KOMPUTASI: Jurnal Ilmiah Ilmu Komputer dan Matematika
Vol.18, No.2, Juli 2021, Hal. 62 – 68
P-ISSN: 1693-7554, E-ISSN: 2654-3990
https://journal.unpak.ac.id/index.php/komputasi

IMPLEMENTASI ALGORITMA C.45 UNTUK KLASIFIKASI DETEKSI SERANGAN PADA PROTOKOL JARINGAN

Irma Anggraeni[1)], Siska Andriani [2)]
[1,2)] Program Studi lmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Pakuan, Bogor, Indonesia
Jalan Pakuan Po.Box 452 Bogor 16143 Jawa Barat Indonesia
Corresponding Author: irmairhamna@unpak.ac.id

Abstrak

Media internet telah menjadi bagian dari kehidupan manusia dalam kebutuhan komunikasi sebagai salah satu faktor kemajuan teknologi. Dengan semakin banyaknya penggunaan jaringan internet, keamanan menjadi aspek yang penting. Keamanan internet dilakukan untuk menghindari serangan terhadap jaringan tersebut. Untuk dapat mengetahui aktivitas penyerangan dalam suatu jaringan, dapat dilihat dari trafik pada jaringan tersebut. Anomali trafik merupakan kondisi tidak stabil yang terjadi pada suatu jaringan. Berdasarkan pendeteksian data trafik, dapat dilakukan analisis untuk mengetahui serangan-serangan yang terjadi pada jaringan. Data trafik jaringan akan diolah dengan klasifikasi dengan menggunakan Algoritma C.45.. Penelitian ini bertujuan untuk membuat analisis serangan dengan mengetahui anomali pada jaringan internet di prodi Ilmu Komputer. Dalam penelitian ini akan dilakukan beberapa tahapan yaitu pengumpulan data menggunakan wireshark, tahap preporessing, kemudian dilakukan proses klasifikasi. Setelah mendapatkan hasil klasifikasi, selanjutnya dilakukan analisis. Hasil klasifikasi didapatkan tingkat akurasi yaitu sebesar 93,67 %.

Kata kunci: *anomali; klasifikasi; trafik jaringan; wireshark*

Abstract

Internet media has become part of human life in communication needs as a factor for technological advancement. With more and more use of the internet network, security has become an important aspect. Internet security is done to avoid attacks on these networks. To be able to know attack activity in a network, it can be seen from the traffic on the network. Traffic anomaly is an unstable condition that occurs in a network. Based on the traffic data detection, analysis can be carried out to determine the attacks that have occurred on the network. Network traffic data will be processed by classification using C.45 algorithm. This study aims to make an analysis of attacks by knowing anomalies in the internet network in the Computer Science study program. In this research, several stages will be carried out, namely data collection using wireshark, preporessing stage, then the classification process is carried out. After obtaining the results of the classification, the analysis is then carried out. The result classification result obtained an accuracy 93,67%.

Keywords: *anomaly; classification; network trafific; wireshark*

1. Pendahuluan

Meningkatnya jumlah pengguna internet menyebabkan banyak sektor yang menggunakan jaringan internet untuk menyediakan layanan kepada para pelanggannya. Universitas merupakan salah satu *stake holder* yang banyak memanfaatkan internet sebagai salah satu fasilitas yang disediakan bagi *civitas*nya. Jaringan internet merupakan salah bagian dari infrastruktur kampus yang harus dapat dijaga [1]. Dengan akses internet yang baik dan handal tentunya mendukung untuk setiap akses perkuliahan, kegiatan akademik dan juga non akademik lainnya.

Dengan meningkatnya layanan akses internet yang baik maka sudah tentu juga semakin dibutuhkan untuk dapat menigkatkan kualitas layanan jaringan. Salah satunya yaitu dengan melakukan *monitoring* trafik jaringan untuk mengetahui dan mengenali penggunaan pada jaringan tersebut. Untuk mengetahui hal tersebut maka dilakukanlah *monitoring* trafik jaringan.

