DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics

Anton Yudhana[1]
Department of Electrical Engineering
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Imam Riadi[2]
Department of Information Systems
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Faizin Ridho[3]
Department of Informatics Engineering
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

***Abstract*—Distributed Denial of Service (DDoS) is a network security problem that continues to grow dynamically and has increased significantly to date. DDoS is a type of attack that is carried out by draining the available resources in the network by flooding the package with a significant intensity so that the system becomes overloaded and stops. This attack resulted in enormous losses for institutions and companies engaged in online services. Prolonged deductions and substantial recovery costs are additional losses for the company due to loss of integrity. The activities of damaging, disrupting, stealing data, and everything that is detrimental to the system owner on a computer network is an illegal act and can be imposed legally in court. Criminals can be punished based on the evidence found with the Forensics network mechanism. DDoS attack classification is based on network traffic activity using the neural network and naïve Bayes methods. Based on the experiments conducted, it was found that the results of accuracy in artificial neural networks were 95.23% and naïve Bayes were 99.9%. The experimental results show that the naïve Bayes method is better than the neural network. The results of the experiment and analysis can be used as evidence in the trial process.**

Keywords*—DDoS; IDS; neural network; naïve bayes; network forensics

I. Introduction

The increasing number of internet users has caused many sectors to use online systems to provide services to their clients. This online service is utilized by several sectors such as education, government, and E-Commerce. Vulnerability in online service systems has the potential to be attacked by hackers. Attacks on online services can occur at any time and need solutions to improve them. The attack that is often carried out by hackers is distributed denial of service (DDoS). Kaspersky labs[1] has issued a report on DDoS attacks using botnets that have occurred in the first quarter of 2018. Researcher Kaspersky notes that attacks are often aimed at countries China, the United States, and South Korea because servers located in the country have the most number of online services. Based on the Benchmark Cisco 2018 study of the Asia Pacific Security Capabilities[2], which states that Indonesia has the highest percentage in Southeast Asia by getting attack warnings with the amount of 250,000 - 500.00 per day.

Long-term embezzlement and substantial recovery costs are additional losses for the company due to loss of integrity[3]. The activities of damaging, disrupting, stealing data, and anything that is detrimental to the system owner on a computer network is an illegal act and can be imposed legally in court[4]. Criminals can be punished based on the evidence found with the Forensics network mechanism.

Attack detection is often carried out using the intrusion detection system (IDS)[5] by monitoring the network traffic that is passed. Investigators usually utilize a network monitoring system such as IDS for forensics purposes, where analysis is performed using IDS logs and attack notification systems. Intrusion Detection System (IDS) works by monitoring and warning of suspicious activities that occur on the network and immediately reported as a warning. Using an intrusion detection system is usually done based on a signature. This causes a lot of errors in detecting attacks due to changes in network traffic that have an impact on the high volume of warnings that continue to increase because the data traffic in the network is not stationary to produce and respond to warnings that occur[6]. This error occurs due to a lack of protocol[7] which results in the attacker being able to send attacks more easily with the Ping, Hping, or LOIC tools[8]. The legacy of the syn protocol in network traffic allows IDS to frequently detect attacks because DDoS is done using syn packages.

Signature-based detection systems and attack notifications[9] are not strong enough to serve as evidence in trials. A new approach mechanism is needed to analyze and test the accuracy of DDoS attacks that have been detected by the intrusion detection system (IDS) to strengthen the evidence. Network packet classification is one mechanism that can be done to detect DDoS. Machine learning techniques, by validating network data provided to classify with legitimate observations based on anomalies, can be used in the network forensic process[10]. DDoS attacks through computer networks, especially Local Area Networks (LANs) can be detected using multi-classification techniques, which is by combining data mining methods to get better accuracy[11]. Classification using the Neural Network method in analyzing DDoS attacks can provide 99.6% results based on Hidden Neural Network Variations[12]. The similar analysis was also carried out with the Naïve Bayes method[13] using the KDD99 data set to find the highest accuracy of 99.7837%.

Based on the background above, the research was carried out to determine the process of a new approach in detecting

and determining the accuracy of DDoS attacks for network forensic purposes. The study was carried out using a dataset of the Research Laboratory of the Master of Information Engineering of Ahmad Dahlan University (LRIS_MTIUAD). A new approach[14] in detecting DDoS attacks is expected to help develop the ability of Intrusion Detection System (IDS) to predict the presence of DDoS.

II. Basic Theory

A. Network Forensics

Network forensics[15][16] is the process of capturing, recording and analyzing network activities to find digital evidence of an attack or committed crime that carried out using a computer network so that the perpetrator can be prosecuted according to applicable law.

