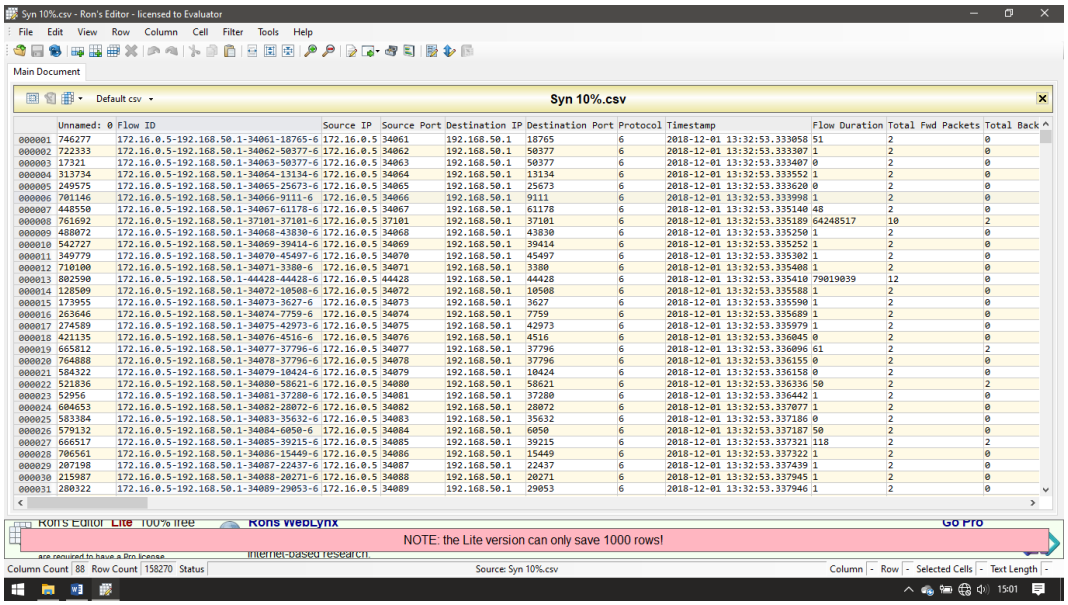
BAB III
METODOLOGI PENELITIAN

Metode penelitian terkait tentang deteksi serangan DDoS dan algoritma *Decision Tree, K-NN, Bayesian Network* dan *OneR* yang akan dilaksanakan dibagi menjadi beberapa tahapan sebagai berikut:

3.1. Pengambilan Data Serangan Jaringan DDoS

Pengambilan log dari simulasi serangan jaringan menggunakan *Dataset* DDoS yang diterbitkan oleh *dataset* jaringan DDoS CICDDoS2019 yang ditulis oleh Canadian Institute for Cybersecurity dalam bentuk format (.pcap). atau dalam bentuk (.csv) atau bisa juga di ubah dalam bentuk format (.arff). Data tersebut nantinya akan di muat kedalam WEKA. Dikarenakan jumlah *record* data pada *dataset* per-serangan DDoS lebih dari 1 juta *record* data, maka penulis menggunakan sampel sebanyak 10% dari *dataset* di tiap serangan DDoS. Adapun total dataset DDoS pada serangan SYN sebanyak 1.582.682 *record* data, pada *dataset* DDoS pada serangan NTP sebanyak 1.217.008 *record* data. *Log* yang ada pada *dataset* DDoS seperti yang tersaji pada Gambar 3.1 berikut.



Gambar 3.1 Traffics Collection *Dataset*

Pada penelitian ini, Dataset kedua serangan yang diantaranya serangan SYN Flood (Berdasarkan Serangan TCP - Serangan Exploitasi), maupun serangan NTP (Berdasarkan Serangan UDP - Serangan Refleksi) terdapat 88 atribut yang digunakan.

Berikut akan dijelaskan pada tabel 3.1 untuk detail fitur/atribut yang ada pada *Dataset* DDoS 2019.

Tabel 3.1 Detail atribut *Dataset* DDoS 2019

No	Feature Name	Description	No	Feature Name	Description
1	Unnamed: 0		45	Bwd Packets/s	Number of backward packets per second
2	Flow ID	Flow Identity	46	Min Packet Length	Minimum length of a flow
3	Source IP	Source IP Address	47	Max Packet Length	Maximum length of a flow
4	Source Port	Source Port	48	Packet Length Mean	Mean length of a flow
5	Destination IP	Destination IP Address	49	Packet Length Std	Standard deviation length of a flow
6	Destination Port	Destination Port	50	Packet Length Variance	Minimum inter-arrival time of packet
7	Protocol	Protocol	51	FIN Flag Count	Number of packets with FIN
8	Timestamp	date format that is distributed on Unix-based servers	52	SYN Flag Count	Number of packets with SYN
9	Flow Duration	Flow Duration	53	RST Flag Count	Number of packets with RST
10	Total Fwd Packets	Total Forward Packets	54	PSH Flag Count	Number of packets with PSH
11	Total Backward Packets	Total Backward Packets	55	ACK Flag Count	Number of packets with ACK
12	Total Length of Fwd Packets	Total Length Forward Packets	56	URG Flag Count	Number of packets with URG

