Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 7 Nomor1, 2024
P-2655-710X e-ISSN 2655-6022

Submitted : 06/01/2024
Reviewed : 09/01/2024
Accepted : 15/01/2024
Published : 17/01/2024

Deni Suprihadi[1]
Ilma Magfira[2]

FORENSIK PADA JARINGAN KOMPUTER LOKAL DENGAN KLASIFIKASI SVM BERBASIS FRAMEWORK TAARA

Abstrak
Sistem SVM (Support Vector Machine) digunakan dalam analisis forensik jaringan komputer lokal (LAN) berbasis framework TAARA untuk mengklasifikasikan data yang terkait dengan keamanan jaringan. SVM adalah algoritma pembelajaran mesin yang dapat digunakan untuk klasifikasi dan regresi. Dalam analisis forensik jaringan komputer, SVM digunakan untuk mengklasifikasikan data yang terkait dengan serangan jaringan seperti serangan DDoS. Framework TAARA digunakan untuk memfasilitasi proses analisis forensik jaringan komputer. Framework ini menyediakan berbagai fitur untuk analisis forensik jaringan komputer, seperti analisis paket, analisis log, dan visualisasi data. Dalam pengujian yang dilakukan, SVM berhasil mengkalsifikasikan data dengan akurasi yang tinggi, sehingga dapat membantu dalam deteksi dan pencegahan serangan jaringan pada jaringan komputer lokal
Kata Kunci: Digital Forensic, Svm, Ddos, Framework Taara, Lan

Abstract
The SVM (Support Vector Machine) system is used in forensic analysis of local computer networks (LANs) based on the TAARA framework to classify data related to network security. SVM is a machine learning algorithm that can be used for classification and regression. In forensic analysis of computer networks, SVM is used to classify data related to network attacks such as DDoS attacks. The TAARA framework is used to facilitate the forensic analysis process of computer networks. The framework provides various features for forensic analysis of computer networks, such as packet analysis, log analysis, and data visualization. In the tests conducted, SVM succeeded in calcifying data with high accuracy, so that it can help in the detection and prevention of network attacks on local computer networks
Keywords: Digital Forensic, Svm, Ddos, Taara Framework, Lan

PENDAHULUAN

Dalam era komunikasi berbasis internet, keamanan siber semakin menjadi perhatian utama. Salah satu ancaman utama yang perlu dicatat adalah serangan DDoS (Distributed Denial of Service), yang memiliki potensi merusak dan mengganggu operasional sistem dan jaringan. Serangan DDoS melibatkan penggunaan botnet untuk mengirimkan lalu lintas data besar-besaran ke target dengan tujuan mengganggu atau mematikan akses pengguna sah. Keamanan jaringan komputer menjadi krusial, terutama setelah Universitas Kebangsaan Republik Indonesia (UKRI) mengalami serangan DDoS yang mengganggu aktivitas jaringan komputer.

Dalam menghadapi ancaman serangan DDoS, penggunaan teknik machine learning, seperti klasifikasi Super Vector Machine (SVM), menjadi pendekatan yang menarik untuk mendeteksi pola lalu lintas abnormal yang terkait dengan serangan tersebut. Serangan semacam ini seringkali sulit diidentifikasi karena terjadi dalam waktu singkat. Oleh karena itu, analisis forensik jaringan komputer dengan menggunakan framework TAARA dan SVM menjadi solusi yang relevan.

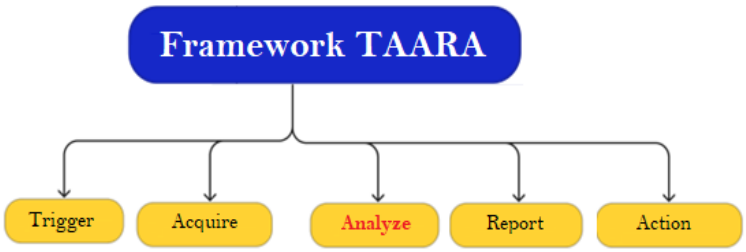
Penelitian ini bertujuan untuk menganalisis bukti digital dan mendeteksi model serangan DDoS dengan akurasi menggunakan SVM. Framework TAARA digunakan dalam analisis investigasi, yang dikembangkan berdasarkan Metodologi Threat Assessment & Remediation Analysis (TARA) dan standar ISO SAE 21434 serta NIST SP-800-30 dan ISO IEC 31010.

