VISUALISASI SERANGAN PAKET *RANSOMWARE* MENGGUNAKAN METODE *DEEP PACKET INSPECTION*

TUGAS AKHIR

OLEH :

DIO AZMI SAPUTRA

09011381621062

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

VISUALISASI SERANGAN PAKET *RANSOMWARE* MENGGUNAKAN METODE *DEEP PACKET INSPECTION*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

DIO AZMI SAPUTRA

09011381621062

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

HALAMAN PENGESAHAN

VISUALISASI SERANGAN PAKET *RANSOMWARE* MENGGUNAKAN METODE *DEEP PACKET INSPECTION*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

DIO AZMI SAPUTRA

09011381621062

Palembang, Juli 2021

Mengetahui

Ketua Jurusan Sistem Komputer,	**Pembimbing Tugas Akhir,**
Dr. Ir. H. Sukemi, M.T.	**Deris Stiawan, M.T., Ph.D.**
NIP.196612032006041001	**NIP.197806172006041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu

Tanggal : 23 Juni 2021

Tim Penguji :

1. **Ketua** : **Sarmayanta Sembiring, S.Si., M.T.**

2. **Sekretaris** : **Iman Saladin B. Azhar, S.Kom., M.MSI.**

3. **Pembimbing** : **Deris Stiawan, M.T., Ph.D.**

4. **Penguji** : **Ahmad Heryanto, S.Kom., M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER JURUSAN SISTEM KOMPUTER

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Dio Azmi Saputra

NIM : 09011381621062

Judul : Visualisasi Serangan Paket *Ransomware* Menggunakan Metode *Deep Packet Inspection*

Hasil Pengecekan *Software iThenticate/Turnitin* : 6 %

Menyatakan bahwa laporan skripsi saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / *Plagiat*. Apabila ditemukan unsur penjiplakan / *plagiat* dalam laporan skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, Juli 2021

Dio Azmi Saputra

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Assalamu'alaikum Wr. Wb.

Alhamdulilahirabbil'alamin. Puji dan Syukur penulis panjatkan kehadirat Allah SWT dan shalwat serta salam kepada junjungan Nabi kita, Nabi Muhammad SAW, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan tugas akhir berjudul "**Visualisasi Serangan Paket *Ransomware* Menggunakan Metode *Deep Packet Inspection*".**

Selesainya Tugas Akhir ini dimaksudkan untuk persyaratan dalam menyelesaikan studi pada jurusan Sistem Komputer Universitas Sriwijaya. Sebagai manusia yang memiliki kelemahan , penulis menyadari bahwa Tugas Akhir yang telah dibuat penulis masih jauh dari kata sempurna. Hal ini berkaitan dengan keterbatasan pengetahuan dan pengalaman dari penulis.

Oleh karena itu, penulis berharap adanya masukan-masukan baik berupa kritik dan saran sebagai bahan perbaikan bagi Tugas Akhir ini. Dalam menyelesaikan Tugas Akhir ini, penulis mendapatkan dukungan, saran serta bimbingan secara langsung dari pembimbing.

Selesainya Tugas Akhir ini tidak terlepas dari peran semua pihak yang mendukung dan membantu dalam menyusun Tugas Akhir ini. Penulis banyak mengucapka terima kasih sebesar-besarnya kepada pihak tak terbatas kepada :

1. Allah SWT yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis sehingga penulis dapat menyelesaikan Tugas Akhir ini.
2. Orang tua tercinta, yaitu Ibu Hj. Sunarwati, S.Pd. dan Bapak H. Suisyanto, S.Sos., M.Si., atas segala cinta dan dukungan dalam setiap do'anya sehingga dapat menempuh pendidikan Strata 1 sampai selesai.
3. Kakak tercinta, yaitu Feri Yanto Perdana, S.Pd., atas segala motivasi hingga memberikan dukungan mental untuk menempuh pendidikan ini.

4. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Julian Supardi, M.T., selaku Wakil Dekan Bidang Akademik Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Dr. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Bapak Deris Stiawan, M.T., Ph.D. selaku pembimbing Tugas Akhir yang banyak memberikan arahan serta motivasi dalam menyelesaikan laporan Tugas Akhir ini.
8. Bapak Ahmad Fali Oklilas, M.T., selaku Kepala Laboratorium Elektronika Dasar dan Sistem Digital yang telah memberikan fasilitas saat melakukan penelitian ini.
9. Moh. Cahyadi, M. Ikhsan, Hapis Reza Syahputra dan M. Nawwar Athalaza yang telah memberikan dukungan dan bantuan untuk menyelesaikan Tugas Akhir ini.
10. Teman-teman seperjuangan terkhususnya jurusan Sistem Komputer Kampus Palembang Angkatan 2016 yang telah banyak memberikan informasi yang sangat berguna.
11. Teman-teman game online khususnya dalam memberikan dukungan positif yang telah memperluas pengetahuan tentang Tugas Akhir ini.
12. Penulis modul, paper dan jurnal serta semua pihak yang tak dapat disebutkan satu persatu dan memberikan informasi dalam menyelesaikan Tugas Akhir ini.

Akhir kata penulis menyampaikan banyak terima kasih dan permohonan maaf apabila ada perkataan penulis, baik yang disegaja maupun yang tak disengaja. Semoga dari penelitian ini bermanfaat bagi kita semua.

Wassalamu'alaikum Wr. Wb.

Palembang, Juli 2021

Penulis

Visualization of Ransomware Packet Attacks Using Deep Packet Inspection Method

Dio Azmi Saputra (09011381621062)

Department of Computer Engineering, Faculty of Computer Science

Sriwijaya University

Email : DioAzmiSaputra@gmail.com

ABSTRACT

Visualization is a technique to present the number of *Ransomware* packet attacks that occur on datasets that have been provided by *Unavarra*. Attacks Visualization aiming to recognize attacks and make it easier to understood. *Deep Packet Inspection* (DPI) is a method to detect anomalies that formed attack of *Ransomware Packets* that happened on the enterprise networks. Packets including *Ransomware WannaCry* attack can be detected by DPI and carried out by attacker to gain access file in the client or server. The attack pattern of *Ransomware Wannacry Packet* on *Unavarra* dataset can be identified by several parameters such as *Protocol, Source Port, Destination Port, TLSv,* and *JA3* has been used. The results obtained from the detection of *Ransomware Wannacry Packet* are *Fingerprint* and can be categorized as *emotet malware*. The results of this study are obtained an attack detection accuracy which have the value 89%, then level of precision of dataset reached 100% and recall value reached 33%. Data of *Ransomware Wannacry Packet* can be visualized in data diagram, plot and dot which is quite good.

Keyword : *Visualization, Ransomware, Wannacry, Deep Packet Inspection, Fingerprint*

Visualisasi Serangan Paket *Ransomware* Menggunakan Metode *Deep Packet Inspection*

Dio Azmi Saputra (09011381621062)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email : DioAzmiSaputra@gmail.com

ABSTRAK

Visualisasi merupakan salah satu teknik untuk mempresentasikan banyaknya serangan paket *Ransomware* yang terjadi pada dataset yang telah disediakan oleh *Unavarra*. Visualisasi serangan bertujuan untuk mempermudah mengenali dan menyimpulkan serangan yang terjadi. *Deep Packet Inspection* (DPI) adalah sebuah metode untuk mendeteksi anomali berupa serangan paket *Ransomware* yang terjadi pada jaringan enterprise. Serangan paket yang dideteksi oleh DPI berupa serangan paket *Ransomware WannaCry* yang dilakukan oleh *attacker* untuk mendapatkan akses ke file yang ada di client maupun server. Pola serangan paket *Ransomware Wannacry* pada dataset *Unavarra* dapat dikenali dengan beberapa parameter seperti, *Protocol, Source Port, Destination Port, TLSv,* serta *JA3* yang digunakan. Hasil yang didapatkan dari pendeteksian terhadap serangan paket *Ransomware Wannacry* berupa *Fingerprint* dan dapat dikategorikan sebagai emotet *malware*. Hasil dari penelitian ini diperoleh nilai akurasi deteksi serangan mencapai 89%, kemudian untuk tingkat presisi dari dataset mencapai 100% dan nilai recall mencapai 33%. Data serangan paket *Ransomware Wannacry* dapat divisualisasikan berupa data diagram, data plot dan dot yang cukup baik.

