Yogyakarta
[3]Komunitas NgeSec Yogyakarta
*e-mail: dedy@unjaya.ac.id

DOI: https://doi.org/10.31603/komtika.v6i2.7943

Received: 27-09-2022, Revised: 21-10- 2022, Accepted: 23-10-2022

ABSTRACT

The use of wireless network devices such as access points needs to be analyzed to avoid intercept or bypass attacks by criminals. Wireless network security inspection activities in intelligent inspection/operations must be carried out confidentially, accurately, and quickly. This study proposes the development of applications for information collection and mapping of access point network devices in intelligence operations by field officers as reference material in presenting reports during the investigation process. The Information collected in this study was carried out using a Signal Intelligence approach that has been aligned with the Signal Intelligence model and the Intelligence Collection System. This research has used both branches in collaboration with chatbot communication to facilitate the analysis process of field officers accompanied by activities to filter network data in the midst of the community.
Keywords*: wardriving, signal intelligence, chatbot, bypass, intercept, cyber crime*

ABSTRAK

Penggunaan perangkat jaringan nirkabel seperti Access Point perlu dianalisis untuk menghindari serangan intersep ataupun bypass oleh pelaku kejahatan. Kegiatan inspeksi keamanan jaringan nirkabel dalam inspeksi/operasi intelijen harus dilakukan secara rahasia, akurat dan cepat. Penelitian ini mengusulkan pengembangan aplikasi pengumpulan informasi dan pemetaan perangkat jaringan access point dalam operasi intelijen oleh petugas lapangan sebagai bahan rujukan dalam penyajian laporan saat proses penyidikan. Pengumpulan informasi pada penelitian ini dilakukan dengan pendekatan Signal Intelligence yang telah diselaraskan dengan model Signal Intelligence dan Intelligence Collection System. Penelitian ini telah menggunakan kedua cabang tersebut dikolaborasikan dengan komunikasi chatbot untuk mempermudah proses analisis petugas lapangan yang disertai dengan aktivitas menyaru data jaringan di tengah-tengah masyarakat.
Kata-kata kunci: wardriving, signal intelligence, chatbot, bypass, intersep, kriminalitas siber

PENDAHULUAN

Serangan terorisme telah masuk ke infrastruktur siber dengan berbagai teknik yang tidak mudah terdeteksi oleh masyarakat umum. Salah satu bentuk operasi terorisme diantaranya melalui media internet [1], [2]. Ketersediaan perangkat jaringan nirkabel di pasar dan kemudahan memasang infrastruktur jaringan nirkabel juga meningkatkan potensi kejahatan siber [3], [4]. Artinya hampir semua orang bisa membeli dan memasang perangkat jaringan nirkabel dengan mudah tidak terkecuali pelaku kejahatan. Walaupun pihak Kementerian Komunikasi dan Informatika telah melakukan penertiban sinyal radio tetapi hanya terbatas pada penyalahgunaan sinyal radio [5]. Padahal, penggunaan perangkat jaringan nirkabel seperti *Access Point* untuk tingkat rumah atau kantor ukuran menengah juga perlu dilakukan

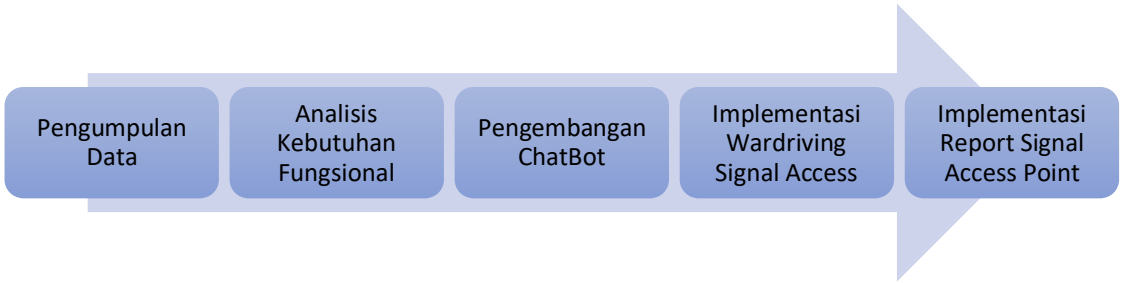
penertiban dan monitoring, agar tidak terjadi serangan penyadapan ataupun *bypass* oleh pelaku kejahatan [6].

