Indonesian Journal of Multidisciplinary on Social and Technology
Homepage: https://journal.ilmudata.co.id/index.php/ijmst
Vol. 1 No. 2 (2023) pp: 176-183
P-ISSN: 2986-6790, e-ISSN: 2986-6782

Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang

Saputra Dio Azmi[1], Stiawan Deris[2], Sutabri Tata[3]
[1]Magister Informatika, Magister Teknik Informatika, Universitas Bina Darma
[2]Sistem Komputer, Sistem Komputer, Universitas Sriwijaya
[3]Magister Informatika, Magister Teknik Informatika, Universitas Bina Darma
[1]dioazmisaputra@gmail.com, [2]stiawanderis @unsri.ac.id [2]tata.sutabril@gmail.com*

Abstrak

Sistem deteksi adalah salah satu teknik untuk mendeteksi dan memberikan alarm bahwa adanya ancaman *Malware* bagi setiap perusahaan di indonesia. Sistem deteksi serangan *Malware* bertujuan untuk mendeteksi dan memberikan alarm agar sistem berfungsi secara optimal. Serangan *Ransomware* dapat menghentikan proses transaksi serta fungsi website SMK Negeri 1 Palembang dan memberikan dampak negatif bagi nasabah SMK Negeri 1 Palembang. *Deep Packet Inspection* (DPI) adalah sebuah metode untuk mendeteksi anomali berupa serangan *Ransomware* yang terjadi pada jaringan enterprise SMK Negeri 1 Palembang. Serangan yang dideteksi oleh DPI berupa serangan *Ransomware WannaCry* yang dilakukan oleh *attacker* untuk mendapatkan akses ke file yang ada di client maupun server. Pola serangan paket *Ransomware Wannacry* pada SMK Negeri 1 Palembang dapat dikenali dengan beberapa parameter seperti, *Protocol, Source Port, Destination Port, TLSv,* serta *JA3* yang digunakan.

Kata kunci: *Deep Packet Inspection, Intrusion Detection System, Ransomware, WannaCry*

1. Pendahuluan

Keamanan jaringan menjadi pelindung data pengguna terhadap serangan *Malware*. Dalam meningkatkan keamanan, di setiap jaringan diperlukan Sistem Pendeteksi untuk melindungi data dari tindak pencurian. Sistem Pendeteksi keamanan jaringan dapat mendeteksi berbagai jenis serangan, serta bersifat otomatis dan dapat mendeteksi semua ancaman. IDS atau bisa disebut juga *Intrusion Dectection System* sebagai perangkat dengan tujuan untuk mendeteksi anomali pada jaringan enterprise(Rodrigues et al., 2017).

Malicous Software atau yang lebih dikenal sebagai *Malware* merupakan perangkat lunak yang secara eksplisit didesain, untuk melakukan aktifitas berbahaya atau perusak perangkat lunak lainnya seperti *Trojan, Virus, Spyware* dan *Exploit* (Ferdiansyah, 2018). *Malware* diciptakan dengan maksud tertentu, yaitu melakukan aktifitas berbahaya yang berdampak sangat merugikan bagi para korbannya (Kolodenker et al., 2017). *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 mempunyai beberapa jenis *family* diantaranya*, Petya, WannaCry, Bad Rabbit, Cerber, CryptoWall* dan *CryptoLocker* (O.Imaji, 2019).

Intrusion Detection System merupakan sistem yang sangat penting dalam melakukan keamanan jaringan serta dapat mendeteksi kemungkinan adanya serangan oleh *WannaCry*. Teknik yang umum digunakan untuk mendeteksi pada *Intrusion Detection System* adalah sistem *Rule base* seperti *attack signature* dan *attack anomaly.* Akan tetapi teknik ini masih memiliki kelemahan seperti ketidakmampuan untuk men-*denied* paket lalu lintas yang masuk dalam jaringan enterprise. *Intrusion Detection System* dengan teknik deteksi *attack signatures* tidak bisa mendeteksi tipe serangan baru yang tidak ada pada *database* serangan. Sedangkan *Intrusion Detection System* yang menggunakan mekanisme *attack anomaly* dapat mendeteksi beberapa variasi serangan baru, tetapi sering menghasilkan *false alarms* yang cukup besar (Rodrigues et al., 2017).

Deep Packet Inspection (DPI) merupakan *Intrusion Detection System* dengan pemanfaatan penyaringan paket data dengan memonitor lalu lintas aliran 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 (Rodrigues

et al., 2017). Identifikasian yang dilakukan memberikan informasi paket berdasarkan 7 *Open System Interconnection* (OSI) *Layers*, mulai dari *Physical Layer* sampai *Application Layer.* Pendeteksian paket akan diperiksa mulai dari *header*, 7 OSI Layer, dan *payload*, serta memungkinkan deteksi paket yang mengandung *malicious signature* dan anomali pada jaringan enterprise(Saad Hafeez B.Eng. & A, 2017). Dengan enkripsi lalu lintas paket yang dibuat oleh *ransomware*, DPI dapat melakukan klasifikasi trafik yang ter-enkripsi dengan *Pattern Matching* dengan, validasi TLSv yang mempunyai *Field* yang terdapat pada *Record Content Type, Protocol Version, Handshake Type* dan *Service* (Salim et al., 2016). 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 (Grant & Parkinson, 2018).

