DETEKSI *DISTRIBUTED DENIAL OF SERVICE* MENGGUNAKAN *RANDOM FOREST*

SKRIPSI

Oleh:
DAMAR ADYUN MUHAMAD
NIM. 16650043

JURUSAN TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2020

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

DETEKSI *DISTRIBUTED DENIAL OF SERVICE*
MENGGUNAKAN *RANDOM FOREST*

SKRIPSI

Diajukan kepada:
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
Untuk Memenuhi Salah Satu Persyaratan Dalam
Memperoleh Gelar Sarjana Komputer (S.Kom)

Oleh:
DAMAR ADYUN MUHAMAD
NIM. 16650043

JURUSAN TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2020

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

HALAMAN PERSETUJUAN

DETEKSI *DISTRIBUTED DENIAL OF SERVICE* MENGGUNAKAN *RANDOM FOREST*

SKRIPSI

Oleh:
DAMAR ADYUN MUHAMAD
NIM. 16650043

Telah Diperiksa dan Disetujui untuk Diuji

Tanggal : 11 Mei 2020

Dosen Pembimbing I	Dosen Pembimbing II
Dr. Cahyo Crysdian	Ajib Hanani, M.T.
NIP. 19740424 200901 1 008	NIDT. 19840731 20160801 1 076

Mengetahui,
Ketua Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang

Dr. Cahyo Crysdian
NIP. 19740424 200901 1 008

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

DETEKSI *DISTRIBUTED DENIAL OF SERVICE*
MENGGUNAKAN *RANDOM FOREST*

SKRIPSI

Oleh:
DAMAR ADYUN MUHAMAD
NIM. 16650043

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Komputer (S.Kom)
Tanggal: 2 Juni 2020

Susunan Dewan Penguji :			**Tanda Tangan**
Penguji Utama	:	Irwan Budi Santoso, M.Kom NIP. 19770103 201101 1 004	( )
Ketua Penguji	:	Dr. M. Amin Hariyadi, M.T NIP. 19670118 200501 1 001	( )
Sekertaris Penguji	:	Dr. Cahyo Crysdian NIP. 19740424 200901 1 008	( )
Anggota Penguji	:	Ajib Hanani, M.T. NIDT. 19840731 20160801 1 076	( )

Mengetahui,
Ketua Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang

Dr. Cahyo Crysdian
NIP. 19740424 200901 1 008

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini,

Nama : Damar Adyun Muhamad

NIM : 16650043

Jurusan : Teknik Informatika

Fakultas : Sains dan Teknologi

Judul Skripsi : Deteksi *Distributed Denial of Service* Menggunakan *Random Forest*

Menyatakan dengan sebenarnya bahwa kripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan saya tersebut.

Malang, 8 Mei 2020

buat pernyataan,



Damar Adyun Muhamad

NIM.16650043

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

KATA PENGANTAR

Assalamu'alaikum Warohmatullaahi Wabarakaatuh

Syukur nikmat terpanjatakan kepada *Ilahi Rabbi*, satu-satunya zat yang selalu memberikan kekuatan kepada penulis untuk dapat menyelesaikan skripsi dengan keadaan yang *insyaAllah* lancar dan baik. Sholawat sekaligus salam penghormatan kepada junjungan nabi *akhirruzzaman*, nabi pembawa kabar kemenangan untuk seluruh umat manusia tanpa terkecuali. Siapapun pengikutnya menantikan syafaatnya kelak di hari akhir. Semoga kita termasuk golongan yang dituntun Allah SWT dan mendapat pertolongan Nabi Muhamad SAW. *Aamiin.*

Selama proses pengerjaan skripsi, penulis mendapatkan banyak bantuan dan dukungan dari berbagai pihak. Maka dari itu, ucapan syukur dan terima kasih penulis sampaikan kepada:

1. Dr. Cahyo Crysdian, selaku Ketua Jurusan Teknik Informatika sekaligus selaku dosen pembimbing I yang telah dengan sabar membimbing penulis, memberikan masukan, saran dan juga arahan sehingga penulis tidak hanya mampu menyelesaikan pengerjaan skripsi tetapi juga dapat mengambil banyak hikmah dan pelajaran.
2. Ajib Hanani, M.T, selaku dosen pembimbing II yang telah teliti membimbing penulis untuk dapat mencapai hasil skripsi yang lebih baik.
3. Dr. M. Amin Hariyadi dan Irwan Budi Santoso, M.T selaku dosen penguji dengan sikap profesional telah menguji seluruh proses ujian skripsi penulis mulai dari seminar proposal hingga sidang skripsi dengan lancar.
4. Seluruh jajaran staf dan dosen jurusan Teknik Informatika yang secara langsung maupun tidak langsung terlibat dalam proses pengerjaan skripsi.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

5. Seluruh teman-teman Andromeda TI 16, kakak tingkat, adik tingkat dan seluruh teman seperjuangan yang secara langsung maupun tidak langsung memberikan bantuan dalam proses pengerjaan skripsi.
6. Ibu, bapak, kakak dan adik menjadi manusia yang luar biasa memberikan dukungan dan semangat tanpa lelah kepada penulis.

Peneliti menyadari bahwa proses penelitian dari awal hingga akhir masih jauh dari kata sempurna. Maka dari itu penulis membuka kesempatan selebar-lebarnya untuk setiap saran dan kritik yang membangun. Terlepas dari itu semua, peneliti berharap ada manfaat yang dapat diambil dari skripsi penulis.

Wassalamu'alaikum Warohmatullaahi Wabarakaatuh

Malang, 18 Mei 2020

Penulis

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

DAFTAR ISI

HALAMAN JUDUL ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
PERNYATAAN KEASLIAN TULISAN ..... **iv**
KATA PENGANTAR ..... **vi**
DAFTAR ISI ..... **viii**
DAFTAR GAMBAR ..... **x**
DAFTAR TABEL ..... **xi**
ABSTRAK ..... **xii**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang Penelitian 1
1.2 Pernyataan Masalah 4
1.3 Tujuan Penelitian 4
1.4 Batasan Masalah 5
1.5 Manfaat Penelitian 5
BAB II STUDI PUSTAKA **6**
2.1 *Distributed Denial of Service* (*DDoS*) 6
2.2 *Random Forest* 8
BAB III METODOLOGI PENELITIAN **11**
3.1 Akuisisi Data 11
a. Konfigurasi *Hacking Environment* 11
b. Simulasi Peretasan *DDoS* 12
c. Perekaman Lalu Lintas Jaringan 13
d. Ektraksi Lalu Lintas Jaringan 14
e. Pelabelan 15
3.2 Perancangan Sistem 16
3.2.1 Praproses Data 18
3.2.2 *Random Forest* 19
3.3 Kerangka Kerja Konseptual 28
BAB IV UJI COBA DAN PEMBAHASAN **31**
4.1 Skenario Uji Coba 31
4.1.1 Akuisisi Data 31

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

4.1.2 Praproses Data 44
4.1.3 *Random Forest* 44
4.1.4 Pengujian Sistem 46
4.2 Hasil Uji Coba 49
4.3 Pembahasan 51
BAB V KESIMPULAN DAN SARAN 56
5.1 Kesimpulan 56
5.2 Saran 57
DAFTAR PUSTAKA 58

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

DAFTAR GAMBAR

Gambar 1.1 Diagram Serangan *DDoS* Berdasar Negara 3
Gambar 2.1 Alur *Random Forest* 9
Gambar 3.1 Blok Diagram Perancangan Sistem 17
Gambar 3.2 *Flowchart Random Forest* untuk Pembuatan Model..... 20
Gambar 3.3 Script Program Proses Random Forest untuk Pembuatan Model ... 25
Gambar 3.4 *Flowchart Random Forest* untuk Deteksi Serangan 26
Gambar 3.5 Script Program Proses Random Forest untuk Deteksi Serangan..... 27
Gambar 3.6 Kerangka Kerja Konseptual..... 28
Gambar 4.1 Tampilan Halaman Muka VirtualBox 32
Gambar 4.2 Pengaturan *Host Network Manager*..... 32
Gambar 4.3 Konfigurasi *Network Settings* 33
Gambar 4.4 *IP Address* BackBox..... 34
Gambar 4.5 *IP Adress* Metasploitable2 35
Gambar 4.6 Metasploit 36
Gambar 4.7 Tampilan Akses *Server Hackable* pada *Client* 36
Gambar 4.8 *Module Options* pada Metasploit..... 37
Gambar 4.9 Proses Penyerangan *DDoS* terhadap *Server* 38
Gambar 4.10 Tanggapan *Server* Metasploitable2 terhadap Serangan *DDoS*..... 38
Gambar 4.11 Perekaman Lalu Lintas Jaringan Normal 39
Gambar 4.12 Peluncuran *DDoS* dengan 4 Tab Bot 40
Gambar 4.13 Perekaman Lalu Lintas Serangan *DDoS*..... 40
Gambar 4.14 Halaman Utama CICFlowMeter..... 41
Gambar 4.15 Tampilan Menu *Offline*..... 42
Gambar 4.16 *Rescaling* Data Numerik..... 44
Gambar 4.17 Sampel *Bootstrapping* pada Data Sekunder 45
Gambar 4.18 Sampel *Random Forest* Model 45
Gambar 4.19 *Flowchart Setting* Uji Coba Durasi Waktu..... 48
Gambar 4.20 *Script* Program Proses Pencatatan Durasi Deteksi 49

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

DAFTAR TABEL

Tabel 3.1 Sampel *Dataset* CICIDS2017 16
Tabel 3.2 Data Perhitungan 22
Tabel 3.3 Mengurutkan Data pada Kolom 22
Tabel 3.4 Rerata Data yang Berdekatan 22
Tabel 3.5 Data Partisi 23
Tabel 3.6 Hasil Perhitungan Gini *Impurity* dan Gini *Index* 24
Tabel 3.7 Kerangka Kerja Konseptual Penelitan Sebelumnya 29
Tabel 4.1 Daftar *IP Address* 35
Tabel 4.2 Jumlah Data Perekaman Lalu Lintas Jaringan 41
Tabel 4.3 Hasil Ektraksi Lalu Lintas Jaringan 42
Tabel 4.4 Parameter Penelitian 43
Tabel 4.5 Total Data dalam Penelitian 44
Tabel 4.6 *Confusion Matrix* 47
Tabel 4.7 Uji Coba dengan Data *Testing* pada Data Sekunder 50
Tabel 4.8 Hasil Uji Coba pada Data Sekunder 50
Tabel 4.9 Uji Coba dengan Data *Testing* pada Data Primer 51
Tabel 4.10 Hasil Uji Coba dengan Data Primer 51
Tabel 4.11 Hasil *Confusion Matrix* 52
Tabel 4.12 Perbedaan Hasil *Confusion Matrix* antara Prediksi Data Primer dan Data Sekunder 52
Tabel 4.13 Pengukuran *Random Forest* Model Data Sekunder dan Data Primer 53

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Muhamad, Damar Adyun. 2020. **Deteksi *Distributed Denial of Service* Menggunakan *Random Forest***. Skripsi. Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang.
Pembimbing: (I) Dr. Cahyo Crysdian. (II) Ajib Hanani, M.T.

Kata kunci: *DDoS*, *Random Forest*, sistem deteksi, *server*.

Distributed Denial of Service (*DDoS*) merupakan salah satu metode peretasan yang digunakan oleh penyerang untuk melumpuhkan sebuah *server* target. Karena serangan *DDoS* dan aktifitas akses *server* normal memiliki karakteristik yang sama yaitu melakukan *request* pada *server*, maka dari itu dibutuhkan sistem deteksi untuk membedakan antara *DDoS* dan akses normal, sehingga dapat diberikan penanganan yang tepat pada *server* yang lumpuh. Adanya sistem deteksi *DDoS* tentu akan sangat membantu permasalahan tersebut. *Random Forest* dipilih sebagai metode penelitian karena *Random Forest* mampu melakukan klasifikasi data dengan baik dan waktu yang singkat. Penelitian ini menggunakan dua jenis set data, yaitu set data primer berasal dari aktifitas simulasi serangan *DDoS* peneliti pada *server* virtual, sedangkan set data sekunder merupakan dataset ahli yaitu dataset CICIDS2017 dari University of New Brunswick Kanada. Dari hasil pengujian pada 266 baris set data primer, didapatkan nilai *accuracy*, *presicion*, *recall* dan *f-measure* secara berturut-turut adalah 99.62%, 98.59%, 100% dan 99.29% dengan durasi pengujian selama 1 detik. sedangkan hasil pengujian pada 169309 baris set data sekunder didapatkan nilai *accuracy*, *presicion*, *recall* dan *f-measure* secara berturut-turut adalah 99.87%, 99.91%, 99.86% dan 99.89% dengan durasi pengujian selama 12 menit 44 detik.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Muhamad, Damar Adyun. 2020. **Distributed Denial of Service Detection Using Random Forest**. Undergraduate thesis. Department of Informatics Engineering, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University of Malang.
Supervisor: (I) Dr. Cahyo Crysdian. (II) Ajib Hanani, M.T.

Keywords: DDoS, Random Forest, detection system, server.

Distributed Denial of Service (DDoS) is one of the hacking methods used by an attacker to disable a target server. Since DDoS attacks and normal access activities have the same characteristics which are making requests on the server, a detection system is needed to distinguish between DDoS and normal access to provide the proper handling for the target. The existence of a DDoS detection system will certainly greatly help these problems. Random Forest was chosen as a research method because Random Forest can classify data well with a short time. This study uses two types of data set, primary data set derived from the simulation activity of DDoS attacks by the researcher on virtual servers, then the secondary data set is CICIDS2017 dataset from the University of New Brunswick, Canada. The test results on 266 rows of primary data set obtained the values of accuracy, precision, recall, and f-measure rate respectively are 99.62%, 98.59%, 100% and 99.29% with a duration of testing of 1 seconds. While the results of testing on 169309 secondary data set lines obtained values of accuracy, precision, recall, and f-measure rate respectively are 99.87%, 99.91%, 99.86% and 99.89% with a duration of testing of 12 minutes 44 seconds.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

محمد , دمر عديون. 2020. **اكتشاف** ***Distributed Denial of Service*** **استعمال Random Forest**. قسم المعلوماتية. كلية العلوم والتكنولوجيا. جامعة الإسلامية الحكومة مولانا مالك إبراهيم مالانج.

ال‌مشرف : (I) جحيو كريسديان الدكتور (II) عجب حنى الماجيستير

الكلمات الرئيسية : *server* , نظام الكشف, *DDoS , Random Forest*

Distributed Denial of Service (*DDoS*) هو واحد من طريق القرصنة الذي يستخدمه المهاجم لتعطيل الخادم الهدف. لأن هجمات *DDoS* ونشاط الوصول العادي إلى الخادم لهما نفس الخصائص وهو تقديم الطلبات على الخادم, لذلك يحتاج إلى نظام الكشف للتمييز بين *DDoS* والوصول العادي حتى يستطيع أن يعطي التوفير المناسب للهدف العاجز. كان نظام *DDoS* مفيدا لهذه المشكلة. اختيارها *Random Forest* كطريق بحث لأن *Random Forest* يمكن أن تصنف البيانات بشكل جيد ووقت قصير. وتستخدم هذا البحث نوعان من المجموعة البيانات ، هما المجموعة البيانات الأولية التي تشتق من أنشطة محاكاة هجمات *DDoS* التي يقوم بها الباحث على حواسيب الخادم الافتراضي, ثم المجموعة البيانات الثانوية هي *CICIDS2017 dataset* من جامعة نيو برونزويك ، كندا. نتائج الاختبار على 266 الصفوف المجموعة البيانات الأولية التي تم الحصول عليه قيم الدقة ، و الاحكام ، و الأذكر ، و f–قياس معدل على التوالي بنسبة 99.62% , 98.59% , 100% و 99.29% مع مدة الاختبار من 1 ثوان. في حين أن نتائج الاختبار على 169309 خطوط المجموعة البيانات الثانوية حصل على قيم من الدقة ، و الاحكام ، و الأذكر ، و f–قياس معدل على التوالي بنسبة 99.87% , 99.91% , 99.86% و 99.89% مع مدة الإختبار 12 دقائق و 44 ثوان.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Tidak bisa dielakkan bahwa internet telah menjadi kebutuhan bagi kehidupan manusia khususnya negara Indonesia yang merupakan salah satu negara besar yang memiliki jumlah penduduk yang banyak. Seperti data yang telah dirilis oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tentang pengguna internet di Indonesia pada tahun 2018. Yaitu 64,8% lebih penduduk Indonesia menggunakan internet sepanjang tahun 2018, yaitu sebanyak 171,17 juta jiwa dari total 264,16 juta jiwa penduduk Indonesia. Jumlah yang besar bagi negara yang besar pula. Banyaknya pengguna internet di Indonesia ternyata berbanding lurus dengan serangan siber yang ditujukan kepada Indonesia. Laporan pemantauan keamanan internet Badan Siber dan Sandi Nasional (BSSN) mencatat ada 232.447.974 serangan siber ke Indonesia sepanjang tahun 2018 (CNN Indonesia, 2019). Jika dirata-rata dengan penduduk Indonesia yang mencapai 264 juta jiwa maka hampir setiap orang penduduk Indonesia pernah mengalami serangan siber sekali dalam setahun. Data tersebut menunjukkan bahwa Indonesia merupakan negara yang masih rapuh dalam menangkal dan menangani serangan siber.

Jika berbicara tentang pengguna internet yang rawan menjadi target serangan, pengguna internet di Indonesia berasal dari latar belakang kepentingan yang bermacam-macam. Terdapat pengguna umum yang hanya menggunakan internet sebagai keperluan untuk berkomunikasi dengan orang lain, kebanyakan pengguna umum internet ini menggunakan telepon genggam sebagai media penggunaan

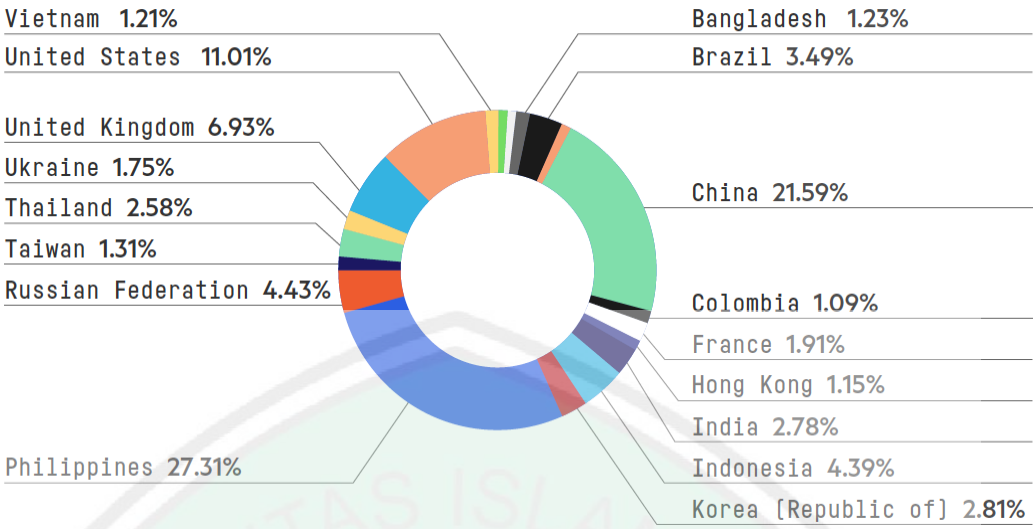
CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

internetnya. Adapula pengguna internet komersial yang menggunakan internet untuk menjalankan bisnis, biasanya pengguna ini memiliki sebuah *website* untuk menampilkan produk maupun jasa bisnis. Tentunya *website* pengguna komersial ini tersambung dengan *server* bisnis dan komputer administrasi perusahaan. Dari dua contoh pengguna internet ini, maka pengguna kedualah yang memiliki resiko peretasan lebih besar. Penyerang dapat masuk ke *server* untuk merusak aset bisnis ataupun penyerang dapat masuk ke komputer administrasi untuk mengakses berkas-berkas penting pengguna.

Besarnya nominal data serangan di Indonesia sekaligus pengguna yang rawan terhadap serangan siber, kesadaran terhadap pentingnya keamanan jaringan masih kurang. Bahkan tidak sedikit pengguna internet di Indonesia yang belum mengenal tentang keamanan jaringan dan bagaimana dampak terhadap penyalahgunaan akses dalam jaringan. Keadaan seperti ini yang akan membuat *hacker* semakin tertarik untuk menyerang situs, *server* ataupun komputer pribadi seseorang yang tidak paham betul tentang keamanan jaringan.

Seperti yang dirilis oleh Imperva Research Lab dalam website imperva.com, mereka merilis salah satu serangan keamanan siber *Distributed Denial of Service* (*DDoS*) pada tahun 2019 bahwasanya Indonesia masuk kedalam 10 besar negara didunia yang mendapat serangan *DDoS* terbanyak yaitu 4,39% dari serangn *DDoS* di seluruh dunia. Gambar 1.1 menunjukkan diagram serangan *DDoS* yang diterima oleh Indonesia sesuai data riset Imperva Research Lab.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 1.1 Diagram Serangan *DDoS* Berdasar Negara

Dari data diatas perlu diperhatikan bahwa serangan *DDoS* tidak dapat diacuhkan begitu saja. Ancaman dari serangan *DDoS* dapat melumpuhkan *server website* dan tentu kerusakan operasi *server* menyebabkan *server* tidak dapat diakses oleh *client* manapun.

DDoS berjalan dengan memanfaatkan arus lalu lintas jaringan dari *client* menuju *server*, sehingga *DDoS* tidak dapat ditolak sebelum *server* mengalami gangguan. Salah satu cara yang dapat dilakukan untuk mencegah *DDoS* yaitu dengan membedakan manakah lalu lintas yang normal dengan lalu lintas serangan *DDoS*. Cara tersebut dapat dilakukan dengan mengimplementasikan salah satu metode *machine learning* yaitu *Random Forest* dengan menggunakan objek lalu lintas jaringan data terdahulu. Merujuk pada penelitian yang dilakukan Alkasassbeh dkk (2016) dalam penelitian *Detecting Distributed Denial of Service Using Data Mining Techniques*, hasil dari deteksi *DDoS* menggunakan metode *Random Forest* memiliki tingkat akurasi sebesar 98,02%.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Dalam Al Qur'an telah ditunjukkan perlunya mengetahui hal yang baik dan buruk, seperti firman Allah SWT dalam surah Al Baqarah[2] ayat 42:

وَلَا تَلْبِسُواْ ٱلْحَقَّ بِٱلْبَـٰطِلِ وَتَكْتُمُواْ ٱلْحَقَّ وَأَنتُمْ تَعْلَمُونَ

Artinya: "Janganlah kalian campur-adukkan antara kebenaran dan kebatilan, dan janganlah kalian sembunyikan yang benar padahal kamu mengetahuinya". (Q.S. Al-Baqarah [2]: 42).

Oleh karena pentingnya membedakan lalu lintas jaringan serangan *DDoS* dan lalu lintas akses normal, maka peneliti memutuskan untuk melakukan penelitian dengan judul "Deteksi *Distributed Denial of Service* Menggunakan *Random Forest*".

1.2 Pernyataan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan, maka peneliti memberikan pernyataan masalah sebagai berikut:

1. Seberapa tinggi *accuracy*, *precision*, *recall* dan *f-measure* metode *Random Forest* dalam mendeteksi *DDoS*?
2. Seberapa cepat metode *Random Forest* dalam mendeteksi *DDoS*?