Wardriving merupakan teknik yang digunakan untuk mengumpulkan informasi dari perangkat *Access Point* yang terpasang pada suatu lokasi. Adapun informasi yang didapatkan diantaranya nama jaringan, tipe enkripsi, merk dari perangkat, dan lokasi pancaran gelombang [7]. *Wardriving* dengan menganalisis pancaran sinyal *Access Point* memungkinkan informasi-informasi yang didapatkan dalam bentuk data tabel analisis keamanan jaringan yang dapat membantu proses inspeksi/operasi intelijen penegak hukum [8].

Oleh sebab itu perlu inspeksi atau operasi intelijen menggunakan aplikasi pemantauan jaringan nirkabel yang bersifat *mobile* [6]. Hal ini untuk mempercepat analisis di lapangan oleh petugas lapangan menggunakan pendekatan *Signal Intelligence* sehingga dapat membantu pengambilan keputusan dalam pengelolaan keamanan jaringan dalam upaya menekan kriminalitas penyadapan dan atau *bypass* oleh pelaku kejahatan.

METODE

Pada penelitian ini mengusulkan pengembangan aplikasi pengumpulan informasi dari pemetaan perangkat *Access Point* dalam operasi intelijen oleh petugas lapangan sebagai bahan rujukan dalam penyajian laporan saat proses penyidikan. Implementasi dari pengolahan dan penyajian telah disesuaikan dengan kebutuhan petugas lapangan. Adapun alur pengembangan aplikasi tersebut dapat dilihat pada Gambar 1.



Gambar 1. Alur Pengembangan Aplikasi Wardriving Berbasis ChatBot

Pengumpulan Data

Data awal didapatkan dari portal www.kaggle.com yang mempermudah klasifikasi terkini jenis keamanan *Access Point*. Data tersebut dianalisis selanjutnya digunakan untuk mengembangkan pustaka keamanan pada Github dan Phyton.

Analisis Kebutuhan Sistem

Detail kebutuhan fungsional dari pengembangan aplikasi *wardriving* pada proses *signal intelligence* dapat dilihat pada tabel 1.

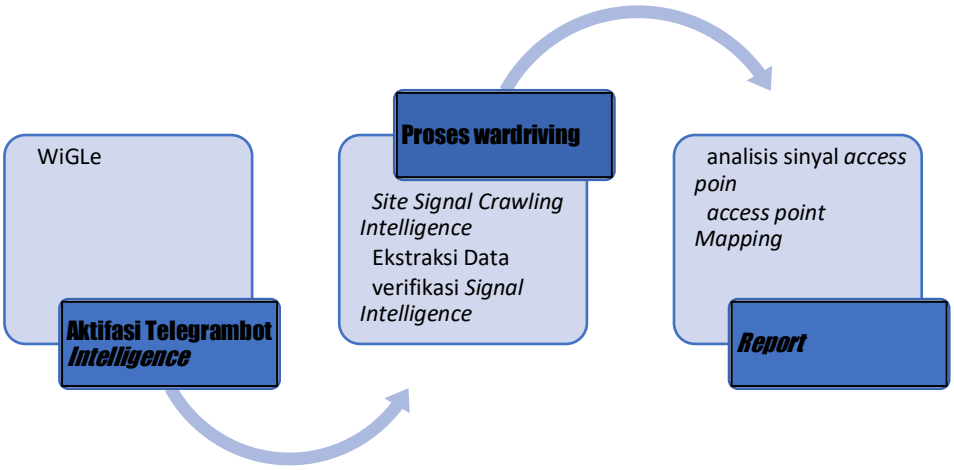
Tabel 1. Analisis Kebutuhan Sistem

Kebutuhan Sistem
Cloud Service
WiGLE Software
Python programming
GitHub
Telegram API
Smartphone Android Device