Penelitian (Cheng & Watson, 2018), 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 (Velea & Margarit, 2017), 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.*

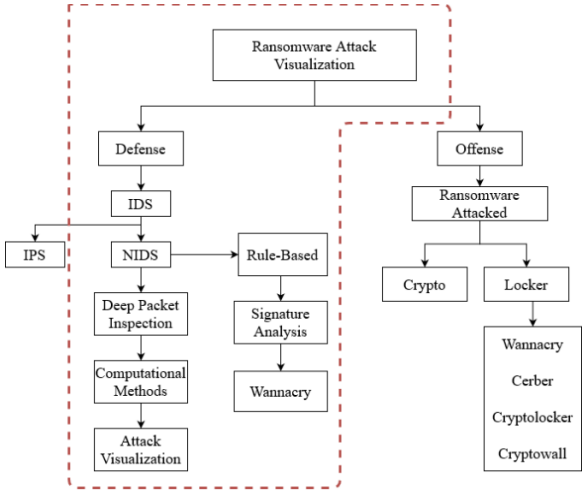
Dari beberapa ulasan diatas, *Intrusion Detection System* dengan metode *Deep Packet Inspection* dapat menggunakan *open-source tools* yang dikenal dengan *Snort* dengan mengaplikasikan *rule based* dari *Deep Packet Inspection*. *OpenDPI* merupakan pengembangan dari *Snort,* yang mengadaptasi pada pengidentifikasian serta pendeteksian protokol komunikasi yang berfokuskan pada lalu lintas internet. Dari hasil yang didapat dalam proses deteksi Snort akan divisualisasikan dalam bentuk diagram dan data hasil *benign* pada paket *behavior* dan *signature ransomware.*

2. Metode Penelitian

Pada tahap pertama penelitian ini adalah perancangan sistem yang akan digunakan seperti penginstallan perangkat lunak dan perangkat keras yang akan digunakan untuk membantu sistem deteksi yang dilakukan oleh DPI.

- Sistem deteksi yang digunakan untuk mendeteksi serangan *Ransomware WannaCry* akan menerapkan sistem *Defense* untuk mengetahui seberapa banyak dan berbahayanya *Ransomware WannaCry*
- *Intrusion Detection System (IDS)* akan melakukan tindakan dalam mendeteksi serangan melalui *Network-based Intrusion Detection System (NIDS)* yang telah menerapkan *rule based signature* dari *Ransomware WannaCry*
- Kemudian Sistem *Deep Packet Inspectio (DPI)* melakukan tindakan pengecekan dan *screening* informasi paket yang melewati jaringan enterprise tersebut.
- Sistem DPI akan melakukan *computational method* yang dimiliki oleh sistem *rule-based signature* dalam paket *Ransomware WannaCry* dalam status "*active"*
- Setelah paket *Ransomware WannaCry* terdeteksi melewati jaringan enterprise, *Deep Packet Inspection (DPI)* akan melakukan *Attack Visualization* berupa informasi *packet header* dan objek gambar yang mengetahui seberapa banyak objek *Ransomware WannaCry* menyamar.

Berikut ini adalah diagram metode penelitian yang dilakukan oleh Snort dan *Deep Packet Inspection* dalam melakukan tindakan pendeteksian *Ransomware WannaCry.*



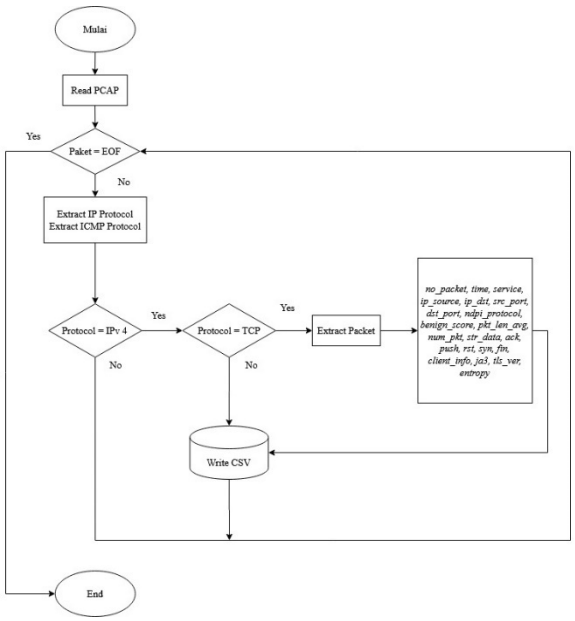
Gambar 2.1. Metode Diagram Penelitian

Kemudian setelah berhasil mendeteksi adanya ancaman *Ransomware WannaCry*, *Deep Packet Inspection* akan melakukan *Collecting* data. Informasi data serangan yang dilakukan *Ransomware WannaCry* akan menghasilkan data format *.pcap.* Format tersebut tidak dapat digunakan untuk mendapatkan informasi yang akurat, akan tetapi harus melakukan proses

DOI: https://doi.org/10.31004/ijmst.v1i2.142

ekstraksi agar dapat mendapatkan informasi yang diinginkan. Tahapan selanjutnya adalah melakukan *Feature Extraction*.

Proses *Feature Extraction* adalah proses ekstraksi akan mendapatkan hasil berupa data *.xls* yang dapat dibaca dan dipahami, serta dapat diproses lebih lanjut dalam proses visualisasi data menjadi data yang matang dan siap disajikan. Proses alur kerja *Feature Extraction* dapat dilihat pada gambar berikut ini.



