



SKRIPSI

PERANCANGAN SISTEM DETEKSI ARP POISONING PADA WIRELESS LAN MENGUNAKAN MACHINE LEARNING: RANDOM FOREST DAN ADABOOST

RAFI DHAFIN ERSAMAZAYA

NPM 21082010222

DOSEN PEMBIMBING

Amalia Anjani Arifiyanti, S.Kom., M.Kom

Dhian Satria Yudha Kartika, S.Kom., M.Kom

**KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI SISTEM INFORMASI
SURABAYA
2025**



SKRIPSI

PERANCANGAN SISTEM DETEKSI ARP POISONING PADA WIRELESS LAN MENGUNAKAN MACHINE LEARNING: RANDOM FOREST DAN ADABOOST

RAFI DHAFIN ERSAMAZAYA

NPM 21082010222

DOSEN PEMBIMBING

Amalia Anjani Arifiyanti, S.Kom., M.Kom

Dhian Satria Yudha Kartika, S.Kom., M.Kom

**KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI SISTEM INFORMASI
SURABAYA
2025**

Halaman ini sengaja dikosongkan

LEMBAR PENGESAHAN

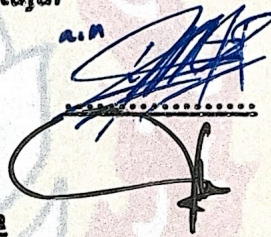
PERANCANGAN SISTEM DETEKSI ARP POISONING PADA WIRELESS LAN MENGGUNAKAN MACHINE LEARNING: RANDOM FOREST DAN ADABOOST

Oleh:
RAFI DHAFIN ERSAMAZAYA
NPM. 21082010222

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi Prodi Sistem Informasi Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jawa Timur Pada tanggal 14 November 2025

Menyetujui

Amalia Anjani Arifiyanti, S.Kom., M.Kom
NIP/NPT 199208122018032001



(Pembimbing I)

Dhian Satria Yudha Kartika, S.Kom., M.Kom
NIP/NPT 20119860522249



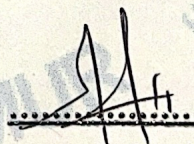
(Pembimbing II)

Eka Dyar Wahyuni, S.Kom, M.Kom
NIP/NPT 198412012021212005



(Ketua Penguji)

Reisa Permatasari, S.T., M.Kom
NIP/NPT 199205142022032007



(Penguji II)

Tri Luhur Indayanti Sugata, S.ST., M.IM
NIP/NPT 199206162024062001



(Penguji III)