Monitoring jaringan adalah suatu proses pengumpulan data trafik untuk kemudian dilakukan analisis terhadap data-data tersebut dengan tujuan memaksimalkan seluruh sumber daya yang dimiliki jaringan [2]. *Monitoring* jaringan ini merupakan bagian yang cukup penting dari manajemen jaringan. Untuk melakukan monitoring jaringan dapat menggunakan *wireshark*. *Wireshark* merupakan sebuah aplikasi atau perangkat lunak yang digunakan untuk dapat melihat dan mengambil paket-paket jaringan kemudian menampilkan informasi di paket tersebut berdasarkan trafik jaringan. *Wireshark* menggunakan *Graphical User Interface* (GUI) yang bersifat *open source* [3]. Tools ini seringkali digunakan untuk menemukan masalah pada jaringan, pengembangan perangkat lunak dan protokol komunikasi, dan pendidikan. *Wireshark* bersifat *cross – platform* dan menggunakan pcap untuk meng-capture paket jaringan. *Wireshark* dapat berjalan pada hampir semua sistem operasi yang tersedia [4]. *Wireshark* dikenal merupakan suatu perangkat lunak berbasis GUI dalam protokol untuk jaringan lalu lintas. Dengan adanya *Wireshark* memungkinkan penggunanya untuk dapat mengetahui jalur paket dari jaringan komputer [5].

Pemantauan data trafik jaringan dapat dimaksudkan untuk mengetahui aktifitas yang terjadi selama koneksi masih berlangsung. Pemantauan aktifitas ini untuk mengetahui apakah terjadi serangan terhadap jaringan yang dapat menganggu. Secara umum serangan yang banyak terjadi pada jaringan internet adalah *Flooding/Denial Of Service* (DOS). DDOS sendiri merupakan jenis serangan pengiriman data skala besar yang sengaja dilakukan untuk mengurangi kinerja *router* dalam media transmisi data. *Flooding* lebih sering digunakan pada layer data link, dikirim dari *layer* fisik menuju data link dan pencatatan *mac address* pada kompresi data dilakukan secara terus menerus tanpa masuk ke *layer* berikutnya. Apabila terjadi *flooding* tentu sangat merugikan *bandwidth* dan juga *user* lain, oleh karena itu perlu adanya proses analisa agar mengetahui ciri-ciri dari flooding data jika terjadi pada sebuah router [6].

Berdasarkan hal tersebut diperlukan suatu analisis jaringan dengan menggunakan *wireshark* yang bertujuan untuk mengetahui trafik yang pada suatu jaringan komputer. Pada penelitian ini studi kasus yang akan digunakan yaitu di program studi Ilmu Komputer. Proses yang dilakukan dalam penetitian ini yaitu dengan menggunakan salah satu metode dari data mining yaitu klasifikasi. *Data mining* sendiri merupakan suatu proses dengan Teknik statistik, matematika, kecerdasan buatan, dan *machine learning* untuk dapat mengekstraksi dan mengidentifikasi suatu informasi dari sejumlah data yang sangat besar [7]. Salah satu metode data mining yaitu metode klasifikasi yang digunakan untuk menyatakan suatu data yang kelas atau kategorinya belum diketahui ke salah satu kelas yang telah didefinisikan sebelumnya berdasarkan atribut dari data yang dimiliki [8].