Pada tahapan selanjutnya adalah mengoreksi hasil dari deteksi DPI, dengan mengelompokkan atribut-atribut dari serangan *ransomware* sebagai pola serangan. Setelah mendapatkan atribut-atribut jenis serangan paket *ransomware*, akan diklasifikasi dengan paket normal. Algoritma visualisasi yang telah disediakan akan digunakan untuk menguji total paket yang menjadi *alert*. Pada tahap akhir, akan dilakukan visualisasi data paket dalam bentuk diagram

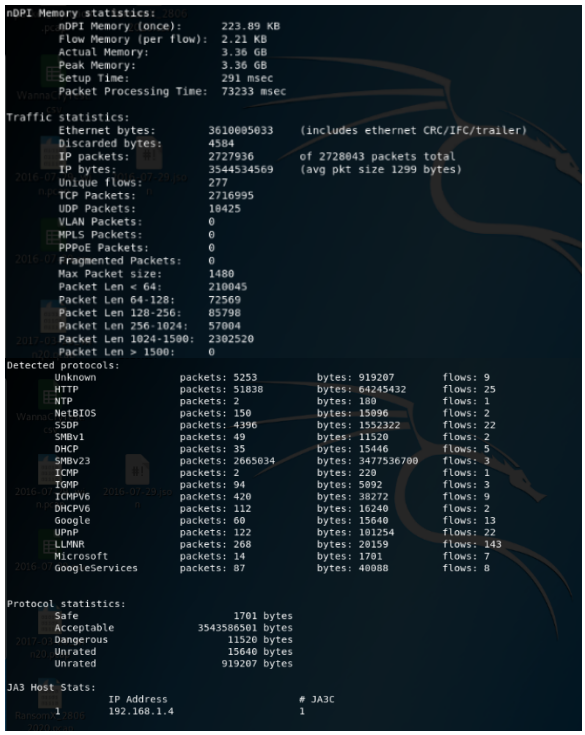
3. Hasil dan Pembahasan

1. Hasil Pendeteksian *Deep Packet Inspection*

Hasil dari pendeteksian yang *dilakukan Deep Packet Inspection* dapat digunakan untuk mengenali sebuah paket serangan, salah satunya adalah dengan pola. Pola paket serangan dapat berupa atribut-atribut unik yang dimiliki sebuah paket misalnya protokol yang digunakan*, port source, port destination,* TLSv, serta *benign score*. Pada penelitian ini pola paket serangan akan digunakan sebagai pengklasifikasian awal. Untuk mendapatkan pola serangan ada beberapa langkah-langkah pada penelitian tugas akhir yaitu sebagai berikut :

- Mendeteksi serangan *Ransomware* untuk dibaca oleh sistem DPI sehingga mendapatkan *alert* yang berisi informasi serangan.
- Hasil pendeteksi yang dilakukan DPI awal berupa informasi protokol yang digunakan pada *headers* paket, kemudian dapat dibandingkan dengan *raw data* dan apakah ada paket lain pada hasil deteksi serangan.
- Mencari atribut-atribut unik seperti TLSv dan JA3 dan *Fingerprint* maka dapat dicari dari hasil *feature extraction*, untuk memastikan bahwa paket tersebut adalah benar serangan.

Kemudian atribut yang dihasilkan pada proses deteksi akan divalidasi dengan hasil ekstraksi, dengan memvalidasi waktu yang didapatkan dengan memanfaatkan atribut *time*. Berikut gambar 3.4 adalah proses validasi serangan dengan data ekstraksi.



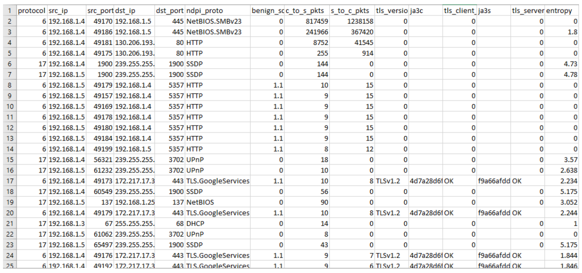
Gambar 3.1. Hasil Dari Pendeteksian DPI

2. Data Hasil Ekstraksi

Hasil dan Pada proses ekstraksi dataset SMK Negeri 1 Palembang berisi berbagai macam protokol, diantaranya adalah HTTP, HTTPS, NTP, NetBIOS, SSDP, SMBv1, ICMP, IGMP, Google, UPnP, dan LLMNR. Dan atribut yang terdapat pada saat ekstraksi dilakukan antaranya, *flow_ID, src_IP, src_port, dst_IP, dst_port, protocol,* dan lainnya. Pada gambar 4.3 berikut ini merupakan salah satu hasil dari Pendeteksian yang dilakukan nDPI terhadap SMK Negeri 1 Palembang Beberapa paket yang telah di ekstraksi antara lain, protokol yang digunakan, *ip_source, port_destination, ip_destination, port_destination,*

DOI: https://doi.org/10.31004/ijmst.v1i2.142

benign_score, total packet, TLSv dan JA3. Pada gambar berikut adalah hasil *Feature Extraction* dari pendeteksian DPI. Gambar berikut merupakan hasil dari ekstraksi data yang mengindikasikan adanya serangan *Ransomware* pada jaringan SMK Negeri 1 Palembang.