[1,2)] Universitas Kebangsaan Republik Indonesia, Bandung, Jawa Barat
email: denisuprihad@ukri.ac.id

Penelitian ini diharapkan dapat memberikan pemahaman yang lebih dalam mengenai serangan DDoS serta memberikan solusi dalam menghadapinya

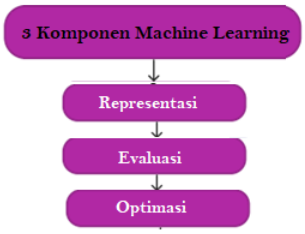
METODE

Dalam penelitian ini, metode Klasifikasi Support Vector Machines (SVM) digunakan pada tahap Analyze dalam framework Trigger, Acquire, Analysis, Report, Action (TAARA) untuk melakukan analisis forensik jaringan komputer lokal (LAN). Penggunaan aplikasi Wireshark untuk akuisisi data dan pengamatan lalu lintas jaringan, serta penggunaan SHA-256 Image untuk mengamankan bukti digital dalam bentuk gambar dengan perhitungan nilai hash. Selain itu, aplikasi Anaconda digunakan untuk analisis data. Data yang diakuisisi melalui Wireshark diubah menjadi dataset untuk analisis SVM sosial. Tahapan penelitian mencakup:



Gambar 1. Framework TAARA

Framework TAARA (Gambar 1) menjadi dasar untuk investigasi forensik jaringan komputer lokal, sementara metode Klasifikasi Support Vector Machines (SVM) akan digunakan dalam tahap Analyze dalam framework tersebut, pada dilihat pada Gambae 2 berikut :



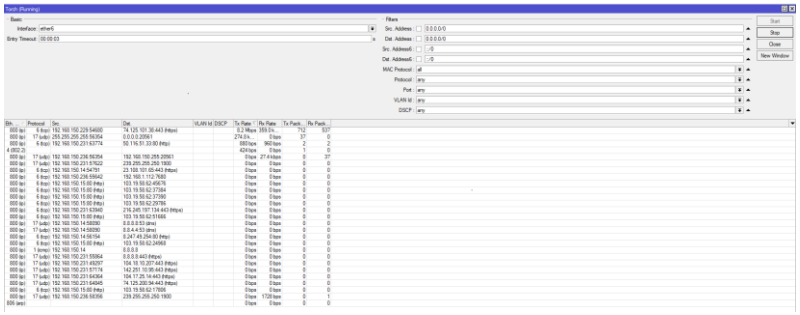
Gambar 2. Support Vektor Machines (SVM)

Representasi dalam cultural studies menekankan pentingnya makna dalam menggambarkan atau menyimbolkan sesuatu. Goldin menggambarkan representasi sebagai bentuk konfigurasi yang mewakili suatu hal, sementara Rosegrant mengartikannya sebagai sesuatu yang mewakili atau menggambarkan objek atau proses terkait dengan suatu hal (Rosengrant et al., 2007). Evaluasi, berasal dari kata "evaluation," merujuk pada proses penilaian yang digunakan untuk menilai hasil dari berbagai kegiatan yang telah direncanakan dan dilaksanakan guna mendukung pencapaian tujuan. Optimasi adalah bidang ilmu matematika yang berkonsentrasi pada pencarian sistematis nilai minimum atau maksimum dari suatu fungsi, peluang, atau pencarian nilai lainnya dalam berbagai konteks.