B. Artificial Neural Network

Artificial Neural Network[17] is a biologically inspired computing model consist of various processing elements (neurons). Neurons are connected to elements or weights that build the structure of neural networks. ANN has elements for processing information, namely transfer functions, weighted inputs, and output. ANN is composed of one layer or several layers of neurons as shown in Figure 1.

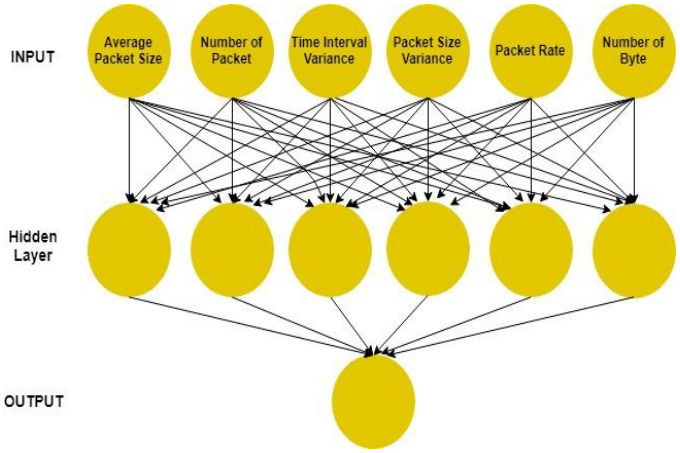

Fig. 1. Artificial Neural Networks

C. Naïve Bayes

Bayes method is used to calculate the probability of an event's occurrence based on the observed observation effect. The Naive Bayes method is a simple probabilistic-based prediction that rely on the application of the Bayes method with a sturdy independence assumption[11][18]. The equation for the Naive Bayes method is:

$$P(H|X) = \frac{P(X|H).\ P(H)}{P(X)} \quad (1)$$

Information:

X : Data with unknown classes

H : Hypothesis X data (a specific class)

P (H | X) : a probability of H hypothesis based on condition X (Posterior Probability)

P (H) : Probability of H Probability (Prior Probability)

P (X | H) : Probability of X based on the condition of hypothesis H

P (X) : Probability of X

III. Research Methodology

This study uses a classification method that consists of 4 stages as shown in Figure 2.

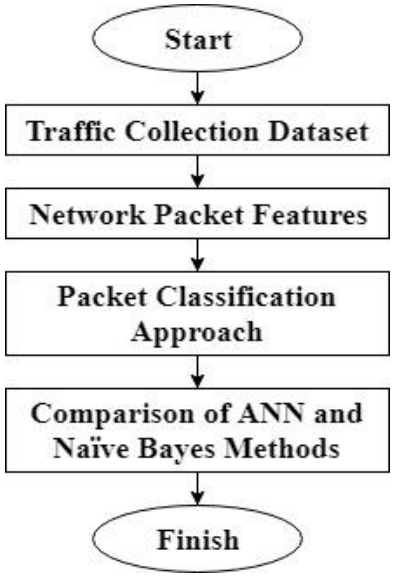

Fig. 2. Classification Method.

Figure 2 can be explained as follows:

A. Traffics Collection Dataset

Traffics Collection is a stage of generating normal datasets and attacks on the Ahmad Dahlan University Research Laboratory network (LRis-UAD) using the Wireshark monitoring application, then the information is stored in the .pcap format as in Figure 3.