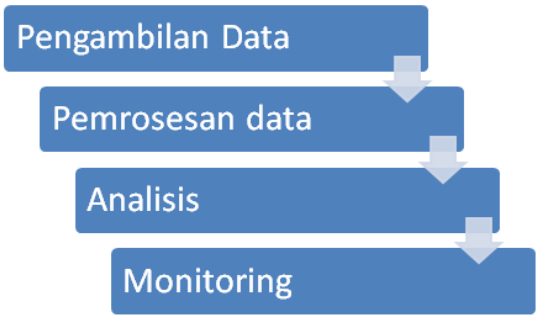
Klasifikasi paket jaringan yang melewati router pada yang tekoneksi dengan jaringan Internet merupakan sebuah proses yang penting untuk dilaksanakan dalam rangka mengurangi adanya resiko dari serangan DDoS [9]. Penelitian dilakukan oleh Khaerani dan handoko tahun 2015 yaitu membuat klasifikasi serangan dengan menggunakan *Intrusion Detection System* (IDS) menggunakan C 4.5 didapat nilai akurasi yaitu 98,67 % [10]. Selain itu Prathivi dan Vidia membuat analisis deteksi worm dan trojan dengan menggunakan algoritma C.45 dan *Naïve Bayes* untuk mengetahui serangan pada jaringan internet [11]. Tahun 2018, Harsono et al mengklasifikasian paket jaringan terhadap serangan DDoS dengan menggunkan metode *Intrusion Detection System* (IDS) cukup sulit untuk mendeteksinya sebagai artefak abnormal dan berakibat pada tingginya *falserate alert* yang dibangkitkan *oleh Intrusion Detection System* (IDS) [12].

Oleh karena itu pada penelitian melakukan proses analisis untuk mengetahui penggunaan internet melalui data jaringan yang terjadi pada jaringan internet di prodi Ilmu Komputer, untuk selanjutnya diproses klasifikasi menggunakan algoritma C.45.

2. Metode Penelitian

Metode penelitian yang digunakan yaitu terdiri dari beberapa tahapan seperti yang ditunjukan pada Gambar 1 dengan urutan proses yaitu:

a. Pengambilan data, yaitu proses pengambilan data trafik lalu lintas paket jaringan internet. Untuk mendeteksi adanya anomali data trafik maka dilakukan capture data jaringan melalui *wireshark*.
b. Praprosessing data, yaitu melakukan konversi file yang telah didapat kedalam format yang sesuai dengan *tools* Weka. Kemudian melakukan *filtering* data yaitu dengan menyesuaikan atribut apa saja yang akan dihitung dalam pada penelitian.
c. Analisis yaitu melakukan analisis kinerja klasifikasi dari paket data dari metode yang digunakan yaitu metiode klasifikasi menggunakan C.45 sehungga hasil deteksi anomali trafik didapatkan.
d. *Monitoring* yaitu melakukan *monitoring* hasil analisis yang telah dilakukan pada jaringan.