HASIL DAN PEMBAHASAN

1. Trigger

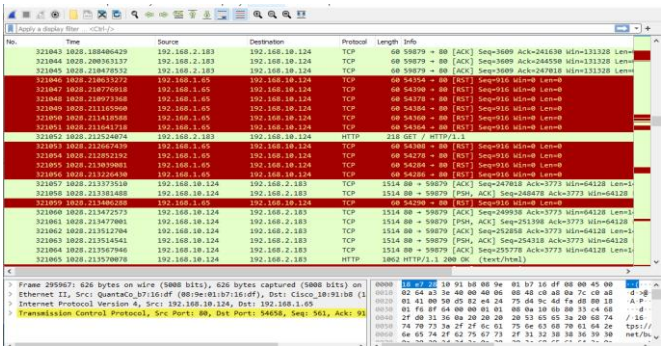
Dalam tahap Trigger Framework TAARA, informasi penting diperoleh dari Unit Pengelola Teknis (UPT) UKRI. Mereka menggunakan aplikasi Winbox Mikrotik untuk memantau lalu lintas jaringan. Aplikasi Winbox Mikrotik yang diperoleh dari UPT UKRI mengungkapkan perilaku pengguna jaringan yang berpotensi mengganggu jaringan komputer lokal (LAN) atau melakukan serangan terhadap jaringan komputer di UKRI.



Gambar 3. Dugaan DDOS Jaringan Komputer

Gambar 3 menampilkan data lalu lintas jaringan komputer UKRI dengan jumlah paket data yang dikirim sebanyak 712 (tx_packet) dan kecepatan pengiriman 8.2 MBps, serta jumlah paket yang diterima sebanyak 512 (rx_packet) dengan kecepatan penerimaan 3.5 MBps pada baris pertama.

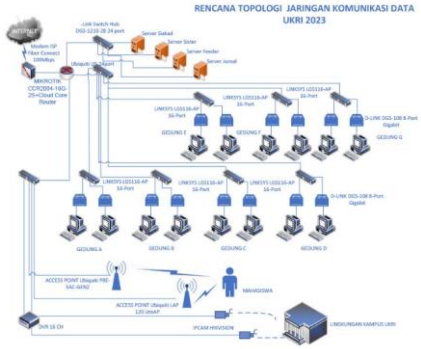
Untuk melengkapi tahap trigger dalam penelitian, penulis mengumpulkan data sekunder mengenai serangan DDOS dari organisasi OWASP Jakarta yang berkompeten dalam bidang Cybercrime. Hal ini dilakukan untuk memastikan hasil penelitian sesuai dengan tujuan yang telah ditetapkan.



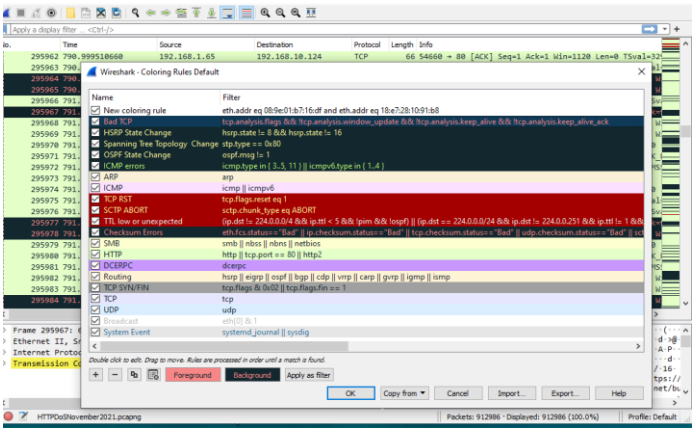
Gambar 4. Bentuk DDOS dari Wireshark

2. Acquire

Acquire adalah tahap pengumpulan bukti dan informasi terkait penyebab gangguan dalam jaringan komputer, dengan beragam kemungkinan bentuk serangan.