Mengetahui,
Dekan Fakultas Ilmu Komputer



Prof. Dr. Ir. Novirina Hendrasarie, MT
NIP. 19681126 199403 2 001

Halaman ini sengaja dikosongkan

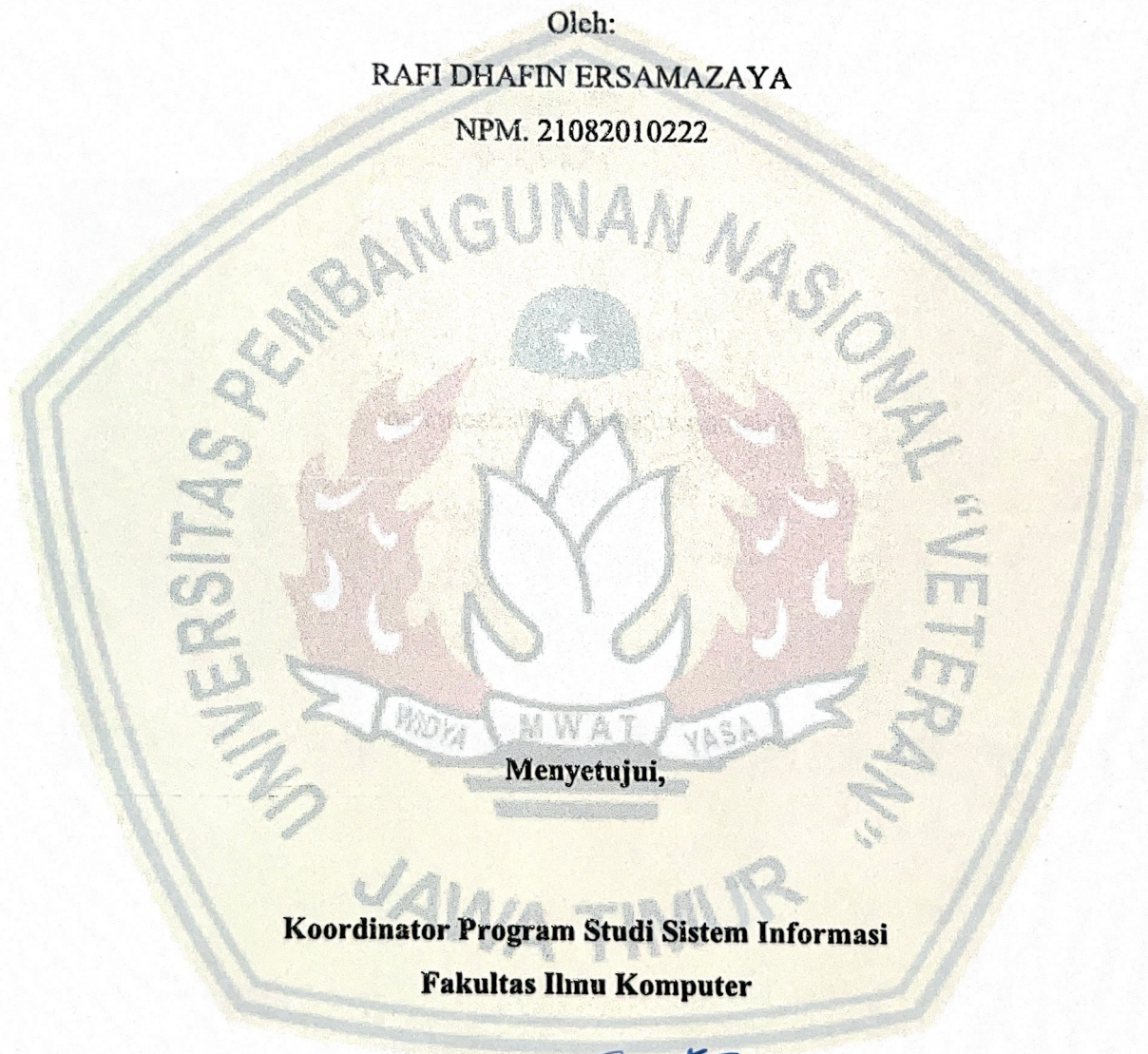
LEMBAR PERSETUJUAN

**PERANCANGAN SISTEM DETEKSI ARP POISONING PADA
WIRELESS LAN MENGGUNAKAN MACHINE LEARNING: RANDOM
FOREST DAN ADABOOST**

Oleh:

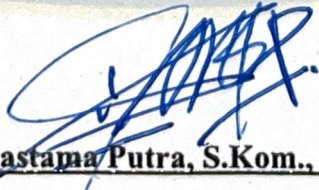
RAFI DHAFIN ERSAMAZAYA

NPM. 21082010222



Menyetujui,

**Koordinator Program Studi Sistem Informasi
Fakultas Ilmu Komputer**


Agung Brastama Putra, S.Kom., M.Kom.

NIP/NPT. 19851124 2021211 003

Halaman ini sengaja dikosongkan

SURAT PERNYATAAN BEBAS PLAGIASI

Yang bertandatangan di bawah ini:

Nama : Rafi Dhafin Ersamazaya

NPM : 21082010222

Program : Sarjana (S1)

Program Studi : Sistem Informasi

Fakultas : Ilmu Komputer

Menyatakan bahwa dalam dokumen ilmiah Skripsi ini tidak terdapat bagian dari karya ilmiah lain yang telah diajukan untuk memperoleh gelar akademik di suatu lembaga Pendidikan Tinggi, dan juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang/lembaga lain, kecuali yang secara tertulis disitasi dalam dokumen ini dan disebutkan secara lengkap dalam daftar pustaka.

Dan saya menyatakan bahwa dokumen ilmiah ini bebas dari unsur-unsur plagiasi. Apabila dikemudian hari ditemukan indikasi plagiat pada Skripsi ini, saya bersedia menerima sanksi sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya tanpa ada paksaan dari siapapun juga dan untuk dipergunakan sebagaimana mestinya.