Lanjutan Tabel 3.1 Detail atribut *Dataset* DDoS 2019

No	Feature Name	Description	No	Feature Name	Description
13	Total Length of Bwd Packets	Total Length Backward Packets	57	CWE Flag Count	Number of packets with CWE
14	Fwd Packet Length Max	Forward Packet Length Max	58	ECE Flag Count	Number of packets with ECE
15	Fwd Packet Length Min	Forward Packet Length Min	59	Down/Up Ratio	Download and upload ratio
16	Fwd Packet Length Mean	Forward Packet Length Mean	60	Average Packet Size	Average size of packet
17	Fwd Packet Length Std	Forward Packet Length Standard	61	Avg Fwd Segment Size	Average size observed in the forward direction
18	Bwd Packet Length Max	Backward Packet Length Max	62	Avg Bwd Segment Size	Average size observed in the backward direction
19	Bwd Packet Length Min	Backward Packet Length Min	63	Fwd Header Length.1	Forward Header Length
20	Bwd Packet Length Mean	Backward Packet Length Mean	64	Fwd Avg Bytes/Bulk	Average number of bytes bulk rate in the forward direction
21	Bwd Packet Length Std	Backward Packet Length Standard	65	Fwd Avg Packets/Bulk	Average number of packets bulk rate in the forward direction
22	Flow Bytes/s	flow byte rate that is number of packets transferred per second	66	Fwd Avg Bulk Rate	Average number of bulk rate in the forward direction
23	Flow Packets/s	flow packets rate that is number of packets transferred per second	67	Bwd Avg Bytes/Bulk	Average number of bytes bulk rate in the backward direction

Lanjutan Tabel 3.1 Detail atribut *Dataset* DDoS 2019

No	Feature Name	Description	No	Feature Name	Description
24	Flow IAT Mean	Mean time between two flows	68	Bwd Avg Packets/Bulk	Average number of packets bulk rate in the backward direction
25	Flow IAT Std	Standard time between two flows	69	Bwd Avg Bulk Rate	Average number of bulk rate in the backward direction
26	Flow IAT Max	Max time between two flows	70	Subflow Fwd Packets	The average number of packets in a sub flow in the forward direction
27	Flow IAT Min	Min time between two flows	71	Subflow Fwd Bytes	The average number of bytes in a sub flow in the forward direction
28	Fwd IAT Total	Total time between two packets sent in the forward direction	72	Subflow Bwd Packets	The average number of packets in a sub flow in the backward direction
29	Fwd IAT Mean	Mean time between two packets sent in the forward direction	73	Subflow Bwd Bytes	The average number of bytes in a sub flow in the backward direction
30	Fwd IAT Std	Standard deviation time between two packets sent in the forward direction	74	Init_Win_bytes_forward	Number of bytes sent in initial window in the forward direction
31	Fwd IAT Max	Maximum time between two packets sent in the forward direction	75	Init_Win_bytes_backward	Number of bytes sent in initial window in the backward direction
32	Fwd IAT Min	Minimum time between two packets sent in the forward direction	76	act_data_pkt_fwd	Number of packets with at least 1 byte of TCP data payload in the forward direction

Lanjutan Tabel 3.1 Detail atribut *Dataset* DDoS 2019

No	Feature Name	Description	No	Feature Name	Description
33	Bwd IAT Total	Maximum time between two packets sent in the forward direction	77	min_seg_size_forward	Minimum segment size observed in the forward direction
34	Bwd IAT Mean	Mean time between two packets sent in the backward direction	78	Active Mean	Mean time a flow was active before becoming idle
35	Bwd IAT Std	Standard deviation time between two packets sent in the backward direction	79	Active Std	Standard deviation time a flow was active before becoming idle
36	Bwd IAT Max	Maximum time between two packets sent in the backward direction	80	Active Max	Maximum time a flow was active before becoming idle
37	Bwd IAT Min	Minimum time between two packets sent in the backward direction	81	Active Min	Minimum time a flow was active before becoming idle
38	Fwd PSH Flags	Number of times the PSH flag was set in packets travelling in the forward direction (0 for UDP)	82	Idle Mean	Mean time a flow was idle before becoming active
39	Bwd PSH Flags	Number of times the PSH flag was set in packets travelling in the backward direction (0 for UDP)	83	Idle Std	Standard deviation time a flow was idle before becoming active