1.3 Tujuan Penelitian

Berikut tujuan penelitan yang sesuai dengan pernyataan masalah yang dipaparkan:

1. Untuk mengukur *accuracy*, *precision*, *recall* dan *f-measure* metode *Random Forest* dalam mendeteksi deteksi *DDoS*.
2. Untuk mengukur kecepatan metode *Random Forest* dalam mendeteksi *DDoS*.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

1.4 Batasan Masalah

Batasan masalah dalam penelitian adalah sebagai berikut.

1. Data yang digunakan dalam penelitian terbagi menjadi 2, yaitu data sekunder dan data primer. Model yang dibangun dari data *training* pada pada sekunder digunakan untuk melakukan deteksi data *testing* pada data sekunder. Begitu juga Model yang dibangun dari data *training* pada data primer digunakan untuk deteksi data *testing* pada data primer.
2. Simulasi peretasan menggunakan target *server* virtual Metasploitable2

1.5 Manfaat Penelitian

Dari penelitian dengan *Random Forest* diharapkan dapat dihasilkan *accuracy* deteksi yang tinggi dengan cara yang efisien. Sehinga penelitian ini diharapkan dapat memunculkan manfaat bagi beberapa pihak, diantaranya adalah:

1. Manfaat bagi seorang sysadmin website, dengan adaanya sistem deteksi *Distributed Denial of Service* dapat membantu evaluasi sistem ketika terjadi aktifitas jaringan yang tidak normal. Sistem dapat membedakan antara trafik jaringan serangan dan trafik jaringan normal sehingga sysadmin dapat memberikan tindakan penanganan yang tepat.
2. Kemudian bagi seorang pengembang perangkat lunak, sistem ini dapat menjadi masukan untuk dikembangkan menjadi perangkat lunak yang dapat digunakan secara meluas. Begitu juga dengan sistem ini pengembang perangkat lunak dapat memanfaatkan untuk *monitoring* perangkat lunak yang telah dibuat.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB II

STUDI PUSTAKA

2.1 *Distributed Denial of Service* (*DDoS*)

Diantara berbagai serangan berbasis internet, serangan *Denial of Service* (*DoS*) merupakan ancaman kritis dan berkelanjutan dalam keamanan dunia maya. Secara umum, serangan *DoS* diimplementasikan dengan memaksa komputer korban untuk mengatur ulang atau menghabiskan sumber dayanya, seperti halnya siklus *CPU*, memori atau bandwidth jaringan. Akibatnya komputer yang ditargetkan tidak lagi dapat memberikan layanan yang dimaksudkan untuk pengguna yang sah. Ketika serangan *DoS* diatur oleh beberapa komputer terdistribusi, itu disebut serangan *Distributed Denial of Service* (*DDoS*) yang merupakan metode serangan populer di dunia maya. Dari buku teks klasik, kita tahu keamanan masuk ke dalam tiga kategori: kerahasiaan, ketersediaan, dan integritas. Jelas bahwa serangan *DDoS* termasuk dalam kategori ketersediaan (Yu, 2013).

Distributed Denial of Service (*DDoS*) menimbulkan ancaman besar terhadap dunia internet, sehingga banyak mekanisme pertahanan telah diusulkan untuk memerangi mereka. Penyerang terus memodifikasi alat-alat serangan untuk melawan sistem keamanan, hingga akhirnya para peniliti mengubah pendekatan dalam menangani serangan baru tersebut. Bidang *DDoS* berkembang sangat cepat dan hal ini akan menjadi semakin sulit untuk dipahami dalam pandangan masalah secara umum (Mirkovic dan Reiher, 2004).

Dengan munculnya paradigma komputasi baru, seperti komputasi *Cloud* dan *Mobile*, dan munculnya teknologi yang saling terkoneksi seperti *Internet of*

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Things, serangan *Denial of Services* (*DDoS*) telah berkembang secara dramatis dalam volume, frekuensi, kecanggihan dan dampaknya menjadikan *DoS* salah satu ancaman paling menantang di Internet. Pada Maret 2015, GitHub menghadapi serangan *DDoS* yang besar. Serangan itu berlangsung selama hampir satu minggu dan menyebabkan kerusakan signifikan. Pada Oktober 2016, serangkaian serangan *DDoS* secara massal dilakukan terhadap server *DNS* Dyn, menyebabkan gangguan pada beberapa situs web utama termasuk Airbnb, Netflix, dan Spotify. Pada bulan September 2017, UK National Lottery menjadi sasaran serangan *DDoS* selama waktu puncak operasi, memaksa organisasi tersebut untuk mengambil offline situs web lotre dan aplikasi seluler selama sekitar 90 menit. Pada Februari 2018, Github dibuat *offline* selama sekitar 10 menit oleh serangan *DDoS* yang memuncak pada 1,35 Tbps. Peristiwa serangan baru-baru ini menunjukkan meningkatnya intensitas serangan dan menunjukkan dampak parah yang terus penyerang timbulkan pada infrastruktur kritis (Liang dan Znati, 2019).

Dalam penelitian *machine learning* yang membahas tentang *DDoS*, tentu dibutuhkan sebuah data pelatihan untuk menunjang pembangunan model pelatihan. Data pelatihan disebut sebagai dataset merupakan data masa lalu yang telah dibuat atau digunakan oleh ahli dalam bidang penelitian tersebut. Sharafaldin dkk (2018) menyadari bahwa pentingnya kebenaran *dataset* untuk data pelatihan sehingga dilakukan evaluasi terhadap sebelas *dataset* sebelumnya yang ada sejak tahun 1998. Mereka mendapatkan hasil bahwa *dataset* di masa sebelumnya telah usang dan tidak dapat diandalkan kegunaannya dalam penelitian. Beberapa *dataset* dianggap kurang terdapat keragaman lalu lintas volume, selain itu beberapa *dataset* lainnya dianggap tidak dapat mencakup berbagai serangan, sementara yang lain

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

menganonimkan informasi paket dan *payload* yang tidak dapat mencerminkan tren saat ini. Penelitian tersebut menghasilkan sebuah *dataset* baru disebut CICIDS2017 yang dianggap telah memperbaiki kekurangan dari *dataset* sebelumnya.

Kemudian Panigrahi dan Borah (2018) melakukan Analisa pada *dataset* CICIDS2017, mereka menganggap dataset tersebut masih memiliki beberapa kekurangan. Penelitian dilakukan dengan menandai ulang dataset dengan memberikan label informasi yang disediakan oleh Canadian Institute Cybersecurity. Didapati beberapa kelas dianggap tidak seimbang, namun masalah tersebut telah dibenahi dengan langkah pelabelan ulang yang dilakukan.

2.2 *Random Forest*

Random forest merupakan pengembangan algoritma dari *Decision Tree* dengan menggunakan beberapa kumpulan dari *Decision Tree*, dimana setiap *Decision Tree* dilakukan pelatihan menggunakan sampel individu yang dikelompokkan ulang secara acak. Pada proses klasifikasi, individunya didasarkan pada *vote* dari suara terbanyak pada kumpulan populasi *tree*. *Random Forest* yang dihasilkan memiliki banyak *tree*, dan setiap *tree* dibangun dengan cara yang sama. *Tree* dengan variabel x akan dibangun sejauh mungkin dengan *tree* dengan variabel y. Dan dalam perkembangannya, sejalan dengan bertambahnya *dataset*, maka *tree* pun ikut berkembang. Penempatan *tree* yang saling berjauhan membuat apabila terdapat *tree* disekitar *tree* x berarti pohon tersebut merupakan perkembangan dari *tree* x (Saputra dkk, 2011).

Metode *Random Forest* dapat meningkatkan hasil *accuracy*, karena dalam membangkitkan simpul anak untuk setiap *node* dilakukan secara acak. Metode ini

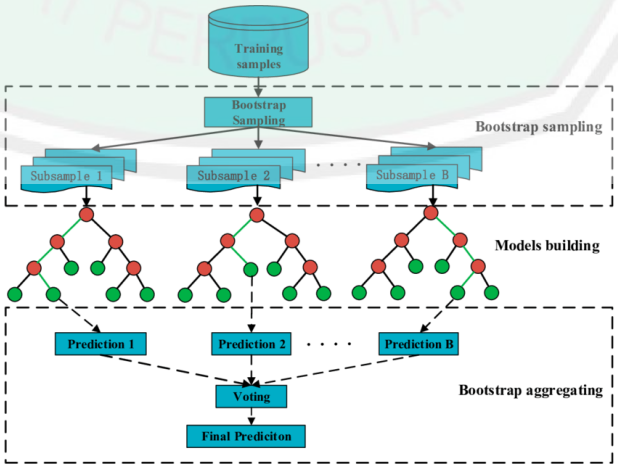
CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

digunakan untuk membangun *decision tree* yang terdiri dari *root node*, *internal node*, dan *leaf node* dengan mengambil atribut data secara acak sesuai ketentuan yang diberlakukan. *Root node* adalah simpul yang terletak paling atas, atau biasa disebut sebagai akar dari pohon keputusan. *Internal node* merupakan simpul percabangan, dimana *node* ini mempunyai keluaran minimal dua atau lebih dan hanya memiliki satu masukan. Sedangkan *leaf node* atau terminal *node* adalah simpul terakhir yang hanya memiliki satu masukan dan tidak mempunyai keluaran (Nugroho dan Emiliyawati, 2017).

Terdapat tiga aspek penting dalam metode *random forest* (Primajaya dan Sari, 2018), yaitu:

1. Melakukan *bootstrap sampling* untuk membangun beberapa pohon prediksi.
2. Masing-masing *tree* memprediksi dengan *predictor* secara acak.
3. *Random forest* melakukan prediksi dengan mengombinasikan hasil dari setiap pohon keputusan dengan cara pemilihan nilai mayoritas untuk klasifikasi atau rata-rata untuk regresi.

Sesuai pada Gambar 2.1 berikut ditampilkan gambaran alur *Random Forest* (Wang dkk, 2019).



Gambar 2.1 Alur *Random Forest*

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Alkasassbeh dkk (2016) melakukan penelitian deteksi *DDoS* menggunakan Teknik *data mining*, diantaranya yaitu *Random Forest*. Mereka memisahkan data secara acak menjadi 60% untuk pelatihan model dan 40% untuk pengujian. Pelatihan dilakukan dengan membangun 500 pohon. Mereka beranggapan bahwa banyaknya pohon tidak menentukan tingginya tingkat *accuracy* bahkan akan membuat waktu pelatihan lebih lama, maka dari itu penyempurnaan parameter random forest perlu diperhatikan dengan baik. Hasil pelatihan dengan *Random Forest* menghasilkan *accuracy* sebesar 98,02%.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB III

METODOLOGI PENELITIAN

3.1 Akuisisi Data

Pada sub-bab ini peneliti menjelaskan data yang digunakan sebagai objek dalam penelitian. Terdapat dua macam data dalam penelitian, yaitu data sekunder dan data primer. Kedua data memiliki peran yang sama, data sekunder merupakan *dataset* dari ahli sedangkan data primer merupakan data yang dibangun oleh peneliti. Setiap data akan dilakukan pembentukan data *training* maupun data *testing*, sebagian data dari data sekunder akan dijadikan sebagai data *training* yang berguna untuk membangun sebuah sistem model pelatihan dan sebagian yang lain dari data sekunder akan dijadikan sebagai data *testing* yang berguna untuk melakukan pengujian pada sistem model yang telah dibangun. Aturan yang sama berlaku pada data primer yang menjadikan sebagian data sebagai data *training* dan sebagian lainnya menjadi data *testing*.

Data primer merupakan data yang didapatkan langsung oleh peneliti berupa baris trafik jaringan. Untuk melakukan akuisisi data primer berupa trafik jaringan, perlu dilakukan beberapa langkah sebagai berikut:

a. Konfigurasi *Hacking Environment*

Akuisisi data primer dimulai dengan membangun sebuah lingkungan yang seakan-akan lingkungan tersebut merupakan lingkungan peretasan. Dalam praktik peretasan peneliti menggunakan sistem operasi BackBox versi 6 berbasis Ubuntu sebagai sistem operasi dari peretas. Sistem operasi BackBox terpasang pada *tools* VirtualBox. Hanya memasang sebuah sistem operasi tentu tidak cukup untuk

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

melakukan peretasan, dibutuhkan sebuah *tools* tambahan untuk dapat menjalankan praktik peretasan *DDoS* pada *server* target. Peneliti menggunakan sebuah *tools* yaitu Metasploit, sebuah *tools* yang berjalan pada sistem operasi berbasis Ubuntu yang salah satu fungsinya yaitu untuk menjalankan praktik peretasan *DDoS* pada suatu *server* target.

Selain digunakan untuk memasang sistem operasi peretas, VirtualBox juga digunakan untuk memasang sebuah *server* virtual yaitu Metasploitable2. Metasploitable2 inilah yang mana selanjutnya diperlakukan sebagai *server* tujuan. Metasploitable2 tentunya sesuai dengan praktik peretasan yang digunakan oleh peneliti karena berdasar pada fungsi awalnya Metasploitable2 ini yaitu sebagai tempat yang aman untuk menjalankan percobaan penetrasi dan penelitian keamanan (Metasploitable 2, 2020).

b. Simulasi Peretasan *DDoS*

Setelah *hacking environment* selesai terkonfigurasi, langkah selanjutnya yaitu melakukan simulasi peretasan dengan metode *DDoS*. VirtualBox digunakan untuk menjalankan *server* virtual yaitu Metasploitble2 dan sistem operasi peretas yaitu BackBox Ubuntu. Ketika Metasploitable2 berjalan di latar belakang sistem, peneliti akan membuka *web browser* Google Chrome sebagai penampil dari *server* virtual Metasploitable2. Di lain sisi, sistem operasi BackBox yang telah dijalankan akan digunakan oleh peneliti untuk menjalankan *tool* Metasploit, yaitu *tool* yang berfungsi untuk menjalankan perintah peretasan *DDoS*. Metasploit berjalan pada pada dua atau lebih *tab windows* yang berarti peretasan dijalankan oleh dua atau lebih *tool* Metasploit (bot) sehingga implementasi dari peretasan yang terdistribusi tercapai yaitu peretasan *Denial of Service* yang terdistribusi oleh bantuan beberapa

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

bot. Selain bertujuan untuk mengimplementasikan terdistribusinya *Denial of Service* pada *server*, beberapa bot ini bertujuan untuk memaksimalkan penetrasi peretasan sehingga target dapat lumpuh dengan waktu yang lebih singkat. Peretasan *DDoS* ditujukan kepada Metasploitable2 yang telah dijalankan sebelumnya.

c. Perekaman Lalu Lintas Jaringan

Disinilah kegunaan dari aplikasi Wireshark. Ketika proses peretasan *server* Metaploitable2 berlangsung, peretas memanfaatkan sumber daya dari *tool* Metasploit untuk terus menerus mengirim request untuk direspon oleh *server* Metasploitable2. Selama *response* lumpuh yang diharapkan oleh peretas dapat tercapai, Wireshark dijalankan untuk memantau lalu lintas jaringan yang berjalan pada server Metaploitable2 tersebut. Pada *tool* Wireshark, konfigurasi diatur untuk menjalankan *capturing* lalu lintas jaringan pada VirtualBox, hal ini disebabkan karena *server* Metasploitable2 berjalan diatas VirtualBox.

Selama proses peretasan berjalan, Wireshark menjalankan fungsinya untuk merekam (*capture*) lalu lintas jaringan antar *server* dengan *client*, dalam kasus ini yang bertindak sebagai *client* adalah tool Metasploit, yang mana tool ini menjalankan peran ganda yaitu sebagai *client* sekaligus peretas.

Langkah perekaman lalu lintas jaringan ini bertujuan untuk mendapatkan data pengujian, sehingga tidak cukup jika hanya mendapatkan data lalu lintas peretasan saja. Selain mendapatkan data peretasan berupa perekaman lalu lintas jaringan dari *request* Metasploit kepada *response* Metasploitable2, juga dibutuhkan sebuah data normal. Data normal didapatkan dari *request* normal pada *client* tanpa menggunakan perintah dari *tool* Metasploit, lalu lintas normal tersebut juga direkam oleh Wireshark yang kemudian diberi diperlakukan sebagai lalu lintas normal.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Semua data lalu lintas jaringan yang terekam oleh Wireshark kemudian disimpan dalam format data PCAP.

d. Ektraksi Lalu Lintas Jaringan

Setelah dilakukan perekaman lalu lintas jaringan, semua data perekaman disimpan dengan format PCAP. Namun format PCAP belum sesuai dengan format semestinya dalam proses pelatihan data, sehingga perlu untuk dilakukan ekstraksi data menjadi sebuah data yang sesuai dengan proses pelatihan data, yaitu format data CSV. *Tool* yang memiliki fungsi untuk merubah data PCAP menjadi CSV adalah CICFlowMeter. CICFlowMeter sendiri merupakan sebuah generator dan alat penganalisa untuk mendeteksi anomali jaringan, yang telah banyak digunakan pada *dataset* keamanan siber seperti Android *Adware-General Malware dataset* (CICAAGM2017), IPS/IDS (CICIDS2017), dan Android *Malware dataset* (CICAndMal2017) (Ahlaskari, 2020).

CICFlowMeter tidak dapat berjalan dengan sendirinya, dibutuhkan *tool* lain untuk menjalan CICFlowMeter ini. Terdapat dua opsi untuk menjalankan CICFlowMeter yaitu menggunakan Intellij IDEA milik JetBrains atau menggunakan Eclipse, peniliti menggunakan Intellij IDEA. CICFlowMeter berjalan pada terminal Intellij IDEA, namun masih diperlukan konfigurasi tambahan dalam terminal IDE yaitu pemasangan Apache Maven. Setelah pemasangan Apache Maven selesai, maka CICFlowMeter dapat dijalankan pada terminal Intellij IDEA. Setelah pemasangan CICFlowMeter tentu *tool* ini difungsikan untuk merubah data berformat PCAP menjadi CSV.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

e. Pelabelan

Data perekaman lalu lintas jaringan telah selesai didapatkan, dan telah diubah menjadi data berformat CSV, data format CSV ini dapat dirubah kembali menjadi data berformat XLSX jika dalam penelitian menggunakan data berformat XLSX. Data yang didapatkan dari hasil simulasi tersebut masih belum memiliki label untuk membedakan mana yang termasuk data lalu lintas peretasan dan mana data lalu lintas normal. Peneliti melakukan pelabelan dengan cara manual, yaitu mempertimbangkan waktu kapan simulasi dilakukan. Peneliti melakukan simulasi secara terpisah antara simulasi peretasan dan simulasi normal, sehingga diharapkan mendapat lalu lintas yang sesuai dengan aktifitas yang dilakukan tanpa tercampur dengan aktifitas yang tidak diharapkan. Pelabelan merupakan langkah terakhir dalam akuisisi data trafik jaringan.

Untuk data yang lain yaitu data sekunder. Data sekunder merupakan data yang dioperoleh dari sumber yang sudah ada. Dalam penelitian ini peniliti memutuskan untuk menggunakan data sekunder yang disebut *Dataset* CICIDS2017 dari Canadian Institute for Cybersecurity University of New Brunswick di Fredericton Kanada. CICIDS2017 berisi trafik jinak dan serangan siber secara umum, yang menyerupai data dunia nyata yang sebenarnya berformat PCAP serta data hasil analisis lalu lintas jaringan menggunakan CICFlowMeter dengan format CSV (CICFlowMeter, 2020). Peneliti menggunakan data berformat CSV/XLSX yang telah sesuai oleh persyaratan proses selanjutnya. Berikut adalah sampel dataset yang diambil dari *dataset* CICIDS2017.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

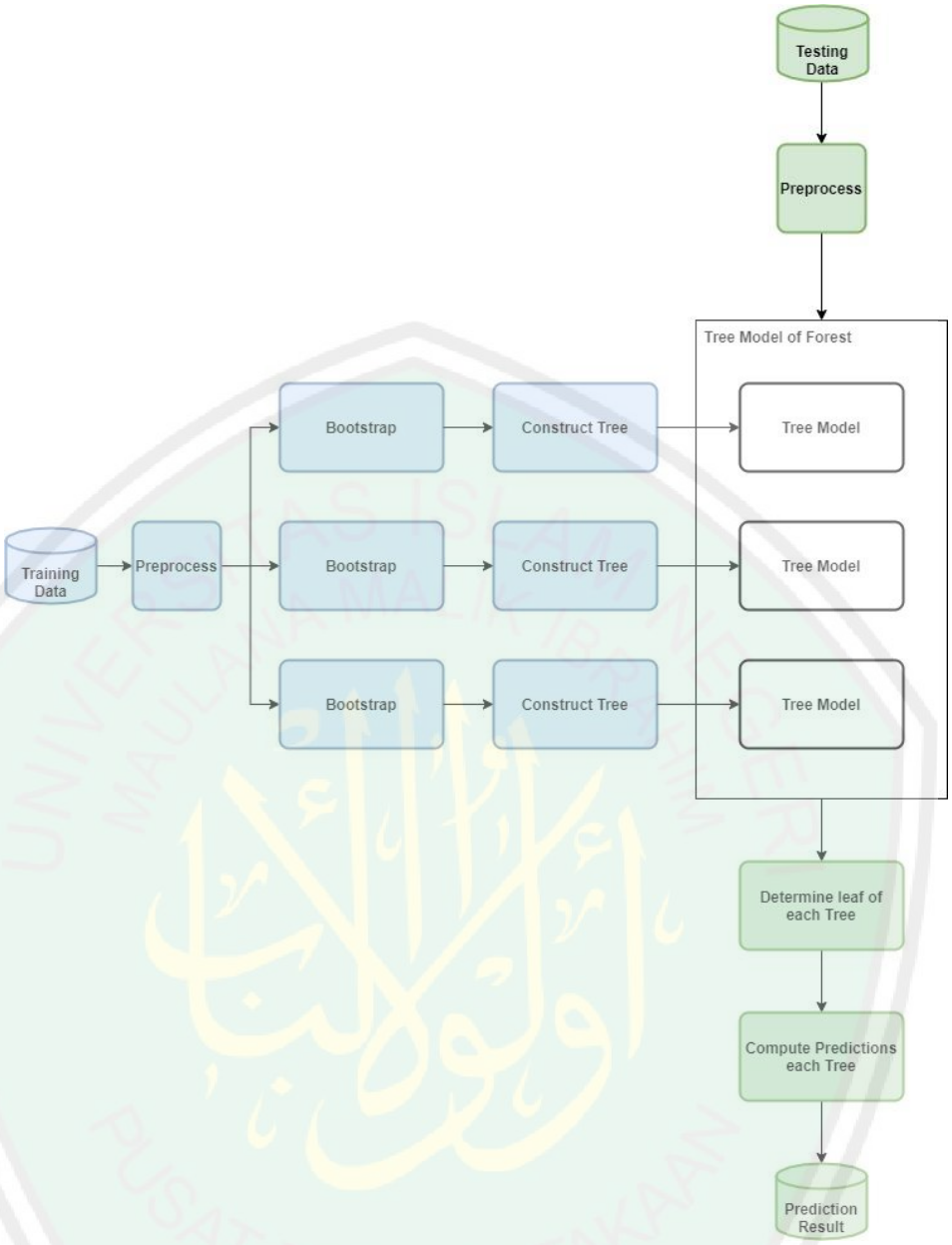
Tabel 3.1 Sampel *Dataset* CICIDS2017

No	Total Length of Fwd Packets	Fwd Packet Length Max	Fwd Packet Length Mean	Avg Fwd Segment Size	Subflow Fwd Bytes	Init Win bytes forward	Act data pkt fwd	Label
1	12	6	6	6	12	32	1	*BENIGN*
2	6	6	6	6	6	30	0	*BENIGN*
3	59	53	29.5	29.5	59	1026	1	*BENIGN*
4	6	6	6	6	6	1026	0	*BENIGN*
5	26	20	8.666.666.667	8.666.666.667	26	8192	2	*DDoS*
6	24	6	6	6	24	256	3	*DDoS*
7	26	20	8.666.666.667	8.666.666.667	26	8192	2	*DDoS*
8	56	20	7	7	56	256	6	*DDoS*

3.2 Perancangan Sistem

Pada bab ini membahas penjelasan tahapan perancangan sistem penelitian seperti yang tercantum pada Gambar 3.1 berikut.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 3.1 Blok Diagram Perancangan Sistem

Dari gambar blok diagram perancangan sistem, ditunjukkan bahwa penelitan dimulai dengan memisahkan set data menjadi dua bagian yaitu data pelatihan dan data pengujian. Pengolahan data pelatihan bertujuan untuk membangun sebuah model pelatihan pada sistem. Langkah pertama dari pembentukan model pelatihan sistem adalah dengan melakukan praproses pada data pelatihan, data pelatihan yang awalnya terdiri dari kumpulan data dengan rentang

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

yang tidak beraturan maka pada tahap praproses dilakukan normalisasi yaitu perubahan rentang data menjadi suatu skala yang sama. Selanjutnya yaitu dilakukan pembentukan sebuah *bootstrap* pada data yang telah dinormalisasi, *bootstrap* yaitu melakukan sampel ulang peletakan data asli pada sub sampel baru. Kemudian dari sub sampel dibentuklah sebuah pohon keputusan. Pada metode *Random Forest* dibutuhkan sekumpulan pohon keputusan yang berperan sebagai sistem model pelatihan.