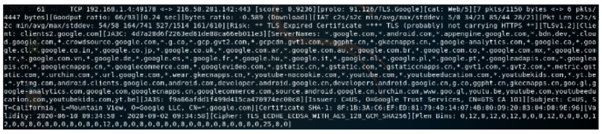


1	protocol	src_ip	src_port	dst_ip	dst_port	ndpi_proto	benign_sc	c_to_s_pkts	s_to_c_pkts	tls_versio	ja3c	tls_client_	ja3s	tls_server	entropy
2	6	192.168.1.4	49170	192.168.1.5	445	NetBIOS.SMBv23	0	817459	1238158	0		0		0	0
3	6	192.168.1.4	49186	192.168.1.5	445	NetBIOS.SMBv23	0	241966	367420	0		0		0	1.8
4	6	192.168.1.4	49181	130.206.193.	80	HTTP	0	8752	41545	0		0		0	0
5	6	192.168.1.4	49175	130.206.193.	80	HTTP	0	255	914	0		0		0	0
6	17	192.168.1.4	1900	239.255.255.	1900	SSDP	0	144	0	0		0		0	4.73
7	17	192.168.1.5	1900	239.255.255.	1900	SSDP	0	144	0	0		0		0	4.78
8	6	192.168.1.5	49179	192.168.1.4	5357	HTTP	1.1	10	15	0		0		0	0
9	6	192.168.1.5	49157	192.168.1.4	5357	HTTP	1.1	9	15	0		0		0	0
10	6	192.168.1.5	49169	192.168.1.4	5357	HTTP	1.1	9	15	0		0		0	0
11	6	192.168.1.5	49178	192.168.1.4	5357	HTTP	1.1	9	15	0		0		0	0
12	6	192.168.1.5	49180	192.168.1.4	5357	HTTP	1.1	9	15	0		0		0	0
13	6	192.168.1.5	49184	192.168.1.4	5357	HTTP	1.1	9	15	0		0		0	0
14	6	192.168.1.4	49199	192.168.1.5	5357	HTTP	1.1	8	12	0		0		0	0
15	17	192.168.1.4	56321	239.255.255.	3702	UPnP	0	18	0	0		0		0	3.57
16	17	192.168.1.5	61232	239.255.255.	3702	UPnP	0	10	0	0		0		0	2.638
17	6	192.168.1.4	49173	172.217.17.3	443	TLS.GoogleServices	1.1	10	8	TLSv1.2	4d7a28d6f	OK	f9a66afdd	OK	2.234
18	17	192.168.1.4	60549	239.255.255.	1900	SSDP	0	56	0	0		0		0	5.175
19	17	192.168.1.5	137	192.168.1.25	137	NetBIOS	0	90	0	0		0		0	3.052
20	6	192.168.1.4	49179	172.217.17.3	443	TLS.GoogleServices	1.1	10	8	TLSv1.2	4d7a28d6f	OK	f9a66afdd	OK	2.244
21	17	192.168.1.3	67	255.255.255.	68	DHCP	0	14	0	0		0		0	1
22	17	192.168.1.5	61062	239.255.255.	3702	UPnP	0	8	0	0		0		0	0
23	17	192.168.1.5	65497	239.255.255.	1900	SSDP	0	43	0	0		0		0	5.175
24	6	192.168.1.4	49176	172.217.17.3	443	TLS.GoogleServices	1.1	9	7	TLSv1.2	4d7a28d6f	OK	f9a66afdd	OK	1.844
25	6	192.168.1.4	49192	172.217.17.3	443	TLS.GoogleServices	1.1	9	6	TLSv1.2	4d7a28d6f	OK	f9a66afdd	OK	1.846

Gambar 3.2. Data hasil ekstraksi

3. Pengenalan pola serangan *Ransomware WannaCry*

Pada tahap selanjutnya berupa pengenalan pola serangan *Ransomware* yang dilakukan pada Bank Syariah Indoensia. Serangan yang dilakukan *Ransomware* ini merupakan serangan *WannaCry* yang melalui protokol TCP. *Alert* yang dapat dideteksi nDPI berupa protokol TCP, *ip_source, port_source, ip_destination, port_destination,* dan *TLSv1.2*. DPI telah mendeteksi beberapa *content* yang digunakan dalam *payload* paket, seperti **.google.com, *.android.com,* dan lainnya. nDPI juga telah mendeteksi adanya JA3 yang digunakan pada *Client Hello* dan *Server Hello* dalam melakukan komunikasi. Pada gambar 3.3. adalah salah satu serangan *Ransomware WannaCry* dengan tabel informasi payloadnya yang diperoleh dari deteksi DPI.