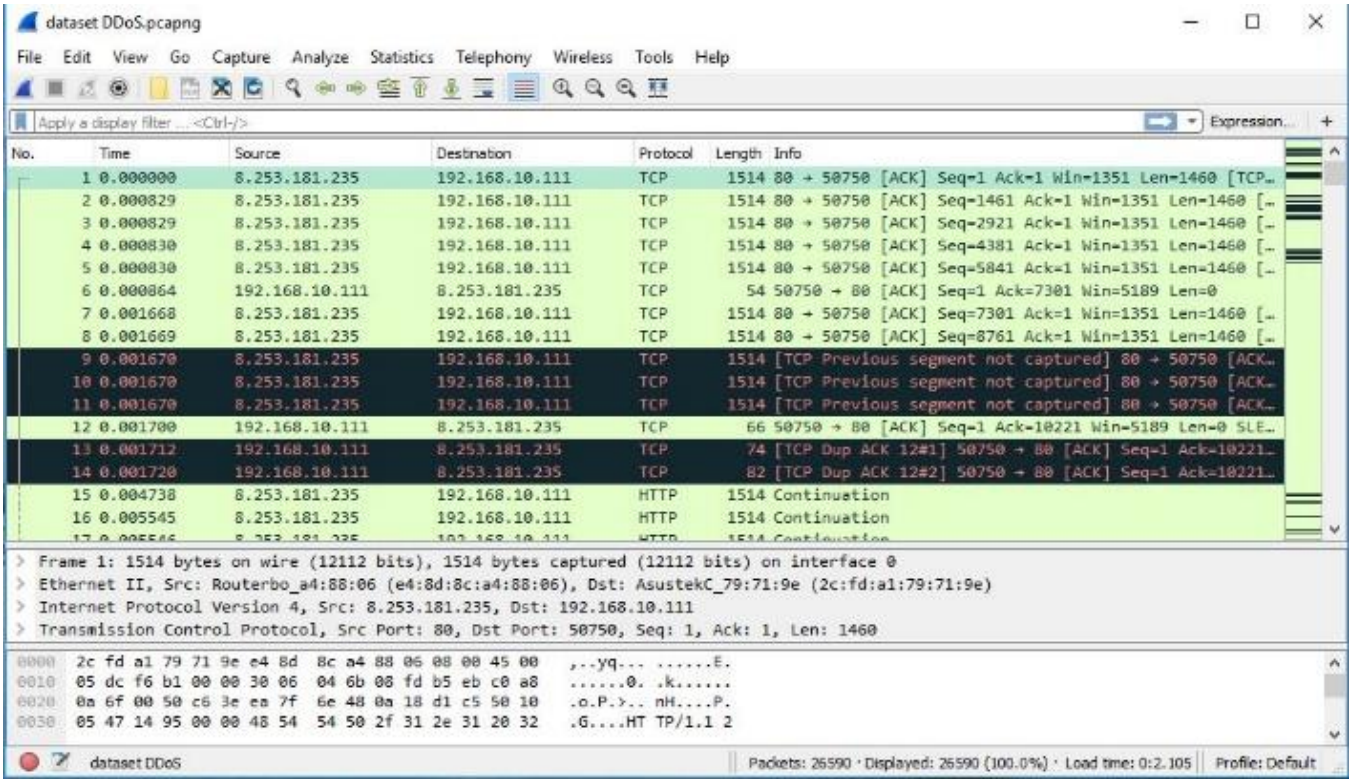

Fig. 3. Traffics Collection Dataset.

B. Network Packet Features

Network Packet Features are stages to extract network features in the dataset. The goal is to determine specific patterns in the data. In this case extraction program is carried out with six features using statistical methods. These features are:

a) Average value of network packet length in a predetermined time frame[12].

b) Value the total number of network packages in a predetermined time frame[12].

c) The value of the variance of the time lag variable for the arrival of the network package originating from a particular IP in a predetermined time frame. The value of the variance is generated from equation 2[12].

$$\text{Time Variation} = \sqrt{\frac{\sum(t_n - t)^2}{n}}$$

t_n = the time the package was received

t = average package time received

d) The variance value of the network packet length variable that originates from a particular IP in a predetermined time frame. The value of the variance is generated from equation 3[12][19].

$$\text{Packet size variance} = \sqrt{\frac{\sum(p_n - p)^2}{n}}$$

p_n = length of package received

p = the average length of the package is accepted

e) Package speed values in a predetermined time frame, calculated by equation 4[12].

$$\text{Package Speed} = np * \frac{1}{T.end - T.early}$$

f) Value the total number of data bits in a predetermined time frame.

C. Packet Classification Approach

1) Artificial neural networks: Classification process on artificial neural networks by applying hidden layers carried out by the steps as shown in Figure 4.

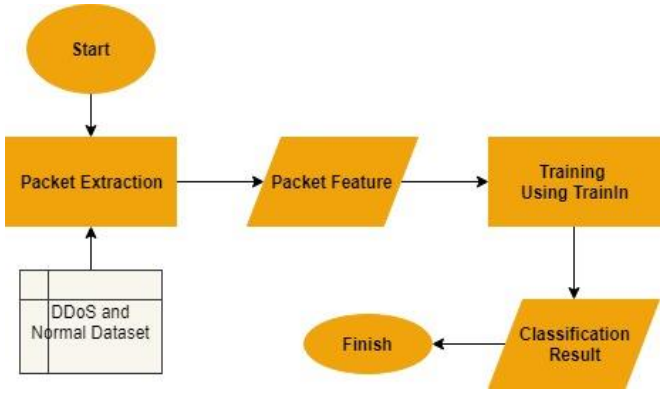

Fig. 4. Neural Network Process.

a) Take a normal dataset and DDoS dataset at the Ahmad Dahlan University Research Laboratory network.

b) Extract network packages using statistical methods to obtain network features, based on 6 inputs: average packet size, number of packages, variant time intervals, package size variants, packet levels, and number of bytes.

c) Use the Tansig, (Tangen Sigmoid), Purelin (Principal Components) and Trainlm (QuasiNewton), training function in Matlab.

d) Classification of classification results using accuracy, mean squared error (MSE), and iteration parameters.