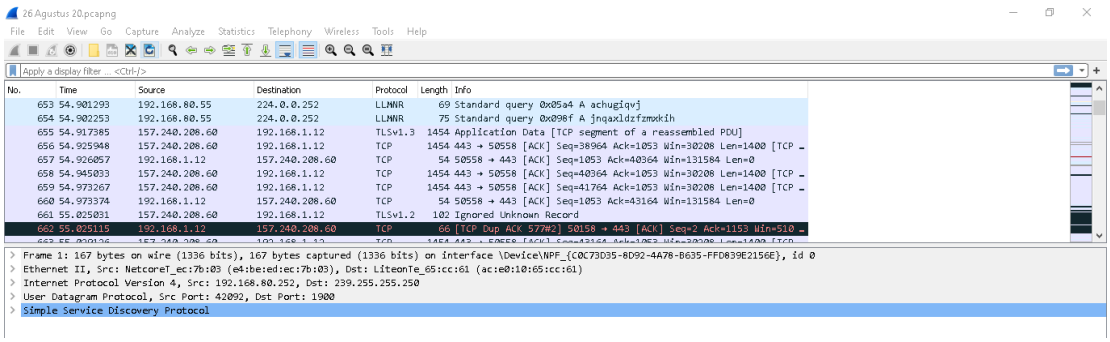


Gambar 1. Tahapan Penelitian

Algoritma C.45 ini merupakan pengembangan dari ID3 sehingga memiliki prinsip dasar yang sama antara C.45 dan ID3 [13]. Algoritma ini merupakan algoritma yang digunakan dalam pembentukan keputusan dalam bentuk pohon [14]. Algoritma ini merupak sutu algoritma yang dapat membuat pohon keputusan berdasarkan pemilihan atribut yang mempunyai prioritas tertinggi atau juga memiliki nilai *gain* tertinggi berdasarkan nilai *entropy* suatu atribut [15] Selanjutnya secara berulang-cabang pohon diperluas sehingga seluruh pohon terbentuk. Terdapat empat langkah dalam proses pembuatan pohon keputusan pada algoritma C4.5, yaitu:
a. Memilih atribut sebagai akar.
b. Membuat cabang untuk masing-masing nilai.
c. Membagi setiap kasus dalam cabang.
d. Mengulangi proses dalam setiap cabang sehingga semua kasus dalam cabang memiliki kelas yang sama untuk selanjutnya dilakukan perhitungan untuk mencari nilai entropy dan gain.

3. Hasil dan Pembahasan

Tahap pengambilan data dilakukan dengan mengcapture data pada jaringan wireless pada Prodi ilmu komputer. Menggunakan *software wireshark* untuk meng*capture* trafik yang melewati jaringan. Setelah mengkoneksikan ke *WiFi* Prodi maka selanjutnya menjalakan *wireshark* selama beberapa waktu untuk mengetahui data jaringan. Data hasil *monitoring* jaringan bisa didapatkan seperti pada Gambar 2 yang dapat melihat kondisi dari paket data yang telah direkam pada *software wireshark*.

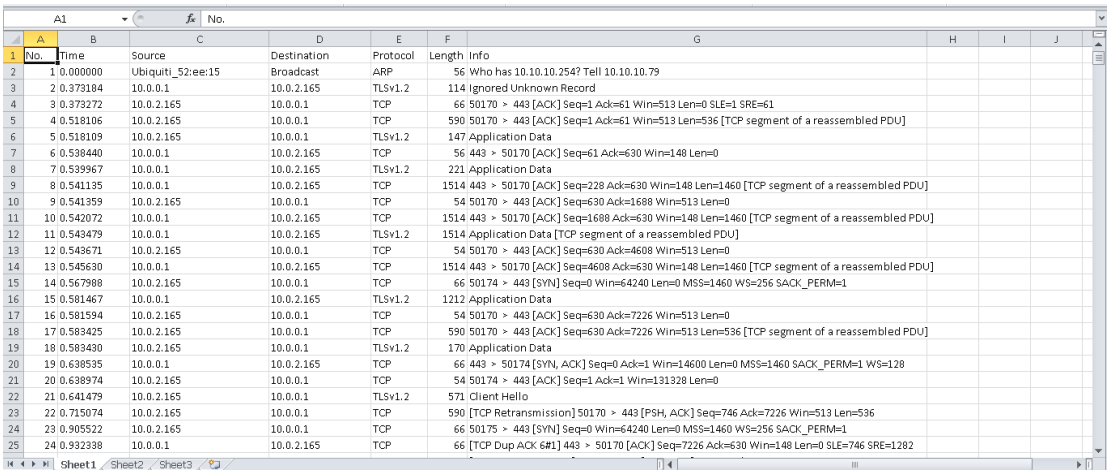


Gambar 2. *Capture* Trafik Jaringan

Data dari *wireshark* akan menampilkan kondisi paket data yang melewati interface yang telah dipilih. Data yang dapat ditampilkan yaitu adalah nomor yang merupakan nomor paket (no), waktu respon paket diterima (*time*), ip *address* asal (*source*), ip *address* tujuan (*destination*), *protocol* yang digunakan (*protocol*), panjang *frame* paket (*length*), serta info. Data inilah yang akan dipakai untuk proses analisa selanjutnya.