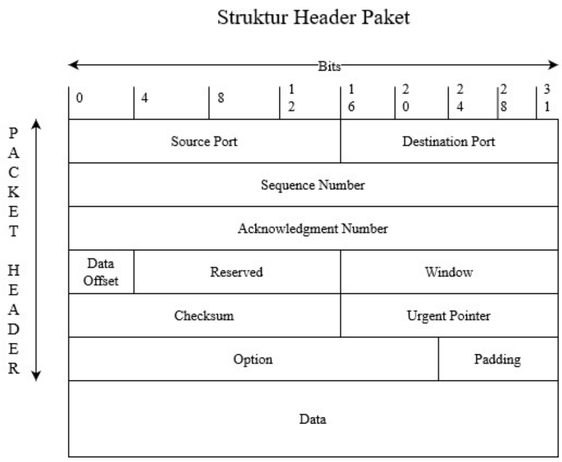


```
61      TCP 192.168.1.4:49178 <-> 216.58.201.142:443 [score: 0.9236][proto: 91.126/TLS.Google][cat: Web/5][7 pkts/1150 bytes <-> 6 pkts/4447 bytes][Goodput ratio: 66/93][0.24 sec][bytes ratio: -0.589 (Download)][IAT c2s/s2c min/avg/max/stddev: 5/8 34/21 85/44 28/21][Pkt Len c2s/s2c min/avg/max/stddev: 54/58 164/741 527/1514 161/610][Risk: ** TLS Expired Certificate **** TLS (probably) not carrying HTTPS **][TLSv1.2][Client: clients2.google.com][JA3C: 4d7a28d6f2263ed61de88ca66eb011e3][ServerNames: *.google.com,*.android.com,*.appengine.google.com,*.bdn.dev,*.cloud.google.com,*.crowdsource.google.com,*.g.co,*.gcp.gvt2.com,*.gcpcdn.gvt1.com,*.ggpht.cn,*.gkecnapps.cn,*.google-analytics.com,*.google.ca,*.google.cl,*.google.co.in,*.google.co.jp,*.google.co.uk,*.google.com.ar,*.google.com.au,*.google.com.br,*.google.com.co,*.google.com.mx,*.google.com.tr,*.google.com.vn,*.google.de,*.google.es,*.google.fr,*.google.hu,*.google.it,*.google.nl,*.google.pl,*.google.pt,*.googleadapis.com,*.googleapis.cn,*.googlecnapps.cn,*.googlecommerce.com,*.googlevideo.com,*.gstatic.cn,*.gstatic.com,*.gstaticcnapps.cn,*.gvt1.com,*.gvt2.com,*.metric.gstatic.com,*.urchin.com,*.url.google.com,*.wear.gkecnapps.cn,*.youtube-nocookie.com,*.youtube.com,*.youtubeeducation.com,*.youtubekids.com,*.yt.be,*.ytimg.com,android.clients.google.com,android.com,developer.android.google.cn,developers.android.google.cn,g.co,ggpht.cn,gkecnapps.cn,goo.gl,google-analytics.com,google.com,googlecnapps.cn,googlecommerce.com,source.android.google.cn,urchin.com,www.goo.gl,youtu.be,youtube.com,youtubeeducation.com,youtubekids.com,yt.be][JA3S: f9a66afdd1f499d415ca470974ec08c8][Issuer: C=US, O=Google Trust Services, CN=GTS CA 1O1][Subject: C=US, ST=California, L=Mountain View, O=Google LLC, CN=*.google.com][Certificate SHA-1: 8F:1B:3A:C6:EF:ED:81:79:4D:14:07:4B:80:D9:20:83:04:D8:9E:96][Validity: 2020-06-10 09:34:58 - 2020-09-02 09:34:58][Cipher: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256][Plen Bins: 0,12,0,12,0,12,0,0,0,12,0,0,0,0,12,0,0,0,0,0,0,0,0,0,12,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,25,0,0]
```

Gambar 3.3. Serangan Ransomware Terhadap SMK Negeri 1 Palembang

4. Struktur *Packet Header*

Banyak serangan jaringan tidak dapat dideteksi dengan pencocokan string, karena dasarnya tidak menampilkan tanda atau pola dalam payload. Ini berarti, untuk setiap serangan, muatan yang berbeda dapat digunakan sehingga proses pencocokan tanda tangan gagal. Dalam kasus seperti itu, untuk mendeteksi serangan ini, pendekatan lain harus diambil. Salah satunya adalah untuk menganalisis konten *header* paket yang dapat menyajikan anomali, memberikan bukti serangan atau penyelidikan sedang berlangsung.



Gambar 3.3. Struktur *Header* Paket.

Tabel 1. Informasi Packet Header

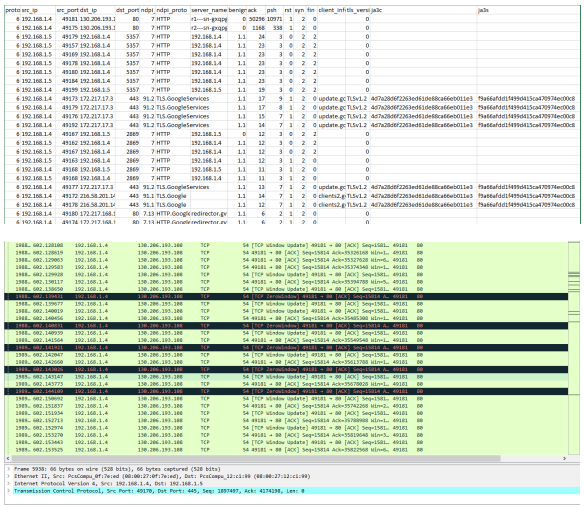
Atribut	Packet Header *Serangan*
Port Source	mempunyai *size* 2 byte atau (16 bit) yang berperan untuk mengindikasi asal muasal *protocol* pada lapisan *application* yang akan mengirimkan bagian dari TCP yang berhubungan. Perpaduan antara field *IP*
Address Source	pada *header* IP dan field *port source* pada field *header* TCP dapat disebut sebagai sumber soket, artinya pada sebuah alamat global dari seluruh jaringan dapat dikirim hanya dengan bagian dari *port source*.
Port Destination	mempunyai *size* 2 byte atau (16 bit) yang berperan untuk mengindikasi tujuan dari *protocol* pada lapisan *application* yang memberikan bagian dari TCP berhubungan, artinya pada alamat global akan mengirimkan bagian dari *port destination*.
Sequence num	mempunyai *size* 4 byte atau (32 bit) yang mengindikasi urutan nomor dari octet pertama pada paket data di dalam sebuah bagian TCP yang akan dikirimkan.
Acknowledgment num	mempunyai *size* 4 byte atau (32 bit). *Acknowledgment number* atau ACK yang mengindikasi urutan nomor dari octet kemudian dalam aliran *byte* dapat diterima oleh pengirim dari sisi client untuk pengiriman selanjutnya. ACK sangatlah penting untuk bagian-bagian TCP dengan *flag* ACK yang diatur ke angka 1.
Offset Data	mempunyai *size* 1 byte atau (4 bit), yang dapat mengindikasi data dari setiap bagian TCP pada saat dimuat.
Reserved	mempunyai *size* (6 bit), pada saat pengiriman bagian TCP akan di atur kedalam bit pada angka 0.
Flags	mempunyai *size* (6 bit), yang dapat mengindikasi flag-flag dari TCP