Dari kumpulan pohon keputusan yang terbentuk itulah dimasukkan sebuah data pengujian. Pada data pengujian dilakukan normlisasi dengan proses yang sama pada data pelatihan. Data pengujian yang telah dinormalisasi maka selanjutnya dimasukkan pada model pelatihan. Hasil yang didapatkan dari pemasukkan data pengujian pada model pelatihan adalah nilai *leaf* (daun) pada setiap pohon keputusan. Nilai *leaf* inilah yang nantinya akan dikumpulkan pada *list* dan diambil mayoritas nilai yang sering muncul, mayoritas nilai yang sering muncul selanjutnya disimpulkan sebagai hasil prediksi dari sistem.

3.2.1 Praproses Data

Data yang didapatkan oleh peniliti tidak serta merta dapat langsung diolah untuk pemodelan pelatihan. Maka sebelum melakukan pemodelan, data primer yang berjumlah 533 baris data terdiri dari 267 sebagai data *training* dan 266 sebagai data *testing* sekaligus data sekunder yang berjumlah 225745 baris data terdiri dari 56436 sebagai data *training* dan 169309 sebagai data *testing*, dari kedua set data diperiksa terlebih dahulu sehingga semua data dapat terolah dan kinerja penelitian dapat berjalan sesuai prosedur. Langkah yang dilakukan dalam tahap praproses adalah normalisasi data numerik. Normalisasi ini bermaksud untuk merubah data

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

numerik yang tersedia menjadi suatu skala yang sama. Perhitungan normalisasi berdasarkan pada persamaan 3.1 berikut.

$$normalisasi(x) = \frac{x_i - x_i min}{x_i \max - x_i min} (new\_\max - new\_min) + new\_min \quad (3.1)$$

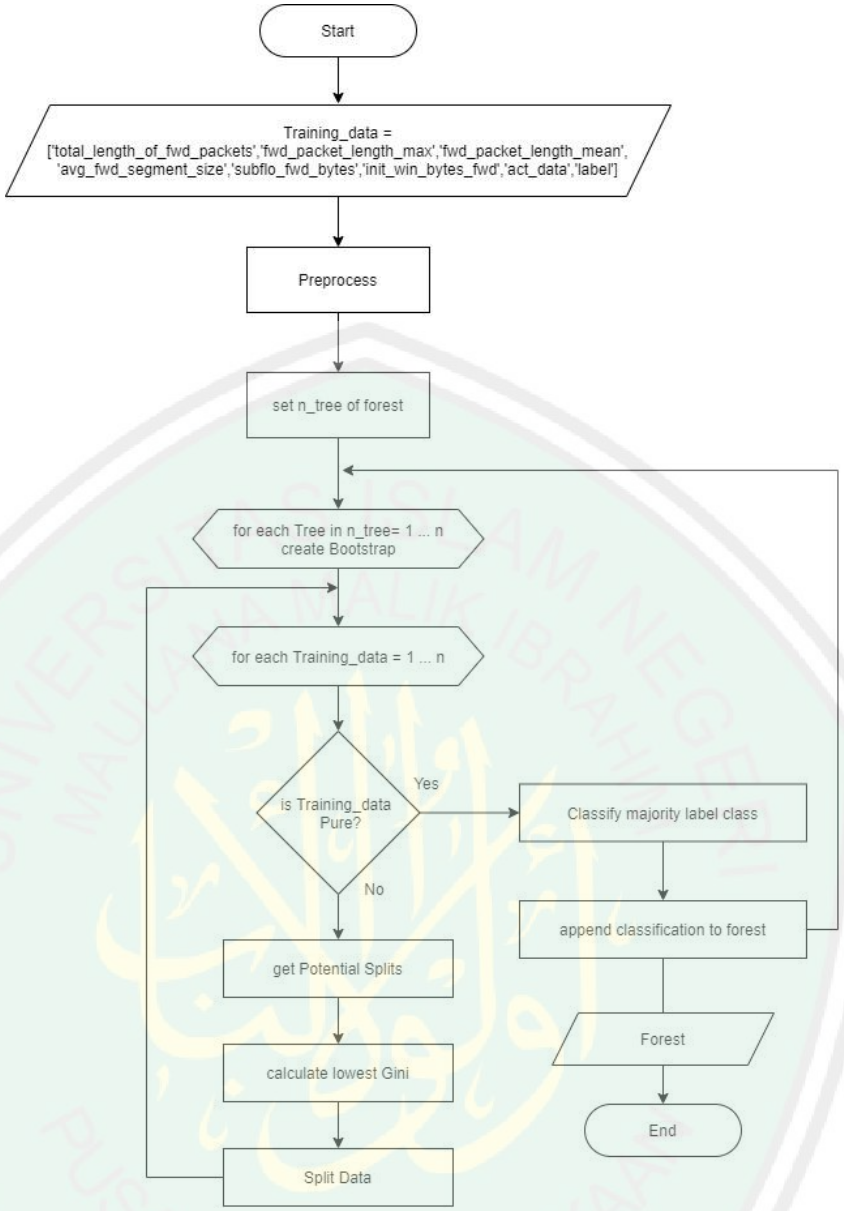
Dimana x_i adalah data ke i, $x_i \max$ dan $x_i min$ adalah data maksimum dan minimum pada data ke *i*, sedangkan *new_max* dan *new_min* adalah nilai maksimum dan minimum yang diharapkan.

3.2.2 *Random Forest*

3.2.2.1 *Random Forest* untuk Pembuatan Mode

Untuk membuat model menggunakan *Random Forest* perlu dibangun sebuah langkah yang runtut dan teratur sesuai dengan Gambar 3.2 berikut.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 3.2 *Flowchart Random Forest* untuk Pembuatan Model

Sesuai gambar *flowchart Random Forest* untuk pembuatan model pelatihan dijelaskan langkah-langkah pembuatan model pelatihan pada sistem. Tahap awal pembuatan model menggunakan *Random Forest* adalah dengan melakukan *resampling* atau melakukan pengambilan *sample* ulang secara acak pada *dataset* yang telah tersedia, dalam *Random Forest* istilah *resampling* memiliki arti yang sama dengan *Bootstrap*. Untuk melakukan *Bootstrap*, dataset perlu disiapkan yang

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

kemudian akan dilakukan pengambilan *sample* ulang secara acak. Kolom dalam set data tetap dijaga sesuai data asli, sedangkan baris pada dataset diacak dan diperbolehkan untuk mengambil baris yang sama pada set data untuk diletakkan pada *sample* data yang baru.

Setelah didapatkan pembentukan sekumpulan *Bootstrap* atau *sample* data yang baru, langkah selanjutnya yaitu dengan membuat pohon pada setiap *Bootstrap* tersebut. Layaknya *Decision Tree*, pohon terbentuk atas tiga hal yaitu *root node* (puncak pohon), *internal node* (cabang pohon), dan *leaf node* (akhir pohon). Pada penelitian ini, pembangunan pohon keputusan ditentukan dengan menggunakan metode Gini *Index*.

Langkah pertama yaitu dengan mendapatkan nilai impuriti, perhitungan gini *impurity* sesuai dengan persamaan 3.2 berikut.

$$Impurity = 1 - \sum P_i^2 \quad (3.2)$$

Dimana P_i adalah probabilitas nilai label yang muncul pada kolom yang bersangkutan.

Sedangkan untuk mendapatkan nilai Gini *Index* dapat dilakukan sesuai perhitungan persamaan 3.3 berikut.

$$Gini(x) = 1 - \sum \frac{n_i}{n} * Impurity \quad (3.3)$$

Dimana n_i adalah banyaknya data partisi pada himpunan, dan n adalah banyak seluruh himpunan.

Berikut disajikan perhitungan manual Gini *Impurity* dan Gini *Index* dengan kasus perhitungan data kolom *Total Length of Fwd Packets* pada Tabel 3.2.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Tabel 3.2 Data Perhitungan

No	Total Length of Fwd Packets	Label
1	12	*BENIGN*
2	12	*BENIGN*
3	6	*BENIGN*
4	59	*BENIGN*
5	6	*BENIGN*
6	26	*DDoS*
7	24	*DDoS*
8	26	*DDoS*
9	56	*DDoS*
10	26	*DDoS*

a. Langkah pertama yaitu dengan mengurutkan data pada kolom terpilih secara menaik dari nilai terkecil. Sesuai pada tabel 3.3 berikut.

Tabel 3.3 Mengurutkan Data pada Kolom

No	Total Length of Fwd Packets	Label
1	6	*BENIGN*
2	6	*BENIGN*
3	12	*BENIGN*
4	12	*BENIGN*
5	24	*DDoS*
6	26	*DDoS*
7	26	*DDoS*
8	26	*DDoS*
9	56	*DDoS*
10	59	*BENIGN*

b. Mengumpulkan data yang bernilai sama kemudian menghitung rerata setiap data pada baris yang saling berdekatan. Sesuai pada tabel 3.4 berikut.

Tabel 3.4 Rerata Data yang Berdekatan

No	Data	Rerata dengan Data Baris Sebelumnya
1	6	
2	12	9

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

3	24	18
4	26	25
5	56	41
6	59	67,5

c. Partisi nilai kolom sesuai rerata pada setiap baris yang berdekatan, dan bergantung pada nilai label yaitu *BENIGN* dan *DDOS*. Sesuai pada tabel 3.5 berikut.

Tabel 3.5 Data Partisi

No	Partisi Data	BENIGN	DDOS	TOTAL ni	TOTAL n
1	<=9	2	0	2	
2	>9	3	5	8	10
3	<=18	4	0	4	
4	>18	1	5	6	10
5	<=25	4	1	5	
6	>25	1	4	5	10
7	<=41	4	4	8	
8	>41	1	1	2	10
9	<=67,5	5	5	10	
10	>67,5	0	0	0	10

d. Menghitung nilai gini *impurity* sekaligus gini *index* pada setiap data. Dimulai pada data yang memiliki nilai terkicil.

$$Impurity(<=9) = 1 - \left(\left(\frac{2}{2}\right)^2 + \left(\frac{0}{2}\right)^2\right)$$

$$= 1 - (1 + 0)$$

$$= 0$$

$$Impurity(>9) = 1 - \left(\left(\frac{3}{8}\right)^2 + \left(\frac{5}{8}\right)^2\right)$$

$$= 1 - (0{,}14 + 0{,}39)$$

$$= 0{,}46875$$

$$Gini(9) = \left(\frac{2}{10} \cdot 0\right) + \left(\frac{8}{10} \cdot 0.46875\right)$$

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

= 0 + 0,375

= 0,375

e. Ulangi perhitungan gini *impurity* dan gini index pada setiap baris data.

f. Hasil perhitungan keseluruhan ditampilkan pada tabel 3.6 berikut.

Tabel 3.6 Hasil Perhitungan Gini *Impurity* dan Gini *Index*

No	Partisi Data	BENIGN	DDOS	TOTAL ni	TOTAL n	GINI IMPURITY	GINI INDEX
1	<=9	2	0	2		0	
2	>9	3	5	8	10	0,46875	0,375
3	<=18	4	0	4		0	
4	>18	1	5	6	10	0,277777778	0,166666667
5	<=25	4	1	5		0,32	
6	>25	1	4	5	10	0,32	0,32
7	<=41	4	4	8		0,5	
8	>41	1	1	2	10	0,5	0,5
9	<=67,5	5	5	10		0,5	
10	>67,5	0	0	0	10	0	0,5

Nilai gini *index* berguna sebagai nilai *splitting* sebuah pohon keputusan, dengan memberikan nilai *splitting* maka akan mudah didapatkan klasifikasi dari nilai *leaf* suatu pohon keputusan. *Leaf* dari setiap pohon keputusan akan dikumpulkan menjadi satu *list* dan didapatkan mayoritas nilai yang sering keluar dan akan menjadi nilai akhir prediksi. *Script* program dari proses *Random Forest* untuk pembentukan model pelatihan diperlihatkan pada Gambar 3.3 berikut.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

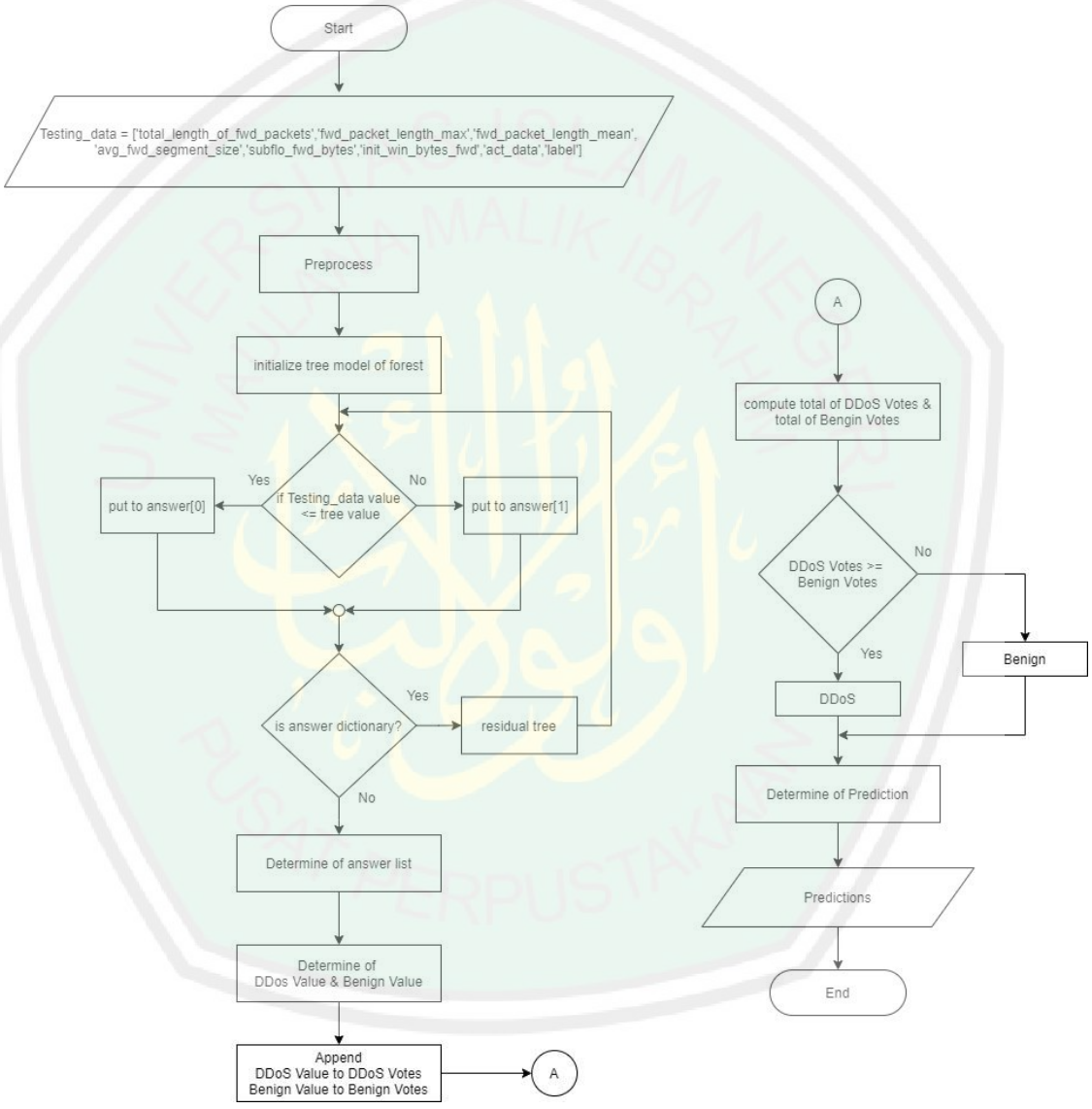
```
# Decision tree algorithm
def decision_tree_algorithm(df, counter=0, min_samples=0, max_depth=5,
random_subspace=None):
    # data preparation
    if counter == 0:
        global COL_HEADERS, FEATURE_TYPES
        COL_HEADERS = df.columns
        FEATURE_TYPES = determine_type_of_feature(df)
        data = df.values
    else:
        data = df
    # recursive part
    else:
        counter += 1
        #helper function
        potential_splits = get_potential_splits(data, random_subspace)
        split_col, split_value, _ = determine_best_split(data, potential_splits)
        data_below, data_above = split_data(data, split_col, split_value)
        #check for empty data
        if len(data_below) == 0 or len(data_above) == 0:
            classification = clasify_data(data)
            return classification
        #determine question
        feature_name = COL_HEADERS[split_col]
        type_of_feature = FEATURE_TYPES[split_col]
        if type_of_feature == "continuous":
            question = "{} <= {}".format(feature_name, split_value)
        #feature categorical
        else:
            question = "{} = {}".format(feature_name, split_value)
        #instantiate sub_tree
        sub_tree = {question: []}
        #find answer(recursion)
        yes_answer = decision_tree_algorithm(data_below, counter, min_samples,
max_depth, random_subspace)
        no_answer = decision_tree_algorithm(data_above, counter, min_samples,
max_depth, random_subspace)
        if yes_answer == no_answer:
            sub_tree = yes_answer
        else:
            sub_tree[question].append(yes_answer)
            sub_tree[question].append(no_answer)
    return sub_tree
# TODO Bootstrapping
def bootstrapping(data, n_bootstrap):
    bootstrap_indices = np.random.randint(low=0, high=len(data), size=n_bootstrap)
    df_bootstrapped = data.iloc[bootstrap_indices]
    return df_bootstrapped
    # base case
    if (check_purity(data)) or (len(data) < min_samples) or (counter == max_depth):
        classification = clasify_data(data)
        return classification
# TODO Random Forest Model
def random_forest_algorithm(data, n_trees, n_bootstrap, n_features, dt_max_depth):
    forest = []
    for i in range(n_trees):
        df_bootstrapped = bootstrapping(data, n_bootstrap)
        tree = decision_tree_algorithm(df_bootstrapped, max_depth=dt_max_depth,
random_subspace=n_features)
        forest.append(tree)
    return forest
```

Gambar 3.3 *Script* Program Proses *Random Forest* untuk Pembuatan Model

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

3.2.2.2 *Random Forest* untuk Deteksi Serangan

Setelah dilakukan pembuatan model dengan *Random Forest*, langkah selanjutnya yaitu dengan melakukan percobaan deteksi serangan *DDoS* pada model tersebut. Seperti tercantum dalam Gambar 3.4 merupakan *Flowchart Random Forest* untuk Deteksi Serangan pada data primer.