Surabaya, 27 November 2025

Yang Membuat Pernyataan



Rafi Dhafin Ersamazaya

NPM. 21082010222

Halaman ini sengaja dikosongkan

ABSTRAK

Nama Mahasiswa / NPM : Rafi Dhafin Ersamazaya / 21082010222
Judul Skripsi : Perancangan Sistem Deteksi ARP Poisoning Pada Wireless LAN Menggunakan Machine Learning: Random Forest dan AdaBoost.
Dosen Pembimbing : 1. Amalia Anjani Arifiyanti, S.Kom., M.Kom
2. Dhian Satria Yudha Kartika, S.Kom., M.Kom

Serangan ARP *Poisoning* merupakan salah satu ancaman serius dalam keamanan jaringan, di mana penyerang memanipulasi tabel *Address Resolution Protocol* (ARP) dengan tujuan mengarahkan lalu lintas data ke perangkat yang tidak sah. Serangan ini dapat menimbulkan dampak signifikan, termasuk penyadapan, modifikasi, hingga pencurian data pada jaringan *Wireless LAN*. Oleh karena itu, diperlukan mekanisme deteksi yang mampu mengidentifikasi aktivitas tersebut secara akurat dan efisien guna memitigasi risiko terhadap keamanan jaringan. Skripsi ini bertujuan untuk merancang dan mengevaluasi sistem deteksi serangan ARP *Poisoning* menggunakan beberapa algoritma *machine learning*, termasuk model *hybrid* Random Forest dan AdaBoost, dengan tujuan membandingkan efektivitasnya terhadap empat model lainnya. Metode penelitian yang diterapkan adalah CRISP-DM (*Cross-Industry Standard Process for Data Mining*), yang mencakup tahapan *business understanding*, *data understanding*, *data preparation*, *modeling*, *evaluation*, dan *deployment*. Proses pengumpulan dataset menghasilkan 11.225 dataset yang terdiri dari kombinasi antara dataset gelateria dan simulasi serangan yang dilakukan proses EDA, *cleaning*, *construct*, *format*, dan *modelling*. Hasil pemodelan menunjukkan bahwa model *hybrid* Random Forest dan AdaBoost memperoleh *accuracy* tinggi, yaitu 99,92% pada data *validation* dan 99,94% pada data *testing*, dengan tingkat kesalahan yang rendah. Hal ini menegaskan efektivitas model tersebut dalam mendeteksi serangan ARP *Poisoning*. Namun, model *hybrid* memiliki *inference time* minimum 517,30 ms yang dimana waktu tersebut cukup lambat dalam melakukan deteksi, sehingga kurang optimal untuk implementasi dalam skenario *real-time*. Sebaliknya, model AdaBoost menunjukkan kinerja yang seimbang dengan tingkat *accuracy* yaitu 99,92% pada data *validation* dan 99,94% pada data *testing*, serta tingkat kesalahan deteksi setara dengan model *hybrid*. Model ini memiliki *inference time* yang jauh lebih cepat, yaitu *maximum* di angka 14,93 ms, sehingga dapat disimpulkan pada skripsi ini model AdaBoost dinilai paling sesuai untuk diterapkan pada sistem deteksi ARP *Poisoning* secara *real-time*.

Kata kunci: ARP Poisoning, Wireless LAN, CRISP-DM, Machine Learning, Random Forest, AdaBoost.

Halaman ini sengaja dikosongkan

ABSTRACT

Student Name / NPM : Rafi Dhafin Ersamazaya / 21082010222
Thesis Title : Design of an ARP Poisoning Detection System on
Wireless LAN Using Machine Learning: Random
Forest and AdaBoost
Advisor : 1. Amalia Anjani Arifiyanti, S.Kom., M.Kom
2. Dhian Satria Yudha Kartika, S.Kom., M.Kom