2) Naïve Bayes method: The naïve Bayes classification process is carried out using the statistical method carried out in Figure 5.

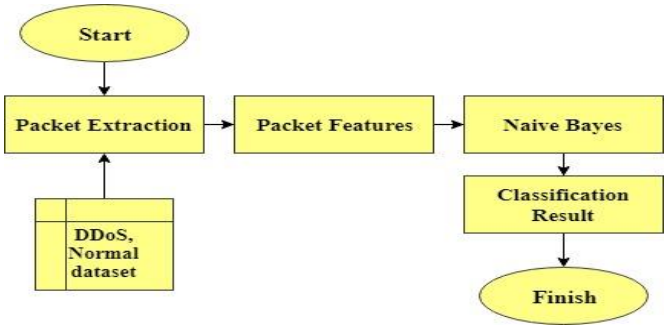

Fig. 5. Naïve Bayes Process.

a) Take a normal dataset and DDoS dataset at the Ahmad Dahlan University Research Laboratory network.

b) Extract network packages using statistical methods to obtain network features, namely the average packet size, number of packages, variant time intervals, package size variants, packet levels, and number of bytes.

c) Perform calculations by looking for standard deviation and threshold based on feature extraction package data.

d) The classification process for naïve Bayes using the Gaussian training phase was tested with test data to determine the success of the introduction of DDoS attacks as predictions.

D. Comparison of ANN and Naïve Bayes Methods

Comparison of artificial neural network and naïve Bayes methods is done to classify and test the best accuracy that can be used in the process of verification in the court. The use and comparison of methods can be carried out as a process of approach to network forensic analysis on DDoS attacks.

IV. Result and Discussion

A. Pre-Processing

Pre-processing data conducted by extracting normal and DDoS datasets with the format. pcap to be .csv so that the statistical calculation process can be performed. The extraction process can be presented in Figure 6.