Gambar 3.4 *Flowchart Random Forest* untuk Deteksi Serangan

Menurut gambar *flowchart Random Forest* untuk deteksi serangan dilakukan proses pemasukan data *testing* pada model sepanjang banyaknya *tree* yang telah dibuat sebelumnya. Tentunya data testing yang dimasukkan pada model

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

deteksi adalah data yang telah dilakukan praproses yaitu normalisasi data. Data yang telah dimasukkan pada model deteksi akan menghasilkan sebuah hasil prediksi yaitu kumpulan atau *list* dari *leaf* pohon keputusan. *Leaf* dari pohon keputusan kemudian akan dipisahkan menjadi data *BENIGN* dan data *DDoS* yang selanjutnya akan didapatkan mayoritas data yang paling sering muncul pada *list leaf* tersebut. Hasil dari mayoritas *list leaf* berperan sebagai hasil deteksi lalu lintas *Random Forest* untuk deteksi serangan. *Script* program dari proses *Random Forest* untuk deteksi serangan ditampilkan pada Gambar 3.5 berikut.

```
def predict_example(example, tree):
  question = list(tree.keys())[0]
  feature_name, comparison_operator, value = question.split(" ")

  # ask question
  if comparison_operator == "<=":
      if example[feature_name] <= float(value):
        answer = tree[question][0]
      else:
        answer = tree[question][1]
  #feature categorical
  else:
      if str(example[feature_name]) == value:
          answer = tree[question][0]
      else:
          answer = tree[question][1]
  # base case
  if not isinstance(answer, dict):
    return answer
  # recursive part
  else:
    residual_tree = answer
    return predict_example(example, residual_tree)

# All example of the test data
def decision_tree_predictions(df, tree):
    predictions = df.apply(predict_example, args=(tree,), axis=1)
    return predictions

# TODO Random Forest Prediction
def random_forest_predictions(data, forest):
    df_predictions = {}
    for i in range(len(forest)):
        col_name = "tree_{}".format(i)
        predictions = decision_tree_predictions(data, tree=forest[i])
        df_predictions[col_name] = predictions
    df_predictions = pd.DataFrame(df_predictions)
    random_forest_predictions = df_predictions.mode(axis=1)[0]

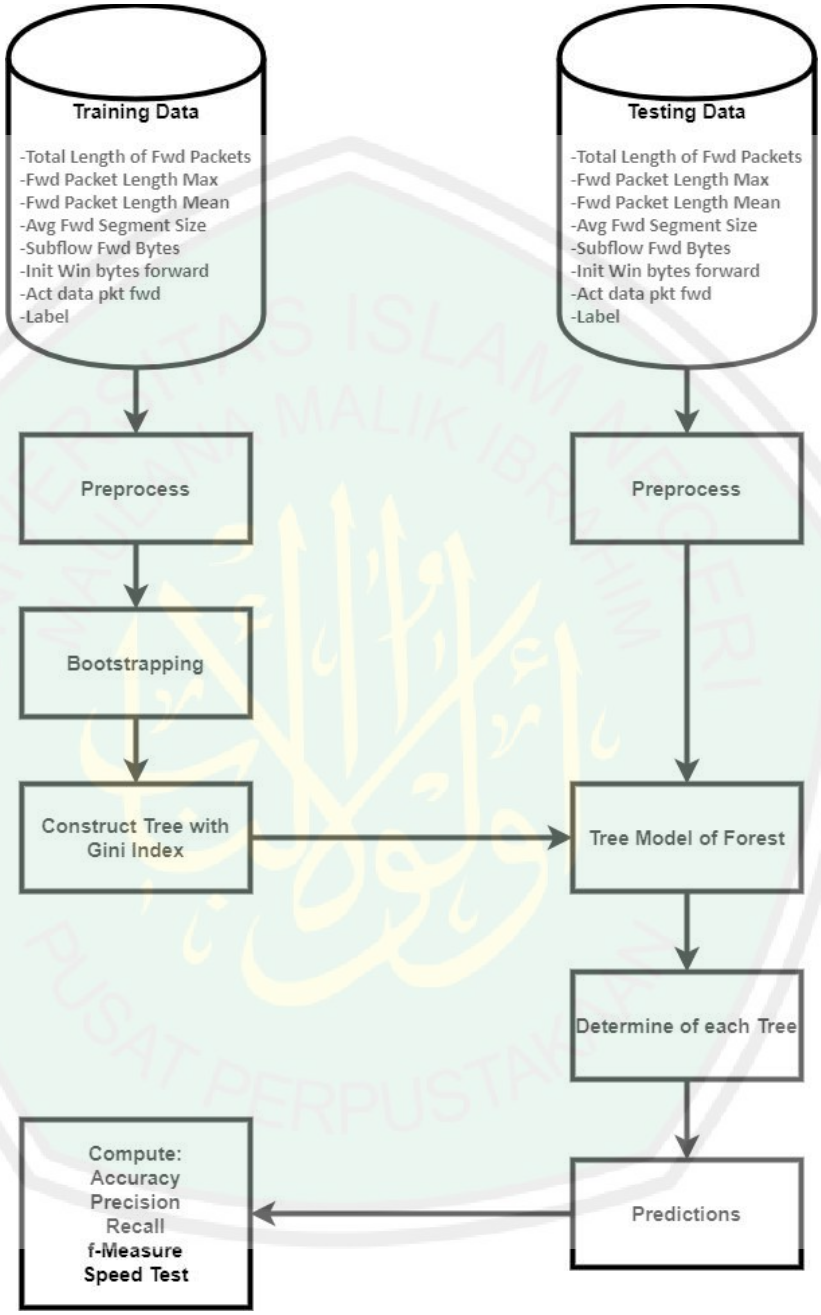
    return random_forest_predictions
```

Gambar 3.5 *Script* Program Proses *Random Forest* untuk Deteksi Serangan

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

3.3 Kerangka Kerja Konseptual

Pada sub-bab ini peneliti menampilkan kerangka kerja konseptual, sesuai dengan Gambar 3.6 berikut



Gambar 3.6 Kerangka Kerja Konseptual

Sesuai Gambar 3.6 dapat diketahui konsep kerangka kerja dalam penelitian, konsep kerangka kerja dalam penelitian ini memiliki beberapa poin perbedaan dengan penelitian sebelumnya. Berikut disajikan perbedaan dengan penelitian sebelumnya.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Tabel 3.7 Perbedaan dengan Penelitian Sebelumnya

No.	Pengarang (Tahun)	Kerangka Kerja	Perbedaan
1.	Alkasassbeh dkk (2016)	a. Menggunakan tiga algoritma yang terkenal, yaitu *Multilayer Perceptron* (*MLP*), *Random Forest* dan *Naïve Bayes.* b. Menggunakan *dataset* baru yang berisi empat jenis serangan *DDoS*, yaitu HTTP *Fload*, SIDDoS, UDP *Flood*, dan *Smurf*. c. Mengelompokkan keluaran penelitian pada empat kelas, yaitu UDP-*Flood*, Smurf, SIDDoS dan HTTP-*Flood* d. Mengukur accuracy, precision, dan *recall*.	a. Menggunakan satu algoritma yaitu *Random Forest* dengan *split tree* Gini *Index*. b. Menggunakan *Dataset* CICIDS2017 sebagai data sekunder dan data trafik jaringan sebagai data primer yang keduanya berisi trafik serangan *DDoS* dan trafik *Benign* (normal). Dengan parameter *Total Length of Fwd Packets, Fwd Packet Length Max, Fwd Packet Length Mean, Avg Fwd Segment Size, Subflow Fwd Bytes, Init Win bytes forward, Act data pkt fwd dan Label*. c. Mengelompokkan keluaran penelitian pada dua kelas, yaitu trafik serangan (*DDoS*) dan trafik normal (*Benign*). d. Mengukur *accuracy*, *precision*, *recall*, *f-measuere* dan durasi *Random Forest* dalam mendeteksi serangan *DDoS*.
2.	Muhammad dkk (2017)	a. Menggunakan algoritma *Neural Network* dengan fungsi *Fixed Moving Average Window*. b. Menggunakan satu jenis data, yaitu data sekunder berupa dataset CAIDA *DDoS Attack* 2007 c. Mengelompokkan keluaran penelitian pada tiga kategori deteksi, yaitu normal, *slow DDoS*, Dan *DDoS*. d. Mengukur prosentase pengenalan deteksi.	a. Menggunakan algoritma *Random Forest* dengan fungsi *split tree* Gini *Index*. b. Menggunakan dua jenis data, yaitu data sekunder *dataset* CICIDS2017 dan data primer berupa trafik yang didapatkan dari simulasi serangan peneliti. c. Pengelompokan klasifikasi penelitian dengan dua klasifikasi, yaitu *DDoS* dan *Benign*. d. Mengukur *accuracy*, *precision*, *recall*, *f-measuere* dan durasi *Random Forest* dalam mendeteksi serangan *DDoS*.
3.	Liang dan Znati (2019)	a. Menggunakan metode berbasis *Machine Learning* dengan berbagai jenis algoritma, diantaranya adalah *Naïve Bayes*, *Decision Tree*, *Support Vector Machine* dan *Artificial Neural Network*. b. Menggunakan berbagai data sekunder, diantaranya adalah	a. Hanya menggunakan algoritma *Random Forest ensamble learning*. b. Menggunakan dua jenis data, yaitu data sekunder *dataset* CICIDS2017 dan data primer berupa trafik yang didapatkan dari simulasi serangan peneliti.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

		dataset DARPA 1999, DARPA 2000, CAIDA 2007, dan LLDOS. c. Melakukan evaluasi pada "pembangunam blok" dari skema deteksi dan pencegahan *DDoS* yang cerdas.	c. Membangun pohon model berbasis *Random Forest* untuk deteksi serangan *DDoS*.
4.	Sihombing dkk (2019)	a. Menggunakan algoritma SVM *Classifier*. b. Menggunakan data primer, yaitu peneliti mengumpulkan *traffic* pada jaringan yang akan dibangun. Dengan kata lain peneliti melakukan akuisisi data yang bersumber dari *traffic* yang dibangun sendiri. c. Mengukur *accuracy* deteksi.	a. Menggunakan algortima *Random Forest*. b. Peneliti menggunakan data primer sekaligus data sekunder. Data primer berisi trafik jaringan yang dibangun dari hasil simulasi serangan, sedankan data sekunder diambil dari dataset CICIDS2017. c. Mengukur *accuracy*, *precision*, *recall*, *f-measure* dan durasi deteksi *DDoS* menggunakan *Random Forest*

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB IV

UJI COBA DAN PEMBAHASAN

4.1 Skenario Uji Coba

4.1.1 Akuisisi Data

Pada sub bab ini peneliti menjelaskan langkah-langkah untuk mendapatkan data primer maupun data sekunder yang digunakan dalam penelitian. Peneliti mendapatkan data primer dengan cara melakukan simulasi kasus, simulasi dilakukan pada *server hackable* yang memang digunakan untuk melakukan praktek simulasi serangan siber yang mana dalam kasus penelitian ini serangan siber yang digunakan adalah serangan siber berjenis *Distributed Denial of Service* (*DDoS*).

Adapun langkah-langkah yang dilakukan oleh peneliti untuk mendapatkan data primer adalah sebagai berikut:

a. Konfigurasi *Hacking Environment*

Langkah yang pertama adalah membangun sebuah lingkungan peretasan yang mirip dengan lingkungan praktek peretasan yang sebenarnya. Peneliti membutuhkan sebuah *virtual machine* yang berguna untuk menjalankan sistem operasi tambahan dan *server hackable* untuk simulasi peretasan. *virtual machine* yang digunakan adalah VirtualBox, dari VirtualBox inilah peneliti akan menjalankan sistem operasi tambahan yang berperan sebagai sistem operasi peretas sekaligus peneliti akan menjalankan *server hackable* yang aman untuk diretas.

Vitual machine VirtualBox berguna untuk menjalankan sistem operasi tambahan sebagai sistem operasi penyerang yaitu BackBox v6 dan *server hackable*

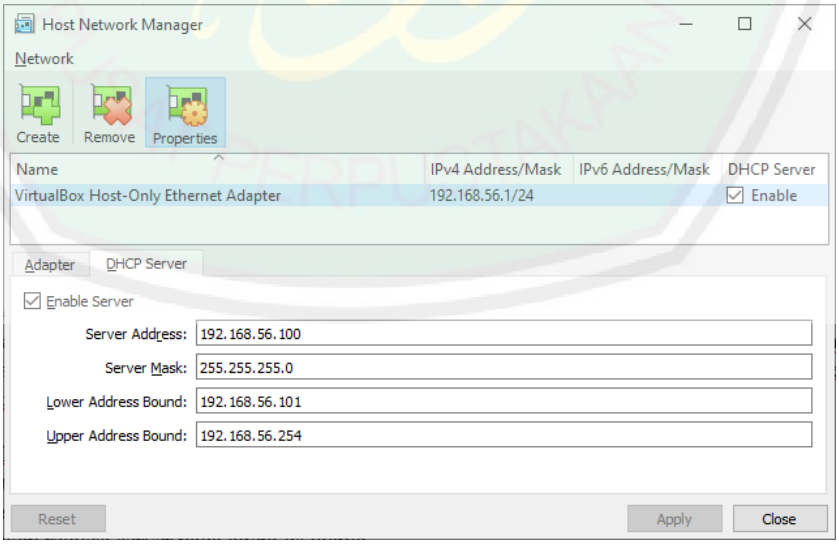
CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

yaitu Metasploitable2. Berikut Gambar 4.1 menampilkan halaman muka VirtualBox yang telah terpasang Backbox dan Metasploitble.



Gambar 4.1 Tampilan Halaman Muka VirtualBox

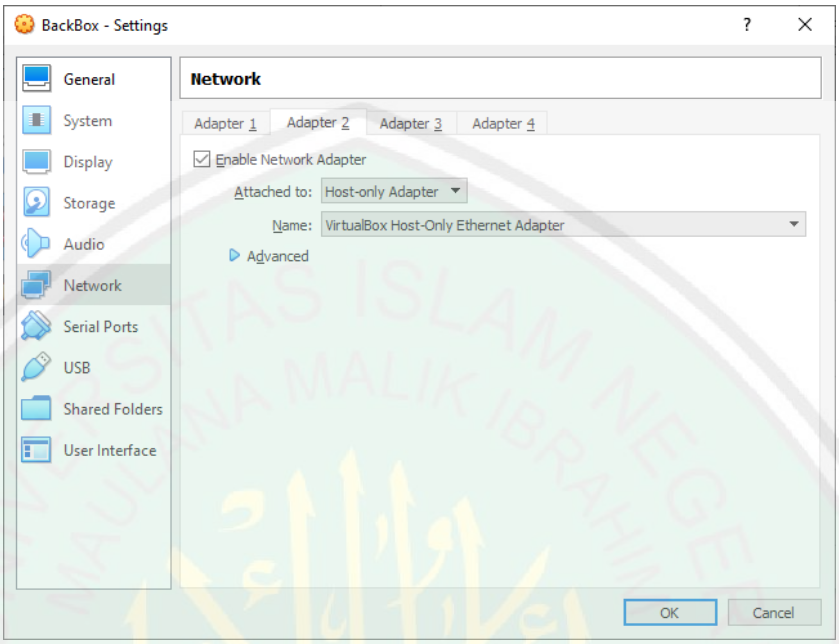
Langkah selanjutnya yaitu mengatur jaringan pada *virtual machine* sehingga semua BackBox dan Metasploitable2 dapat berjalan dalam satu jaringan yang sama. Pada menu *Berkas* dalam halaman muka aplikasi VirtualBox pilih *setting Host Network Manager*. Tambahkan *Host-Only Ethernet Adapter* dan centang *enable* pada bilah "*DHCP Server*" seperti pada Gambar 4.2 berikut.



Gambar 4.2 Pengaturan *Host Network Manager*

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Kemudian melakukan konfigurasi *network* pada BackBox dan Metasploitable2. Pilih BackBox > *Settings* > *Network*, pada bilah *Adapter* centang *Enable Network Adapter* kemudian *Attached to Host-only Adapter*.

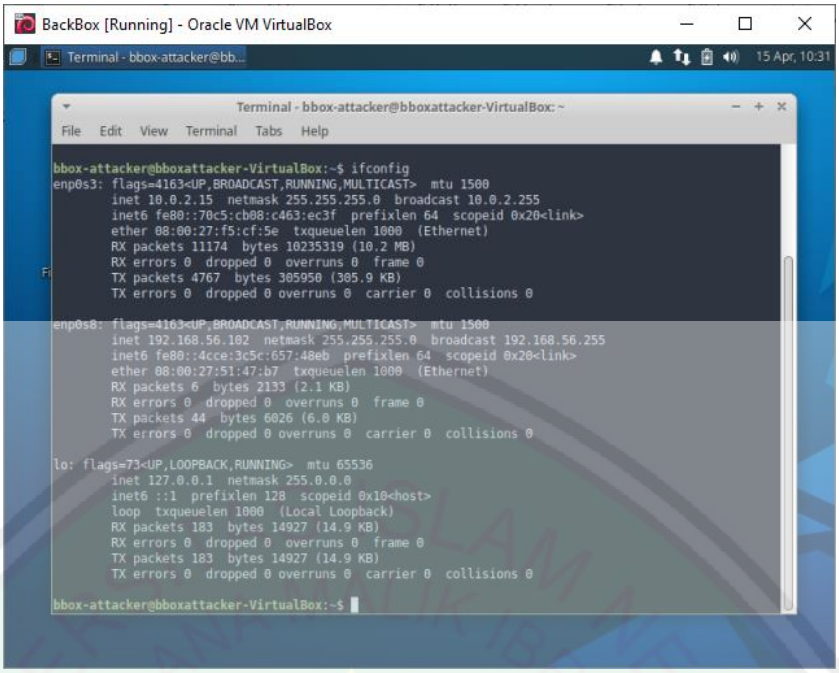


Gambar 4.3 Konfigurasi *Network Settings*

Konfigurasi *Network Settings* tersebut dilakukan pada Backbox sekaligus pada Metasploitable2. Setelah melalui langkah konfigurasi pada *virtual machine* tersebut, selanjutnya yaitu menjalankan sistem operasi penyerang untuk BackBox dan *server hackable* Metasploitable2.

Sesuai Gambar 4.4 berikut adalah tampilan pada sistem operasi BackBox yang akan berperan sebagai penyerang dalam jaringan.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

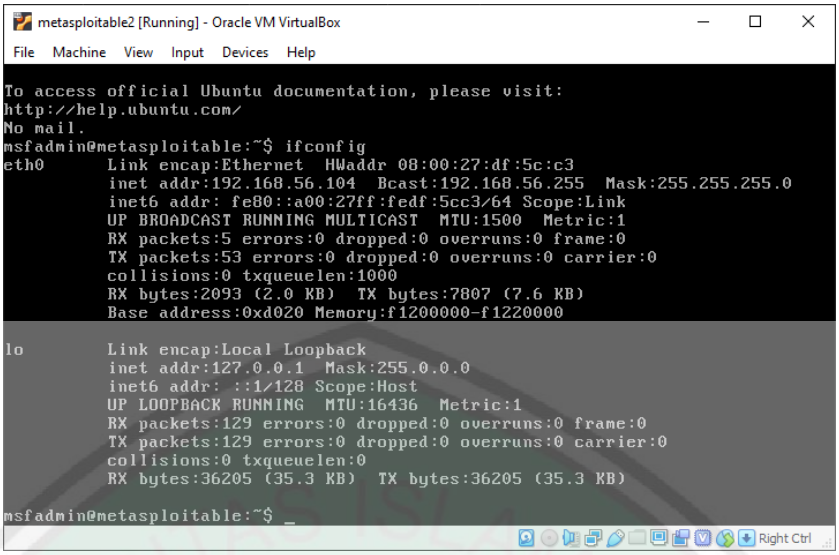


Gambar 4.4 *IP Address* BackBox

Dengan menggunakan perintah “ifconfig” pada Terminal BackBox dapat diketahui bahwa sistem operasi BackBox memiliki *IP address* 192.168.56.102.

Langkah selanjutnya yaitu menjalankan *server* Metasploitable2, hal ini bertujuan untuk mendapatkan *IP address* yang kemudian *IP address* tersebut akan berguna sebagai alamat akses terhadap *server* Metasploitable2. Dengan menjalankan perintah “ifconfig” pada Terminal Metasploitable2 dapat diketahui pula bahwa *IP address* dari *server* Metasploitable2 adalah 192.168.56.104 sesuai dengan Gambar 4.5 berikut.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 4.5 *IP Address* Metasploitable2

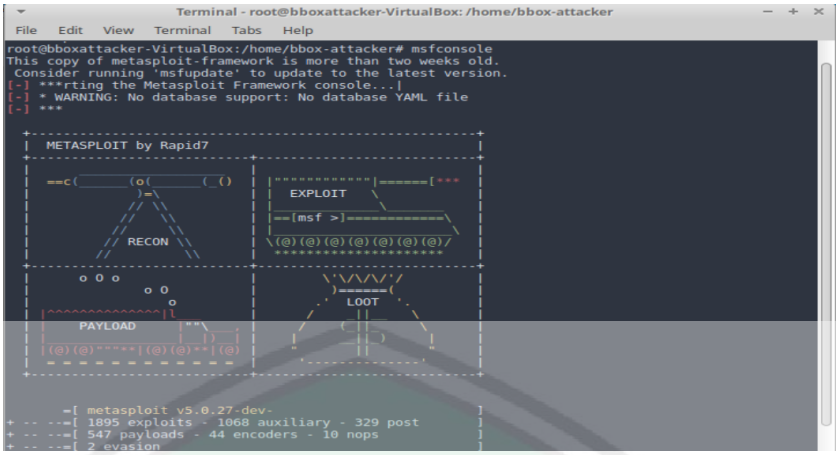
Berikut adalah tabel daftar *IP address* pada *virtual machine* untuk dapat melakukan komunikasi pada jaringan.

Tabel 4.1 Daftar *IP Address*

No	*Virtual Machine*	Peran	*IP Address*
1.	BackBox v6	Penyerang	192.168.56.102
2.	Metasploitable2	*Server*	192.168.56.104

Proses peretasan tidak dapat dilakukan hanya dengan sistem operasi penyerang dan *server* saja, dibutuhkan sebuah *tool* penyerang untuk melancarkan perintah dan kegiatan penyerangan. Peneliti menggunakan *tool* Metasploit yang terpasang pada sistem operasi penyerang. Metasploit inilah yang kemudian berperan sebagai bot *DDoS Executor*. Metasploit dijalankan pada Terminal BackBox dengan perintah “msfconsole” seperti pada Gambar 4.6 berikut.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 4.6 Metasploit

b. Simulasi peretasan

Simulasi peretasan dilakukan dengan menjalankan *tool* Metasploit sebagai bot *DDoS executor* dan menjalankan Metasploitable2 sebagai *server*. Langkah pertama yaitu dengan menjalankan Metasploitable2. Metasploitable2 dijalankan pada VirtualBox yang kemudian akan diakses oleh sistem operasi utama yang berperan sebagai *client* yaitu sistem operasi Windows 10. Setelah Metaspoitable2 sukses dijalankan pada VirtualBox, sistem operasi Windows menjalankan *browser* dan mengetikkan *IP address* dari Metasploitable2 yaitu 192.168.56.104. Disajikan tampilan akses *server* pada layer *client* sesuai Gambar 4.7 berikut.

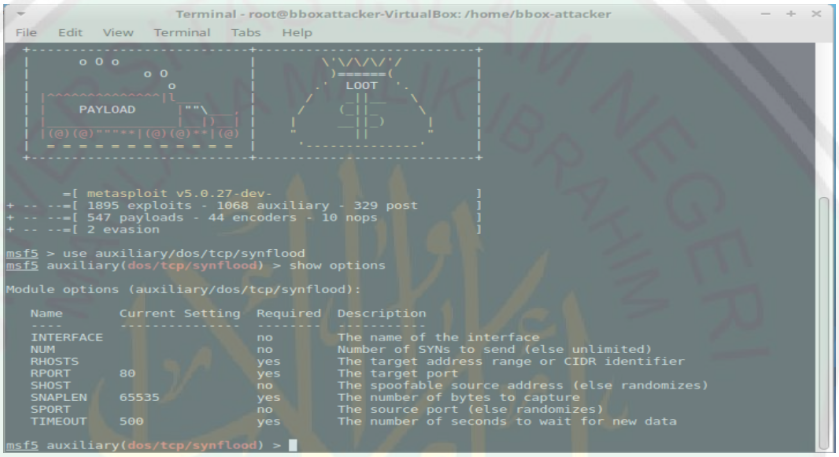


Gambar 4.7 Tampilan Akses *Server Hackable* pada *Client*

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Kemudian Metasploit dijalankan untuk melakukan serangan pada *server* Metasploitable2 tersebut. Berikut adalah perintah yang harus dilakukan melakukan serangan *DDoS*:

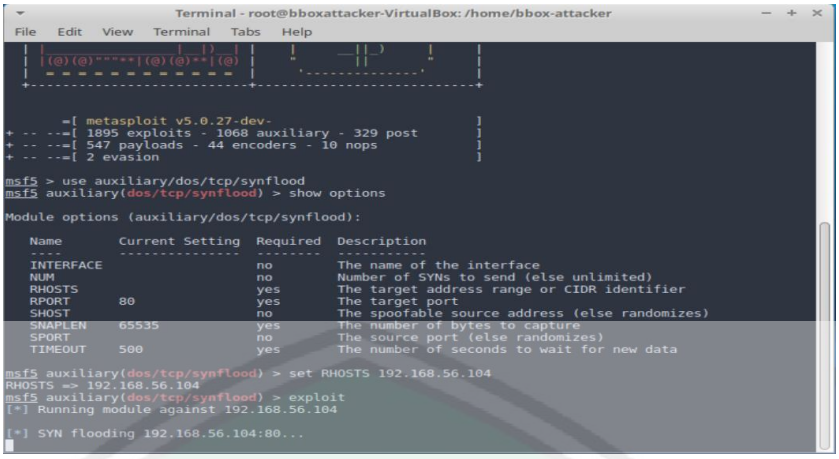
1. Memastikan bahwa Metasploit telah berjalan pada Terminal BackBox.
2. Ketikkan perintah "*use auxiliary/dos/tcp/synflood*".
3. Lanjutkan dengan mengetik "*show options*".
4. Lalu akan muncul menu *Module Options* seperti Gambar 4.8 berikut.