Gambar 5. Topologi Jaringan UKRI



Gambar 6. Pengaturan Default Warna Filter Wireshark

3. Analyze

Analyze adalah tahap penyelidikan mendalam berdasarkan data akuisisi. Dalam penelitian ini, penulis menggunakan metode Klasifikasi Support Vector Machines (SVM) untuk menghasilkan kesimpulan dari bukti yang ada. Pada tahap ini, data akuisisi dari Wireshark diubah menjadi dataset (CSV) untuk analisis, yang menghasilkan pola serangan DDoS dan akurasi data akhir. Pada tahap ini, terdapat proses sebagai berikut :

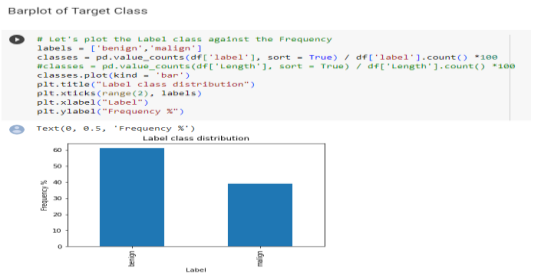
a. Representasi, Pada tahap representasi, koleksi library file dan dataset yang dihasilkan dari tahap Acquire dikumpulkan untuk digunakan dalam proses klasifikasi data SVM.

Gambar 7. Listing Kode Dataset, Info dan Statistik Dataset

Pada tahap representasi, dataset yang terdiri dari 104,345 row dan 23 collums dapat dilihat seperti yang ditunjukkan pada Gambar 7, dan ini akan digunakan dalam tahap evaluasi berikutnya.

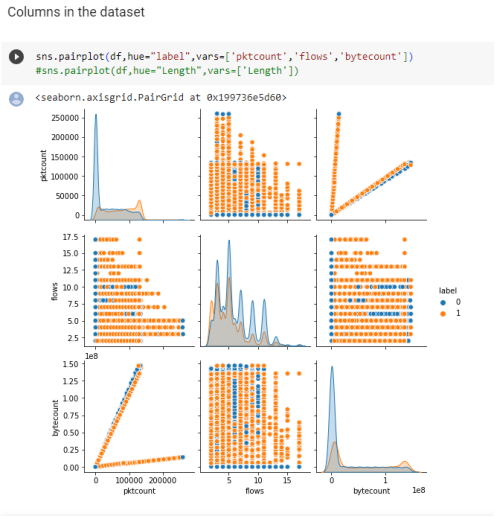
b. Evaluasi, Pada tahap evaluasi, dataset diisi dengan label satu untuk DDoS Attack dan nol untuk bukan DDoS Attack, sambil memeriksa nilai-nilai yang kosong (null). Hasilnya, terdapat indikasi DDoS Attack sebesar 39.01% dalam dataset, seperti yang ditunjukkan pada Gambar 8.

Gambar 8. Listing Kode Perhitungan Presentase Attact



Gambar 9. Listing Kode BarPlot

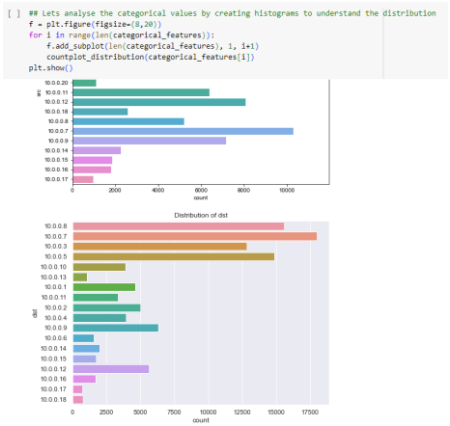
Pada Gambar 9 terlihat pada Bar Plot terdapat 39% serangan dan 61 % bukan serangan pada jaringan komputer