ARP Poisoning attacks represent a serious threat to network security, wherein an attacker manipulates the Address Resolution Protocol (ARP) table with the intention of redirecting data traffic to an unauthorized device. Such attacks can cause significant impacts, including eavesdropping, data modification, and data theft within Wireless LAN environments. Therefore, an effective detection mechanism capable of accurately and efficiently identifying such activities is required to mitigate risks to network security. This thesis aims to design and evaluate an ARP Poisoning attack detection system using several machine learning algorithms, including a hybrid model combining Random Forest and AdaBoost, with the objective of comparing its effectiveness against four other models. The research employs the CRISP-DM (Cross-Industry Standard Process for Data Mining) methodology, which consists of the stages of business understanding, data understanding, data preparation, modeling, evaluation, and deployment. The dataset collection process resulted in 11,225 records composed of a combination of the Gelateria dataset and attack simulation data, which subsequently underwent EDA, cleaning, construction, formatting, and modeling. The modeling results indicate that the hybrid Random Forest–AdaBoost model achieved high accuracy, namely 99.92% on the validation data and 99.94% on the testing data, with a low error rate. This confirms the effectiveness of the hybrid model in detecting ARP Poisoning attacks. However, the hybrid model has a minimum inference time of 517.30 ms, which is relatively slow for detection tasks, making it less optimal for real-time implementation. Conversely, the AdaBoost model demonstrates more balanced performance, with an accuracy of 99.92% on the validation data and 99.94% on the testing data, and an error rate comparable to the hybrid model. This model exhibits a significantly faster inference time, with a maximum of 14.93 ms. Therefore, this thesis concludes that the AdaBoost model is the most suitable for real-time ARP Poisoning detection systems.

Keywords: ARP *Poisoning*, *Wireless LAN*, CRISP-DM, *Machine Learning*, Random Forest, AdaBoost.

Halaman ini sengaja dikosongkan

KATA PENGANTAR

Puji syukur kehadiran Allah SWT atas segala rahmat, hidayah dan karunia-Nya kepada penulis sehingga skripsi dengan judul “Perancangan Design of an ARP Poisoning Detection System on Wireless LAN Using Machine Learning: Random Forest and AdaBoost” dapat terselesaikan dengan baik. Laporan skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Ilmu Komputer pada Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional “Veteran” Jawa Timur. Penulis mengucapkan terima kasih atas segala dukungan, doa, semangat, dan bantuan yang telah diberikan oleh berbagai pihak selama proses penyusunan skripsi ini.

1. Penulis menyampaikan rasa terima kasih yang tulus kepada kedua orang tua dan seluruh keluarga tercinta atas doa, cinta, dan dukungan yang tiada henti dalam setiap langkah kehidupan penulis.
2. Ibu Eristya Maya Safitri, S.Kom, M.Kom. selaku Dosen Wali, atas bimbingan dan arahannya selama masa studi.
3. Ibu Amalia Anjani Arifiyanti, S.Kom., M.Kom, selaku Dosen Pembimbing I, yang telah meluangkan waktu untuk memberikan bimbingan, arahan, serta masukan berharga selama proses penyusunan skripsi ini. Penulis sangat menghargai ketelatenan dan dedikasi beliau dalam menjawab setiap pertanyaan hingga skripsi ini dapat terselesaikan dengan baik.
4. Bapak Dhian Satria Yudha Kartika, S.Kom., M.Kom selaku Dosen Pembimbing II, yang telah memberikan banyak bimbingan, masukan, dan pengarahan. Penulis mengucapkan terima kasih atas bimbingan, motivasi, dan masukan yang diberikan dengan jelas dan penuh kesabaran selama masa bimbingan.
5. Seluruh Dosen Program Studi Sistem Informasi Universitas Pembangunan Nasional “Veteran” Jawa Timur, atas ilmu dan dukungan yang telah diberikan selama masa perkuliahan.

6. Pihak dari studi kasus yang terlibat, terimakasih atas kesempatan yang diberikan kepada penulis untuk melakukan penelitian sebagai bagian dari penyusunan skripsi ini.
7. Ananda Julian Mahesa dan Fidela Zerlina yang senantiasa menemani dan telah memberikan dukungan, semangat dan motivasi tanpa henti secara konsisten, selama proses penelitian dari awal hingga akhir. Dan menjadi sumber penyemangat dalam setiap tahap yang dilalui, sehingga penulis mampu menyelesaikan penelitian ini dengan baik.
8. Seluruh teman seperjuangan Sistem Informasi 2021, atas dukungan dan kerjasamanya selama menempuh studi.
9. Seluruh pihak terkait yang tidak bisa disebutkan satu per satu yang terlibat dalam penyusunan proposal skripsi ini sehingga dapat selesai dengan baik.

Penulis menyadari sepenuhnya bahwa skripsi ini masih memiliki berbagai kekurangan. Oleh karena itu, penulis sangat mengapresiasi segala bentuk masukan dan saran yang bersifat membangun dari berbagai pihak guna perbaikan dan penyempurnaan di masa yang akan datang. Penulis berharap, karya ini dapat memberikan manfaat bagi para pembaca serta menjadi referensi yang berguna bagi penelitian-penelitian selanjutnya.