Gambar 4.8 *Module Options* pada Metasploit

5. Pilih RHOSTS untuk melakukan penyerangan *DDoS*, dengan mengetikkan perintah "*set* [*menu_name*] [*IP_target*]". Dalam hal ini Metasploitable sebagai target memiliki *IP* 192.168.56.104, sehingga perintah yang harus diberikan adalah "*set* RHOSTS 192.168.56.104".
6. Untuk meluncurkan perintah serangan, ketik perintah "*exploit*". Sesuai Gamber 4.9 berikut ditampilkan proses ketika peretasan berjalan.

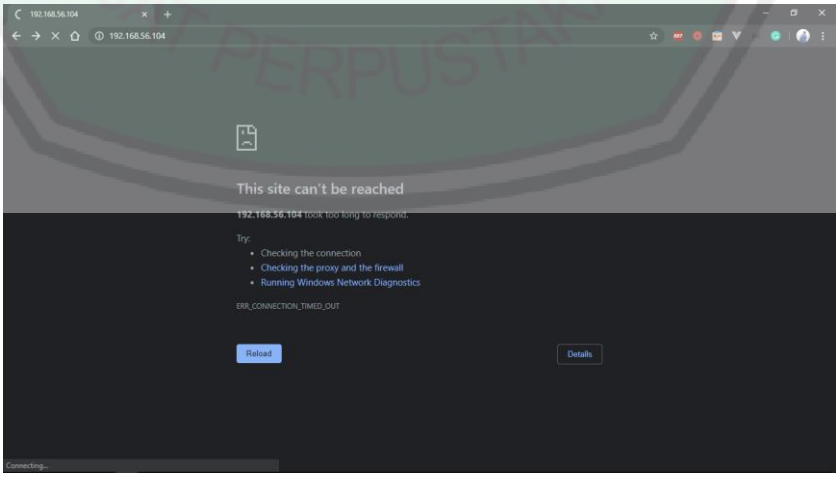
CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 4.9 Proses Penyerangan *DDoS* terhadap *Server*

7. Untuk mewujudkan praktek *DDoS*, maka satu bot *executor* tidak cukup untuk menjalankan serangan *DDoS*. Dibutuhkan setidaknya dua bot *executor* sehingga dapat disebut sebagai *Distributed DoS* (*DDoS*). Maka tambahkan tab pada Terminal dan lakukan penyerangan seperti pada langkah nomor 1-6. Tunggu hingga terjadi respon pada *server*.

Ketika proses peluncuran paket serangan, *server* Metasploitable2 akan terus menerus dibanjiri *request* yang diberikan oleh bot *executor* dalam hal ini yaitu Metasploit. Berikut ditampilkan tanggapan *server* terhadap serangan *DDoS* sesuai pada Gambar 4.10.



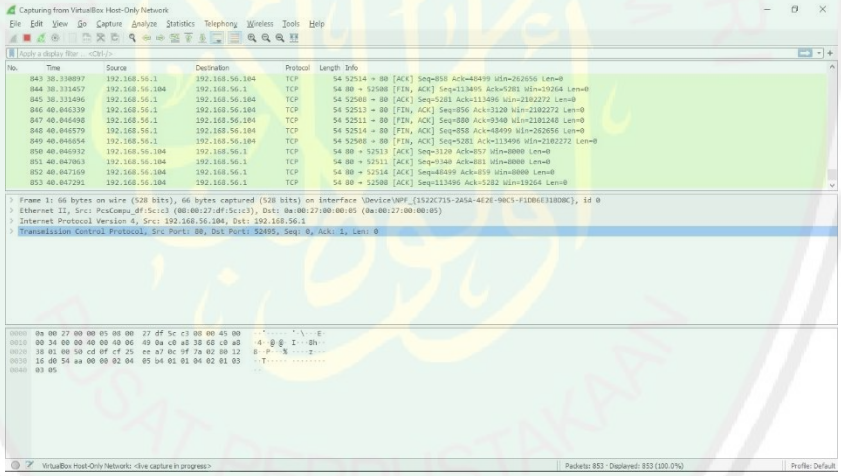
Gambar 4.10 Tanggapan *Server* Metasploitable2 terhadap Serangan *DDoS*

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Peneliti menggunakan 4 tab Metasploit dan membutuhkan waktu kurang lebih 5 menit untuk dapat melihat tanggapan gagal akses pada *server* Metasploitable2.

c. Perekaman Lalu Lintas Jaringan

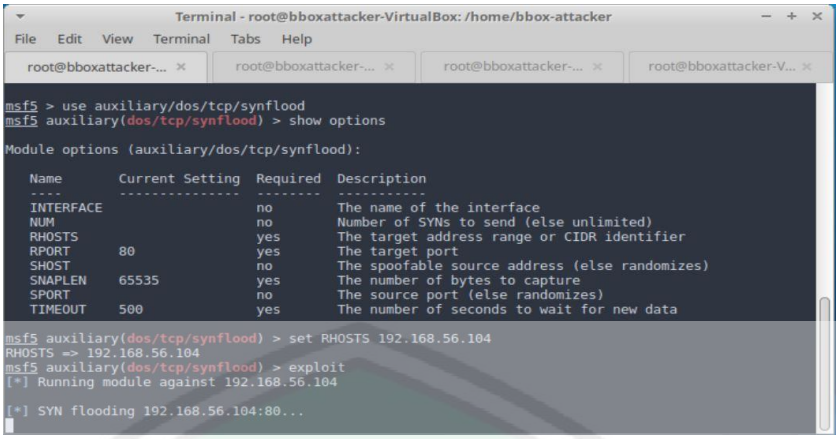
Dalam melakukan perekaman lalu lintas jaringan, diperlukan sebuah *tool* yang dapat merekam lalu lintas jaringan yang berlangsung pada suatu jaringan, *tool* yang digunakan yaitu WireShark. Karena WireShark bertugas untuk melakukan perekaman lalu lintas jaringan, tentu *tool* WireShark harus dijalankan sebelum hingga sesudah peretasan berlangsung, dengan begitu data lalu lintas peretasan dapat terekam dengan sempurna dan tidak ada data yang rusak atau hilang. Sesuai Gambar 4.11 ditampilkan proses perekeman lalu lintas jaringan ketika serangan *DDoS* belum diluncurkan.



Gambar 4.11 Perekaman Lalu Lintas Jaringan Normal

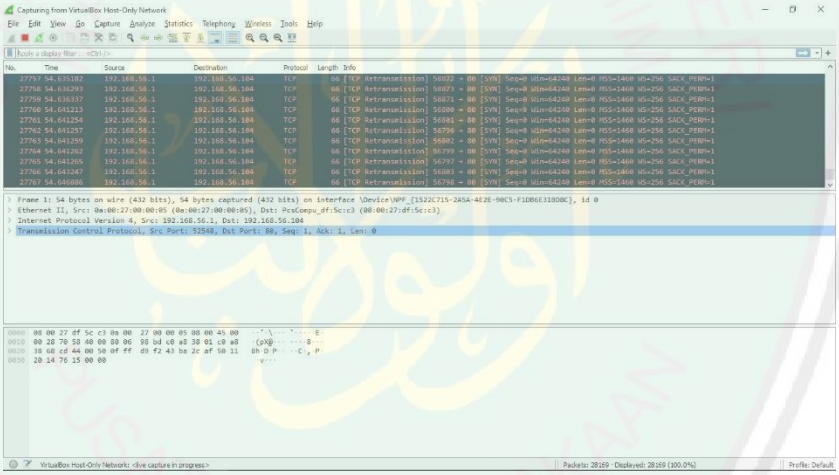
Ketika WireShark sudah siap dalam melakukan perekaman, maka bot Metasploit siap untuk melakukan serangan *DDoS*. Seperti Langkah sebelumnya, peneliti menggunakan 4 tab bot Metasploit, sesuai dengan Gambar 4.12 berikut.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 4.12 Peluncuran *DDoS* dengan 4 Tab Bot

Pada saat yang bersamaan WireShark melakukan perekaman lalu lintas pada jaringan *environment hacking*. Berikut ditampilkan pada Gambar 4.13 proses perekaman lalu lintas peretasan *DDoS*.



Gambar 4.13 Perekaman Lalu Lintas Serangan *DDoS*

Untuk mendapatkan data yang sah dan murni, peneliti tidak menyampur adukan proses akses pada *server*. Untuk akses jaringan normal dilakukan terlebih dahulu, kemudian proses perekaman disimpan dengan nama berkas "Trafik_Normal". Setelah proses perekaman jaringan normal selesai, peneliti melakukan perekaman pada berkas WireShark yang baru khusus untuk perekaman lalu lintas serangan

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

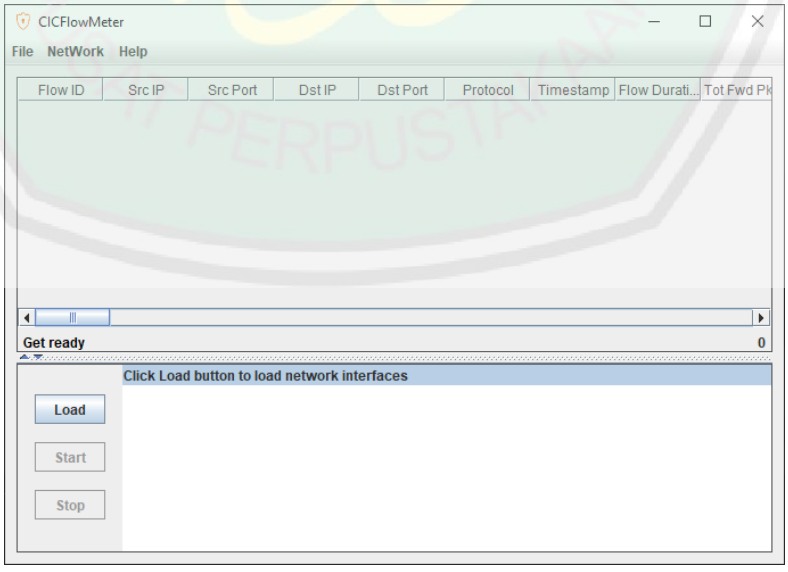
DDoS dan menyimpannya dengan nama berkas "Trafik_DDoS". Pada Tabel 4.2 berikut disajikan jumlah baris data yang berhasil direkam.

Tabel 4.2 Jumlah Data Perekaman Lalu Lintas Jaringan

No	Lalu Lintas Jaringan	Baris Data Perekaman
1.	Normal (*Benign*)	1048
2.	Serangan (*DDoS*)	458

d. Ektraksi Lalu Lintas Jaringan

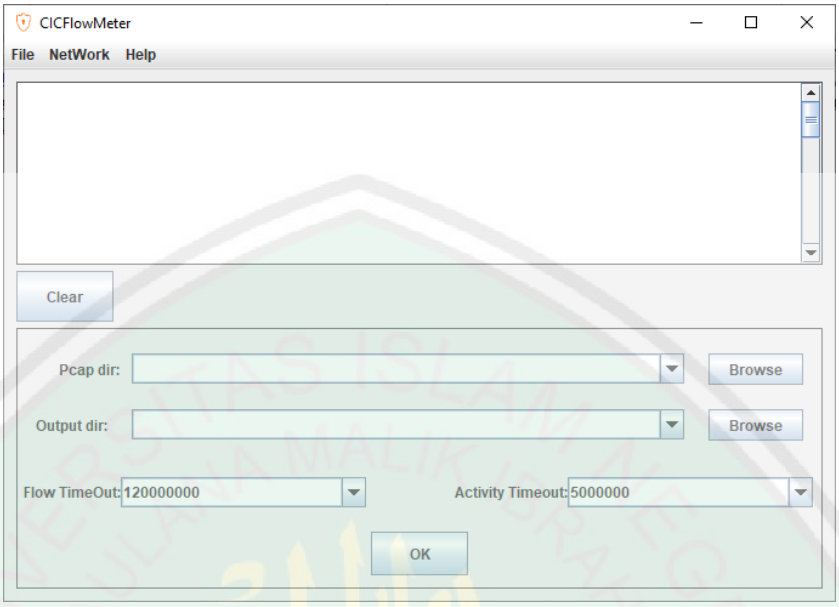
Setelah proses perekaman lalu lintas jaringan selesai, maka langkah selanjutnya yang perlu dilakukan adalah ekstraksi data lalu lintas jaringan. *Tool* yang digunakan pada Langkah ini adalah CICFlowMeter v4.0. Berkas *tool* CICFlowmeter v4.0 secara terbuka dapat diakses pada Github (https://github.com/ahlashkari/CICFlowMeter, 2020). Berkas CICFLowMeter yang telah diakses dari Github dijalankan menggunakan Intellij IDEA, pada Terminal Intellij ketik perintah "gradlew *execute*" untuk dapat menjalan kan CICFlowMeter v4.0. Berikut ditampilkan halaman utama dari CICFlowMeter sesuai Gambar 4.14.



Gambar 4.14 Halaman Utama CICFlowMeter

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Untuk dapat melakukan perintah ektraksi jaringan, pada menu utama pilih *NetWork>Offline*, sehingga muncul halaman sesuai Gambar 4.15 berikut.



Gambar 4.15 Tampilan Menu *Offline*

Pada *form* "Pcap dir" klik tombol *Browse* dan pilih berkas berektensi ".pcap" untuk dilakukan ekstraksi jaringan. Atur *directory* keluaran berkas ekstraksi jaringan pada form "*Output* dir". Jika semua sudah diatur maka klik tombol OK. Pada Tabel 4.3 berikut disajikan hasil dari ektraksi lalu lintas jaringan.

Tabel 4.3 Hasil Ektraksi Lalu Lintas Jaringan

No	Lalu Lintas Jaringan	Baris Data Ektraksi
1	*BENIGN*	396
2	*DDoS*	137
	Total	533

e. Pelabelan

Sesuai dengan langkah sebelumnya, peneliti memisahkan antara proses akses lalu lintas jaringan normal dengan akses lalu lintas jaringan serangan, hal ini bertujuan untuk mendapatkan trafik yang benar-benar murni dan tidak tercampur adukkan antara lalu lintas jaringan normal dengan lalu lintas jaringan serangan.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Dari hasil ekstraksi didapatkan baris data lalu lintas jaringan normal sebanyak 396, untuk baris data lalu lintas serangan sebanyak 137. Baris data pada lalu lintas jaringan normal diberi label "*BENIGN*" sedangkan untuk baris data pada lalu lintas jaringan serangan diberi label "*DDOS*". Kemudian kedua trafik digabungkan menjadi satu berkas XLSX sebagai data primer yang mana selanjutnya akan digunakan sebagai data pengujian model sesuai algoritma yang digunakan.

Sedangkan untuk data sekunder dalam penelitian, peneliti menggunakan *dataset* CICIDS2017. Peneliti menggunakan beberapa parameter yang diambil dari *dataset* CICIDS2017 tersebut. Berikut Tabel 4.4 berisi parameter-parameter dalam penelitian yang diambil dari dataset CICIDS2017.

Tabel 4.4 Parameter Penelitian

No	Fitur *Dataset*	Parameter Penelitian
1	TotLen Fwd Pkts	Total_length_of_fwd_packets
2	Fwd Pkt Len Max	Fwd_packet_length_max
3	Fwd Pkt Len Mean	Fwd_packet_length_mean
4	Fwd Seg Size Avg	Avg_fwd_segment_size
5	Subflow Fwd Byts	Subflow_fwd_bytes
6	Init Fwd Win Byts	Init_win_bytes_forward
7	Fwd Act Data Pkts	Act_data
8	Label	Label

Adapun data yang digunakan dalam penelitian secara terperinci disajikan pada Tabel 4.5 seperti berikut.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Tabel 4.5 Total Data dalam Penelitian

Jenis Data	Jenis Lalu Lintas Jaringan	Jumlah Baris Data	Total (Baris x Kolom)
Data Primer	*BENIGN*	396	533 x 8
	DDOS	137	
Data Sekunder	*BENIGN*	18883	225745 x 8
	DDOS	206862	

4.1.2 Praproses Data

Sebelum data diproses dalam sistem, peneliti melakukan *rescaling* data terlebih dahulu. *Rescaling* dilakukan oleh peneliti dengan tujuan merubah ulang skala data penelitian. Data yang dilakukan *rescaling* adalah data berjenis numerik. Peneliti menggunakan metode *rescale* data dengan metode *Minimum Maximum Rescaling*, yaitu merubah skala data pada nilai *minimum* dan nilai *maximum* yang disamakan. Dalam kasus ini peneliti merubaha *minimum* data menjadi 0 dan *maximum* data menjadi 1, dengan kata lain data akan dilakukan rescaling menjadi data dengan rentang 0 sampai dengan 1. Berikut ditampilkan hasil dari *rescaling* data numerik dalam sistem sesuai pada Gambar 4.16.

	total_length_of_fwd_packets	fwd_packet_length_max	fwd_packet_length_mean	avg_fwd_segment_size	sublfow_fwd_bytes	init_win_bytes_fwd	act_data	label
0	0.000066	0.000514	6.004289e-10	6.004289e-10	0.000066	0.000519	0.000518	BENIGN
1	0.000033	0.000514	6.004289e-10	6.004289e-10	0.000033	0.000458	0.000000	BENIGN
2	0.000033	0.000514	6.004289e-10	6.004289e-10	0.000033	0.000458	0.000000	BENIGN
3	0.000033	0.000514	6.004289e-10	6.004289e-10	0.000033	0.000488	0.000000	BENIGN
4	0.000066	0.000514	6.004289e-10	6.004289e-10	0.000066	0.000504	0.000518	BENIGN
	...	...	...	...	...	...	...	...
225740	0.000033	0.000514	6.004289e-10	6.004289e-10	0.000033	0.004410	0.000000	BENIGN
225741	0.000033	0.000514	6.004289e-10	6.004289e-10	0.000033	0.004410	0.000000	BENIGN
225742	0.000033	0.000514	6.004289e-10	6.004289e-10	0.000033	0.004410	0.000000	BENIGN
225743	0.000066	0.000514	6.004289e-10	6.004289e-10	0.000066	0.072021	0.000518	BENIGN
225744	0.000033	0.000514	6.004289e-10	6.004289e-10	0.000033	0.200516	0.000000	BENIGN

[225745 rows x 8 columns]

Gambar 4.16 *Rescaling* Data Numerik

4.1.3 *Random Forest*

Algoritma *Random Forest* digunakan untuk melakukan pemodelan pelatihan dan melakukan pengujian dari model yang dibentuk tersebut. Langkah pertama yaitu membangun sebuah *resample* dengan mengacak data *training*, data *training* disini adalah sebagain dari data sekunder maupun primer, tahap ini disebut

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

sebagai tahap *bootstrapping*. *Bootstrapping* dibangun secara berulang sebanyak jumlah pohon yang ditentukan. Sesuai dengan Gambar 4.17 disajikan contoh hasil dari salah satu *bootstrapping*.

	total_length_of_fwd_packets	fwd_packet_length_max	fwd_packet_length_mean	avg_fwd_segment_size	sublfow_fwd_bytes	init_win_bytes_fwd	act_data	label
64733	0.000164	0.000514	6.004289e-10	6.004289e-10	0.000164	0.003922	0.002071	DDoS
169269	0.000306	0.001712	7.005004e-10	7.005004e-10	0.000306	0.003922	0.003107	DDoS
93916	0.000306	0.001712	7.005004e-10	7.005004e-10	0.000306	0.003922	0.003107	DDoS
139472	0.000033	0.000514	6.004289e-10	6.004289e-10	0.000033	0.003510	0.000000	BENIGN
49669	0.000066	0.000514	6.004289e-10	6.004289e-10	0.000066	0.005508	0.000518	BENIGN
	...	...	...	...	...	...	...	...
107154	0.000142	0.001712	8.672862e-01	8.672862e-01	0.000142	0.125015	0.001036	DDoS
118479	0.000142	0.001712	8.672862e-01	8.672862e-01	0.000142	0.125015	0.001036	DDoS
1382	0.004841	0.042123	5.910889e-01	5.910889e-01	0.004841	0.125015	0.007250	BENIGN
26537	0.000164	0.000514	6.004289e-10	6.004289e-10	0.000164	0.003922	0.002071	DDoS
180821	0.000339	0.001712	6.893813e-01	6.893813e-01	0.000339	0.003922	0.003625	DDoS

[800 rows x 8 columns]

Gambar 4.17 Sampel *Bootstrapping* pada Data Sekunder

Sekumpulan *bootstrapping* yang telah dibangun akan diproses menjadi kumpulan *tree model*. *Tree model* atau yang selanjutnya disebut sebagai *Random Forest* Model dibangun untuk menjadi model pelatihan baris data primer. Sesuai dengan Gambar 4.18 ditampilkan contoh sebagian *Random Forest* Model.

```
{'fwd_packet_length_max <= 0.0017123287671232876': [{'sublfow_fwd_bytes <= 9.835420628155 53e-05': ['BENIGN',
                                                                                                      'DDoS']},
                                                    'BENIGN']},
 {'fwd_packet_length_max <= 0.0017123287671232876': [{'total_length_of_fwd_packets <= 6.55694708543702e-05': ['BENIGN',
                                                                                                              'DDoS']},
                                                     'BENIGN']},
 {'fwd_packet_length_max <= 0.0017123287671232876': [{'total_length_of_fwd_packets <= 9.83542062815553e-05': ['BENIGN',
                                                                                                              'DDoS']},
                                                     'BENIGN']},
 {'init_win_bytes_fwd <= 0.0038909912109375': ['BENIGN',
                                               {'fwd_packet_length_max <= 0.0017123287671232876': [{'total_length_of_fwd_packets <= 9.835420628155 53e-05': ['BENIGN',
                                                                                                                                                              'DDoS']},
                                                                                                   'BENIGN']}]},
 {'init_win_bytes_fwd <= 0.0038909912109375': ['BENIGN',
                                               {'fwd_packet_length_max <= 0.0017123287671232876': [{'total_length_of_fwd_packets <= 9.835420628155 53e-05': ['BENIGN',
                                                                                                                                                              'DDoS']},
                                                                                                   'BENIGN']}]},
```

Gambar 4.18 Sampel *Random Forest* Model

Dari hasil pembangunan model pelatihan berupa kumpulan *tree* (*forest*), maka dilanjutkan dengan tahap prediksi atau disebut juga sebagai tahap deteksi lalu lintas jaringan. *Random Forest* Model yang dibangun dari data *training* pada pada sekunder tentu digunakan untuk melakukan deteksi data *testing* pada data sekunder. Begitu juga *Random Forest* Model yang dibangun dari data *training* pada data primer digunakan untuk deteksi data *testing* pada data primer. Kemudian disamping

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

proses deteksi berlangsung, peneliti meletakkan pemicu pada sistem untuk dapat mendapatkan waktu permulaan deteksi dan waktu akhir dari deteksi. Pemicu waktu inilah yang akan berperan sebagai masukan untuk menghitung durasi tahap deteksi lalu lintas jaringan menggunakan *Random Forest*. Setelah proses deteksi lalu lintas jaringan selesai, keluaran dari sistem deteksi data lalu lintas jaringan tersebut akan diukur untuk didapatkan seberapa besar *accuracy, precision, recall, f-measure* sekaligus durasi waktu proses deteksi lalu lintas jaringan tersebut.