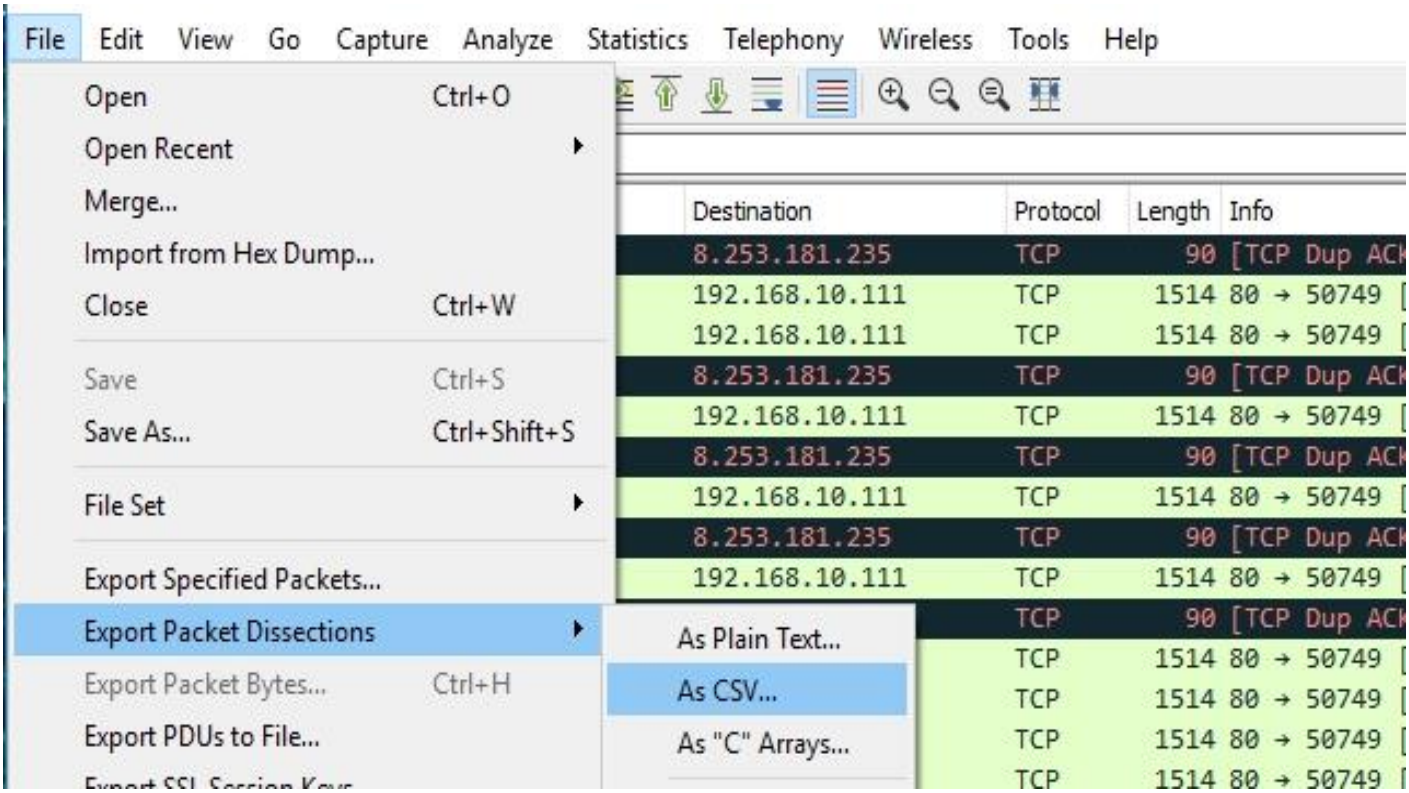

Fig. 6. Extracting .pcap Format Into .csv Format.

B. Packet Extraction

Packet extraction conducted by using 2014b Matlab environment that runs on Windows 10 64-bit. The training process on ANN and naïve Bayes was carried out using 70 DDoS data and 30 Normal Data. Testing process is conducted using 20 data logs on the intrusion detection system (IDS). Data processing is conducted by determining feature extraction based on statistical calculations[6][19]. The summation is conducted by using a fixed moving average window[20] with a duration of 3000 seconds and a 5-second pause with 6 inputs based on the average packet size, number of packages, variant time intervals, package size variants, packet levels, and number of bytes. The quantification process aims to characterize network activity characteristics within a span of time and facilitate the process of training and testing data classification with neural networks. Feature extraction results can be seen in Table 1.

TABLE I. FEATURE EXTRACTION USING STATISTIC

	Average packet size	**Number of packets**	**Time interval variance**	**Packet size variance**	**Packet rate**	**Number of bytes**
Normal	641561	2962	146844	685999	594251	190030
DDoS	553674	3199	142005	637087	778706	177120

Table 1 shows that the range of data values in the network features looks quite large. While the DDoS package after its feature extraction produces values that tend to be monotonous. It can be seen that the difference in data value on the feature extracted from the DDoS package looks quite small.

C. Training and Testing Process on Neural Networks

Training for each variation of artificial neural network architecture in this study is using the Tansig, (Tangen Sigmoid), Purelin (Principal Components) and Trainlm (Levenberg-Marquardt) functions. The purpose of a variety of training functions that provide the highest accuracy in recognizing normal traffic and attacks. Processing of the training process is done using the Matlab program.

The implementation of network package classification training from the method applied using the number of neurons (30-20-1) scheme with Epoch 100 (iteration) and with an MSE value of 0.001. Distribution of datasets for training, validation, and testing is done randomly to avoid bias in the sample pattern. The training process in the hidden layer is done using the sigmoid function. The basic parameters used in the training process are time = 100, function performance = mse, goal = 1e-6, maximum failure = 6, minimum gradient = 1.00e-7, 1.00e + 10. All variations of ANN are trained until the error performance function the mean square error (MSE) is less than 0.001. As presented in Figure 7.

The performance of neural networks after being trained is able to produce a regression value of R-test 0.99 which means that the connection weights between neurons in each layer of neural networks have been able to provide optimal results in recognizing input data patterns. The results of the regression value can be seen in Figure 8.

