

**ANALISIS DAN IMPLEMENTASI *INTRUSION DETECTION*  
*SYSTEM* (IDS) PADA SISTEM *MONITORING* KAMERA  
BERBASIS IOT**

**TUGAS AKHIR**



Yusuf Laurensius Harefa

NIM. 180155201051

**PROGRAM STUDI TEKNIK INFORMATIKA  
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA  
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN  
UNIVERSITAS MARITIM RAJA ALI HAJI  
TANJUNGPINANG  
2026**

**ANALISIS DAN IMPLEMENTASI *INTRUSION DETECTION*  
*SYSTEM* (IDS) PADA SISTEM *MONITORING* KAMERA  
BERBASIS IOT**

Tugas Akhir

Skema Skripsi

*Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar Sarjana*

*Teknik pada Program Studi Teknik Informatika*



Yusuf Laurensius Harefa

NIM. 180155201051

**PROGRAM STUDI TEKNIK INFORMATIKA  
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA  
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN  
UNIVERSITAS MARITIM RAJA ALI HAJI  
TANJUNGPINANG  
2026**

## PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

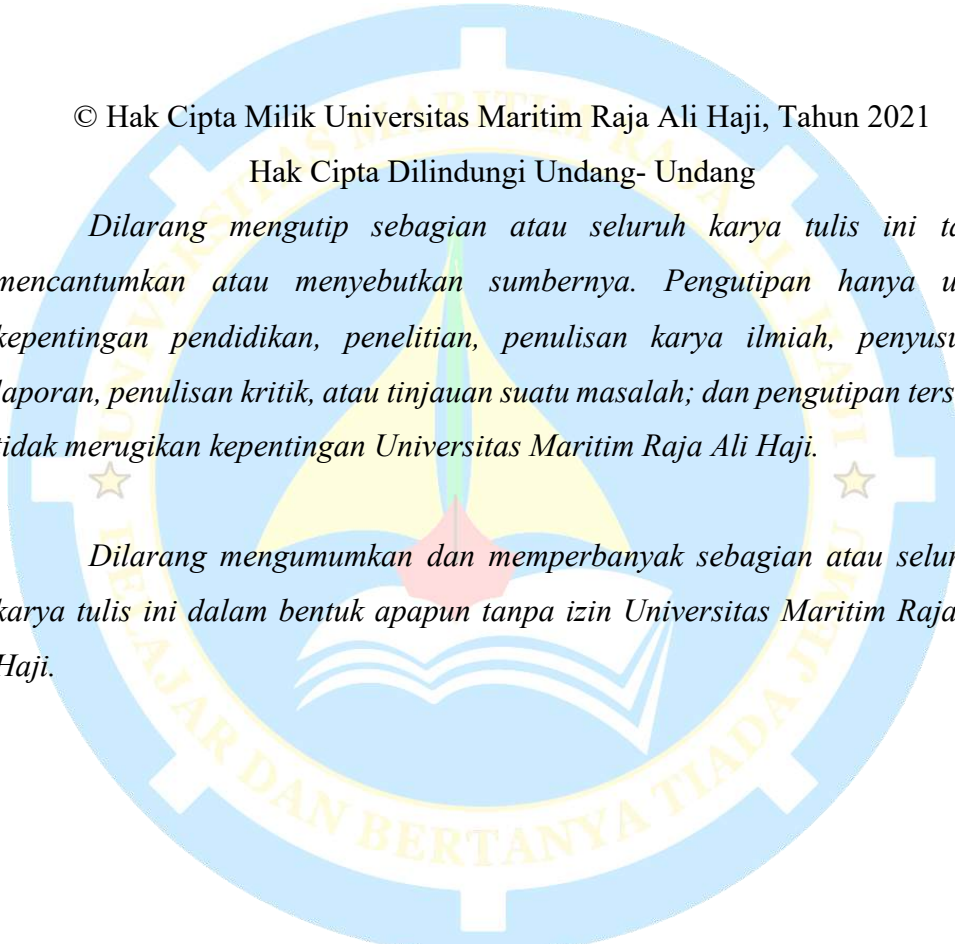
Dengan ini saya menyatakan bahwa tugas akhir berjudul “ANALISIS DAN IMPLEMENTASI *INTRUSIN DETECTION SYSTEM* (IDS) PADA SISTEM MONITORING KAMERA BERBASIS IOT” adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Apabila di kemudian hari terbukti pernyataan saya tidak benar dan melanggar peraturan yang berlaku dalam karya tulis dan hak intelektual, maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji dan menerima sanksi lainnya sesuai dengan peraturan yang berlaku. Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Maritim Raja Ali Haji.