HASIL DAN PEMBAHASAN

Pengembangan ChatBot

Saat melakukan operasi intelijen kecepatan dan ketepatan dalam menyajikan informasi sangat tinggi. Oleh sebab itu aplikasi pendukung penyajian data berbasis *mobile* sangat diperlukan. Aplikasi yang terpasang pada ponsel cerdas juga harus bersifat baik dari sistem komunikasi atau bentuk yang tidak mengundang kecurigaan pengguna lainnya. Proses penggunaan ponsel cerdas dalam operasi intelijen harus mengutamakan kerahasiaan dan/atau seolah-olah melakukan kegiatan wajar seperti orang lain [9]. Selain itu komunikasi *ChatBot* menggunakan protokol aman yaitu https dengan sertifikat yang tervalidasi oleh RootCA [10]. Maka atas dasar kerahasiaan data dan keamanan, pengembangan aplikasi pada penelitian ini menggunakan server yang terletak di Indonesia dan protokol keamanan tervalidasi RootCA. *Pipeline* aplikasi *Wardriving* pada proses *Signal Intelligence* disajikan pada Gambar 2.



Gambar 2. *Pipeline Telegrambot Signal Intelligence*

Pengumpulan informasi dengan pendekatan *Signal Intelligence* perlu diselaraskan dengan *Intelligence Collection System* [11] seperti *Human Intelligence*, *Open Source Intelligence,* dan *Geospatial Intelligence*. Penelitian ini telah menggunakan ketiga cabang tersebut yang dikolaborasikan dengan komunikasi chatbot dalam rangka mempermudah proses analisis petugas lapangan yang disertai dengan aktivitas menyatu di tengah-tengah masyarakat [12], sehingga petugas lapangan mendapatkan informasi yang komprehensif

Proses pengumpulan data pancaran sinyal *access point* menggunakan teknik *wardriving*. Sehubungan bagian dari operasi intelijen maka alat yang digunakan adalah peralatan yang wajar di sekitar, seperti ponsel cerdas. Aplikasi yang digunakan pada ponsel cerdas berbasis Android adalah WiGLE yaitu sebuah aplikasi yang khusus dikembangkan untuk mengumpulkan data dari jaringan nirkabel seperti Wi-Fi, Bluetooth, BLE, dan jaringan seluler [13]. Namun, pada penelitian ini fokus pada pengumpulan pancaran sinyal dari *access point*.

Luaran dari aplikasi WiGLE dalam bentuk CSV atau pun KML yang terkompresi menggunakan GNU Zip. Analisis di lapangan dengan luaran GNU Zip, CSV, dan KML tidak mudah maka dikembangkan aplikasi yang mempermudah analisis pancaran sinyal *access point*. Pada penelitian ini proses analisis dilakukan di server *ChatBot* dan analisis data dan transfer data menggunakan *instant messenger* Telegram. Pemanfaatan Telegram sebagai

ChatBot untuk pendukung pengiriman dan penyajian data petugas lapangan dalam mempermudah operasi intelijen.

Pengembangan *ChatBot* Telegram dan pengolahan data menggunakan bahasa pemrograman python dengan beberapa pustaka yang digunakan diantaranya: telepot, pdfkit, folium, gzip, shutil, time, csv, dan os. Pada penelitian ini terdapat 3 proses utama, yaitu *ChatBot*, pengolahan data, dan penyajian. Untuk ChatBot memanfaatkan pustaka telepot, implementasi fungsi yang memanfaatkan telepot seperti pada pseudocode berikut:

```
Pseudocode:
import telepot
bot = telepot.Bot('TOKEN_TELEGRAM')
def handle(msg):
    content_type, chat_type, chat_id = telepot.glance(msg)
    print(content_type, chat_type, chat_id)
    chat_id = msg['chat']['id']
```

Penelitian ini juga mengambangkan *library* metode keamanan untuk mempermudah analisis otentikasi wireless yang diinjeksi ke dalam sistem telegram bot *wardriving intelligence*. *Library* Keamanan *Access Point* dan otentikasi diinterpretasikan dalam bentuk Tabel 2.