Kata Kunci : Visualisasi, *Ransomware, Wannacry, Deep Packet Inspection, Fingerprint*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Deep Packet Inspection (DPI) merupakan sistem penyaringan paket dengan memonitor lalu lintas aliran paket-paket, yang berisikan informasi penting yang ada di *header* maupun *payload*. DPI dapat membedakan asal paket tersebut melalui *header* paket, bahkan dapat mengetahui aktifitas-aktifitas paket tersebut [1]. Pengidentifikasian DPI memberikan informasi paket berdasarkan 7 *Open System Interconnection* (OSI) *Layers*, mulai dari *Physical Layer* sampai *Application Layer*. Pengidentifikasian paket akan diperiksa mulai dari *header*, 7 OSI Layer, dan *payload*, serta memungkinkan mendeteksi paket yang mengandung *malicious signature* dan anomali pada jaringan [2].

DPI dapat memeriksa paket berupa *malicious* seperti *Ransomware*. *Ransomware* merupakan salah satu *malicious software* yang dapat meng-*encryption* file, serta dapat menyebarkan diri ke komputer lain dalam jaringan yang sama. Jenis paket *ransomware* yang dapat diidentifikasikan sebagai ancaman adalah *Crypto* dan *Locker*, serta memiliki beberapa jenis *family* diantaranya, *Petya*, *WannaCry*, *Bad Rabbit*, *Cerber*, *CryptoWall* dan *CryptoLocker* [3]. *Ransomware* menyerang komputer dengan *mailspam* berupa file *.xml*, *.doc*, *.gif*, *.zip* dan *.exe*. Komputer yang telah terinfeksi *ransomware* akan terkunci dengan enkripsi file, dan dimintai sejumlah uang untuk mendapatkan kunci *decryption*. Dalam proses pembayaran, komputer yang telah dienkripsi tidak berarti *ransomware* akan dihapus dari sistemnya, dan tidak akan menjamin keamanan komputer tersebut [4].

Dengan enkripsi lalu lintas paket yang dibuat oleh *ransomware*, DPI dapat melakukan klasifikasi trafik yang ter-enkripsi dengan *Pattern Matching* dengan, validasi TLS atau SSL yang mempunyai *Field* yang terdapat pada *Record Content Type*, *Protocol Version*, *Handshake Type* dan *Service* [5]. Dengan menemukan lalu lintas yang berbahaya dan tak dikenal, DPI akan mengelompokkan fitur berupa atribut-atribut yang dimiliki paket *ransomware*.

Seperti port yang diakses, url yang dibuka, serta aktifitas-aktifitas yang ada di dalam paket tersebut [6].

Penelitian [7], membahas permasalahan pengidentifikasian *Malware* menggunakan DPI dengan arsitektur *Deep Learning*, untuk memproses *payload* dari perilaku *malware* dengan tanda paket *benign*. Dengan menggunakan *Deep Learning*, penelitian ini dapat memprediksi *traffic* pada *host* dan *client*, serta membangun fungsi seperti *Intrusion Detection System* (IDS).

Pada penelitian yang dilakukan [8], membahas tentang visualisasi menggunakan pararel *k-means* pada lalu lintas jaringan, dengan *Shallow Packet Inspection* (SPI). Visualisasi *k-means* hanya yang menghasilkan *average packet interval, data transfered, duration,* dan *packet count*, dengan dibagi beberapa *centroids*.

Dari beberapa ulasan diatas, pemeriksaan paket dengan metode DPI dapat menggunakan *open-source tools* yang dikenal dengan nDPI. nDPI merupakan pengembangan dari *OpenDPI*, yang mengadaptasi pada pengidentifikasian protokol komunikasi yang berfokuskan pada lalu lintas internet. Dari hasil yang didapat dalam proses deteksi nDPI akan divisualisasikan dalam bentuk diagram dan data hasil *benign* pada paket *behavior* dan *signature ransomware*.

1.2. TUJUAN

Penelitian ini fokus untuk memvisualisasi lalu lintas paket *ransomware* dengan *Deep Packet Inspection*. Tujuan yang ingin diperoleh dalam penelitian skripsi ini diantara-nya adalah :

1. Mendapatkan TLSv dan JA3 *fingerprint* dalam serangan paket *ransomware.*
2. Membuat algoritma untuk visualisasi paket yang merupakan serangan *ransomware* dalam bentuk diagram.