Surabaya, 14 November 2025

Penulis

DAFTAR ISI

LEMBAR PENGESAHAN.....	iii
LEMBAR PERSETUJUAN	v
SURAT PERNYATAAN BEBAS PLAGIASI.....	vii
ABSTRAK.....	ix
ABSTRACT	xi
KATA PENGANTAR	xiii
DAFTAR ISI.....	xv
DAFTAR GAMBAR	xix
DAFTAR TABEL.....	xxiii
DAFTAR LAMPIRAN	xxv
BAB 1 PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah.....	3
1.3. Batasan Masalah	3
1.4. Tujuan Penelitian	4
1.5. Manfaat Penelitian	4
BAB 2 TINJAUAN PUSTAKA.....	5
2.1. Penelitian Terdahulu	5
2.2. Landasan Teori	9
2.2.1. Keterangan Lokasi Perekaman	10
2.2.2. <i>Wireless Local Area Network</i>	10
2.2.3. Hacking	11
2.2.4. ARP (<i>Address Resolution Protocol</i>)	11
2.2.5. ARP <i>Poisoning</i>	12
2.2.6. Wireshark.....	12
2.2.7. Machine Learning	13
2.2.8. Klasifikasi <i>Machine Learning</i>	13
2.2.8.1. Evaluasi Hasil (<i>Confusion Matrix</i>)	14
2.2.9. CRISP-DM.....	15
2.2.10. <i>Class Weighting</i>	16
2.2.11. Random Forest	17
2.2.12. AdaBoost	18

2.2.13.	Scapy	18
BAB 3 METODOLOGI PENELITIAN		21
3.1.	Analisis Sistem	21
3.2.	Alur Kerja Sistem.....	22
3.2.1.	Business Understanding.....	23
3.2.1.1.	<i>Determining Business Subjective</i>	23
3.2.1.2.	<i>Assess Situation</i>	23
3.2.1.3.	<i>Determining Data Mining Goals</i>	23
3.2.1.4.	<i>Produce Project Plan</i>	24
3.2.2.	Data Understanding.....	25
3.2.2.1.	<i>Collect Data</i>	25
3.2.2.2.	<i>Integrate Data</i>	27
3.2.2.3.	<i>Explore and Verify Data</i>	27
3.2.3.	Data Preparation	27
3.2.3.1.	<i>Select data</i>	28
3.2.3.2.	<i>Clean data</i>	28
3.2.3.3.	<i>Construct data</i>	28
3.2.3.4.	<i>Format data</i>	29
3.2.4.	Modelling	29
3.2.4.1.	<i>Select Modelling Technique</i>	29
3.2.4.2.	<i>Generate Test Design</i>	29
3.2.4.3.	<i>Build Model</i>	30
3.2.4.4.	<i>Assess Model</i>	31
3.2.5.	Evaluation	31
3.2.5.1.	<i>Evaluate Result</i>	31
3.2.6.	Deployment	32
3.2.6.1.	<i>Deployment</i>	32
3.2.6.2.	<i>Testing Project</i>	32
3.2.6.3.	<i>Produce Final Report</i>	32
BAB 4 HASIL DAN PEMBAHASAN		33
4.1.	Alur Kerja Sistem.....	33
4.1.1.	Data Understanding	33
4.1.1.1.	<i>Collect Data</i>	33
4.1.1.2.	<i>Integrate Data</i>	35

4.1.1.3.	<i>Explore and Verify Data</i>	37
4.1.2.	<i>Data Preparation</i>	56
4.1.2.1.	<i>Select Data</i>	56
4.1.2.2.	<i>Clean Data</i>	58
4.1.2.3.	<i>Construct Data</i>	59
4.1.2.4.	<i>Format Data</i>	64
4.1.3.	<i>Modelling</i>	65
4.1.3.1.	<i>Select Modelling Technique</i>	65
4.1.3.2.	<i>Generate Test Design</i>	66
4.1.3.3.	<i>Build Model</i>	71
4.1.3.4.	<i>Asses Model</i>	77
4.1.4.	<i>Evaluation</i>	85
4.1.4.1.	<i>Evaluate Result</i>	85
4.1.5.	<i>Deployment</i>	92
4.1.5.1.	<i>Deployment</i>	92
4.1.5.2.	<i>Testing Project</i>	96
4.1.5.3.	<i>Produce Final Report</i>	106
BAB 5	KESIMPULAN DAN SARAN	109
5.1.	<i>Kesimpulan</i>	109
5.2.	<i>Saran</i>	110
DAFTAR PUSTAKA		111
LAMPIRAN		115