4.1.4 Pengujian Sistem

Sub-bab ini menampilkan bagaimana cara untuk mengukur *accuracy, precision, recall, f-measure* dan menghitung lama durasi *Random Forest* dalam mendeteksi serangan *DDoS*. Dalam perhitungan *accuracy, precision, recall, dan f-measure* peneliti menggunakan keluaran dari hasil deteksi sistem.

Accuracy mengukur presentasi perbandingan antara percobaan dengan prediksi benar terhadap seluruh percobaan yang dilakukan. Pengukuran *accuracy* sesuai dengan persamaan 4.1 berikut (Alkasassbeh dkk, 2016).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \qquad (4.1)$$

Precision mengukur presentasi perbandingan antara prediksi benar positif dengan keseluruhan hasil yang diprediksi positif. Pengukuran *precission* sesuai dengan persamaan 4.2 berikut (Alkasassbeh dkk, 2016).

$$Precision = \frac{TP}{TP + FP} \times 100\% \qquad (4.2)$$

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Recall mengukur presentasi perbandingan antara prediksi benar positif dengan semua kemungkinan prediksi data yang positif. Pengukuran *recall* sesuai dengan persamaan 4.3 berikut (Alkasassbeh dkk, 2016).

$$Recall = \frac{TP}{TP + FN} \times 100\% \quad (4.3)$$

f-measure mengukur efektivitas pengujian dengan memperhatikan *precission* dan *recall.* Pengukuran *f-measure* sesuai dengan persamaan 4.4 berikut (Bestari dkk, 2018).

$$f\text{-}meaure = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} \quad (4.4)$$

Dimana pengertian untuk istilah diatas adalah sebagai berikut.

-*True Positive* (TP) adalah data peretasan dan dianggap sebagai peretasan.

-*False Positive* (FP) adalah data normal namun dianggap sebagai peretasan.

-*True Negative* (TN) adalah data normal dan dianggap sebagai normal.

-*False Negative* (FN) adalah data peretasan namun diaggap sebagai normal.

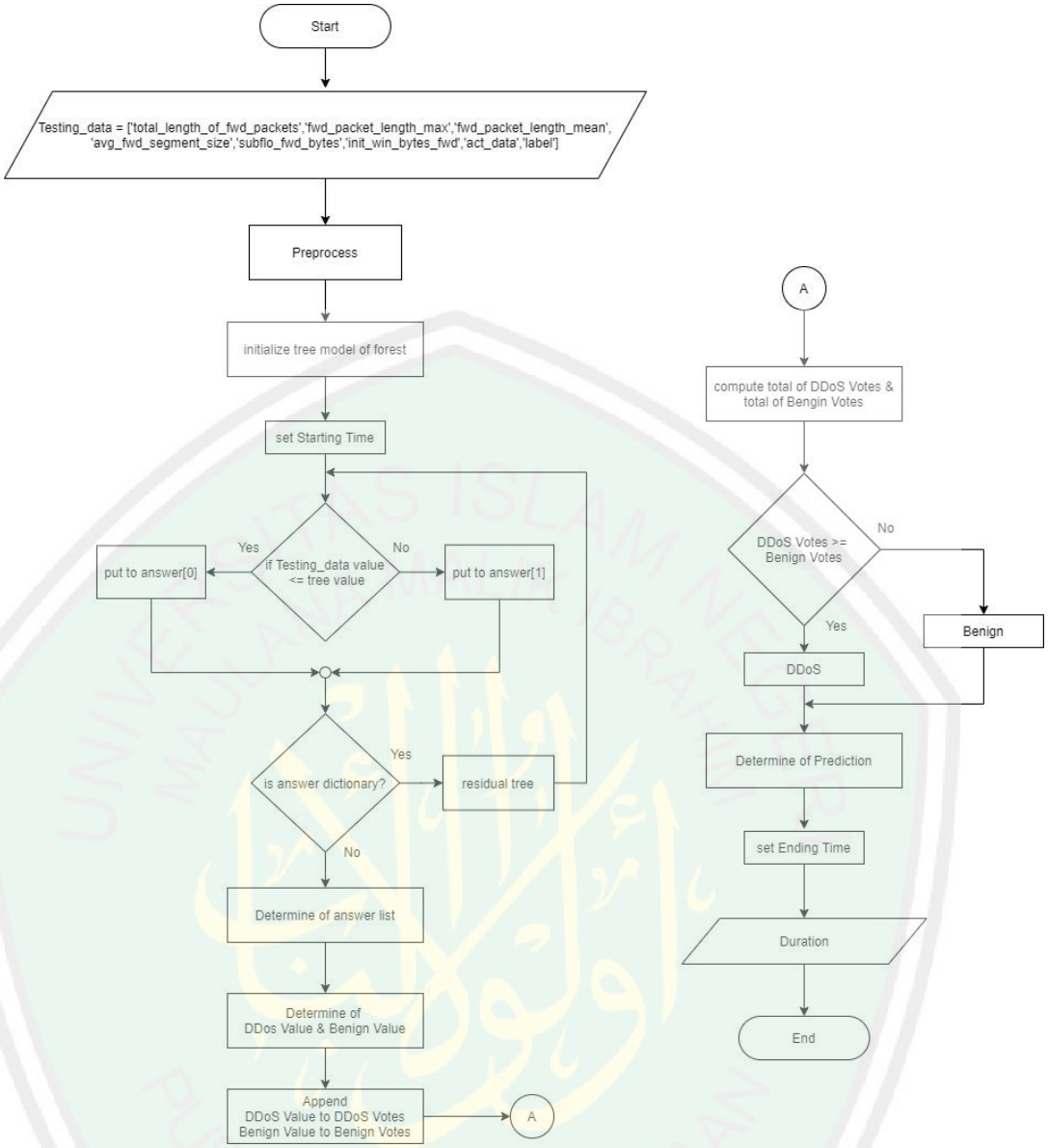
Berikut disajikan tabel 4.6 merupakan *confusion matrix* untuk mempermudah pemahaman antara data aktual dengan data prediksi.

Tabel 4.6 *Confusion Matrix*

Aktual / Prediksi	DDoS	Normal
DDoS	TP	FP
Normal	FN	TN

Sedangkan untuk mengetahui durasi deteksi serangan menggunakan algoritma sesuai alur pada Gambar 4.19.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG



Gambar 4.19 *Flowchart Setting* Uji Coba Durasi Waktu

Ketika deteksi serangan dijalankan maka waktu program akan mulai dijalankan, ini sebagai tanda waktu mulai berjalan. Ketika hasil deteksi didapatkan, maka waktu akhir program akan didapatkan. Perhitungan durasi pengujian sesuai persamaan 4.5 berikut

$$t_{total} = t_{finish} - t_{start} \quad (4.5)$$

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Dimana t_{total} adalah durasi pengujian, sedangkan t_{start} adalah waktu mulai pengujian dijalankan dan t_{finish} adalah waktu selesai pengujian. *Script* program untuk proses mendapatkan waktu pelatihan pada sistem ditampilkan pada Gambar 4.20 berikut.

```
# Determine local time
def localtime_in_sec(localtime):
    time = localtime()
    hour = time.tm_hour * 3600
    minute = time.tm_min * 60
    second = time.tm_sec
    localtime_sec = hour + minute + second

    return localtime_sec

# TODO Starting time
now = localtime_in_sec(localtime)
print("Starting time:", now, "second")

# TODO Ending time and Print Duration
# Ending time
later = localtime_in_sec(localtime)

# Print Duration
duration = int(later-now)
```

Gambar 4.20 *Script* Program Proses Pencatatan Durasi Deteksi

4.2 Hasil Uji Coba

Pada tahap hasil uji coba penelitian ini, peneliti menampilkan hasil percobaan sesuai dengan tahap-tahap skenario uji coba yang telah dipaparkan. Peneliti melakukan uji coba sistem pada data sekunder maupun data primer. Hasil dari kedua data akan didapatkan sebagai hasil dari uji coba. Dalam Tabel 4.7 disajikan pengujian *Random Forest* Model menggunakan data *testing* dari data sekunder.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Tabel 4.7 Uji Coba dengan Data *Testing* pada Data Sekunder

Nomor Baris Data	Data Prediksi	Data Aktual
33290	BENIGN	BENIGN
109592	DDoS	DDoS
113450	DDoS	DDoS
12380	BENIGN	BENIGN
66581	DDoS	DDoS
	...	...
206921	BENIGN	BENIGN
182672	DDoS	DDoS
155812	BENIGN	BENIGN
4661	BENIGN	BENIGN
58697	DDoS	DDoS

```
duration 764 second
akurasi:  99.87596642824657
presisi:  99.91369898622303
recall:  99.86800943680562
f-measure:  99.89084898697465
```

Dari hasil uji coba *Random Forest* Model dengan menggunakan data *testing* dari data sekunder, dapat diambil kesimpulan hasil uji coba sesuai dengan Tabel 4.8 berikut.

Tabel 4.8 Hasil Uji Coba pada Data Sekunder

Durasi Deteksi Random Forest	12 Menit 44 Detik
Accuracy	99,87%
Precision	99,91%
Recall	99,86%
f-*Measure*	99,89%

Berikutnya peneliti melakukan uji coba data *testing* pada data primer. Berikut dalam Tabel 4.9 disajikan pengujian *Random Forest* Model menggunakan data *testing* dari data primer.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Tabel 4.9 Uji Coba dengan Data *Testing* pada Data Primer

Nomor Baris Data	Data Prediksi	Data Aktual
73	BENIGN	BENIGN
437	DDoS	DDoS
502	DDoS	DDoS
206	BENIGN	BENIGN
438	DDoS	DDoS
263	BENIGN	BENIGN
171	BENIGN	BENIGN
242	BENIGN	BENIGN
203	BENIGN	BENIGN
482	DDoS	DDoS

```
duration 1 second
akurasi:  99.62406015037594
presisi:  98.59154929577466
recall:  100.0
f-measure:  99.29078014184398
```

Dari hasil uji coba deteksi sistem menggunakan data testing pada data primer, dapat diambil kesimpulan hasil uji coba sesuai dengan Tabel 4.10 berikut.

Tabel 4.10 Hasil Uji Coba dengan Data Primer

Durasi Deteksi Random Forest	1 Detik
Accuracy	99,62%
Precision	98,59%
Recall	100%
f-*Measure*	99,29%

4.3 Pembahasan

Setelah seluruh proses pengujian telah selesai dilalui, maka akan nampak bahwa hasil dari pengujian dari kedua set data. Terlebih dahulu peneliti akan menampilkan *confusion matrix* dari setiap hasil uji coba. Berikut hasil *confusion matrix* pada setiap set data ditunjukkan pada Tabel 4.11.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Tabel 4.11 Hasil *Confusion Matrix*

***Confusion Matrix* pada Data Primer**		
Aktual / Prediksi	**DDoS**	**Normal**
DDoS	70	1
Normal	0	195
***Confusion Matrix* pada Data Sekunder**		
Aktual / Prediksi	**DDoS**	**Normal**
DDoS	96092	83
Normal	127	73007

Dari tabel *confusion matrix* didapatkan beberapa perbedaan antara hasil prediksi dari data primer dan hasil prediksi dari data sekunder. Berikut perbedaan hasil confusion matrix sesuai pada Tabel 4.12.

Tabel 4.12 Perbedaan Hasil *Confusion Matrix* antara Prediksi Data Primer dan Data Sekunder

Data Primer	Data Sekunder
Length: 266 True Negative: 195 False Positive: 1 False Negative: 0 True Positive: 70 ['BENIGN' 'DDoS'] [195 71]	Length: 169309 True Negative: 73007 False Positive: 83 False Negative: 127 True Positive: 96092 ['BENIGN' 'DDoS'] [73134 96175]

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Kemudian dari hasil *accuracy*, *precision*, *recall*, f-*measure* dan durasi yang dihasilkan oleh pengujian *Random Forest* model menggunakan dari data *testing* pada data sekunder maupun primer menunjukkan bahwa algortima *Random Forest* merupakan algortima yang handal dalam membangun sistem model pelatihan karena menunjukkan *accuracy*, *precision*, *recall*, f-*measure* dan durasi seperti pada Tabel 4.13 berikut.

Tabel 4.13 Pengukuran *Random Forest* Model Data Sekunder dan Data Primer

	Data Sekunder	**Data Primer**
Durasi	12 menit 44 detik	1 detik
Accuracy	99,87%	99,62%
Precision	99,91%	98,59%
Recall	99,86%	100%
f-*Measure*	99,89%	99,29%

Tindakan peretasan atau dalam istilah lain disebut sebagai *hacking* merupakan suatu tindakan yang dapat meresahkan dan merugikan bagi pihak target peretasan. Istilah peretasan sejatinya memperlakukan suatu hal tidak sesuai dengan semestinya atau jika dalam istilah keislaman terdapat istilah "dzalim" yang tentu merugikan pihak lain. Sehingga pada tindakan peretasan ini perlu adanya penanganan secara serius sehingga dapat diminimalisir atau bahkan dihilangkan. Sesuai dengan bahasan penelitian yaitu deteksi *Distributed Denial of Service* (salah satu metode peretasan) perlu dilakukan guna untuk mewujudkan usaha penanganan secara serius terhadap tindakan peretasan di bidang teknologi informasi dan komunikasi.

Sistem deteksi erat kaitannya dengan pengelompokan beberapa kasus ke dalam suatu kelas-kelas untuk dilakukan analisa yang lebih mendalam. Berhubungan dengan penelitian ini yaitu pengelompokkan lalu lintas jaringan normal (*BENIGN*) dengan jaringan peretasan (*DDOS*) memiliki keterkaitan dengan

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

ajaran islam yaitu pengelompokan suatu hal yang benar (*HAQ*) dan suatu hal yang bohong atau buruk (*BATHIL*). Lalu lintas jaringan normal merupakan bentuk dari suatu hal yang benar sedangkan lalu lintas jaringan peretasan merupakan bentuk suatu hal yang bohong. Dalam ajaran islam, jika terdapat dua hal yang saling kontradiktif antara nilai kebenaran dan kebohongan, maka perlu untuk dipisahkan dan tidak boleh dicampur adukkan, karena pencampur adukan kedua hal yang berlainan ini akan menimbulkan dampak yang buruk terhadap kehidupan seorang mahluk. Hal ini disampaikan pada Al Qur'an Surat Al Baqarah ayat 42 sebagai berikut.

وَلَاتَلْبِسُواٱلْحَقَّ بِٱلْبَٰطِلِ وَتَكْتُمُواٱلْحَقّ وَأَنتُمْ تَعْلَمُونَ

Artinya: "Janganlah kalian campur-adukkan antara kebenaran dan kebatilan, dan janganlah kalian sembunyikan yang benar padahal kamu mengetahuinya". (Q.S. Al-Baqarah [2]: 42).

Menurut tafsir Jalalain dalam Al-Qur'an Al-Hadi (Al Qur'an Alhadi Interaktif, 2020) ayat tersebut memiliki penjelasan sebagi berikut,

ولا تخلِطوا الحق الذي بيَّنته لكم بالباطل الذي افتريتموه، واحذروا كتمان الحق الصريح من صفة نبي الله ورسوله محمد صلى الله عليه وسلم التي في كتبكم، وأنتم تجدونها مكتوبة عندكم، فيما تعلمون من الكتب التي بأيديكم.

Dengan makna sebagai berikut, "dan janganlah kalian campur aduk barang yang hak yang telah kuturunkan kepada kalian dengan barang yang bathil yang kamu ada-adakan dan jangan pula kalian sembunyikan yang hak berupa sifat dan ciri-ciri Muhammad sedangkan kalian mengetahui bahwa ia hak adanya."

Dalam tafsir Al Misbah, M Quraish Shihab menjelaskan bahwa ayat ini merupakan ayat tuntunan kepada Bani Isra'il. Mereka dilarang untuk menyesatkan

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

yang sebelumnya mereka juga dilarang terjerumus dalam kesesatan. Bentuk penyesatan ini terdapat dalam dua cara, yaitu sebagai berikut:

1. Pada lafal (وَلَا تَلْبِسُوا الْحَقَّ بِالْبَاطِلِ) ini memiliki penafsiran bahwa kebeneran yang ingin dipertahankan dengan ketidak benaran dengan maksud untuk disebarluaskan. Hal ini merupakan bentuk praktik dari propaganda yang sebagian isinya benar, namun celah kebenaran tersebut disisipi kebohongan-kebohongan dalam bentuk yang sangat halus.
2. Pada lafal (وَتَكْتُمُوا الْحَقَّ) yaitu menyembunyikan kebenaran tersebut atas mereka yang tidak tahu, sedangkan kalian mengetahui sehingga pengetahuan itu wajib disampaikan kepada yang tidak tahu.

Menurut Qurasih Shihab menyembunyikan kebenaran dapat terjadi dengan mengingkarinya atau tidak menyampaikan saat dibutuhkan. Karena itu diamnya seseorang yang tahu tentang suatu hal persoalan merupakan sebuah bentuk penyembunyian dari kebenaran tersebut.

Maka dengan adanya penelitian ini, merupakan bentuk ikhtiar seorang hamba untuk melakukan upaya pencegahan pada serangan keamanan jaringan. Harapan dari peneliti terhadap sistem yang telah dibuat yaitu untuk memisahkan manakah upaya peretasan dan manakah yang bukan upaya peretasan. Dengan begitu maka dapat dilakukan pemberlakukan penanganan yang tepat terhadap permasalahan keamanan jaringan.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian yang telah dilakukan merupakan penelitian deteksi *Distributed Denial of Service* (*DDoS*) menggunakan algoritma *Random Forest* dengan objek penelitian lalu lintas jaringan yang berlabelkan lalu lintas jaringan *BENIGN* (normal) dan *DDOS* (serangan). Terdapat dua data yang digunakan dalam penelitian yaitu terdiri dari data sekunder dan data primer. Data sekunder yang digunakan merupakan *dataset* CICIDS2017 yang mana data tersebut merupakan sekumpulan baris data lalu lintas jaringan yang dibangun oleh para ahli dalam bidang keamanan siber dan digunakan untuk keperluan penelitian. Sedangkan data primer yang digunakan merupakan baris data lalu lintas jaringan yang dibangun oleh peneliti sendiri dan didapatkan dari hasil simulasi praktek peretasan *DDOS*. Kedua jenis data memiliki peran yang sama yaitu sebagai masukan sistem deteksi *Distributed Denial of Service* (*DDOS*) yang dibangun oleh peneliti. Dari kedua data akan dibagi menjadi dua bagian untuk keperluan sistem *training* dan sistem *testing*, sebagian data dari data sekunder digunakan sebagai data *training* dan sebagian lainnya digunakan sebagai data *testing*, aturan yang sama berlaku pada data primer.

Model yang dibangun dari data *training* pada data sekunder digunakan untuk melakukan deteksi data *testing* pada data sekunder. Begitu juga model yang dibangun dari data *training* pada data primer digunakan untuk deteksi data *testing* pada data primer. Pada penelitian ini kesimpulan yang didapat adalah sebagai berikut:

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

1. Dari hasil uji yang dilakukan pada setiap data secara bergantian, peneliti melakukan uji coba pada data sekunder terlebih dahulu hingga menemukan hasil, kemudian dilanjutkan uji coba pada data primer. Dari data sekunder didapatkan hasil bahwa *Random Forest* dapat mendeteksi data *testing* pada data sekunder dengan hasil *accuracy* sebesar 99,87%, hasil *precision* sebesar 99,91%, hasi *recall* sebesar 99,86% dan *f-Measure* sebesar 99,89%. Sedangkan data *testing* pada data primer dengan hasil *accuracy* sebesar 99,62%, hasil *precision* sebesar 98,59%, hasi *recall* sebesar 100% dan *f-Measure* sebesar 99,29%.
2. Durasi waktu yang dibutuhkan *Random Forest* untuk mendeteksi data *testing* pada data sekunder adalah selama 12 menit 44 detik sejumlah 169309 baris data, sedangkan data *testing* pada data primer adalah selama 1 detik sejumlah 266 baris data.

5.2 Saran

Peneliti menyadari bahwa proses penelitian dari awal hingga akhir masih jauh dari kata sempurna, alangkah baiknya jika terus dilakukan pengembangan sehingga mendapatkan proses dan hasil yang lebih baik. Dari seluruh proses data dan hasil yang telah didaptkan oleh peneliti, berikut beberapa saran peneliti yang dapat bermanfaat bagi pihak yang berkepentingan antara lain:

a. Dalam membentuk *hacking environment* dan simulasi serangan diharapkan untuk lebih memperhatikan prosedur sehingga dapat menghasilkan set data primer yang tepat dan sesuai.
b. Lebih teliti dalam menggunakan data yang digunakan dalam penelitian.
c. Menambahkan *user interface application* pada kode program.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

DAFTAR PUSTAKA

Ahlaskari. (2020, Maret 2). *CICFlowMeter*. Diambil kembali dari Github: https://github.com/ahlashkari/CICFlowMeter

Alkasassbeh, M., Hasanat, A. B., Almseidin, M., & Al-Naymat, G. (2016). Detecting Distributed Denial of Service Attacks Using Data Mining Techniques. *International Journal of Advances Computer Science and Applications*, 436-445.

APJII. (2018). *PENETRASI & PROFIL PERILAKU PENGGUNA INTERNET INDONESIA*. Jakarta: APJII.

Avital, N., Zawoznik, A., Azaria, J., & Lambert, K. (2020, Februari 4). *2019 Global DDoS Threat Landscape Report*. Diambil kembali dari www.imperva.com: https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/

Bestari, D. P., Saptono, R., & Anggrainingsih, R. (2018). ACADEMIC ARTICLES CLASSIFICATION USING NAIVE BAYES CLASSIFIER. *Jurnal Ilmiah Teknologi dan Informasi*, 74-81.

CNN Indonesia. (2019, April 29). *BSSN: 232,45 Juta Serangan Siber 'Serbu' Indonesia di 2018*. Diambil kembali dari www.cnnindonesia.com: https://www.cnnindonesia.com/teknologi/20190426125843-192-389855/bssn-23245-juta-serangan-siber-serbu-indonesia-di-2018

Fathullah, A. L. (2020, April 19). *Al-Qur'an Interaktif*. Diambil kembali dari Al-Qur'an Al-Hadi: https://alquranalhadi.com/interactive

Intrusion Detection Evaluation Dataset CICIDS2017. (2020, Maret 2). Diambil kembali dari University of New Brunswick: https://www.unb.ca/cic/datasets/ids-2017.html

Liang, X., & Znati, T. (2019). On the Performance of Intelligent Techniques for Intensive and Stealthy DDoS Detection. *Computer Network*.

Metasploitable 2. (2020, Maret 2). Diambil kembali dari Rapid7: https://metasploit.help.rapid7.com/docs/metasploitable-2

Mirkovic, J., & Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanism. *ACM SIGCOMM Computer Communication*, 39-54.

Muhammad, A. W., Riadi, I., & Sunardi. (2017). Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window . *JISKa*, 115 – 122.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Nugroho, Y. S., & Emiliyawati, N. (2017). Sistem Klasifikasi Variabel Tingkat Penerimaan Konsumen Terhadap Mobil Menggunakan Metode Random Forest. *Jurnal Teknik Elektro Vol. 9 No. 1*, 24-29.

Panigrahi, R., & Borah, S. (2018). A Detailed Analysis of CICDS2017 Dataset for Designing Intrusion Detection System. *International Journal of Engineering & Technology*, 479-482.

Primajaya, A., & Sari, N. (2018). Random Forest Algoritm for Prediction of Precipitation. *Indonesian Journal of Articial Intelligence and Data Science (IJAIDM) Vol.1 No. 1*, 27-31.