DOI: https://doi.org/10.31004/ijmst.v1i2.142

Atribut	Packet Header ***Serangan***
	sebagai *Ack*, *Push*, *Reset*, *Urgent*, *Syn,* dan *Fin*.
Window	mempunyai *size* 2 byte atau (16 bit), yang dapat mengindikasi jumlah dari byte yang sebenarnya dimiliki oleh *buffer* dari host penerima bagian yang bersangkutan. Tujuannya adalah untuk menyusun data dan mengatur lalu lintas data atau *control flow*
Checksum	mempunyai *size* 2 byte atau (16 bit), yang dapat melakukan pemeriksaan integritas dari bagian TCP (*payload* dan *header*). Angka dari field *checksum* akan diset ke angka 0, selama proses perhitungan pada *checksum*.
Urgent Pointer	mempunyai *size* 4 byte atau (16 bit), yang melambangkan lokasi paket data yang dianggap penting atau "*urgent*" dalam bagiannya
Padding and Option	mempunyai *size* 4 byte (32 bit), yang berperan seperti tempat penampung data dari beberapa opsi tambahan dalam bagian TCP

5. Pola serangan *Ransomware WannaCry*

Pola serangan berupa *Fingerprint Ransomware WannaCry* pada dataset SMK Negeri 1 Palembang menggunakan *Payload* dan *Header*. Pada *header* paket terdapat beberapa informasi penting mengenai IP dan Port yang dituju. Sedangkan pada *payload* mempunyai konten variabel dan TLSv yang digunakan saat *handshake* antara Client dan Server. Dari TLSv dan *Cipher* yang digunakan akan membentuk *string* MD5 kemudian di *hash* untuk mendapatkan JA3 *Fingerprint*. Berikut informasi pada client dan JA3C pada serangan paket *ransomware wannacry*. Berikut kecocok dari hasil pada struktur data dari *Packet Header* yang dimiliki *Ransomware Wannacry*.



Gambar 3.4. Pola *Packet Header* dari *Ransomware WannaCry*

Pada tabel 2. Pola Serangan *Ransomware Wannacry* menjelaskan pola-pola serangan paket *Ransomware WannaCry* yang terdeteksi di dalam jaringan SMK Negeri 1 Palembang yang akan digunakan pada proses pendeteksian menggunakan DPI.

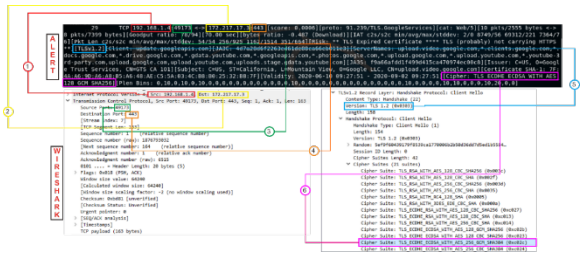
Tabel 2. Pola Serangan *Ransomware WannaCry*

Ransom Flow	Pola *Ransomware*	
	TLSv	***Payload***
Ransom 1	1.2	.google.com, .android.com, .appengine.com
Ransom 2	1.2	.bdn.com, .cloud.google.com, crowdsource.google.com,
Ransom 3	1.2	.g.co, gcp.gvt2.com, .gcpcpdn.gvt1.com, ggpht.cn, gkecnapps.cn
Ransom 4	1.2	.google-analitics.com, .google.ca, .google.cl, .google.co.in
Ransom 5	1.2	.google.co.jp, .youtube.com, .gstatic.cn, .youtube-nocookie.com
Ransom 6	1.2	.google.de, .googlevideo.com, .gstatic.com, .google.com.mx, .google.com.tr
Ransom 7	1.2	.google.cocnapps.cn, .google.commerce.com, .yt.be, .ytimg.com.

6. Pengidentifikasian TLSv pada *Client Hello*

Proses Identifikasian JA3C yang berupa observasi lanjutan dari pola serangan dari *Ransomware WannaCry*. Dengan memvalidasi protokol yang digunakan dalam dataset, yang berisikan konten serangan berupa protokol TCP, IP, Port dan TLSv pada Client. *Handshake* yang disetujui oleh Client terhadap server dengan memverifikasi Cipher yang digunakan. Pada Gambar 3.5 adalah protokol, TLSv dan *Cipher* yang digunakan dalam serangan *Ransowmware WannaCry* saat melakukan *handshake* terhadap *Server Hello*.