3.1 Pemrosesan Data

Pengambilan data trafik pada jaringan wireshark menghasilkan rekaman data dengan jumlah ribuan dengan atribut yaitu *Number*, *time*, *source*, *length*, protokol, *destination* dan info. Dengan jumlah data yang banyak dan bervariasi maka dibutuhkan proses selanjutnya yaitu *filtering* data. Data *filtering* merupakan pemilihan atribut data yang akan digunakan sebagai proses perhitungan klasifikasi. Pada penelitian ini atribut yang digunakan adalah lima atribut yaitu *time*, *source*, *length*, protokol, *destination*. Hasil *capturing* data *traffic* berupa data mentah diproses dan difilter menggunakan *Tool* Weka. Setelah data hasil *capture* pada *wireshark* didapatkan dseperti pada Gambar 3, maka data tersebut di simpan dalam format.csv.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Ubiquiti_52:ee:15	Broadcast	ARP	56	Who has 10.10.10.254? Tell 10.10.10.79
2	0.373184	10.0.0.1	10.0.2.165	TLSv1.2	114	Ignored Unknown Record
3	0.373272	10.0.2.165	10.0.0.1	TCP	66	50170 > 443 [ACK] Seq=1 Ack=61 Win=513 Len=0 SLE=1 SRE=61
4	0.518106	10.0.2.165	10.0.0.1	TCP	590	50170 > 443 [ACK] Seq=1 Ack=61 Win=513 Len=536 [TCP segment of a reassembled PDU]
5	0.518109	10.0.2.165	10.0.0.1	TLSv1.2	147	Application Data
6	0.538440	10.0.0.1	10.0.2.165	TCP	56	443 > 50170 [ACK] Seq=61 Ack=630 Win=148 Len=0
7	0.539967	10.0.0.1	10.0.2.165	TLSv1.2	221	Application Data
8	0.541135	10.0.0.1	10.0.2.165	TCP	1514	443 > 50170 [ACK] Seq=228 Ack=630 Win=148 Len=1460 [TCP segment of a reassembled PDU]
9	0.541359	10.0.2.165	10.0.0.1	TCP	54	50170 > 443 [ACK] Seq=630 Ack=1688 Win=513 Len=0
10	0.542072	10.0.0.1	10.0.2.165	TCP	1514	443 > 50170 [ACK] Seq=1688 Ack=630 Win=148 Len=1460 [TCP segment of a reassembled PDU]
11	0.543479	10.0.0.1	10.0.2.165	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
12	0.543671	10.0.2.165	10.0.0.1	TCP	54	50170 > 443 [ACK] Seq=630 Ack=4608 Win=513 Len=0
13	0.545630	10.0.0.1	10.0.2.165	TCP	1514	443 > 50170 [ACK] Seq=4608 Ack=630 Win=148 Len=1460 [TCP segment of a reassembled PDU]
14	0.567988	10.0.2.165	10.0.0.1	TCP	66	50174 > 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	0.581467	10.0.0.1	10.0.2.165	TLSv1.2	1212	Application Data
16	0.581594	10.0.2.165	10.0.0.1	TCP	54	50170 > 443 [ACK] Seq=630 Ack=7226 Win=513 Len=0
17	0.583425	10.0.2.165	10.0.0.1	TCP	590	50170 > 443 [ACK] Seq=630 Ack=7226 Win=513 Len=536 [TCP segment of a reassembled PDU]
18	0.583430	10.0.2.165	10.0.0.1	TLSv1.2	170	Application Data
19	0.638535	10.0.0.1	10.0.2.165	TCP	66	443 > 50174 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
20	0.638974	10.0.2.165	10.0.0.1	TCP	54	50174 > 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
21	0.641479	10.0.2.165	10.0.0.1	TLSv1.2	571	Client Hello
22	0.715074	10.0.2.165	10.0.0.1	TCP	590	[TCP Retransmission] 50170 > 443 [PSH, ACK] Seq=746 Ack=7226 Win=513 Len=536
23	0.905522	10.0.2.165	10.0.0.1	TCP	66	50175 > 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	0.932338	10.0.0.1	10.0.2.165	TCP	66	[TCP Dup ACK 6#1] 443 > 50170 [ACK] Seq=7226 Ack=630 Win=148 Len=0 SLE=746 SRE=1282

Gambar 3. Data *Filtering* dalam format .csv

Sehingga hasil *filtering* data telah dibuat dalam format .csv maka selanjutnya data akan diproses dengan menggunakan *software* Weka. Untuk memproses data tersebut maka harus dirubah dalam bentuk format .arff. Mengubah data menjadi .arff dengan memasukan data ke dalam Weka seperti hasil pada Gambar 4 yang sudah berubah dalam bentuk format .arv sehingga bisa dilakukan proses klasifikasi selanjutnya.