Saputra, W. S., Sujatmika, A. R., & Arifin, A. Z. (2011). Seleksi Fitur Menggunakan Random Forest dan Neural Network. *The 13th Industrial Electronics Seminar 2011* (hal. 93-97). Surabaya: EEPIS.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Trafic Characterization. *in Proceedings of the 4th International Conference on Information Systems Security and Privacy* (hal. 108-116). Madeira: Scitepress.

Shihab, M. Q. (2002). Tafsir Al-Misbah. In M. Q. Shihab, *Tafsir Al-Misbah* (pp. 174-175). Jakarta: Lentera Hati.

Sihombing, J. C., Kartikasari, D. P., & Bhawiyuga, A. (2019). Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software Defined Network (SDN). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 9608-9613.

Wang, H., Lei, M., Chen , Y., Li, M., & Zou, L. (2019). Intelligent Identification of Maceral Components of Coal Based on Image Segmentation and Classification . *Applied Sciences*, 1-15.

Yu, S. (2013). Distributed Denial of Service Attack and Defence. Dalam S. Yu, *Distributed Denial of Service Attack and Defence* (hal. 9). Melbourne: Springer.

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

LAMPIRAN – LAMPIRAN

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Uji Coba pada Set Data Primer

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

```
C:\Users\damar\PycharmProjects\Latihan\venv\Scripts\python.exe "C:\Program Files\JetBrains\PyCharm 2019.3.2\plugins\python\
helpers\pydev\pydevconsole.py" --mode=client --port=55927

import sys; print('Python %s on %s' % (sys.version, sys.platform))
sys.path.extend(['C:\\Users\\damar\\PycharmProjects\\Latihan', 'C:/Users/damar/PycharmProjects/Latihan'])

PyDev console: starting.

Python 3.7.6 (tags/v3.7.6:43364a7ae0, Dec 19 2019, 00:42:30) [MSC v.1916 64 bit (AMD64)] on win32
>>> runfile('C:/Users/damar/PycharmProjects/Latihan/RandomForest.py', wdir='C:/Users/damar/PycharmProjects/Latihan')
DATA TRAINING
      TotLenFwdPckt  FwdPcktLenMax  FwdPcktLenMean  AvgFwdSgmnSize  SubFlFwdByts  InitWinBytsFwd  ActvData   Label
268        0.012147       0.021338    2.081994e-09    2.081994e-09      0.012147        0.003723  0.000000  BENIGN
455        0.000000       0.000000    0.000000e+00    0.000000e+00      0.000000        0.000000  0.000000    DDoS
226        0.012147       0.017878    2.081994e-09    2.081994e-09      0.012147        0.000488  0.025641  BENIGN
61         0.027249       0.026528    3.113612e-01    3.113612e-01      0.027249        0.002472  0.051282  BENIGN
25         0.172685       0.303345    5.919614e-08    5.919614e-08      0.172685        0.076202  0.000000  BENIGN
125        0.057781       0.025375    4.951768e-09    4.951768e-09      0.057781        0.000000  0.076923  BENIGN
487        0.000000       0.000000    0.000000e+00    0.000000e+00      0.000000        0.000000  0.000000    DDoS
411        0.000000       0.000000    0.000000e+00    0.000000e+00      0.000000        0.000000  0.000000    DDoS
331        0.022981       0.020185    3.938907e-09    3.938907e-09      0.022981        0.000000  0.025641  BENIGN
398        0.000000       0.000000    0.000000e+00    0.000000e+00      0.000000        0.000000  0.000000    DDoS
477        0.000000       0.000000    0.000000e+00    0.000000e+00      0.000000        0.000000  0.000000    DDoS
184        0.014773       0.025952    5.064309e-09    5.064309e-09      0.014773        0.000000  0.000000  BENIGN
277        0.487525       0.423875    2.089027e-05    2.089027e-05      0.487525        0.445572  0.179487  BENIGN
353        0.021011       0.018454    3.601286e-09    3.601286e-09      0.021011        0.000000  0.025641  BENIGN
44         0.012147       0.017878    2.081994e-09    2.081994e-09      0.012147        0.000488  0.025641  BENIGN
324        0.143467       0.252018    3.073754e-05    3.073754e-05      0.143467        0.445572  0.025641  BENIGN
55         0.001970       0.003460    6.752412e-10    6.752412e-10      0.001970        0.004501  0.000000  BENIGN
377        0.022981       0.020185    3.938907e-09    3.938907e-09      0.022981        0.000000  0.025641  BENIGN
333        0.022981       0.020185    3.938907e-09    3.938907e-09      0.022981        0.000000  0.025641  BENIGN
65         0.003940       0.003460    6.752412e-10    6.752412e-10      0.003940        0.014847  0.025641  BENIGN
130        0.044320       0.026528    3.038585e-09    3.038585e-09      0.044320        0.003860  0.102564  BENIGN
337        0.022981       0.020185    3.938907e-09    3.938907e-09      0.022981        0.000000  0.025641  BENIGN
214        0.003940       0.003460    6.752412e-10    6.752412e-10      0.003940        0.003922  0.025641  BENIGN
13         0.001970       0.003460    6.752412e-10    6.752412e-10      0.001970        0.014450  0.000000  BENIGN
```

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

273	0.773802	0.446367	6.631431e-06	6.631431e-06	0.773802	0.445572	1.000000	BENIGN
355	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
143	0.033487	0.029412	5.739550e-09	5.739550e-09	0.033487	0.000000	0.025641	BENIGN
405	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
86	0.021668	0.019031	3.713826e-09	3.713826e-09	0.021668	0.000000	0.025641	BENIGN
361	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
149	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.000015	0.025641	BENIGN
186	0.037426	0.032872	4.276527e-09	4.276527e-09	0.037426	0.022049	0.025641	BENIGN
275	0.237689	0.403691	1.357985e-01	1.357985e-01	0.237689	0.445572	0.128205	BENIGN
18	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.001923	0.025641	BENIGN
1	0.003940	0.003460	4.501608e-10	4.501608e-10	0.003940	0.125015	0.051282	BENIGN
290	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004013	0.000000	BENIGN
424	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
140	0.033487	0.029412	5.739550e-09	5.739550e-09	0.033487	0.000000	0.025641	BENIGN
352	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
165	0.314511	0.196655	4.492229e-01	4.492229e-01	0.314511	1.000000	0.307692	BENIGN
444	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
282	0.611622	0.359285	2.329582e-08	2.329582e-08	0.611622	0.445572	0.205128	BENIGN
469	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
456	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
83	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000946	0.000000	BENIGN
461	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
218	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
363	0.025607	0.022491	4.389068e-09	4.389068e-09	0.025607	0.000000	0.025641	BENIGN
187	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.022049	0.000000	BENIGN
236	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.000488	0.025641	BENIGN
272	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.005249	0.000000	BENIGN
441	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
388	0.021668	0.019031	3.713826e-09	3.713826e-09	0.021668	0.000000	0.025641	BENIGN
470	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
101	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.006607	0.102564	BENIGN
276	0.615890	0.374856	2.345838e-01	2.345838e-01	0.615890	0.445572	0.205128	BENIGN
349	0.020355	0.017878	3.488746e-09	3.488746e-09	0.020355	0.000000	0.025641	BENIGN
22	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.001755	0.000000	BENIGN
108	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
159	0.015758	0.027682	5.401929e-09	5.401929e-09	0.015758	0.000000	0.000000	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

72	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005371	0.025641	BENIGN
128	0.034143	0.029988	5.852090e-09	5.852090e-09	0.034143	0.000000	0.025641	BENIGN
31	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
479	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
473	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
475	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
334	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
99	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003906	0.000000	BENIGN
121	0.042022	0.018454	3.601286e-09	3.601286e-09	0.042022	0.000000	0.076923	BENIGN
112	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003891	0.102564	BENIGN
250	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.001694	0.025641	BENIGN
169	0.022324	0.019608	3.826367e-09	3.826367e-09	0.022324	0.000000	0.025641	BENIGN
323	0.015758	0.027682	5.401929e-09	5.401929e-09	0.015758	0.000000	0.000000	BENIGN
420	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
160	0.015758	0.027682	5.401929e-09	5.401929e-09	0.015758	0.000000	0.000000	BENIGN
423	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
391	0.024951	0.021915	4.276527e-09	4.276527e-09	0.024951	0.000000	0.025641	BENIGN
98	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003922	0.102564	BENIGN
116	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003891	0.102564	BENIGN
357	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
57	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004501	0.000000	BENIGN
447	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
75	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.006393	0.025641	BENIGN
190	0.230794	0.153979	8.790640e-01	8.790640e-01	0.230794	0.445572	0.102564	BENIGN
103	0.021011	0.026528	1.800643e-09	1.800643e-09	0.021011	0.003906	0.076923	BENIGN
478	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
199	0.031517	0.027682	5.401929e-09	5.401929e-09	0.031517	0.000000	0.025641	BENIGN
296	0.973736	0.337947	2.781618e-01	2.781618e-01	0.973736	0.445572	0.282051	BENIGN
213	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
338	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
457	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
486	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
37	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000504	0.025641	BENIGN
350	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
362	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
91	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003906	0.102564	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

367	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
284	0.819107	0.371972	2.807878e-08	2.807878e-08	0.819107	0.445572	0.230769	BENIGN
127	0.055154	0.024221	4.726688e-09	4.726688e-09	0.055154	0.000000	0.076923	BENIGN
480	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
188	0.230794	0.153979	8.790640e-01	8.790640e-01	0.230794	0.445572	0.102564	BENIGN
164	0.409718	0.445790	6.688103e-01	6.688103e-01	0.409718	1.000000	0.153846	BENIGN
211	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
48	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
157	0.143467	0.252018	3.073754e-05	3.073754e-05	0.143467	0.445572	0.025641	BENIGN
383	0.022324	0.019608	3.826367e-09	3.826367e-09	0.022324	0.000000	0.025641	BENIGN
139	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
516	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
33	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000504	0.025641	BENIGN
453	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
179	0.017400	0.030565	5.964630e-09	5.964630e-09	0.017400	0.000000	0.000000	BENIGN
194	0.022324	0.019608	3.826367e-09	3.826367e-09	0.022324	0.000000	0.025641	BENIGN
261	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.001816	0.000000	BENIGN
20	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.001892	0.025641	BENIGN
254	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.001770	0.000000	BENIGN
235	0.001970	0.003460	3.376206e-10	3.376206e-10	0.001970	0.000488	0.025641	BENIGN
227	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
126	0.039396	0.017301	3.376206e-09	3.376206e-09	0.039396	0.000000	0.076923	BENIGN
230	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.000458	0.025641	BENIGN
495	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
310	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004135	0.000000	BENIGN
303	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003891	0.000000	BENIGN
427	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
269	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.000458	0.000000	BENIGN
500	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
135	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
212	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
425	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
132	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.125015	0.000000	BENIGN
313	0.224228	0.393887	2.562165e-01	2.562165e-01	0.224228	0.445572	0.025641	BENIGN
156	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.445572	0.000000	BENIGN
309	1.000000	1.000000	5.713290e-01	5.713290e-01	1.000000	0.445572	0.128205	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

394	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
7	0.014117	0.017878	1.613076e-01	1.613076e-01	0.014117	0.003754	0.051282	BENIGN
412	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
167	0.301707	0.279700	7.955726e-01	7.955726e-01	0.301707	1.000000	0.128205	BENIGN
521	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
245	0.087656	0.132641	1.001608e-08	1.001608e-08	0.087656	0.003632	0.051282	BENIGN
458	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
523	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
356	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
29	0.024622	0.021915	2.813505e-09	2.813505e-09	0.024622	0.000488	0.051282	BENIGN
439	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
8	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.008926	0.025641	BENIGN
152	0.120486	0.121107	5.162781e-06	5.162781e-06	0.120486	0.445572	0.076923	BENIGN
207	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.125015	0.000000	BENIGN
364	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
527	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
129	0.048588	0.021338	4.163987e-09	4.163987e-09	0.048588	0.000000	0.076923	BENIGN
511	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
142	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
529	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
287	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003632	0.000000	BENIGN
321	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.006042	0.000000	BENIGN
382	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
446	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
89	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.003632	0.000000	BENIGN
347	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
258	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.001816	0.000000	BENIGN
9	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.005768	0.000000	BENIGN
505	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
241	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
376	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
525	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
148	0.423835	0.192618	8.071633e-01	8.071633e-01	0.423835	0.445572	0.128205	BENIGN
307	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004013	0.000000	BENIGN
490	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
32	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

421	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
450	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
308	0.003940	0.003460	4.501608e-10	4.501608e-10	0.003940	0.445572	0.051282	BENIGN
343	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
2	0.003940	0.003460	4.501608e-10	4.501608e-10	0.003940	0.125015	0.051282	BENIGN
208	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.028381	0.025641	BENIGN
372	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
520	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
21	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.001892	0.025641	BENIGN
463	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
410	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
297	0.586999	0.337947	2.235798e-01	2.235798e-01	0.586999	0.445572	0.205128	BENIGN
4	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.014847	0.000000	BENIGN
485	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
436	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
201	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.125015	0.000000	BENIGN
358	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
173	0.014117	0.024798	4.839228e-09	4.839228e-09	0.014117	0.000000	0.000000	BENIGN
499	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
94	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003952	0.000000	BENIGN
224	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.001953	0.025641	BENIGN
58	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.000519	0.025641	BENIGN
46	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
0	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
488	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
481	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
409	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
111	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
465	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
181	0.019041	0.033449	6.527331e-09	6.527331e-09	0.019041	0.000000	0.000000	BENIGN
209	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
5	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
300	0.779383	0.337947	2.671704e-08	2.671704e-08	0.779383	0.445572	0.230769	BENIGN
345	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
124	0.023638	0.020761	4.051447e-09	4.051447e-09	0.023638	0.000000	0.025641	BENIGN
217	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

265	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004379	0.000000	BENIGN
278	0.247538	0.420992	1.414255e-01	1.414255e-01	0.247538	0.445572	0.128205	BENIGN
3	0.311228	0.250865	6.275771e-01	6.275771e-01	0.311228	0.125015	0.384615	BENIGN
82	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.002762	0.025641	BENIGN
174	0.018056	0.031719	6.189711e-09	6.189711e-09	0.018056	0.000000	0.000000	BENIGN
472	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
215	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003922	0.000000	BENIGN
34	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000504	0.025641	BENIGN
120	0.042022	0.018454	3.601286e-09	3.601286e-09	0.042022	0.000000	0.076923	BENIGN
304	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004013	0.000000	BENIGN
506	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
312	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.003632	0.000000	BENIGN
448	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
397	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
237	0.003940	0.003460	4.501608e-10	4.501608e-10	0.003940	0.000488	0.025641	BENIGN
315	0.219961	0.382930	2.513398e-01	2.513398e-01	0.219961	0.445572	0.051282	BENIGN
384	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
454	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
508	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
74	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005646	0.025641	BENIGN
76	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.005386	0.000000	BENIGN
471	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
204	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003922	0.000000	BENIGN
104	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003922	0.102564	BENIGN
79	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005508	0.025641	BENIGN
530	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
24	0.308601	0.542099	1.057878e-07	1.057878e-07	0.308601	0.075577	0.000000	BENIGN
317	0.280696	0.248558	3.006933e-04	3.006933e-04	0.280696	0.445572	0.051282	BENIGN
369	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
102	0.017072	0.026528	2.926045e-09	2.926045e-09	0.017072	0.003922	0.025641	BENIGN
459	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
318	0.143467	0.252018	4.918006e-09	4.918006e-09	0.143467	0.445572	0.025641	BENIGN
69	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005920	0.025641	BENIGN
23	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.010376	0.000000	BENIGN
443	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
371	0.025607	0.022491	4.389068e-09	4.389068e-09	0.025607	0.000000	0.025641	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

113	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
110	0.188444	0.105536	6.459807e-09	6.459807e-09	0.188444	0.003906	0.230769	BENIGN
39	0.014117	0.017878	1.613076e-01	1.613076e-01	0.014117	0.000488	0.051282	BENIGN
322	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.018723	0.000000	BENIGN
141	0.027577	0.024221	4.726688e-09	4.726688e-09	0.027577	0.000000	0.025641	BENIGN
513	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
92	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003906	0.000000	BENIGN
406	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
225	0.014117	0.017878	1.613076e-01	1.613076e-01	0.014117	0.001953	0.051282	BENIGN
387	0.021668	0.019031	3.713826e-09	3.713826e-09	0.021668	0.000000	0.025641	BENIGN
35	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000504	0.025641	BENIGN
84	0.040381	0.026528	2.768489e-09	2.768489e-09	0.040381	0.004837	0.051282	BENIGN
238	0.003940	0.003460	4.501608e-10	4.501608e-10	0.003940	0.000488	0.025641	BENIGN
239	0.003940	0.003460	4.501608e-10	4.501608e-10	0.003940	0.000488	0.025641	BENIGN
64	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005508	0.025641	BENIGN
491	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
175	0.015430	0.027105	5.289389e-09	5.289389e-09	0.015430	0.000000	0.000000	BENIGN
115	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003922	0.102564	BENIGN
96	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003891	0.102564	BENIGN
166	0.012147	0.021338	1.040997e-09	1.040997e-09	0.012147	1.000000	0.025641	BENIGN
154	0.120486	0.121107	4.589139e-01	4.589139e-01	0.120486	0.445572	0.076923	BENIGN
316	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003632	0.025641	BENIGN
266	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004379	0.000000	BENIGN
496	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
170	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.000015	0.025641	BENIGN
155	0.120486	0.121107	4.589139e-01	4.589139e-01	0.120486	0.445572	0.076923	BENIGN

==========

DATA TESTING

	TotLenFwdPckt	FwdPcktLenMax	FwdPcktLenMean	AvgFwdSgmnSize	SubFlFwdByts	InitWinBytsFwd	ActvData	Label
73	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005371	0.025641	BENIGN
437	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
502	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
206	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003860	0.025641	BENIGN
438	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
263	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.004364	0.000000	BENIGN
171	0.043007	0.065167	2.948553e-09	2.948553e-09	0.043007	1.000000	0.102564	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

242	0.001970	0.003460	3.376206e-10	3.376206e-10	0.001970	0.000488	0.025641	BENIGN
203	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
482	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
193	0.022324	0.019608	3.826367e-09	3.826367e-09	0.022324	0.000000	0.025641	BENIGN
305	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004135	0.000000	BENIGN
202	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
314	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.003632	0.000000	BENIGN
325	0.364084	0.238754	5.943194e-01	5.943194e-01	0.364084	0.445572	0.230769	BENIGN
385	0.021668	0.019031	3.713826e-09	3.713826e-09	0.021668	0.000000	0.025641	BENIGN
354	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
392	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
52	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.004364	0.000000	BENIGN
375	0.020355	0.017878	3.488746e-09	3.488746e-09	0.020355	0.000000	0.025641	BENIGN
232	0.001970	0.003460	3.376206e-10	3.376206e-10	0.001970	0.000488	0.025641	BENIGN
280	0.811884	0.362168	2.783119e-08	2.783119e-08	0.811884	0.445572	0.230769	BENIGN
45	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
430	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
240	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
117	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
195	0.022324	0.019608	3.826367e-09	3.826367e-09	0.022324	0.000000	0.025641	BENIGN
87	0.040381	0.026528	2.768489e-09	2.768489e-09	0.040381	0.006531	0.051282	BENIGN
396	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
416	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
88	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.003662	0.000000	BENIGN
136	0.149376	0.248558	8.534298e-01	8.534298e-01	0.149376	0.125015	0.128205	BENIGN
183	0.028890	0.050750	9.903537e-09	9.903537e-09	0.028890	0.000000	0.000000	BENIGN
66	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005630	0.025641	BENIGN
510	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
257	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.001816	0.000000	BENIGN
260	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.001816	0.000000	BENIGN
442	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
172	0.014117	0.024798	4.839228e-09	4.839228e-09	0.014117	0.000000	0.000000	BENIGN
346	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
12	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.014450	0.000000	BENIGN
467	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
134	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003860	0.102564	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

299	0.777413	0.337947	2.961058e-01	2.961058e-01	0.777413	0.445572	0.205128	BENIGN
106	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
389	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
419	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
223	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.000473	0.000000	BENIGN
507	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
210	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
476	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
359	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
220	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
81	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005768	0.025641	BENIGN
196	0.453053	0.208766	9.706592e-09	9.706592e-09	0.453053	0.125015	0.384615	BENIGN
365	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
105	0.120158	0.110150	5.884244e-01	5.884244e-01	0.120158	0.125015	0.153846	BENIGN
221	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003876	0.025641	BENIGN
433	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
514	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
168	0.012147	0.021338	1.387996e-01	1.387996e-01	0.012147	0.995132	0.025641	BENIGN
150	0.120486	0.121107	4.589139e-01	4.589139e-01	0.120486	0.445572	0.076923	BENIGN
59	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.007767	0.000000	BENIGN
320	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.009369	0.000000	BENIGN
54	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004471	0.000000	BENIGN
26	0.138214	0.242791	4.737942e-08	4.737942e-08	0.138214	0.076782	0.000000	BENIGN
298	0.777413	0.337947	2.961058e-01	2.961058e-01	0.777413	0.445572	0.205128	BENIGN
205	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
401	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
509	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
95	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003937	0.102564	BENIGN
78	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005630	0.025641	BENIGN
30	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
244	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.006042	0.025641	BENIGN
379	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
274	0.005909	0.003460	5.064309e-10	5.064309e-10	0.005909	0.445572	0.076923	BENIGN
283	0.593894	0.350058	2.262058e-08	2.262058e-08	0.593894	0.445572	0.205128	BENIGN
378	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
522	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

368	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
519	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
19	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.001923	0.025641	BENIGN
249	0.027249	0.026528	3.113612e-01	3.113612e-01	0.027249	0.001923	0.051282	BENIGN
51	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
370	0.020355	0.017878	3.488746e-09	3.488746e-09	0.020355	0.000000	0.025641	BENIGN
49	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
271	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.001770	0.000000	BENIGN
14	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.014969	0.000000	BENIGN
17	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.001892	0.000000	BENIGN
339	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
504	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
360	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
63	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005630	0.025641	BENIGN
151	0.120486	0.121107	4.589139e-01	4.589139e-01	0.120486	0.445572	0.076923	BENIGN
329	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
528	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
395	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
158	0.143467	0.252018	3.073754e-05	3.073754e-05	0.143467	0.445572	0.025641	BENIGN
404	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
366	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
41	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
526	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
407	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
53	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.004364	0.000000	BENIGN
293	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004013	0.000000	BENIGN
118	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003876	0.102564	BENIGN
489	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
47	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
11	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.000015	0.000000	BENIGN
326	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
279	0.256074	0.435986	1.463023e-08	1.463023e-08	0.256074	0.445572	0.128205	BENIGN
10	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005768	0.025641	BENIGN
27	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.066849	0.000000	BENIGN
492	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
512	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