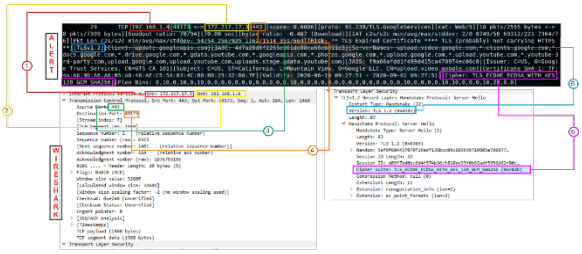
DOI: https://doi.org/10.31004/ijmst.v1i2.142



Gambar 3.5. Validasi TLSv dan *Cipher* pada *Client Hello*

7. Pengidentifikasian TLSv pada *Server Hello*

Proses Identifikasi informasi yang akan diberikan dari Server ke Client, yang dimana TLSv yang telah disepakati antara Server dan Client dengan *Cipher* yang sama. Proses validasi yang dilakukan adalah untuk mencari JA3S *Fingerprint* dengan kecocokan *raw data* dan hasil dari deteksi. JA3S adalah *Fingerprint* yang dibuat oleh Server dengan *Cipher* yang akan digunakan dalam serangan *Ransomware WannaCry*. Pada gambar 3.6 adalah validasi TLSv yang digunakan dalam *Server Hello* dan informasi berupa *cipher* yang digunakan *Ransomware WannaCry*.



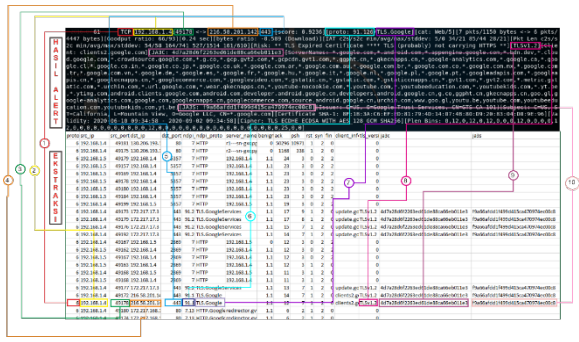
Gambar 3.6. Validasi *Cipher* dan TLSv pada Server Hello

8. Korelasi serangan *Ransomware Wannacry* dengan data hasil ekstraksi

Korelasi serangan antara *alert* yang dihasilkan *Deep Packet Inspection* dan hasil *Feature Extraction*, yang dimana terdapat beberapa informasi diantaranya pada client didapati pola *fingerprint Ransomware Wannacry* yang menggunakan JA3C yang sama dan pada client berbeda. Berikut adalah korelasi tabel 2. Dan gambar 3.7.

Tabel 2. Fingerprint Ransomware

Client	Pola *Ransomware* *JA3C*
update.googleapis.com	4d7a28d6f2263ed61de88ca66eb011e3
clients2.google.com	4d7a28d6f2263ed61de88ca66eb011e3



Gambar 3.7. Informasi yang diperoleh dari pendeteksian DPI

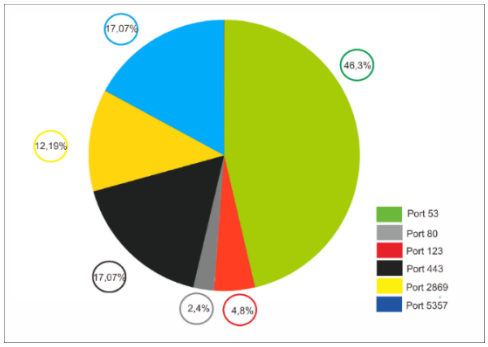
- Pada nomor 1 menjelaskan protokol yang digunakan yaitu TCP.
- Pada nomor 2 menunjukkan *IP Source Address* yang digunakan Client.
- Pada nomor 3 menunjukkan *Port Source* yang digunakan Client untuk *Request* informasi dengan mengirim beberapa *Cipher* yang akan disetujui.
- Pada nomor 4 menunjukkan *IP Destination Address* yang digunakan pada Server.
- Pada nomor 5 menunjukkan *Port Destination* yang digunakan Server untuk mengirim informasi yang telah disetujui oleh *Cipher* yang digunakan.
- Pada nomor 6 adalah protokol yang digunakan pada nDPI.
- Pada nomor 7 adalah nama protokol *Deep Packet Inspection*.
- Pada nomor 8 adalah TLSv 1.2 yang digunakan untuk *handshake* antara *Client Hello* dan *Server Hello*.
- Pada nomor 9 adalah JA3C yang berupa *Fingerprint* dengan memvalidasi keamanan dari TLSv dan *Cipher* yang digunakan.
- Pada nomor 10 adalah JA3S yang dibuat server dari TLSv dan *Cipher* yang disepakati dengan client

9. Hasil Diagram yang memvisualisasikan serangan *Ransomware Wannacry*

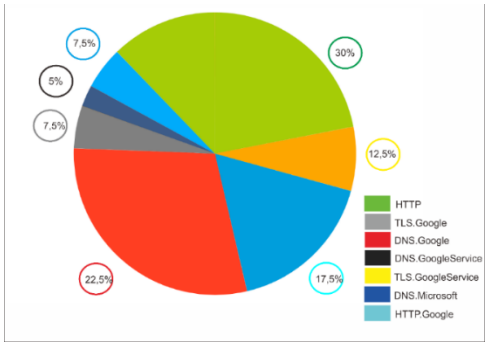
Hasil diagram visual dari proses klasifikasi atribut yang terdapat pada jaringan SMK Negeri 1 Palembang. Atribut yang didapat saat proses klasifikasi berupa *destionation port* dan *protocol name* pada dataset *RansomX*. Pada data yang telah didapat, ada beberapa serangan yang tidak menggunakan TLS dan hanya menggunakan *port* tujuan berupa *alert*. *Alert* inilah yang diambil

DOI: https://doi.org/10.31004/ijmst.v1i2.142

sebagai sampel data untuk menghitung berapa banyak serangan yang terjadi. Ini dapat membuktikan adanya paket serangan dengan nilai *benign* pada paket tersebut. Dengan data ini, maka dapat diklasifikasi menjadi bentuk diagram dengan menggunakan *open-source tool,* yang merujuk pada metode *clustering* yang akan mendapatkan hasil visual yang lebih konsisten.