Tabel 2. Library Keamanan Access Poin

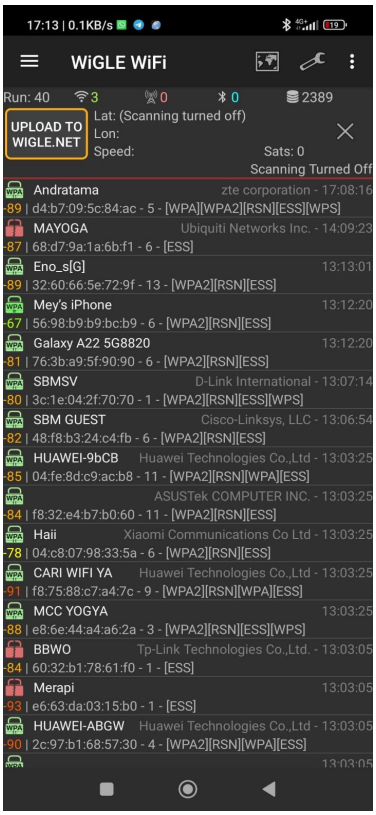
AuthMode	Otentikasi
WPA2-PSK-CCMP	WPA/WPA2
WPA-PSK-TKIP+CCMP	WPA/WPA2
WPA-PSK-CCMP+TKIP	WPA/WPA2
WPA2-PSK-CCMP+TKIP	WPA/WPA2
WPA2-PSK-TKIP+CCMP	WPA/WPA2
WPA-PSK-CCMP	WPA/WPA2
RSN-SAE-CCMP	WPA3
WPA2-EAP-CCMP	WPA Enterprise
WPA2-EAP+FT/EAP-CCMP	WPA Enterprise
ESS	No Encryption

WPA merupakan jaringan yang aman untuk jaringan rumah dan kantor kecil dengan mengenkripsi lalu lintas jaringan 128-bit dari kunci bersama 256-bit. WPA2 merupakan jaringan yang lebih aman dari pada WPA karena menggunakan AES (*Advanced Encryption Standard)* dan menggunakan kunci identifikasi. WPA3 Personal tersedia sebagai pengaturan di antarmuka pengguna (UI) browser lokal. WPA-Enterprise merupakan mekanisme keamanan nirkabel yang dirancang untuk jaringan nirkabel perusahaan kecil hingga besar dengan otentikasi dan enkripsi tingkat lanjut. Sementara, *No Encryption* didefinisikan dalam library pada tabel 2 sebagai jenis jaringan yang sangat tidak aman karena tidak menerapkan otentikasi.

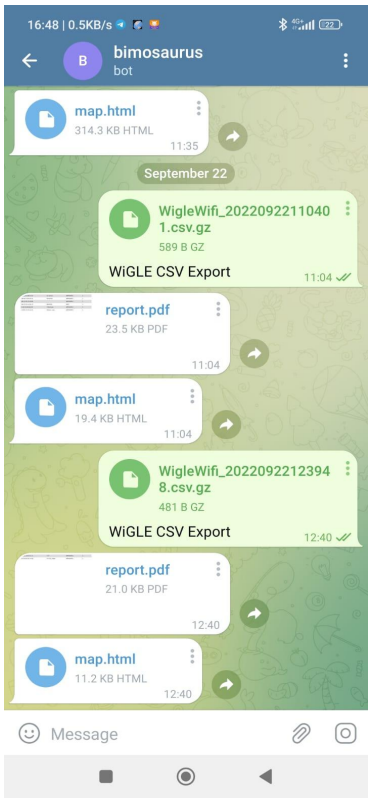
Implementasi *Wardriving Signal Access Point*

Inspeksi atau operasi intelijen terhadap keamanan siber dilakukan dengan mengaktifkan WiGLE sembari berkeliling di wilayah target operandi. Aplikasi ini mampu melakukan *crawling* data sinyal *Access Point* dengan lingkup target kurang lebih radius 100 meter. Proses *crawling* data sinyal *Access Point* dapat dilihat pada gambar 3. Terdapat 2 sub proses WiGLE pada saat *crawling* data sinyal *Access Point* yaitu: 1) ekstraksi berkas dengan format GNU Zip, 2) mengolah berkas hasil ekstraksi berupa berkas CSV, dan 3) penggunaan *library* metode keamanan.