Gambar 10. Listing Kode Pairplot dengan Seaborn

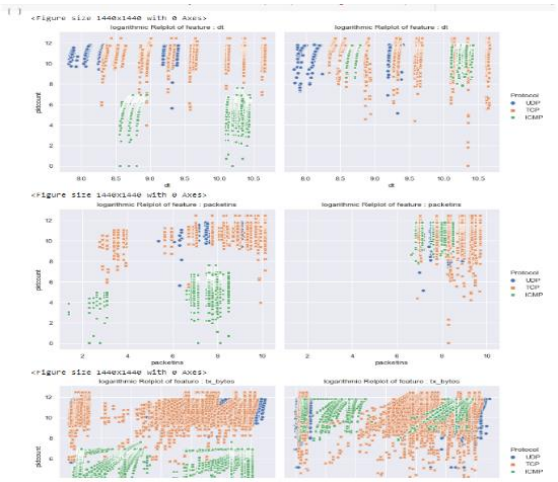
Menggunakan pairplot pada dataset yang sudah diberi label, terlihat linearitas garis yang menunjukkan adanya aliran paket dalam jumlah besar dalam jaringan komputer, berdasarkan pktcount, byte count, dan flow control.

Analisis selanjutnya adalah mengamati penyebaran data dalam dataset, terutama jumlah sumber dan tujuan, seperti yang terlihat pada Gambar 11.

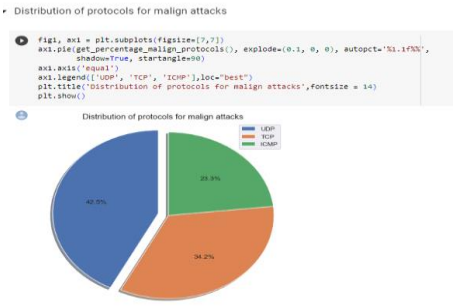


Gambar 11. Listing Kode Distribusi Jumlah Sumber dan Tujuan.

SVM terlihat jelas pada Gambar 12, dengan klasifikasi berdasarkan protokol UDP, TCP, dan ICMP (email), yang membentuk pola linearitas dengan warna yang serupa.

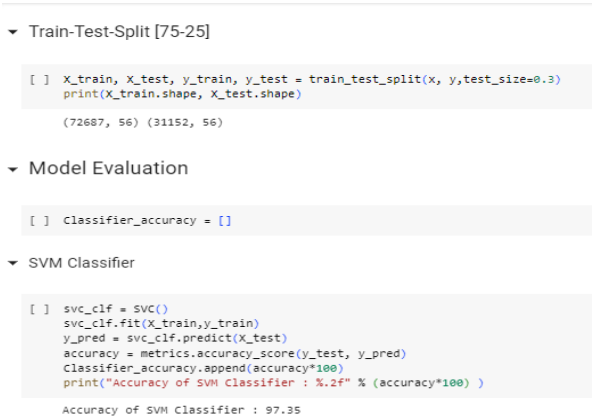


Gambar 12. Klasisfikasi Data Terhadap Protokol UDP, TCP, dan ICMP



Gambar 13. Presentase DDOS Terhadap Protokol UDP, TCP, dan ICMP

c. Optimasi, Untuk memastikan kualitas dataset yang telah dianalisis sebelumnya, dilakukan pengujian dan penghitungan akurasi model baru. Hasilnya, akurasi mencapai 97.35% seperti yang terlihat pada Gambar 14 berdasarkan kode program SVM yang telah dibuat.



Gambar 14. Akurasi Klasifikasi SVM

Untuk lebih jelasnya Perhitungan akurasi klasifikasi dapat dibuat dalam bentuk matriks yang dihasilkan dari pengkodean seperti Gambar 15

Classification Report

```
[ ]  print(classification_report(y_test, y_pred, target_names = labels))

                precision    recall  f1-score   support

       benign       0.98      0.98      0.98     18976
       malign       0.97      0.97      0.97     12176

     accuracy                           0.97     31152
    macro avg       0.97      0.97      0.97     31152
 weighted avg       0.97      0.97      0.97     31152
```