Tanjungpinang, Januari 2026



*Yusuf Laurensius Harefa*  
NIM 180155201051



© Hak Cipta Milik Universitas Maritim Raja Ali Haji, Tahun 2021

Hak Cipta Dilindungi Undang- Undang

*Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah; dan pengutipan tersebut tidak merugikan kepentingan Universitas Maritim Raja Ali Haji.*

*Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Universitas Maritim Raja Ali Haji.*

## HALAMAN PERSETUJUAN

Judul : Analisis dan Implementasi *Intrusion Detection System* (IDS) pada Sistem *Monitoring* Kamera berbasis IoT

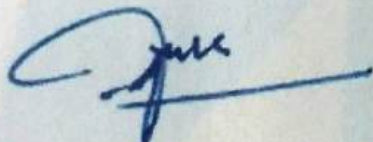
Nama : Yusuf Laurensius Harefa

NIM : 180155201051

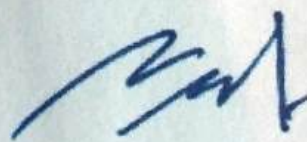
Program Studi : Teknik Informatika

Tanggal Persetujuan : 14 Januari 2026

Disetujui oleh,  
Komisi Pembimbing



**Hendra Kurniawan, S.Kom.,**  
**M.Sc.Eng., Ph.D.**  
**(Ketua)**



**Nolan Efranda, M.Kom.**  
**(Anggota)**

## HALAMAN PENGESAHAN

Judul : Analisis dan Implementasi *Intrusion Detection System (IDS)* pada Sistem *Monitoring Kamera* berbasis IoT

Nama : Yusuf Laurensius Harefa

NIM : 180155201051

Telah berhasil dipertahankan di hadapan Komisi Penguji sebagai bagian persyaratan yang diperlukan dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

### KOMISI PENGUJI

|             |                                                |         |
|-------------|------------------------------------------------|---------|
| Ketua       | : Nurfalinda, S.T., M.Cs                       | (.....) |
| Anggota I   | : Novrizal Fattah Fahmitra, S.Kom., M.Kom      | (.....) |
| Anggota II  | : Muhamad Fadli, M.Kom                         | (.....) |
| Anggota III | : Hendra Kurniawan, S.Kom., M.Sc.Eng.,<br>Ph.D | (.....) |
| Anggota IV  | : Nolan Efranda, M.Kom                         | (.....) |

Mengetahui,

Ketua Jurusan Teknik Elektro dan Informatika


Hollanda Arief Kusuma, S.IK., M.Si  
NIP. 198904012019031016

Tanggal Ujian: 19 Januari 2026

Tanggal Lulus:

## PRAKATA

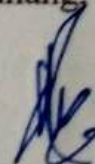
Puji syukur penulis panjatkan kehadiran Tuhan yang Maha Esa atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis dan Implementasi *Intrusion Detection System* (IDS) pada Sistem *Monitoring* Kamera Berbasis IoT".

Penulisan skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji. Dalam proses penyusunannya, penulis menyadari bahwa keberhasilan ini tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih yang tulus kepada:

1. Bapak Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D, selaku Dosen Pembimbing I yang telah sabar memberikan arahan, ilmu, dan bimbingan yang sangat berharga selama penyusunan skripsi ini.
2. Bapak Nolan Efranda, M.Kom, selaku Dosen Pembimbing II atas saran dan masukan demi kesempurnaan penelitian ini.
3. Kedua Orang Tua dan Keluarga Besar, yang senantiasa memberikan doa, dukungan moral, maupun materiil yang tak terhingga sehingga penulis dapat menyelesaikan studi ini.
4. Pihak-pihak lain yang tidak dapat disebutkan satu per satu, yang telah membantu kelancaran penelitian ini baik secara langsung maupun tidak langsung.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun demi perbaikan di masa mendatang. Akhir kata, semoga skripsi ini dapat memberikan manfaat bagi perkembangan ilmu pengetahuan, khususnya di bidang keamanan jaringan IoT..