Proses selanjutnya adalah ekstraksi data CSV ke laporan berbentuk *.pdf yang langsung dapat dilaporkan ke pimpinan oleh petugas lapangan yang sedang melakukan inspeksi atau operasi intelijen,. Proses ini dilakukan dengan men-trigger Telegram Bot seperti disajikan pada gambar 4.



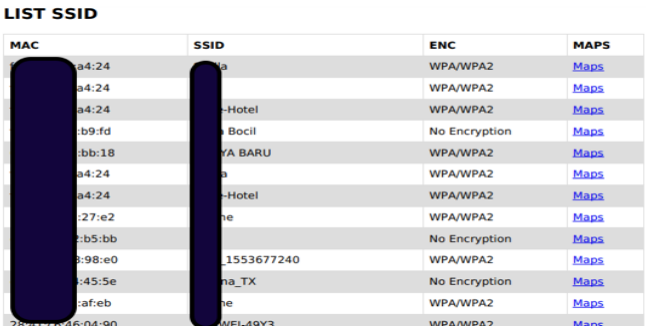
Gambar 3. Proses *Wardriving Signal Access Point* dengan WiGLE



Gambar 4. Proses *Trigger Telegram Bot Signal Intelligence*

Implementasi Proses *Report Signal Access Point*

Bentuk reprot.pdf pada gambar 4, ketika dibuka akan menghasilkan laporan analisis sinyal keamanan *access point* pada gambar 5. Pada gambar 5 dapat dilihat bahwa aplikasi *Wardriving* Berbasis ChatBot dapat menemukan jenis-jenis *access point* aman dan tidak aman.



Gambar 5 . Laporan Analisis Sinyal Keamanan *Access Point*

Gambar 6 . Laporan Analisis Sinyal Keamanan *Access Point*

Pada gambar 5 ditemukan beberapa jaringan dengan status *'No encryption'*, mengartikan bahwa jaringan tersebut menggunakan sistem berbasis *captive portal* atau bahkan tidak menerapkan sistem otentikasi apapun, sehingga memiliki celah keamanan proses mengakses SSID.Potensi celah keamanannya diantaranya adalah serangan MITM mengakibatkan lalu lintas data bisa disadap ataupun *bypass*. Lokasi perkiraan *access point* yang dianalisis dapat dilihat pada gambar 6.

KESIMPULAN

Penelitian ini terbukti mampu melakukan *crawling* data *access point* dengan teknik *wardriving* untuk mengidentifikasi sistem otentikasi yang terbuka dan tidak aman dengan perangkat mobile. Laporan dari aplikasi *wardriving* pada penelitian ini bersifat real time yang dapat didownload dalam bentuk *pdf/*csv dan dapat diketahui posisi *access point* yang tidak aman dalam bentuk peta lokasi. Sehingga aplikasi wardriving dapat membantu pihak terkait (dalam hal ini pihak militer/kepolisian) untuk menganalisa dan memberi keputusan lebih lanjut dalam upaya menekan kriminalitas siber seperti melakukan penyadapan/*bypass* jaringan dalam upaya mencuri data pribadi yang bersifat spesifik. Meskipun aplikasi ini mampu melakukan *wardriving* dengan radius 100 meter tetapi tingkat akurasi pemetaan lokasi tergantung ponsel yang digunakan.

UCAPAN TERIMA KASIH

Kementerian Pendidikan, Kebudayaan, Riset, Dan Teknologi, Direktorat Jenderal Pendidikan Vokasi yang telah memberikan bantuan dana Hibah Penelitian 2022 sehingga penelitian ini dapat dilaksanakan dan dipublikasi untuk dapat dibaca oleh masyarakat dan para akademisi. Terimakasih kepada mahasiswa Teknik Komputer Bintang Aji Saputra dan Akbar Syarif Pratama Puta yang telah membantu dalam pengumpulan data di objek-objek penelitian.