Gambar 15. Matriks Klasifikasi SVM Terhadap Train

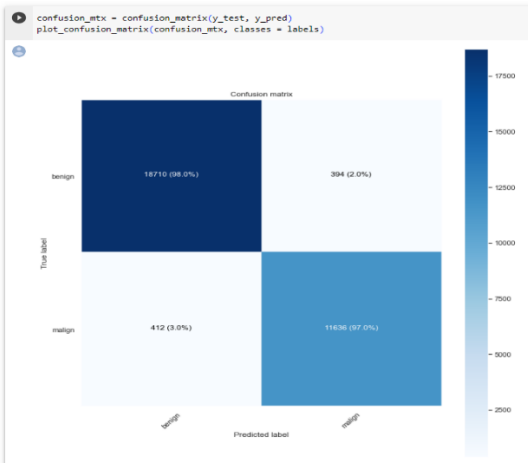
Langkah terakhir dalam optimasi adalah mengukur kebenaran data dengan confusion matrix dengan pengkodean dalam bentuk python seperti pada Gambar 16

Plotting Confusion Matrix

```
[ ] from itertools import product
    def plot_confusion_matrix(cm, classes, normalize=True, title='Confusion matrix', cmap=plt.cm.Blues):
        plt.figure(figsize=(10,10))
        plt.grid(False)
        plt.imshow(cm, interpolation='nearest', cmap=cmap)
        plt.title(title)
        plt.colorbar()
        tick_marks = np.arange(len(classes))
        plt.xticks(tick_marks, classes, rotation=45)
        plt.yticks(tick_marks, classes)
        cm1 = cm
        if normalize:
            cm = cm.astype('float') / cm.sum(axis=1)[:, np.newaxis]
            cm = np.around(cm, decimals=2)
            cm[np.isnan(cm)]
            thresh = cm.max() / 2.
        for i, j in product(range(cm.shape[0]), range(cm.shape[1])):
            plt.text(j, i, str(cm1[i, j])+ " ("+ str(cm[i, j]*100)+"%)",
                     horizontalalignment="center",
                     color="white" if cm[i, j] > thresh else "black")
        plt.tight_layout()
        plt.ylabel('True label')
        plt.xlabel('Predicted label')
```

Gambar 16. Ploting Confusion Matrix

```
confusion_mtx = confusion_matrix(y_test, y_pred)
plot_confusion_matrix(confusion_mtx, classes = labels)
```



Gambar 17. Hasil Ploting Confusion Matrix

Dari confusion matrix pada Gambar 17, didapatkan akurasi 98% pada nilai True True dan 97% pada nilai False False, menunjukkan tingkat kebenaran data sebesar 98% dan tingkat ketidakkebenaran (penyerangan) sebesar 97%.

4. Report

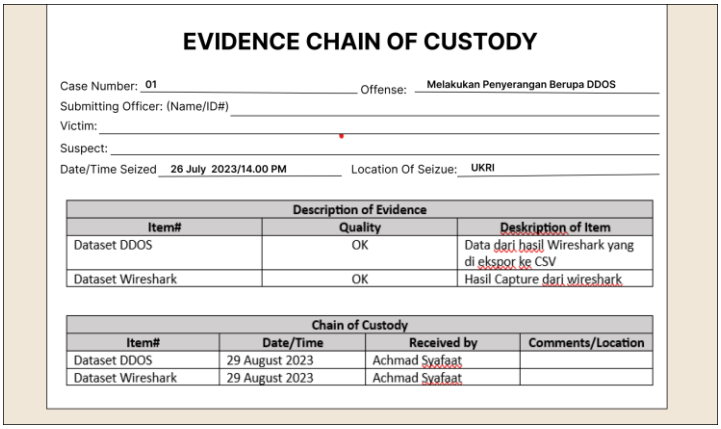
Report adalah tahap penyusunan hasil analisis dan penyelidikan terhadap bukti-bukti dalam jaringan komputer. Untuk menjaga keaslian bukti, dilakukan pengecekan nilai SHA-256 dari masing-masing bukti, yang hasilnya dapat ditemukan pada table di bawah ini:

Tabel 1 Nilai SHA-256 dari barang bukti yang didapat

No	Nama Barang Bukti	Nilai SHA-256
1	Dugaan DDOS Jaringan Komputer UKRI	193cc77775bdcbcd9e95112eefd2516124468f04136a6715f58c762a1338e4c8
2	Bentuk DDOS dari Wireshark	B81b2745b54fc13b4a6c339ee9a00dd6b5e7ffd710fb28dcd8faaf27d622efa
3	Pengaturan Default Warna Filter	2ca9b2ee8e5643f402014dc73549b4baf814b07742f

	Wireshark	1f49424a783c87288f0c4

Berdasarkan tahapan yang telah dilakukan, diperoleh Chain of Custody yang hasilnya dapat dilihat pada gambar 18. berikut.



EVIDENCE CHAIN OF CUSTODY

Case Number: 01 Offense: Melakukan Penyerangan Berupa DDOS

Submitting Officer: (Name/ID#)

Victim:

Suspect:

Date/Time Seized 26 July 2023/14.00 PM Location Of Seizue: UKRI

Description of Evidence		
Item#	**Quality**	**Deskription of Item**
Dataset DDOS	OK	Data dari hasil Wireshark yang di ekspor ke CSV
Dataset Wireshark	OK	Hasil Capture dari wireshark

Chain of Custody			
Item#	**Date/Time**	**Received by**	**Comments/Location**
Dataset DDOS	29 August 2023	Achmad Syafaat	
Dataset Wireshark	29 August 2023	Achmad Syafaat	

Gambar 18. Laporan Chain of Custody

5. Action

Action adalah saran yang dapat diterapkan berdasarkan hasil analisis, untuk meningkatkan pengelolaan keamanan jaringan komputer.

SIMPULAN

Berdasarkan penelitian ini, dapat disimpulkan: Penerapan Klasifikasi Support Vector Machines (SVM) pada tahap Analyze dalam framework TAARA dapat menghasilkan gambaran atau pola-pola serangan denial-of-service (DDoS) dengan tingkat akurasi yang tinggi.Hasil ini dapat menjadi barang bukti yang kuat untuk penyelidikan lebih lanjut oleh pihak berwenang.

Saran untuk peneltian selanjutnya, framework TAARA dapat dikembangkan kolaboratif dengan teknik-teknik AI untuk menjadi alat investigasi jaringan komputer yang dapat menangani berbagai jenis serangan selain DdoS

DAFTAR PUSTAKA

Al-Azhar Nuh, Muhammad. 2011. “Audio Forensics : Theory and Analysis,” 1-38 Akses, Kode, Sistem Elektronik, and Kode Akses. 2008. “Electronic Data Interchange (EDI)”

Artha, Komang Sidhi, Edi Winarko, and Departemen Ilmu. 2016. “Perbandingan Eros, Euclidean Distance Dan Dynamic Time Warping Dalam Klasifikasi Data Multivariate Time Series Menggunakan KNN,” no. Senapati.

Brogan, Chris. (2010). “Social Media 101: Tactics and Tips to Develop Your Business Online”. John Wiley & Sons, 2010.

D. Rachamawati, J. T. Tarigan dan A. B. C. Ginting, “A Comparative Study of Message Digest 5 (MD5) and SHA-256 Algorithm,” dalam 2nd International Conference on Computing and Applied Informatics 2017, Medan, 2018

Kom, F. Y. S., Kom, M., Prayudi, Y., & Kom, M. (2022). Pengembangan Framework Digital Forensics Investigation (FDFI) Pada Sosial Media Dengan Metode System Development Life Cycle (SDLC).

Lewis, B.K. (2010) Social Media and Strategic Communication: Attitudes and Perceptions among College Students. Public Relations Journal, 4, 1-23