1.3. MANFAAT

Manfaat yang dapat diperoleh dari penelitian skripsi yang dilakukan antara lain :

1. Dapat memahami cara kerja identifikasi paket pada sistem deteksi DPI.
2. Dapat memahami atribut yang digunakan pada serangan paket *Ransomware WannaCry* secara visual.

1.4. RUMUSAN MASALAH

Berdasarkan dari latar belakang masalah, permasalahan yang akan ditelaah dalam penelitian ini ada dua, yaitu :

1. Bagaimana cara metode DPI mendeteksi serangan paket *ransomware* pada dataset *RansomX* menggunakan *nDPI*?
2. Bagaimana cara memvisualisasikan fitur dan atribut pada paket *ransomware* dengan bentuk diagram?

1.5. BATASAN MASALAH

Batasan masalah mengenai judul yang didapat adalah :

1. Mekanisme pendeteksian serangan *Ransomware* menggunakan nDPI
2. Tidak Menjelaskan proses pencegahan paket serangan *ransomware*
3. Jenis *ransomware* yang dideteksi adalah *WannaCr*y pada dataset *RansomX Unavarra*
4. Serangan *Ransomware WannaCry* yang diujikan akan menghasilkan TLSv dan JA3 *fingerprint*
5. Proses visualisasi data serangan *Ransomware WannaCry* tidak dilakukan secara *real-time*

1.6. METODOLOGI PENELITIAN

Untuk mencapai tujuan dalam penelitian tugas akhir ini berikut ini adalah tahapan penelitian :

1. Tahapan Pertama (Studi Pustaka / Studi Literatur)

Pada Tahapan Pertama, diawali dengan mencari beberapa masalah yang sesuai untuk diangkat menjadi sebuah penelitian. Kemudian setelah itu, mencari beberapa sumber-sumber terkait seperti jurnal, artikel, buku, serta *raw* data yang berkaitan langsung dengan tugas akhir.

2. Tahapan Kedua (Perencanaan Sistem)

   Pada Tahapan Kedua akan membahas proses mengenai bagaimana merancang dan menerapkan metode yang baik pada sistem perangkat lunak. Selain itu, alat apa saja yang digunakan untuk mengatur sistem konfigurasi *raw* data dan penerapan kode yang digunakan untuk visualisasi.

3. Tahap Ketiga (Pengujian / Percobaan)

   Tahapan ini adalah tahap Pengujian untuk memeriksa sistem dan *raw* data yang berdasarkan penelitian metodologi serta pengujian sebelumnya, sampai mendapatkan hasil yang sesuai dengan hasil pada dataset.