Tanjungpinang, Januari 2026



Yusuf Laurensius Harefa

## DAFTAR ISI

|                                                      |      |
|------------------------------------------------------|------|
| HALAMAN PERSETUJUAN .....                            | iv   |
| HALAMAN PENGESAHAN .....                             | v    |
| ABSTRAK.....                                         | vi   |
| ABSTRACT .....                                       | vii  |
| PRAKATA .....                                        | viii |
| DAFTAR ISI.....                                      | ix   |
| DAFTAR TABEL.....                                    | xiii |
| DAFTAR GAMBAR .....                                  | xiv  |
| BAB I PENDAHULUAN .....                              | 16   |
| 1.1. Latar Belakang .....                            | 16   |
| 1.2. Perumusan Masalah.....                          | 17   |
| 1.3. Batasan Penelitian .....                        | 17   |
| 1.4. Tujuan Penelitian.....                          | 18   |
| 1.5. Manfaat Penelitian.....                         | 18   |
| BAB II KAJIAN LITERATUR.....                         | 20   |
| 2.1. Tinjauan Pustaka .....                          | 20   |
| 2.2. Landasan Teori .....                            | 27   |
| 2.2.1. <i>Internet of Things</i> .....               | 27   |
| 2.2.2. Keamanan Jaringan IoT.....                    | 28   |
| 2.2.3. <i>Intrusion Detection System (IDS)</i> ..... | 28   |
| 2.2.4. <i>Virtual Private Server (VPS)</i> .....     | 29   |
| 2.2.5. <i>Snort</i> .....                            | 30   |
| 2.2.6. <i>ICMP Ping Flood Attack</i> .....           | 31   |
| 2.2.7. <i>TCP Syn Flood</i> .....                    | 31   |
| 2.2.8. <i>UDP Flood</i> .....                        | 32   |

|                                       |                                                                    |           |
|---------------------------------------|--------------------------------------------------------------------|-----------|
| 2.2.9.                                | ESP32-CAM.....                                                     | 32        |
| 2.2.10.                               | Sensor PIR ( <i>Passive Infrared</i> ) .....                       | 33        |
| <b>BAB III METODE PENELITIAN.....</b> |                                                                    | <b>34</b> |
| 3.1.                                  | Jenis dan Metode Penelitian .....                                  | 34        |
| 3.2.                                  | Waktu dan Tempat Penelitian.....                                   | 34        |
| 3.3.                                  | Bahan dan Alat .....                                               | 34        |
| 3.4.                                  | Prosedur Pelaksanaan Penelitian .....                              | 37        |
| 3.4.1.                                | Studi Literatur.....                                               | 37        |
| 3.4.2.                                | Perancangan Sistem.....                                            | 37        |
| 3.4.2.1.                              | Arsitektur Jaringan .....                                          | 38        |
| 3.4.2.2.                              | Alur Kerja Integrasi Sistem.....                                   | 39        |
| 3.4.2.3.                              | Perancangan Antarmuka ( <i>User Interface</i> ) bot Telegram ..... | 40        |
| 3.4.3.                                | Implementasi Sistem .....                                          | 40        |
| 3.4.3.1.                              | Implementasi <i>Edge Device</i> .....                              | 40        |
| 3.4.3.1.1.                            | Perakitan perangkat Keras .....                                    | 40        |
| 3.4.3.1.2.                            | Pengunggahan kode program ( <i>firmware</i> ) .....                | 41        |
| 3.4.3.1.3.                            | Integrasi <i>Library</i> .....                                     | 41        |
| 3.4.3.1.4.                            | Logika Eksekusi.....                                               | 42        |
| 3.4.3.1.5.                            | Konektivitas .....                                                 | 42        |
| 3.4.3.2.                              | Implementasi VPS.....                                              | 42        |
| 3.4.3.2.1.                            | Konfigurasi lingkungan server .....                                | 42        |
| 3.4.3.2.2.                            | Instalasi dan konfigurasi <i>snort</i> IDS .....                   | 43        |
| 3.4.3.2.3.                            | Pemrograman otomatisasi notifikasi .....                           | 44        |
| 3.4.3.2.4.                            | Pengaturan <i>firewall</i> dan keamanan.....                       | 44        |
| 3.4.3.3.                              | Implementasi komputer penyerang .....                              | 45        |
| 3.4.3.4.                              | Implementasi Komunikasi bot Telegram .....                         | 47        |