Halaman ini sengaja dikosongkan

DAFTAR GAMBAR

Gambar 2.1. <i>Wireless Local Area Network</i> (Sciepub, 2013)	11
Gambar 2.2 ARP (<i>Address Resolution Protocol</i>) (Ahuja et.al, 2022)	12
Gambar 2.3 ARP <i>Poisoning</i> (Ahuja et.al, 2022).....	12
Gambar 2.4 <i>Machine Learning</i> (Intelliarts, 2024).....	13
Gambar 2.5 <i>CRISP-DM</i>	16
Gambar 2.6 Random Forest <i>Bagging and Aggregating</i> (Trivusi, 2022)	17
Gambar 2.7 <i>Bagging vs Boosting</i>	18
Gambar 3.1 Diagram Penelitian	21
Gambar 3.2 Diagram <i>Business Understanding</i>	23
Gambar 3.3 <i>Data Understanding</i>	25
Gambar 3.4 <i>Data Preparation</i>	27
Gambar 3.5. Diagram <i>Modelling</i>	29
Gambar 3.6 Diagram <i>Deployment</i>	32
Gambar 4.1. Data Gelateria Wireshark.....	33
Gambar 4.2. Data <i>Train</i> Utama Simulasi Serangan Wireshark.	34
Gambar 4.3. Jumlah Dataset Gelateria dan Serangan Wireshark.	35
Gambar 4.4. Proses Integrasi Data <i>Training</i>	35
Gambar 4.5. <i>Integrate Data</i>	36
Gambar 4.6. <i>Import Data</i>	37
Gambar 4.7 Kategori Kolom	40
Gambar 4.8 Cek <i>Missing Value</i>	40
Gambar 4.9 Hasil <i>Missing Value</i>	41
Gambar 4.10 <i>Code Source IP & MAC</i>	42
Gambar 4.11 Top 10 <i>Source IP & MAC</i>	43
Gambar 4.12 <i>Code Destination IP & MAC</i>	44
Gambar 4.13 Top 10 <i>Destination IP & MAC</i>	45
Gambar 4.14 <i>Code perhitungan opcode</i>	45
Gambar 4.15 Hasil <i>run</i> perhitungan <i>opcode</i>	46
Gambar 4.16 <i>Code Perhitungan Source IP</i>	47
Gambar 4.17 Hasil <i>Run</i> perhitungan <i>Source IP</i>	49

Gambar 4.18 <i>Code</i> Perhitungan <i>Source</i> MAC.....	50
Gambar 4.19 Hasil <i>Run</i> perhitungan <i>Source</i> MAC.....	51
Gambar 4.20 <i>Code</i> <i>Heatmap</i> <i>Source</i> IP & MAC	52
Gambar 4.21 Hasil <i>Run</i> <i>Heatmap</i> <i>Source</i> IP & MAC.....	53
Gambar 4.22 <i>Code</i> <i>Heatmap</i> <i>Destination</i> IP & MAC	54
Gambar 4.23. Hasil <i>Run</i> <i>Heatmap</i> <i>Destination</i> IP & MAC	55
Gambar 4.24 <i>Code</i> <i>cleaning</i>	58
Gambar 4.25 <i>Code</i> proses data <i>cleaning</i>	59
Gambar 4.26 Hasil Data setelah <i>Cleaning</i>	59
Gambar 4.27 Proses <i>Labelling</i>	64
Gambar 4.28 Proses <i>Encoding</i> Data <i>Training</i>	64
Gambar 4.29 <i>Final Result</i> data <i>Preparation</i>	65
Gambar 4.30 Dataset <i>Testing</i> Merge.....	66
Gambar 4.31 hasil olah data <i>training time - session</i>	67
Gambar 4.32 hasil olah data <i>training arp count request</i> – label serangan.....	67
Gambar 4.33 Dataset <i>Validation</i> Merge	68
Gambar 4.34 hasil olah data <i>validation time - session</i>	68
Gambar 4.35 hasil olah data <i>validation arp count request</i> – label serangan.	69
Gambar 4.36 Dataset <i>Testing</i> Merge	69
Gambar 4.37 hasil olah dataset <i>testing time – session</i>	70
Gambar 4.38 hasil olah dataset <i>testing arp count request</i> – label serangan.	70
Gambar 4.39 <i>Import</i> data	71
Gambar 4.40 <i>Load</i> Dataset.....	71
Gambar 4.41 <i>feature</i> dan <i>target column</i>	72
Gambar 4.42 step 1 <i>multiclass</i> model	73
Gambar 4.43 step 2 <i>multiclass</i> model	74
Gambar 4.44 step 3 <i>multiclass</i> model	75
Gambar 4.45 step 4 <i>multiclass</i> model	75
Gambar 4.46 <i>Build</i> 5 model	76
Gambar 4.47 Dataset <i>Summary</i>	77
Gambar 4.48 Random Forest Model.....	79
Gambar 4.49 Random Forest (<i>class weight</i>) Model	80