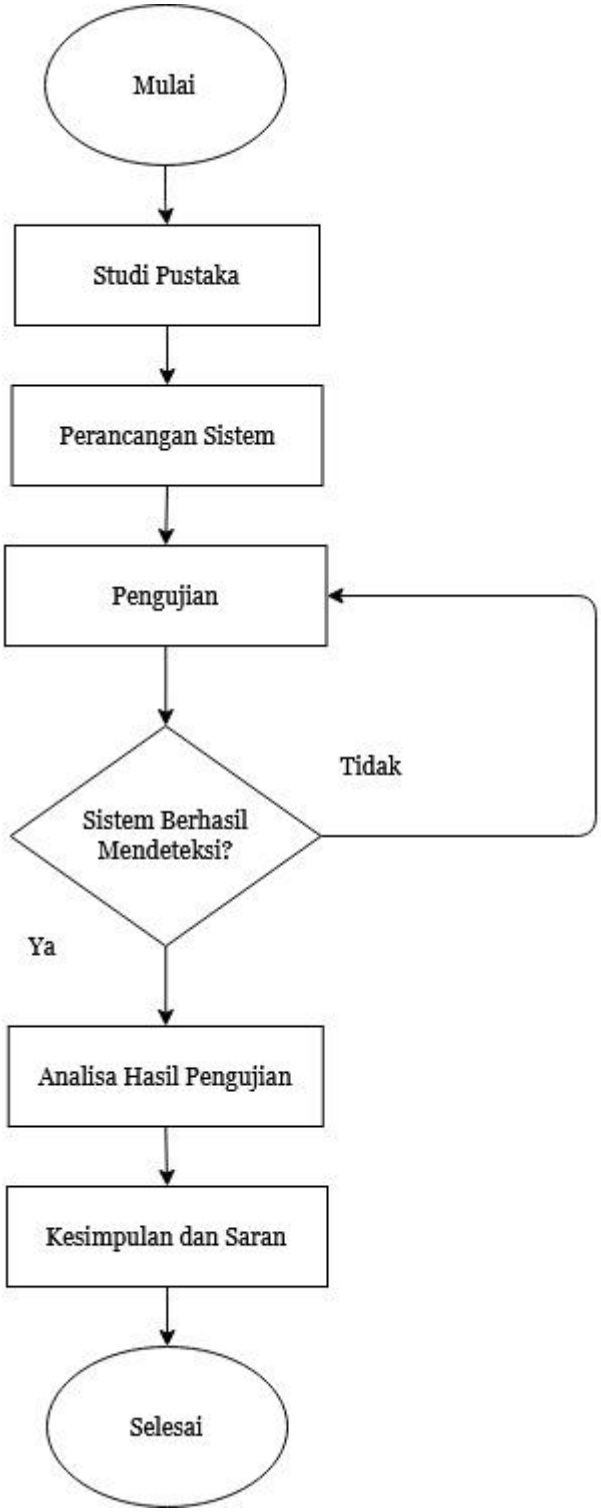
4. Tahap Keempat (Analisis)

   Pada Tahapan Keempat, dapat dilakukan pengolahan dan analisis dataset dari hasil uji yang sesuai dengan diterapkan pendekatan tertentu, hingga didapat hasil visual yang baik pada dataset. Dimana *raw* data diproses menjadi dataset dari pengujian.

5. Tahap Kelima (Kesimpulan dan Saran)

   Pada Tahap ini, akan merumuskan beberapa kesimpulan dari permasalahan yang didapat dari tahapan-tahapan sebelumnya. Selain itu, akan menambahkan beberapa saran yang baik serta dapat dijadikan dasar untuk penelitian selanjutnya.

   Pada gambar berikut ini gambar 1.1. dapat ditampilkan metodologi penelitian sebagai visual dalam bentuk diagram alir yang mempresentasikan pelaksanaan proses penelitian :



Gambar 1.1 : Diagram Alir Metodologi Penelitian

1.7. SISTEMATIKA PENULISAN

Untuk dapat mempermudah proses dalam penyusunan tugas akhir dan memperjelas isi dari setiap bagian bab, maka akan dibuat untuk sistematika penulisan berikut ini :

BAB I. PENDAHULUAN

Pada bab ini berisikan tentang penjelasan terpadu mengenai landasan penelitian, yang meliputi latar belakang, manfaat, tujuan, rumusan masalah, dan batasan masalah setelah itu metodologi penelitian serta penulisan yang terstruktur.

BAB II. TINJAUAN PUSTAKA

Pada bab ini berisi landasan dasar teori mengenai metode *Deep Packet Inspection*, *Ransomware*, isi paket serangan *ransomware*, dataset dan *open-source visualization tools*, yang berkaitan langsung dengan penelitian.

BAB III. METODOLOGI PENELITIAN

Pada bab ini menjelaskan proses penelitian dengan sistematis. Penjelasan di sub bab ini mencakup pada tahapan pengaturan sistem dan penerapan metode pada sistem dalam penelitian ini.

BAB IV. HASIL DAN ANALISA

Pada bab ini akan menjelaskan hasil dari pengujian metode sistem dari proses serta analisis secara visual dari tiap data yang didapatkan dari hasil pengujian.

BAB V. KESIMPULAN

Pada bab ini berisikan kesimpulan serta saran mengenai penelitian yang telah dilakukan, serta akan menanggapi tujuan yang akan diperoleh pada BAB I (Pendahuluan)

DAFTAR PUSTAKA

[1] G. A. P. Rodrigues *et al.*, "Cybersecurity and network forensics: Analysis of malicious traffic towards a honeynet with deep packet inspection," *Appl. Sci.*, vol. 7, no. 10, pp. 1–29, 2017, doi: 10.3390/app7101082.