DAFTAR PUSTAKA

[1] J. Veilleux and S. Dinar, "A Global Analysis of Water-Related Terrorism, 1970–2016," *Terror. Polit. Violence*, vol. 33, no. 6, pp. 1191–1216, Aug. 2021, doi: 10.1080/09546553.2019.1599863.

[2] P. Dong-kyun and J. Sung-gu, "Periodical and Spatial Differences of Terrorism Examining Global TERRORISM Database from 1970~ 2018," *Int. J. Terror. Natl. Secur.*, vol. 5, no. 1, 2020.

[3] M. Subani, I. Ramadhan, A. Syah Putra, and A. Al Muslim, "Perkembangan Internet of Think (IOT) dan Instalasi Komputer Terhadap Perkembangan Kota Pintar di Ibukota DKI Jakarta," *IKRA-ITH Inform. J. Komput. dan Inform.*, vol. 5, no. 1, pp. 88–93, 2021, [Online]. Available: https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/918.

[4] K. Aldubaikhy, W. Wu, N. Zhang, N. Cheng, and X. Shen, "mmWave IEEE 802.11ay for 5G Fixed Wireless Access," *IEEE Wirel. Commun.*, vol. 27, no. 2, pp. 88–95, 2020, doi: 10.1109/MWC.001.1900174.

[5] T. Aswin, F. Imansyah, F. T. P. W, J. Marpaung, and R. R. Yacoub, "Analisis Penerapan Access Point Dalam Rentang Frekuensi 2400 ─ 2500 Mhz Di Balmon Kelas Ii Pontianak," *J. Tek. Elektro*, vol. 2, no. 1, pp. 1–11, 2021, [Online]. Available: https://jurnal.untan.ac.id/index.php/jteuntan/article/view/51176.

[6] N. Christianto and W. Sulistyo, "Model Pemantauan Keamanan Jaringan Melalui Aplikasi Telegram Dengan Snort," *J. Tek. Inform. dan Sist. Inf.*, vol. 7, no. 3, pp. 702–714, 2021, doi: 10.28932/jutisi.v7i3.4088.

[7] A. M. Thomas, G. A. Kumaran, R. Ramaguru, R. Harish, and K. Praveen, "Evaluation of Wireless Access Point Security and Best Practices for Mitigation," in *2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*, 2021, pp. 422–427, doi: 10.1109/ICEECCOT52851.2021.9707914.

[8] S. Lindroos, A. Hakkala, and S. Virtanen, "A systematic methodology for continuous WLAN abundance and security analysis," *Comput. Networks*, vol. 197, p. 108359, 2021, doi: https://doi.org/10.1016/j.comnet.2021.108359.

[9] G. T. P. Siregar and M. R. Lubis, "Juridical analysis of religious blasphemy crimes through smartphone applications based on the information and electronic transactions (ite)," *J. Contemp. Issues Bus. Gov.*, vol. 27, no. 02, 2021, doi: 10.47750/cibg.2021.27.02.120.

[10] D. Hariyadi, I. P. Santoso, and R. Saputra, "Implementasi Proteksi Client-Side Pada Private Cloud Storage Nextcloud," *J. Manaj. Inform. dan Sist. Inf.*, vol. 2, no. 1, p. 16, 2019, doi: 10.36595/misi.v2i1.65.

[11] B. D. Berkowitz and A. E. Goodman, *Strategic Intelligence for American National Security*. Princeton University Press.

[12] M. Ghita, B. Siham, M. Hicham, and G. Hafid, "Artificial and Geospatial Intelligence Driven Digital Twins' Architecture Development Against the Worldwide Twin Crisis Caused by COVID-19 BT - Geospatial Intelligence: Applications and Future Trends,"

in *Geospatial Intelligence*, F. Barramou, E. H. El Brirchi, K. Mansouri, and Y. Dehbi, Eds. Cham: Springer International Publishing, 2022, pp. 79–104.

[13] R. P. Rizky Wahyu Ismail, "Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi," *J. Mhs. Bina Insa.*, vol. 5, no. 1, pp. 53–62, 2020.