ARFF-Viewer - D:\hibah LPPm\17 okt 2808.csv.arff

File Edit View

17 okt 2808.csv.arff

Relation: 17 okt 2808

No.	1: No Numeric	2: Time String	3: Source Nominal	4: Destination Nominal	5: Protocol Nominal	6: **Length** Numeric
1	1.0	0.00...	Ubiqui...	Broadcast	ARP	56.0
2	2.0	0.37...	10.0.0.1	10.0.2.165	TLSv1.2	114.0
3	3.0	0.37...	10.0.2....	10.0.0.1	TCP	66.0
4	4.0	0.51...	10.0.2....	10.0.0.1	TCP	590.0
5	5.0	0.51...	10.0.2....	10.0.0.1	TLSv1.2	147.0
6	6.0	0.53...	10.0.0.1	10.0.2.165	TCP	56.0
7	7.0	0.53...	10.0.0.1	10.0.2.165	TLSv1.2	221.0
8	8.0	0.54...	10.0.0.1	10.0.2.165	TCP	1514.0
9	9.0	0.54...	10.0.2....	10.0.0.1	TCP	54.0
10	10.0	0.54...	10.0.0.1	10.0.2.165	TCP	1514.0
11	11.0	0.54...	10.0.0.1	10.0.2.165	TLSv1.2	1514.0
12	12.0	0.54...	10.0.2....	10.0.0.1	TCP	54.0
13	13.0	0.54...	10.0.0.1	10.0.2.165	TCP	1514.0
14	14.0	0.56...	10.0.2....	10.0.0.1	TCP	66.0
15	15.0	0.58...	10.0.0.1	10.0.2.165	TLSv1.2	1212.0
16	16.0	0.58...	10.0.2....	10.0.0.1	TCP	54.0
17	17.0	0.58...	10.0.2....	10.0.0.1	TCP	590.0
18	18.0	0.58...	10.0.2....	10.0.0.1	TLSv1.2	170.0
19	19.0	0.63...	10.0.0.1	10.0.2.165	TCP	66.0
20	20.0	0.63...	10.0.2....	10.0.0.1	TCP	54.0
21	21.0	0.64...	10.0.2....	10.0.0.1	TLSv1.2	571.0
22	22.0	0.71...	10.0.2....	10.0.0.1	TCP	590.0
23	23.0	0.90...	10.0.2....	10.0.0.1	TCP	66.0
24	24.0	0.93...	10.0.0.1	10.0.2.165	TCP	66.0
25	25.0	0.94...	10.0.2....	10.0.0.1	TCP	571.0
26	26.0	0.97...	10.0.0.1	10.0.2.165	TCP	56.0
27	27.0	0.98...	10.0.0.1	10.0.2.165	TCP	66.0
28	28.0	0.98...	10.0.2....	10.0.0.1	TCP	54.0
29	29.0	0.98...	10.0.2....	10.0.0.1	TLSv1.2	571.0
30	30.0	1.01...	Ubiqui...	Broadcast	ARP	56.0
31	31.0	1.01...	10.0.2....	10.0.0.1	TCP	590.0
32	32.0	1.03...	10.0.0.1	10.0.2.165	TLSv1.2	1514.0
33	33.0	1.03...	10.0.0.1	10.0.2.165	TLSv1.2	488.0
34	34.0	1.03...	10.0.2....	10.0.0.1	TCP	54.0
35	35.0	1.04...	0.0.0.0	255.255.25...	DHCP	344.0
36	36.0	1.05...	10.0.2....	10.0.0.1	TLSv1.2	180.0
37	37.0	1.07...	10.0.2....	10.0.0.1	TCP	66.0

Gambar 4. Data format arff

3.2 Analisis

Setelah proses pengambilan dan pemrosesan data langkah selanjutnya yaitu melakukan analisis dari data trafik tersebut. Analisis yang dilakukan yaitu dengan membaca hasil dari paket data yang telah diambil melalui *software wireshark*, mulai dari setiap atribut yang ada pada paket data tersebut.