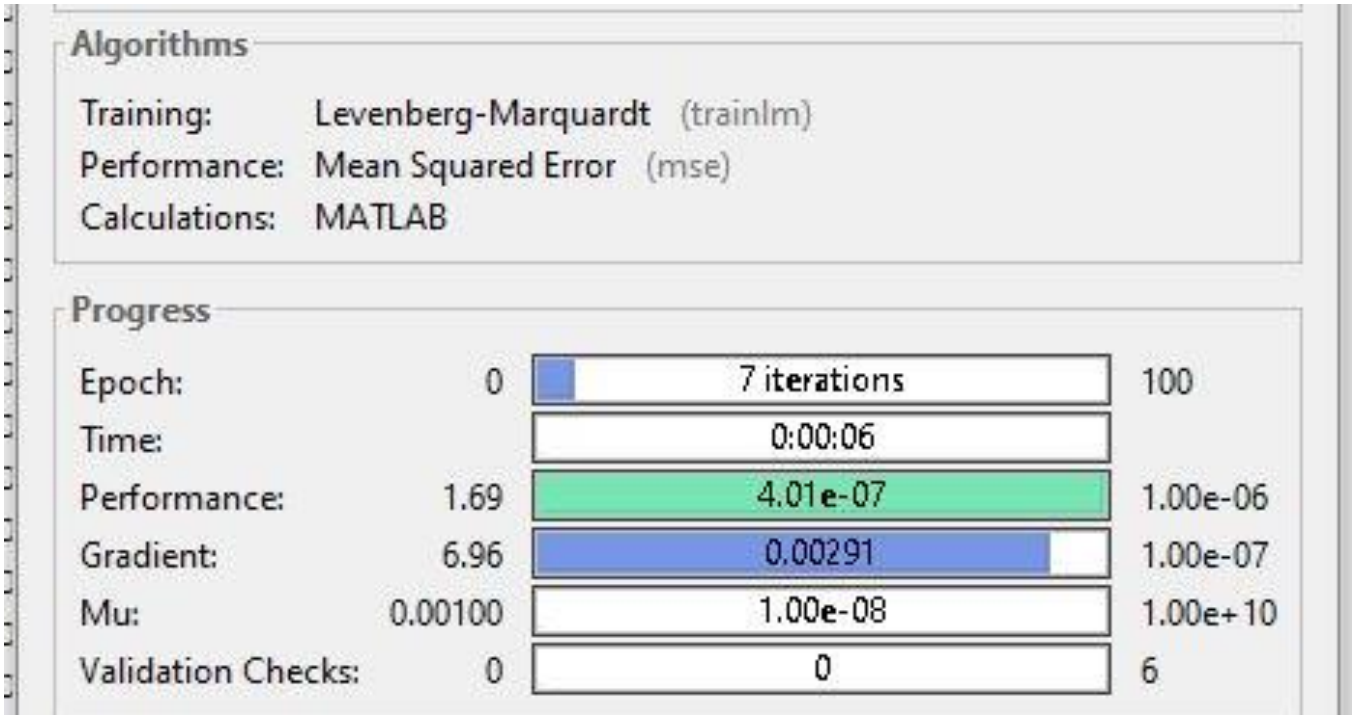

Fig. 7. Training Process on Neural Network.

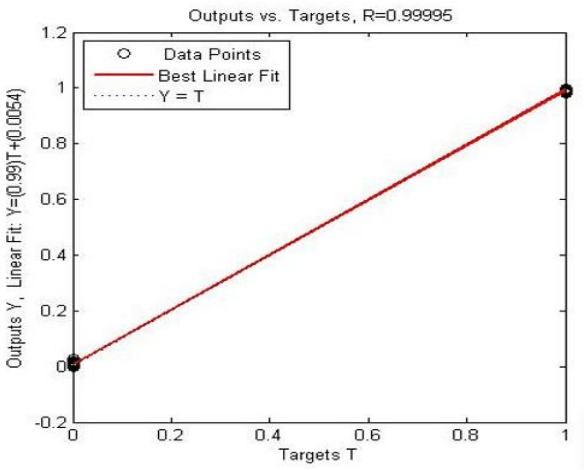

Fig. 8. Results of the Regression Value.

Testing on the neural network is carried out using 20 log data on the IDS to see the DDoS accuracy value. The results of the tests that have been conducted show that the logs stored on the IDS system are detected as DDoS attacks with an accuracy value of 95.23% as shown in Figure 9.

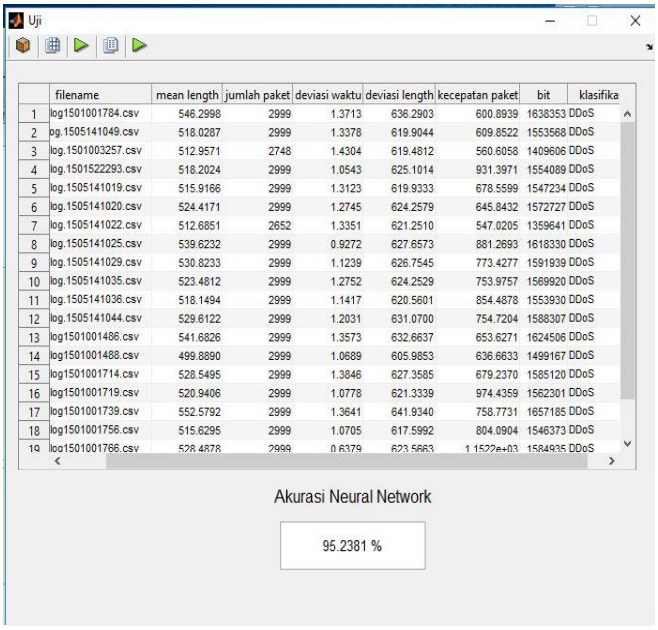

Fig. 9. Classification Results using Neural Network.