[2] T. I. U. of B. Saad Hafeez B.Eng. and A, "Deep Packet Inspection using Snort," *Deep Pack. Insp. using Snort*, p. 24, 2017, [Online]. Available: http://on-demand.gputechconf.com/gtc/2017/presentation/s7468-wenji-wu-network-traffic-analysis-using-gpus.pdf.

[3] A. O.Imaji, "Ransomware Attacks : Critical Analysis , Threats , and Prevention methods," no. March, pp. 1–32, 2019.

[4] M. U. Kiru and A. Jantan, "Ransomware Evolution: Solving Ransomware Attack Challenges," *Evol. Bus. Cyber Age*, no. January, pp. 193–229, 2020, doi: 10.1201/9780429276484-9.

[5] T. Salim, S. A. Valianta, and D. Stiawan, "Klasifikasi Trafik Terenkripsi Menggunakan Metode Deep Packet Inspection (Dpi)," vol. 2, no. 1, pp. 424–429, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.

[6] L. Grant and S. Parkinson, "Identifying File Interaction Patterns in Ransomware Behaviour," no. September, pp. 317–335, 2018, doi: 10.1007/978-3-319-92624-7_14.

[7] R. Cheng and G. Watson, "D 2 PI : Identifying Malware through Deep Packet Inspection with Deep Learning," 2018.

[8] R. Velea and L. Margarit, "Network Traffic Anomaly Detection Using Shallow Packet Inspection and Parallel K-means Data Clustering," no. December, 2017, doi: 10.24846/v26i4y201702.

[9] S. A. V. Jatti and V. J. K. Kishor Sontif, "Intrusion detection systems," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 11, pp. 3976–3983, 2019, doi: 10.35940/ijrte.B1540.0982S1119.

[10] N. Meghanathan and L. A. Moore, "F ORENSICS," no. January 2010,

2014.

[11] E. A. Winanto, A. Heryanto, and D. Stiawan, “Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means,” *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.

[12] T. J. Parvat and P. Chandra, “A novel approach to deep packet inspection for intrusion detection,” *Procedia Comput. Sci.*, vol. 45, no. C, pp. 506–513, 2015, doi: 10.1016/j.procs.2015.03.091.

[13] J. Grashöfer and C. Titze, “Attacks on Dynamic Protocol Detection of Open Source Network Security Monitoring Tools,” pp. 1–11.

[14] L. F. Sikos, “Packet analysis for network forensics: A comprehensive survey,” *Forensic Sci. Int. Digit. Investig.*, vol. 32, p. 200892, 2020, doi: 10.1016/j.fsidi.2019.200892.

[15] M. Al-Hisnawi and M. Ahmadi, “Deep packet inspection using Cuckoo filter,” *2017 Annu. Conf. New Trends Inf. Commun. Technol. Appl. NTICT 2017*, no. October 2019, pp. 197–202, 2017, doi: 10.1109/NTICT.2017.7976111.

[16] Ferdiansyah, “Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware,” *JUSIFO (Jurnal Sist. Informasi)*, vol. 2, no. 1, pp. 44–59, 2018, [Online]. Available: http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf.

[17] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, “PayBreak : Defense against cryptographic ransomware,” *ASIA CCS 2017 - Proc. 2017 ACM Asia Conf. Comput. Commun. Secur.*, pp. 599–611, 2017, doi: 10.1145/3052973.3053035.

[18] C. Xu, S. Chen, J. Su, S. M. Yiu, and L. C. K. Hui, “A Survey on Regular Expression Matching for Deep Packet Inspection: Applications, Algorithms, and Hardware Platforms,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 4, pp. 2991–3029, 2016, doi: 10.1109/COMST.2016.2566669.

[19] L. Deri, M. Martinelli, A. Cardigliano, and I. I. T. Cnr, “nDPI : Open-Source High-Speed Deep Packet Inspection.”

[20] E. Berrueta, D. Morato, E. Magana, and M. Izal, “Open Repository for the Evaluation of Ransomware Detection Tools,” *IEEE Access*, vol. 8, pp. 65658–65669, 2020, doi: 10.1109/ACCESS.2020.2984187.