Selanjutnya pada data yang didapatkan pada jaringan prodi ilmu komputer ini dilakukan perbandingan dengan menggunakan algoritma yang lainnya yaitu algoritma C.45. berikut adalah gambar 5 hasil klasifikasi menggunakan algoritma tersebut

```
Correctly Classified Instances        1762               93.6736 %
Incorrectly Classified Instances       119                6.3264 %
Kappa statistic                          0.912
Mean absolute error                      0.0095
Root mean squared error                  0.0736
Relative absolute error                 12.3995 %
Root relative squared error             37.6498 %
Total Number of Instances             1881
```

Gambar 5. Akurasi algoritma C.45

```
=== Confusion Matrix ===

   a   b   c   d   e   f   g   h   i   j   k   l   m   n   o   p   q   r   s   <-- classified as
 339   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0 |   a = ARP
   0 111  64   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0 |   b = TLSv1.2
   0  22 856   0   0   4   0   2   0   0   0   2   0   0   4   0   0   0   0 |   c = TCP
   0   0   0  80   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0 |   d = DHCP
   0   0   0   0  35   0   0   0   0   0   0   0   0   0   0   0   0   0   0 |   e = DNS
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0 |   f = AJP13
   0   0   0   0   0   0  80   0   0   0   0   0   0   0   0   0   0   0   0 |   g = MDNS
   0   6   7   0   0   0   0  26   0   0   0   0   0   0   1   0   0   0   0 |   h = HTTP
   0   0   0   0   0   0   0   0  55   0   0   0   0   0   0   0   0   0   0 |   i = NBNS
   0   0   0   0   0   0   0   0   0  47   0   0   0   0   0   0   0   0   0 |   j = LLMNR
   0   0   0   0   0   0   0   0   0   0  15   0   0   0   0   0   0   0   0 |   k = SSDP
   0   0   0   0   0   0   0   0   0   0   0  89   0   0   2   0   0   0   0 |   l = UDP
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0 |   m = IAPP
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0 |   n = BROWSER
   0   0   2   0   0   0   0   0   0   0   0   3   0   0  18   0   0   0   0 |   o = TLSv1.3
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   1   0   0   0 |   p = HTTP/XML
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   2   0   0 |   q = ICMPv6
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   4   0 |   r = IGMPv3
   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   4 |   s = DHCPv6
```

Gambar 6. *confusion matrix*

Dalam klasifikasi menggunakan algoritma C.45 ini maka, dilakukan penentuan hasil akurasi yang paling tinggi dengan melakukan pembagian data training dan data uji yaitu pengujian dengan 75 % data training dan 25 % data uji didaptkan hasil akurasi yaitu sebesar 93,59 %, kemudian pembagian 80% data latih dan 20% data uji didapat hasil kaurasi yaitu sebesar 93,62 %. Berdasarkan hasil penelitian dengan menggunakan Algoritma C.45 ternyata dapat diketahui bahwa hasil klasifikasi dengan nilai akurasi yang paling tinggi yaitu menggunakan algoritma C.45 dengan pembagian data sebesar 80% sebagai data training dan 20 % data Uji. Pada Gambar 6 ditunjukan juga hasil *confusion* matriks hasil klasifikasi menggunakan C.45.