Gambar 3.8. Klasifikasi *Destination Port* terhadap *benign score*



Gambar 3.9. Klasifikasi nama server yang diakses terhadap *benign score.*

4. Kesimpulan

Deep Packet Inspection adalah cara pendeteksian serangan *Ransomware* dengan menerapkan pada sistem keamanan SMK Negeri 1 Palembang. *Snort* dapat membantu dalam sistem pendeteksian dengan bantuan *Deep Packet Inspection* untuk mendeteksi serangan *Ransomware WannaCry*, dengan memvalidasi keamanan TLSv dan penggantian kunci *Cipher.* Dalam mendapatkan *Fingerprint Deep Packet Inspection* menggunakan metode *String Matching* pada sistem Snort dan dapat memvalidasikan TLSv yang digunakan *Ransomware WannaCry*, pada saat proses *handshake* yang dilakukan *Client Hello* dan *Server Hello.* Saat proses *Handshake* berlangsung *Deep Packet Inspection* menghasilkan JA3 sebagai bukti *Fingerprint.* Hasil deteksi yang diperoleh dari *Deep Packet Inspection* akan mendapatkan pola *Fingerprint* dari hasil validasi keamanan TLSv dan *Cipher* yang digunakan. Penelitian selanjutnya, dapat menerapkan pendeteksian secara *real-time* menggunakan plot yang lainnya. Menerapkan algoritma *clustering* lain dalam menentukan titik puncak serangan paket *Ransomware WannaCry*. Penelitian tahap selanjutnya dapat berupa *Intrusion Detection System* dengan bantuan snort dalam penerapan *String Matching* dan dapat memblokir serangan yang terdeteksi.

Reference

Al-Hisnawi, M., & Ahmadi, M. (2017). Deep packet inspection using Cuckoo filter. *2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT 2017*, *October 2019*, 197–202. https://doi.org/10.1109/NTICT.2017.7976111

Cheng, R., & Watson, G. (2018). *D 2 PI : Identifying Malware through Deep Packet Inspection with Deep Learning*.

Ferdiansyah. (2018). Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware. *JUSIFO (Jurnal Sistem Informasi)*, *2*(1), 44–59. http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf

Grant, L., & Parkinson, S. (2018). *Identifying File Interaction Patterns in Ransomware Behaviour*. *September*, 317–335. https://doi.org/10.1007/978-3-319-92624-7_14

Jatti, S. A. V., & Kishor Sontif, V. J. K. (2019). Intrusion detection systems. *International Journal of Recent Technology and Engineering*, *8*(2 Special Issue 11), 3976–3983. https://doi.org/10.35940/ijrte.B1540.0982S1119

Kiru, M. U., & Jantan, A. (2020). Ransomware Evolution: Solving Ransomware Attack Challenges. *The Evolution of Business in the Cyber Age*, *January*, 193–229. https://doi.org/10.1201/9780429276484-9

Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017). PayBreak : Defense against cryptographic ransomware. *ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security*, 599–611. https://doi.org/10.1145/3052973.3053035

O.Imaji, A. (2019). *Ransomware Attacks : Critical Analysis , Threats , and Prevention methods*. *March*, 1–32.

Rodrigues, G. A. P., de Oliveira Albuquerque, R., de Deus, F. E. G., de Sousa, R. T., de Oliveira Júnior, G. A., Villalba, L. J. G., & Kim, T. H. (2017). Cybersecurity and network forensics: Analysis of malicious traffic towards a honeynet with deep packet inspection. *Applied Sciences (Switzerland)*, *7*(10), 1–29. https://doi.org/10.3390/app7101082

DOI: https://doi.org/10.31004/ijmst.v1i2.142

Saad Hafeez B.Eng., T. I. U. of B., & A. (2017). Deep Packet Inspection using Snort. *Deep Packet Inspection Using Snort*, 24. http://on-demand.gputechconf.com/gtc/2017/presentation/s7468-wenji-wu-network-traffic-analysis-using-gpus.pdf

Salim, T., Valianta, S. A., & Stiawan, D. (2016). *Klasifikasi Trafik Terenkripsi Menggunakan Metode Deep Packet Inspection (Dpi)*. *2*(1), 424–429. http://ars.ilkom.unsri.ac.id

Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, *32*, 200892. https://doi.org/10.1016/j.fsidi.2019.200892

Velea, R., & Margarit, L. (2017). *Network Traffic Anomaly Detection Using Shallow Packet Inspection and Parallel K-means Data Clustering*. *December*. https://doi.org/10.24846/v26i4y201702

Winanto, E. A., Heryanto, A., & Stiawan, D. (2016). Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means. *Annual Research Seminar 2016*, *2*(1), 359–362.

Xu, C., Chen, S., Su, J., Yiu, S. M., & Hui, L. C. K. (2016). A Survey on Regular Expression Matching for Deep Packet Inspection: Applications, Algorithms, and Hardware Platforms. *IEEE Communications Surveys and Tutorials*, *18*(4), 2991–3029. https://doi.org/10.1109/COMST.2016.2566669

DOI: https://doi.org/10.31004/ijmst.v1i2.142