281	0.806632	0.359285	2.765113e-08	2.765113e-08	0.806632	0.445572	0.230769	BENIGN
484	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
332	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
256	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.001816	0.000000	BENIGN
119	0.123769	0.168973	2.651728e-05	2.651728e-05	0.123769	0.125015	0.384615	BENIGN
36	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000504	0.025641	BENIGN
180	0.020355	0.035755	6.977492e-09	6.977492e-09	0.020355	0.000000	0.000000	BENIGN
107	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.000015	0.000000	BENIGN
288	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003891	0.000000	BENIGN
386	0.023638	0.020761	4.051447e-09	4.051447e-09	0.023638	0.000000	0.025641	BENIGN
62	0.027249	0.026528	3.113612e-01	3.113612e-01	0.027249	0.006058	0.051282	BENIGN
144	0.027577	0.024221	4.726688e-09	4.726688e-09	0.027577	0.000000	0.025641	BENIGN
43	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
252	0.010177	0.017878	1.744373e-09	1.744373e-09	0.010177	0.001831	0.000000	BENIGN
306	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003891	0.000000	BENIGN
153	0.120486	0.121107	4.589139e-01	4.589139e-01	0.120486	0.445572	0.076923	BENIGN
114	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003952	0.000000	BENIGN
259	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.001816	0.000000	BENIGN
248	0.027249	0.026528	3.113612e-01	3.113612e-01	0.027249	0.001968	0.051282	BENIGN
435	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
426	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
270	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.001770	0.000000	BENIGN
380	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
413	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
393	0.021668	0.019031	3.713826e-09	3.713826e-09	0.021668	0.000000	0.025641	BENIGN
518	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
163	0.015758	0.027682	5.401929e-09	5.401929e-09	0.015758	0.000000	0.000000	BENIGN
494	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
501	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
162	0.015758	0.027682	5.401929e-09	5.401929e-09	0.015758	0.000000	0.000000	BENIGN
255	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.002014	0.025641	BENIGN
251	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.001785	0.000000	BENIGN
177	0.015758	0.027682	5.401929e-09	5.401929e-09	0.015758	0.000000	0.000000	BENIGN
178	0.020355	0.035755	6.977492e-09	6.977492e-09	0.020355	0.000000	0.000000	BENIGN
40	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
234	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.000488	0.025641	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

122	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
294	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004013	0.000000	BENIGN
264	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.004333	0.000000	BENIGN
336	0.020355	0.017878	3.488746e-09	3.488746e-09	0.020355	0.000000	0.025641	BENIGN
198	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
182	0.017400	0.030565	5.964630e-09	5.964630e-09	0.017400	0.000000	0.000000	BENIGN
468	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
301	0.586999	0.337947	2.235798e-01	2.235798e-01	0.586999	0.445572	0.205128	BENIGN
498	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
161	0.015758	0.027682	5.401929e-09	5.401929e-09	0.015758	0.000000	0.000000	BENIGN
267	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	BENIGN
445	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
327	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
286	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003632	0.000000	BENIGN
524	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
381	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
253	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.001770	0.000000	BENIGN
434	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
464	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
451	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
402	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
460	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
138	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
243	0.007879	0.003460	6.752412e-10	6.752412e-10	0.007879	0.010117	0.076923	BENIGN
531	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
295	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.015366	0.000000	BENIGN
285	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003632	0.000000	BENIGN
428	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
429	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
16	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.014450	0.000000	BENIGN
262	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.007843	0.000000	BENIGN
70	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005707	0.025641	BENIGN
344	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
247	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.014450	0.000000	BENIGN
493	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
503	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

432	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
80	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005768	0.025641	BENIGN
191	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.004883	0.000000	BENIGN
147	0.117531	0.115917	4.476599e-01	4.476599e-01	0.117531	0.445572	0.076923	BENIGN
85	0.021668	0.019031	3.713826e-09	3.713826e-09	0.021668	0.000000	0.025641	BENIGN
145	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
292	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003754	0.000000	BENIGN
15	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.014450	0.000000	BENIGN
319	0.150033	0.263552	3.214429e-05	3.214429e-05	0.150033	0.445572	0.025641	BENIGN
176	0.021011	0.036909	7.202572e-09	7.202572e-09	0.021011	0.000000	0.000000	BENIGN
330	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
311	0.224885	0.395040	2.569668e-01	2.569668e-01	0.224885	0.445572	0.025641	BENIGN
415	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
233	0.003940	0.003460	4.501608e-10	4.501608e-10	0.003940	0.000488	0.025641	BENIGN
222	0.408404	0.337947	1.000000e+00	1.000000e+00	0.408404	0.003922	0.333333	BENIGN
56	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004654	0.000000	BENIGN
38	0.014117	0.017878	1.613076e-01	1.613076e-01	0.014117	0.000488	0.051282	BENIGN
497	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
131	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003845	0.102564	BENIGN
246	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.005722	0.000000	BENIGN
189	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.004654	0.000000	BENIGN
291	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003891	0.000000	BENIGN
42	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
100	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.125015	0.000000	BENIGN
466	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
408	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
185	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.125015	0.000000	BENIGN
483	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
342	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
71	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005508	0.025641	BENIGN
348	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
341	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
123	0.028890	0.025375	4.951768e-09	4.951768e-09	0.028890	0.000000	0.025641	BENIGN
228	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
146	0.015758	0.027682	5.401929e-09	5.401929e-09	0.015758	0.000000	0.000000	BENIGN
403	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

374	0.020355	0.017878	3.488746e-09	3.488746e-09	0.020355	0.000000	0.025641	BENIGN
474	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
414	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
60	0.102101	0.158016	1.166667e-01	1.166667e-01	0.102101	0.003632	0.051282	BENIGN
90	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003906	0.102564	BENIGN
422	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
515	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
373	0.025607	0.022491	4.389068e-09	4.389068e-09	0.025607	0.000000	0.025641	BENIGN
302	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.004013	0.000000	BENIGN
400	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
50	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
133	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.125015	0.000000	BENIGN
399	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
192	0.022324	0.019608	3.826367e-09	3.826367e-09	0.022324	0.000000	0.025641	BENIGN
289	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003891	0.000000	BENIGN
449	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
93	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
28	0.024622	0.021915	2.813505e-09	2.813505e-09	0.024622	0.000488	0.051282	BENIGN
231	0.001970	0.003460	3.376206e-10	3.376206e-10	0.001970	0.000488	0.025641	BENIGN
418	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
340	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
328	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
68	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.005341	0.000000	BENIGN
216	0.001970	0.003460	6.752412e-10	6.752412e-10	0.001970	0.003922	0.000000	BENIGN
517	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
351	0.021011	0.018454	3.601286e-09	3.601286e-09	0.021011	0.000000	0.025641	BENIGN
6	0.012147	0.017878	2.081994e-09	2.081994e-09	0.012147	0.000488	0.025641	BENIGN
200	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.125015	0.000000	BENIGN
462	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
335	0.022981	0.020185	3.938907e-09	3.938907e-09	0.022981	0.000000	0.025641	BENIGN
109	0.044320	0.026528	3.038585e-09	3.038585e-09	0.044320	0.003952	0.102564	BENIGN
67	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.005508	0.025641	BENIGN
431	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS
219	0.003940	0.003460	6.752412e-10	6.752412e-10	0.003940	0.003922	0.025641	BENIGN
197	0.016087	0.021338	1.838156e-01	1.838156e-01	0.016087	0.249100	0.051282	BENIGN
440	0.000000	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000	DDoS

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

```
77        0.000000        0.000000    0.000000e+00    0.000000e+00    0.000000        0.005234  0.000000  BENIGN
452       0.000000        0.000000    0.000000e+00    0.000000e+00    0.000000        0.000000  0.000000    DDoS
137       0.003940        0.003460    6.752412e-10    6.752412e-10    0.003940        0.003922  0.025641  BENIGN
97        0.044320        0.026528    3.038585e-09    3.038585e-09    0.044320        0.003937  0.102564  BENIGN
390       0.021668        0.019031    3.713826e-09    3.713826e-09    0.021668        0.000000  0.025641  BENIGN
417       0.000000        0.000000    0.000000e+00    0.000000e+00    0.000000        0.000000  0.000000    DDoS
229       0.003940        0.003460    6.752412e-10    6.752412e-10    0.003940        0.000473  0.025641  BENIGN
==========
Starting time: 33924 second
==========
DATA PREDIKSI
 73     BENIGN
437      DDoS
502      DDoS
206    BENIGN
438      DDoS
263    BENIGN
171    BENIGN
242    BENIGN
203    BENIGN
482      DDoS
193    BENIGN
305    BENIGN
202    BENIGN
314    BENIGN
325    BENIGN
385    BENIGN
354    BENIGN
392    BENIGN
52     BENIGN
375    BENIGN
232    BENIGN
280    BENIGN
45     BENIGN
430      DDoS
240    BENIGN
```

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

117	BENIGN
195	BENIGN
87	BENIGN
396	DDoS
416	DDoS
88	BENIGN
136	BENIGN
183	BENIGN
66	BENIGN
510	DDoS
257	BENIGN
260	BENIGN
442	DDoS
172	BENIGN
346	BENIGN
12	BENIGN
467	DDoS
134	BENIGN
299	BENIGN
106	BENIGN
389	BENIGN
419	DDoS
223	BENIGN
507	DDoS
210	BENIGN
476	DDoS
359	BENIGN
220	BENIGN
81	BENIGN
196	BENIGN
365	BENIGN
105	BENIGN
221	BENIGN
433	DDoS
514	DDoS
168	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

150	BENIGN
59	BENIGN
320	BENIGN
54	BENIGN
26	BENIGN
298	BENIGN
205	BENIGN
401	DDoS
509	DDoS
95	BENIGN
78	BENIGN
30	BENIGN
244	BENIGN
379	BENIGN
274	BENIGN
283	BENIGN
378	BENIGN
522	DDoS
368	BENIGN
519	DDoS
19	BENIGN
249	BENIGN
51	BENIGN
370	BENIGN
49	BENIGN
271	BENIGN
14	BENIGN
17	BENIGN
339	BENIGN
504	DDoS
360	BENIGN
63	BENIGN
151	BENIGN
329	BENIGN
528	DDoS
395	DDoS

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

158	BENIGN
404	DDoS
366	BENIGN
41	BENIGN
526	DDoS
407	DDoS
53	BENIGN
293	BENIGN
118	BENIGN
489	DDoS
47	BENIGN
11	BENIGN
326	BENIGN
279	BENIGN
10	BENIGN
27	BENIGN
492	DDoS
512	DDoS
281	BENIGN
484	DDoS
332	BENIGN
256	BENIGN
119	BENIGN
36	BENIGN
180	BENIGN
107	BENIGN
288	BENIGN
386	BENIGN
62	BENIGN
144	BENIGN
43	BENIGN
252	BENIGN
306	BENIGN
153	BENIGN
114	BENIGN
259	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

248	BENIGN
435	DDoS
426	DDoS
270	BENIGN
380	BENIGN
413	DDoS
393	BENIGN
518	DDoS
163	BENIGN
494	DDoS
501	DDoS
162	BENIGN
255	BENIGN
251	BENIGN
177	BENIGN
178	BENIGN
40	BENIGN
234	BENIGN
122	BENIGN
294	BENIGN
264	BENIGN
336	BENIGN
198	BENIGN
182	BENIGN
468	DDoS
301	BENIGN
498	DDoS
161	BENIGN
267	DDoS
445	DDoS
327	BENIGN
286	BENIGN
524	DDoS
381	BENIGN
253	BENIGN
434	DDoS

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

464	DDoS
451	DDoS
402	DDoS
460	DDoS
138	BENIGN
243	BENIGN
531	DDoS
295	BENIGN
285	BENIGN
428	DDoS
429	DDoS
16	BENIGN
262	BENIGN
70	BENIGN
344	BENIGN
247	BENIGN
493	DDoS
503	DDoS
432	DDoS
80	BENIGN
191	BENIGN
147	BENIGN
85	BENIGN
145	BENIGN
292	BENIGN
15	BENIGN
319	BENIGN
176	BENIGN
330	BENIGN
311	BENIGN
415	DDoS
233	BENIGN
222	BENIGN
56	BENIGN
38	BENIGN
497	DDoS

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

131	BENIGN
246	BENIGN
189	BENIGN
291	BENIGN
42	BENIGN
100	BENIGN
466	DDoS
408	DDoS
185	BENIGN
483	DDoS
342	BENIGN
71	BENIGN
348	BENIGN
341	BENIGN
123	BENIGN
228	BENIGN
146	BENIGN
403	DDoS
374	BENIGN
474	DDoS
414	DDoS
60	BENIGN
90	BENIGN
422	DDoS
515	DDoS
373	BENIGN
302	BENIGN
400	DDoS
50	BENIGN
133	BENIGN
399	DDoS
192	BENIGN
289	BENIGN
449	DDoS
93	BENIGN
28	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

```
231    BENIGN
418      DDoS
340    BENIGN
328    BENIGN
68     BENIGN
216    BENIGN
517      DDoS
351    BENIGN
6      BENIGN
200    BENIGN
462      DDoS
335    BENIGN
109    BENIGN
67     BENIGN
431      DDoS
219    BENIGN
197    BENIGN
440      DDoS
77     BENIGN
452      DDoS
137    BENIGN
97     BENIGN
390    BENIGN
417      DDoS
229    BENIGN
Name: 0, dtype: object
==========
DATA AKTUAL
 73     BENIGN
437      DDoS
502      DDoS
206    BENIGN
438      DDoS
263    BENIGN
171    BENIGN
242    BENIGN
```

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

203	BENIGN
482	DDoS
193	BENIGN
305	BENIGN
202	BENIGN
314	BENIGN
325	BENIGN
385	BENIGN
354	BENIGN
392	BENIGN
52	BENIGN
375	BENIGN
232	BENIGN
280	BENIGN
45	BENIGN
430	DDoS
240	BENIGN
117	BENIGN
195	BENIGN
87	BENIGN
396	DDoS
416	DDoS
88	BENIGN
136	BENIGN
183	BENIGN
66	BENIGN
510	DDoS
257	BENIGN
260	BENIGN
442	DDoS
172	BENIGN
346	BENIGN
12	BENIGN
467	DDoS
134	BENIGN
299	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

106	BENIGN
389	BENIGN
419	DDoS
223	BENIGN
507	DDoS
210	BENIGN
476	DDoS
359	BENIGN
220	BENIGN
81	BENIGN
196	BENIGN
365	BENIGN
105	BENIGN
221	BENIGN
433	DDoS
514	DDoS
168	BENIGN
150	BENIGN
59	BENIGN
320	BENIGN
54	BENIGN
26	BENIGN
298	BENIGN
205	BENIGN
401	DDoS
509	DDoS
95	BENIGN
78	BENIGN
30	BENIGN
244	BENIGN
379	BENIGN
274	BENIGN
283	BENIGN
378	BENIGN
522	DDoS
368	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

519	DDoS
19	BENIGN
249	BENIGN
51	BENIGN
370	BENIGN
49	BENIGN
271	BENIGN
14	BENIGN
17	BENIGN
339	BENIGN
504	DDoS
360	BENIGN
63	BENIGN
151	BENIGN
329	BENIGN
528	DDoS
395	DDoS
158	BENIGN
404	DDoS
366	BENIGN
41	BENIGN
526	DDoS
407	DDoS
53	BENIGN
293	BENIGN
118	BENIGN
489	DDoS
47	BENIGN
11	BENIGN
326	BENIGN
279	BENIGN
10	BENIGN
27	BENIGN
492	DDoS
512	DDoS
281	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

484	DDoS
332	BENIGN
256	BENIGN
119	BENIGN
36	BENIGN
180	BENIGN
107	BENIGN
288	BENIGN
386	BENIGN
62	BENIGN
144	BENIGN
43	BENIGN
252	BENIGN
306	BENIGN
153	BENIGN
114	BENIGN
259	BENIGN
248	BENIGN
435	DDoS
426	DDoS
270	BENIGN
380	BENIGN
413	DDoS
393	BENIGN
518	DDoS
163	BENIGN
494	DDoS
501	DDoS
162	BENIGN
255	BENIGN
251	BENIGN
177	BENIGN
178	BENIGN
40	BENIGN
234	BENIGN
122	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

294	BENIGN
264	BENIGN
336	BENIGN
198	BENIGN
182	BENIGN
468	DDoS
301	BENIGN
498	DDoS
161	BENIGN
267	BENIGN
445	DDoS
327	BENIGN
286	BENIGN
524	DDoS
381	BENIGN
253	BENIGN
434	DDoS
464	DDoS
451	DDoS
402	DDoS
460	DDoS
138	BENIGN
243	BENIGN
531	DDoS
295	BENIGN
285	BENIGN
428	DDoS
429	DDoS
16	BENIGN
262	BENIGN
70	BENIGN
344	BENIGN
247	BENIGN
493	DDoS
503	DDoS
432	DDoS

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

80	BENIGN
191	BENIGN
147	BENIGN
85	BENIGN
145	BENIGN
292	BENIGN
15	BENIGN
319	BENIGN
176	BENIGN
330	BENIGN
311	BENIGN
415	DDoS
233	BENIGN
222	BENIGN
56	BENIGN
38	BENIGN
497	DDoS
131	BENIGN
246	BENIGN
189	BENIGN
291	BENIGN
42	BENIGN
100	BENIGN
466	DDoS
408	DDoS
185	BENIGN
483	DDoS
342	BENIGN
71	BENIGN
348	BENIGN
341	BENIGN
123	BENIGN
228	BENIGN
146	BENIGN
403	DDoS
374	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

474	DDoS
414	DDoS
60	BENIGN
90	BENIGN
422	DDoS
515	DDoS
373	BENIGN
302	BENIGN
400	DDoS
50	BENIGN
133	BENIGN
399	DDoS
192	BENIGN
289	BENIGN
449	DDoS
93	BENIGN
28	BENIGN
231	BENIGN
418	DDoS
340	BENIGN
328	BENIGN
68	BENIGN
216	BENIGN
517	DDoS
351	BENIGN
6	BENIGN
200	BENIGN
462	DDoS
335	BENIGN
109	BENIGN
67	BENIGN
431	DDoS
219	BENIGN
197	BENIGN
440	DDoS
77	BENIGN

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

```
452      DDoS
137    BENIGN
97     BENIGN
390    BENIGN
417      DDoS
229    BENIGN
Name: Label, dtype: object
==========
Ending time:  33925 second
==========
Berikut adalah confusion matrix :
 [[195   1]
 [  0  70]]
==========
 True Negative:  195
 False Positive:  1
 False Negative:  0
 True Positive:  70
==========
['BENIGN' 'DDoS']
[195  71]
==========
duration 1 second
akurasi:  99.62406015037594
presisi:  98.59154929577466
recall:  100.0
f-measure:  99.29078014184398
```

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

Uji Coba pada Set Data Sekunder

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

```
C:\Users\damar\PycharmProjects\Latihan\venv\Scripts\python.exe "C:\Program Files\JetBrains\PyCharm 2019.3.2\plugins\python\
helpers\pydev\pydevconsole.py" --mode=client --port=64864

import sys; print('Python %s on %s' % (sys.version, sys.platform))
sys.path.extend(['C:\\Users\\damar\\PycharmProjects\\Latihan', 'C:/Users/damar/PycharmProjects/Latihan'])

PyDev console: starting.

Python 3.7.6 (tags/v3.7.6:43364a7ae0, Dec 19 2019, 00:42:30) [MSC v.1916 64 bit (AMD64)] on win32
>>> runfile('C:/Users/damar/PycharmProjects/Latihan/RandomForest.py', wdir='C:/Users/damar/PycharmProjects/Latihan')
DATA TRAINING
        TotLenFwdPckt  FwdPcktLenMax  FwdPcktLenMean  AvgFwdSgmnSize  SubFlFwdByts  InitWinBytsFwd  ActvData   Label
30576        0.000306       0.001712    7.005004e-10    7.005004e-10      0.000306        0.003922  0.003107    DDoS
27564        0.000142       0.001712    8.672862e-01    8.672862e-01      0.000142        0.125015  0.001036    DDoS
21202        0.000306       0.001712    7.005004e-10    7.005004e-10      0.000306        0.003922  0.003107    DDoS
2367         0.000470       0.003682    4.303074e-09    4.303074e-09      0.000470        0.000000  0.000518  BENIGN
41348        0.000377       0.005908    6.904932e-09    6.904932e-09      0.000377        0.000000  0.000000  BENIGN
              ...            ...             ...             ...           ...             ...       ...     ...
126839       0.000142       0.001712    8.672862e-01    8.672862e-01      0.000142        0.125015  0.001036    DDoS
64142        0.000142       0.001712    8.672862e-01    8.672862e-01      0.000142        0.125015  0.001036    DDoS
178353       0.000164       0.000514    6.004289e-10    6.004289e-10      0.000164        0.003922  0.002071    DDoS
119368       0.000361       0.002825    3.302359e-09    3.302359e-09      0.000361        0.000000  0.000518  BENIGN
94417        0.000306       0.001712    7.005004e-10    7.005004e-10      0.000306        0.003922  0.003107    DDoS

[56436 rows x 8 columns]
==========
DATA TESTING
        TotLenFwdPckt  FwdPcktLenMax  FwdPcktLenMean  AvgFwdSgmnSize  SubFlFwdByts  InitWinBytsFwd  ActvData   Label
33290        0.005076       0.079538    9.296640e-08    9.296640e-08      0.005076        0.075684  0.000000  BENIGN
109592       0.000142       0.001712    8.672862e-01    8.672862e-01      0.000142        0.125015  0.001036    DDoS
113450       0.000131       0.000514    6.004289e-10    6.004289e-10      0.000131        0.003922  0.001554    DDoS
12380        0.000000       0.000000    0.000000e+00    0.000000e+00      0.000000        0.001053  0.000000  BENIGN
66581        0.000306       0.001712    7.005004e-10    7.005004e-10      0.000306        0.003922  0.003107    DDoS
              ...            ...             ...             ...           ...             ...       ...     ...
206921       0.000066       0.000514    6.004289e-10    6.004289e-10      0.000066        0.003922  0.000518  BENIGN
182672       0.000142       0.001712    8.672862e-01    8.672862e-01      0.000142        0.125015  0.001036    DDoS
```

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

```
155812       0.000290       0.004538    5.303788e-09    5.303788e-09       0.000290       0.000000  0.000000  BENIGN
4661         0.000443       0.006935    8.105790e-09    8.105790e-09       0.000443       0.000000  0.000000  BENIGN
58697        0.000142       0.001712    8.672862e-01    8.672862e-01       0.000142       0.125015  0.001036    DDoS

[169309 rows x 8 columns]
==========
Starting time: 30060 second
==========
DATA PREDIKSI
 33290     BENIGN
109592      DDoS
113450      DDoS
12380     BENIGN
66581       DDoS
           ...
206921    BENIGN
182672      DDoS
155812    BENIGN
4661      BENIGN
58697       DDoS
Name: 0, Length: 169309, dtype: object
==========
DATA AKTUAL
 33290     BENIGN
109592      DDoS
113450      DDoS
12380     BENIGN
66581       DDoS
           ...
206921    BENIGN
182672      DDoS
155812    BENIGN
4661      BENIGN
58697       DDoS
Name: Label, Length: 169309, dtype: object
==========
```

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG

File - unknown

```
Ending time:  30824 second
==========
Berikut adalah confusion matrix :
 [[73007    83]
 [  127 96092]]
==========
 True Negative:  73007
 False Positive:  83
 False Negative:  127
 True Positive:  96092
==========
['BENIGN' 'DDoS']
[73134 96175]
==========
duration 764 second
akurasi:  99.87596642824657
presisi:  99.91369898622303
recall:  99.86800943680562
f-measure:  99.89084898697465
```

File - unknown

CENTRAL LIBRARY OF MAULANA MALIK IBRAHIM STATE ISLAMIC UNIVERSITY OF MALANG