Figure 9. Shows that 20 IDS logs tested using artificial neural networks fall into the DDoS category.

D. Training and Testing Process using Naïve Bayes

The naïve Bayes extraction process is carried out by processing feature extraction on normal data and DDoS data using statistical calculations. Normal extraction and DDoS results are stored with file name *featureall* made as input data. Extraction results are processed by looking for probability values and standard deviations in DDoS data and normal data as shown in Figure 10. Data processing is done by loading feature all, where feature all contains the results of normal data extraction and DDoS data.

```
%% load feature
load featureall
% Train
%% prob
f=0;
j=0;
clast=featureall(:,end);
for k=1:size(clast,1)
   d=clast(k,:);
   if d==0
      f=f+1;
   else
      j=j+1;
   end
end
proba1=f/(f+j);
proba2=j/(f+j);
proba=[proba1,proba2];

%% mean & std | 0= Normal & 1= DDoS
m0=mean(featureall(1:5,1:end-1))
s0=std(featureall(1:5,1:end-1))
m1=mean(featureall(6:end,1:end-1))
s1=std(featureall(6:end,1:end-1))
```

Fig. 10. Probability Formulas and Standard Deviations.

The formula in Figure 10 shows the probability value in DDoS = 0.5232 and Normal = 0.4767 is found. Average values on DDoS and Normal can be seen in Table 2.

TABLE II. AVERAGE VALUE OF EXTRACTION PACKAGES

	Average packet size	**Number of packets**	**Time interval variance**	**Packet size variance**	**Packet rate**	**Number of bytes**
Normal	7,54541 E+14	1,6816E +14	1,02094 E+14	6,85827 E+14	3,43983 E+14	1,25262 E+14
DDoS	6,49411 E+14	2,30874 E+14	1,18789 E+14	6,54486 E+14	6,06509 E+14	1,38847 E+14

The results of the standard deviation values in Figure 10 are presented in Table 3.

TABLE III. STANDARD VALUE OF EXTRACTION PACKAGE DEVIATION

	Average packet size	**Number of packets**	**Time interval variance**	**Packet size variance**	**Packet rate**	**Number of bytes**
Normal	9,40058 E+14	1,06763 E+14	0.425 49	1,51057 E+14	2,15221 E+14	8,01087 E+14
DDoS	1,40532 E+14	1,07386 E+14	0.320 42	3,39475 E+14	6,92154 E+14	5,89783 E+14

The test is carried out using 20 log data on IDS that have been extracted using statistical formulas. Extraction results are stored with the *featureuji* file name as test data. The training and testing were carried out using the naïve Bayes Gaussian method[11] with a formula which can be seen in Figure 11.

```
load featureuji
%% Test
for ii=1:size(featureuji,1)
   x=featureuji(ii,1:end-1);

   %% normal
   m = m0;
   s = s0;
   Y = normpdf(x,m,s)';
   y=1;
   for i=1:size(Y,1)
         y=y*Y(i);
   end
     y1=y*proba(:,1);

   %% serangan / DDoS
   m = m1;
   s = s1;

   Y = normpdf(x,m,s)';
   y=1;
   for i=1:size(Y,1)
         y=y*Y(i);
   end
     y2=y*proba(:,2);

     if y1>y2
        C1=0;
     else
        C1=1;
     end
   C2=y1/(y1+y2)
   C3=y2/(y1+y2)

   anew(ii,:)=C1;
end
```

Fig. 11. Naive Bayes Training and Testing.

The testing conducted shows an accuracy value of 99.9% was found. As presented in Figure 12.

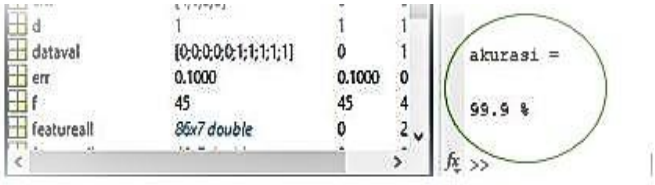

Fig. 12. Classification Results using Naïve Bayes.

V. Conclusion and Future Work

The experiments carried out concluded that attack information that has been detected by signature-based IDS needs to be re-tested for accuracy using classification with statistical calculations. The test is done by an artificial neural network and naïve Bayes. Based on the analysis and testing conducted, it was found that the accuracy of the artificial neural network was 95.2381% and naïve Bayes was 99.9%. Based on experiments carried out shows that the naïve Bayes method is better than the neural network method. Methods of artificial neural networks and naïve Bayes can be applied in the field of network forensics in determining accurate results and help strengthen evidence in the court.