4. Kesimpulan

Berdasarkan hasil penelitian didapatkan bahwa dari pengambilan data pada tanggal 28 Agustus 2020, yaitu sebanyak 125543 data terdapat deteksi *worm trojan* yaitu sebanyak 28 paket data. Hasil analisis klasifikasi data jaringan dengan menggunakan menggunakan algoritma C.45 didapatkan nilai akurasi yaitu 93,62 %. Penelitian ini melakukan klasifikasi berdasarkan protocol jaringan yang digunakan, selanjutnya dapat mengukur parameter lain dalam jaringan dan menggunakan algoritma *data mining* yang lainnya.

Referensi

[1] Networks., 2016. World Wide Infrastrucure Security Report

[2] Paramita. B, Leon A.A, Edi S. N. 2016. Analisis Monitoring Traffic Jaringan Pada Pt Kai Divisi Regional Iii Sumsel. Sentikom

[3] Sihombing, R.O.L, Zulfin,M . 2013. Analisis Kinerja Trafik Web Browser Dengan Wireshark Network Protocol Analyzer Pada Sistem Client-Server. Singuda Ensikom Vol. 2 No. 3/Juni 2013.

[4] Wulandari, R. 2016. Analisis Qos (Quality Of Service) Pada Jaringan Internet (Studi Kasus : Upt Loka Uji Teknik Penambangan Jampang Kulon – Lipi. Jurnal Teknik Informatika dan Sistem Informasi,vol. 2,no. 2,pp. 162-172.

[5] Sujana, A.P. 2014. Perangkat Pendukung Forensik Lalu Lintas Jaringan. Jurnal Teknik Komputer Unikom – Komputika – Volume 3, No.1 – 2014.

[6] Hendrawan, A.H. 2016. Analisis Serangan Flooding Data Pada Router Mikrotik. J u r n a l K r e a -T I F V o l: 0 4 N o : 1.

[7] Mujib R, Hadi S, dan M. Sarosa. 2013. Penerapan Data Mining Untuk Evaluasi Kinerja

Akademik Mahasiswa Menggunakan Algoritma Naive Bayes Classifier. Jurnal EECCIS Vol. 7, No. 1, Juni 2013

[8] Sunjana, 2010. Aplikasi Mining Data Mahasiswa dengan Metode Klasifikasi Decision Tree. Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010) ISSN: 1907-5022 Yogyakarta, 19 Juni 2010

[9] Diansyah, T,M. 2015. Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Menggunakan Wireshark. Jurnal TIMES , Vol. IV No 2 : 20-23 , 2015 ISSN : 2337 - 3601 .

[10] Khaerani, I dan Handoko, L.B. 2015. Implementasi Dan Analisa Hasil Data Mining Untuk Klasifikasi Serangan Pada Intrusion Detection System (Ids) Dengan Algoritma C4.5. Techno.COM, Vol. 14, No. 3, Agustus 2015: 181-188

[11] Prativhi, R dan Vensy, V. 2017. Analisa Pendeteksian Worm Dan Trojan Pada Jaringan Internet Universitas Semarang Menggunakan Metode Kalsifikasi Pada Data Mining C45 Dan Bayesian Network. JURNAL TRANSFORMATIKA, Volume 14, Nomor 2, Januari 2017.

[12] Harsono, Chambali, M. , Muhammad, A.W. 2018. Klasifikasi Paket Jaringan Berbasis Analisis Statistik dan Neural Network. Jurnal Informatika: Jurnal Pengembangan IT (JPIT), Vol.03, No.1, Januari 2018.

[13] Ika W. 2013. Jurnal Ilmiah INOVASI, Vol.13. No.2, Hal. 107-111, Mei-Agustus 2013, ISSN 1411-5549

[14] Purushottam, Saxena, K., & Sharma, R. 2016. Efficient Heart Disease Prediction System using Decision Tree. International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 15-16 May. 72-77. DOI: 10.1109/CCAA.2015.7148346

[15] Yogiek, I.K. 2018. Perbandingan Algoritma Naive Bayes Dan C.45 Dalam Klasifikasi Data Mining. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) Vol. 5, No. 4, September 2018, hlm. 455-464