Lanjutan Tabel 3.1 Detail atribut *Dataset* DDoS 2019

No	Feature Name	Description	No	Feature Name	Description
40	Fwd URG Flags	Number of times the URG flag was set in packets travelling in the forward direction (0 for UDP)	84	Idle Max	Maximum time a flow was idle before becoming active
41	Bwd URG Flags	Number of times the URG flag was set in packets travelling in the backward direction (0 for UDP)	85	Idle Min	Minimum time a flow was idle before becoming active
42	Fwd Header Length	Total bytes used for headers in the forward direction	86	SimillarHTTP	HTTP Simillarity
43	Bwd Header Length	Total bytes used for headers in the Backward direction	87	Inbound	Inbound Traffic
44	Fwd Packets/s	Number of forward packets per second	88	Label	Label Attack

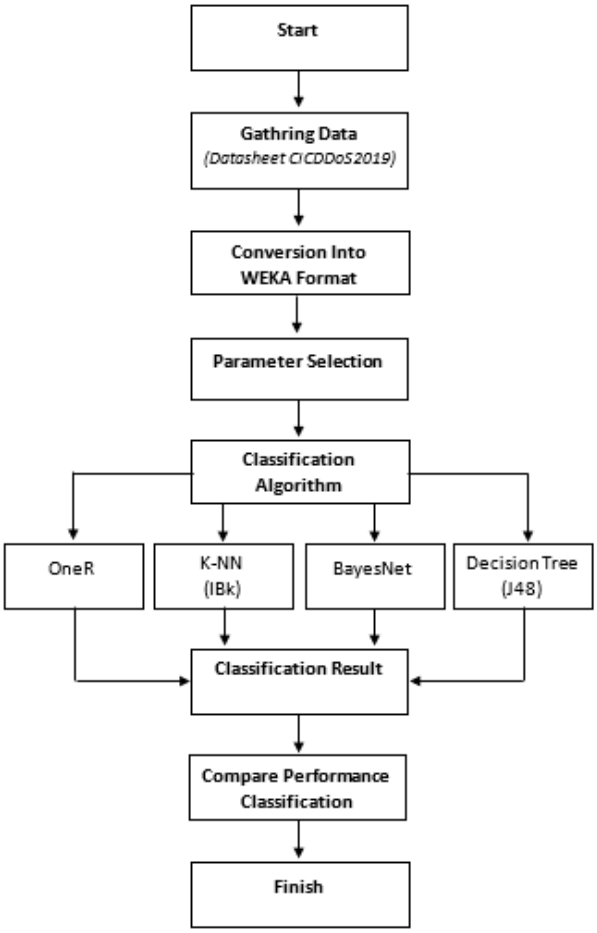
3.2. Proses Klasifikasi Data Serangan Jaringan DDoS

Pada penelitian ini menggunakan WEKA-3.9 sebagai alat *data mining* untuk memilih dan mengevaluasi akurasi algoritma. Tabel dibawah ini akan menunjukkan algoritma yang digunakan dalam percobaan.

Tabel 3.2. Algoritma yang digunakan

Kategori	**Algoritma yang digunakan**
Bayes	*BayesNet (Bayesian Network)*
Lazy	*IBk (K-NN)*
Rules	*One-R*
Trees	*J48 (Decision Tree)*

Pada penelitian ini proses klasifikasi menggunakan *dataset* dari CICDDoS2019 dengan menggunakan metode pengujian *Cross-Validation* dengan beberapa algoritma *Classifier* diantaranya *Decision Tree*, *K-NN*, *Bayesian Network* dan *OneR*. Berikut langkah-langkah klasifikasi menggunakan WEKA seperti yang ditunjukkan pada gambar 3.2.



Gambar 3.2 Langkah-langkah klasifikasi dari Algoritma *Decision Tree, K-NN, Bayesian Network* dan *OneR*

3.3. Perbandingan Klasifikasi Algoritma

Metode klasifikasi dapat dilakukan untuk menganalisa hasil uji klasifikasi terhadap serangan DDoS. Algoritma yang digunakan dalam menilai hasil klasifikasi yaitu *Decision Tree, K-NN, Bayesian Network* dan *OneR*. Dengan beberapa metode klasifikasi tersebut akan memunculkan hasil pengujian yang berbeda pada serangan DDoS yang diteliti. Untuk mengetahui klasifikasi mana yang terbaik dalam melakukan pengujian serangan DDoS, diperlukan pembandingan diantara algoritma klasifikasi yang digunakan [12]. Hal yang dilakukan pada proses pembandingan adalah dengan menganalisa beberapa hasil klasifikasi pada algoritma yang digunakan.

Parameter yang di analisa diantaranya sebagai berikut:

a. Klasifikasi *Correctly* dan *Incorrectly Instance.*
b. *Kappa Statistics.*
c. *Errors.*
    1) *Mean Absolute Error (MAE)* dan *Root Mean Squared Error (RMSE).*
    2) *Relative Absolute Error (RAE)* dan *Root Relative Squared Error (RRSE).*
d. *Accuracy Measurement.*

Hasil akhir pada pembandingan ini yakni diketahuinya pengukuran akurasi terbaik dari algoritma yang digunakan dalam mendeteksi serangan DDoS SYN dan NTP tersebut.