Gambar 4.50 AdaBoost Model	81
Gambar 4.51 AdaBoost (<i>class weight</i>) Model.....	83
Gambar 4.52 Random Forest x AdaBoost (<i>hybrid</i>) Model.....	84
Gambar 4.53 <i>inference time</i> vs <i>confusion matrix</i>	92
Gambar 4.54 <i>Import</i> Model Pickle	92
Gambar 4.55 pembuatan bot (<i>botfather</i>)	92
Gambar 4.56 konfigurasi bot dan <i>.env</i>	93
Gambar 4.57 Struktur Folder VSCode	93
Gambar 4.58 <i>code handler</i> /start	94
Gambar 4.59 <i>code handler</i> /arp.	95
Gambar 4.60 <i>code handler</i> /log.	95
Gambar 4.61 <i>code handler</i> /stop.....	96
Gambar 4.62 Testing <i>Run Bot</i>	97
Gambar 4.63 <i>handler</i> /start	97
Gambar 4.64 <i>handler</i> /arp.....	98
Gambar 4.65 <i>handler</i> /log.....	98
Gambar 4.66 <i>handler</i> /stop	99
Gambar 4.67 Identitas Target.....	99
Gambar 4.68 Identitas <i>Attacker</i> (Penyerang).....	100
Gambar 4.69 Simulasi Serangan ARPSpoof	100
Gambar 4.70 Deteksi Wireshark.....	101
Gambar 4.71 Deteksi Bot Telegram (basis log).....	101
Gambar 4.72 <i>Alert</i> Serangan Bot.....	102
Gambar 4.73 Wireshark Deteksi (komparasi)	103
Gambar 4.74 Bot Telegram /log (komparasi)	103
Gambar 4.75 Implementasi Sistem di <i>Public</i>	104
Gambar 4.76 Verifikasi identitas router.....	104
Gambar 4.77 <i>Testing Bot Wifi Public</i>	105
Gambar 4.78 Log Wifi <i>Public</i>	105
Gambar 4.79 Contoh <i>Case Sniffing</i>	106

Halaman ini sengaja dikosongkan

DAFTAR TABEL

Tabel 2.1. Penelitian Terdahulu	5
Tabel 3.1 Representasi Turunan CRISP-DM.....	22
Tabel 3.2. Produce Project Plan	24
Tabel 3.3. Kolom Wireshark	26
Tabel 3.4 Skenario Model.....	30
Tabel 4.1 Tools Serangan.....	34
Tabel 4.2 Column Description	38
Tabel 4.3 Kolom Terpilih.....	56
Tabel 4.4 Kolom terhapus	57
Tabel 4.5 column construct.....	60
Tabel 4.6 Skenario Model.....	66
Tabel 4.7 Label 1	78
Tabel 4.8 Label 2	78
Tabel 4.9 Label 3	78
Tabel 4.10 Evaluasi Statistic 5 Model Validation	85
Tabel 4.11 Evaluasi Statistic 5 Model Testing.....	86
Tabel 4.12 Statistic Inference Time	87
Tabel 4.13 Evaluasi deskriptif 5 Model.....	87

Halaman ini sengaja dikosongkan

DAFTAR LAMPIRAN

Surat Pengantar Skripsi	115
Surat Balasan Mitra.....	116
Perizinan secara langsung dengan manajer Gelateria	117
IP dan MAC router wifi Gelateria.....	117
Jumlah Perangkat Wifi Gelateria pada pukul 19.12	118

Halaman ini sengaja dikosongkan