Further, research will be conducted improved on other parameters such as increasing sample size input patterns presented to the network, variations of hidden layers, reduce the target error and use more training methods. Perform testing using other classification methods such as Support Vector Machine (SVM), K-Means to get better accuracy so that it can be presented in court.

References

[1] Symantec, "Kaspersky DDoS Attacks Report in Q1 2018," 2018.

[2] R. B. Readiness, "Cisco 2018 Asia Pacific Security Capabilities Benchmark Study Regional Breach Readiness Table of Contents," 2018.

[3] S. Geges and W. Wibisono, "Pengembangan Pencegahan Serangan Distributed Denial of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle," JUTI J. Ilm. Teknol. Inf., vol. 13, no. 1, pp. 53–67, 2015.

[4] A. Fadlil, I. Riadi, and S. Aji, "Development Of Computer Network Security Systems So That Network Forensic Analysis," J. Ilmu Tek. Elektro Komput. dan Inform., vol. 3, no. 1, pp. 11–18, 2017.

[5] G. Wang, "Neural Network Based Web Log Analysis for Web Intrusion Detection," IEICE Trans. Inf. Syst., vol. E100D, no. 10, pp. 2265–2266, 2017.

[6] M. Chambali, A. W. Muhammad, and Harsono, "Classification of Network Packages Based on Statistical Analysis and Neural Network," J. Pengemb. IT, vol. 03, no. 1, pp. 67–70, 2018.

[7] R. F. Fouladi, C. E. Kayatas, and E. Anarim, "Frequency based DDoS attack detection approach using naive Bayes classification," 39th Telecommun. Signal Process. (TSP), Int. Conf., pp. 104–107, 2016.

[8] A. Iswardani and I. Riadi, "Denial of service log analysis using density k-means method," J. Theor. Appl. Inf. Technol., vol. 83, no. 2, p. 2, 2016.

[9] J. Fahana, R. Umar, and F. Ridho, "Pemanfaatan Telegram sebagai Notifikasi Serangan untuk Jaringan Forensik," Query J. Inf. Syst., vol. 1, no. 2, pp. 6–14, 2017.

[10] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards Developing Network forensic mechanism for Botnet Activities in the IoT based on Machine Learning Techniques," arXiv Prepr., 2017.

[11] A. Fadlil, I. Riadi, and S. Aji, "DDoS Attacks Classification using Numeric Attribute-based Gaussian Naive Bayes," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 8, pp. 42–50, 2017.

[12] I. Riadi and A. W. Muhammad, "Network Packet Classification using Neural Network based on Training Function and Hidden Layer Neuron Number Variation," IJACSA) Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 6, pp. 248–252, 2017.

[13] V. D. Katkar and S. V. Kulkarni, "Experiments on detection of Denial of Service attacks using ensemble of classifiers," 2013 Int. Conf. Green Comput. Commun. Conserv. Energy, vol. 2, no. 1, pp. 837–842, 2013.

[14] A. Fadlil, I. Riadi, and S. Aji, "Review of detection DDOS attack detection using naive bayes classifier for network forensics," Bull. Electr. Eng. Informatics, vol. 6, no. 2, pp. 140–148, 2017.

[15] D. Mualfah and I. Riadi, "Network Forensics For Detecting Flooding Attack On Web Server," IJCSIS) Int. J. Comput. Sci. Inf. Secur., vol. 15, no. 2, pp. 326–331, 2017.

[16] M. Elavarasi, "Network Forensics And Its Investigation Methodology," Int. J. Emerg. Trends Sci. Technol., vol. 03, no. 05, pp. 852–859, 2016.

[17] A. S. Rawat, A. Rana, A. Kumar, and A. Bagwari, "Application of Multi Layer Artificial Neural Network in the Diagnosis System : A Systematic Review," vol. 7, no. 3, pp. 138–142, 2018.

[18] M. I. Rahman, N. A. Samsudin, A. Mustapha, and A. Abdullahi, "Comparative Analysis for Topic Classification in Juz Al-Baqarah," vol. 12, no. 1, pp. 406–411, 2018.

[19] I. Riadi, A. W. Muhammad, and Sunardi, "Neural network-based ddos detection regarding hidden layer variation," J. Theor. Appl. Inf. Technol., vol. 95, no. 15, pp. 3684–3691, 2017.

[20] J. Ali, S.H Furutani, N Ozawa, sei-ichi Ban, & T Shimamura, "Distributed Denial of Service (DDoS) Backscatter Detection System Using Resource Allocating Network with Data Selection," Mem. Grad. Sch. Eng. Syst. Informatics Kobe Univ., no. 7, pp. 8–13, 2015.