|               |                                                                                 |           |
|---------------|---------------------------------------------------------------------------------|-----------|
| 3.4.4.        | Konfigurasi dan Penyesuaian Aturan ( <i>rules</i> ) pada IDS <i>snort</i> ..... | 48        |
| 3.4.5.        | Pengujian dan Simulasi Sistem .....                                             | 48        |
| 3.4.6.        | Analisis Data dan Evaluasi .....                                                | 50        |
| 3.4.6.1.      | Identifikasi Data .....                                                         | 50        |
| 3.4.6.2.      | Metode Analisis .....                                                           | 50        |
| 3.4.6.3.      | Penyajian Data .....                                                            | 50        |
| <b>BAB IV</b> | <b>HASIL DAN PEMBAHASAN .....</b>                                               | <b>51</b> |
| 4.1.          | Hasil dan Implementasi Sistem .....                                             | 51        |
| 4.1.1.        | Hasil Implementasi Perangkat Keras ( <i>Hardware</i> ).....                     | 51        |
| 4.1.2.        | Hasil Implementasi Kode Program ( <i>firmware</i> ) .....                       | 51        |
| 4.1.3.        | Hasil Implementasi Lingkungan Server (VPS) .....                                | 52        |
| 4.1.4.        | Hasil Implementasi Komputer Penyerang.....                                      | 54        |
| 4.1.5.        | Hasil Implementasi bot Telegram.....                                            | 54        |
| 4.1.6.        | ★ Hasil Implementasi <i>rules</i> pada <i>snort</i> .....                       | 56        |
| 4.2.          | Langkah-langkah pengujian .....                                                 | 57        |
| 4.2.1.        | Persiapan sisi perangkat ESP32-CAM .....                                        | 57        |
| 4.2.2.        | Persiapan sisi server VPS .....                                                 | 58        |
| 4.2.3.        | Pelaksanaan Pengujian Deteksi Normal .....                                      | 59        |
| 4.2.4.        | Pelaksanaan Keamanan Jaringan (Simulasi serangan) .....                         | 59        |
| 4.2.5.        | Prosedur <i>Maintenance Log</i> .....                                           | 61        |
| 4.3.          | Pembahasan hasil analisis pengujian .....                                       | 61        |
| 4.3.1.        | Analisis Sistem pada Kondisi Normal.....                                        | 61        |
| 4.3.2.        | Analisis Pengujian Serangan Jaringan.....                                       | 62        |
| 4.3.2.1.      | Analisis TCP <i>Syn Flood</i> .....                                             | 62        |
| 4.3.2.2.      | Analisis UDP <i>Flood</i> .....                                                 | 63        |
| 4.3.2.3.      | Analisis ICMP <i>Ping Flood</i> .....                                           | 65        |

|                                       |                                                    |           |
|---------------------------------------|----------------------------------------------------|-----------|
| 4.3.3.                                | Analisis performa dan latensi pengiriman data..... | 67        |
| 4.4.                                  | Kelebihan dan kekurangan sistem.....               | 68        |
| <b>BAB V SIMPULAN DAN SARAN .....</b> |                                                    | <b>70</b> |
| 5.1.                                  | Simpulan.....                                      | 70        |
| 5.2.                                  | Saran.....                                         | 71        |
| <b>DAFTAR PUSTAKA .....</b>           |                                                    | <b>72</b> |



## DAFTAR TABEL

|                                                          |    |
|----------------------------------------------------------|----|
| Tabel 2.1 Penelitian Terdahulu.....                      | 23 |
| Tabel 3.1 Perangkat Keras.....                           | 35 |
| Tabel 3.2 Perangkat Lunak.....                           | 35 |
| Tabel 3.3 Server Penelitian.....                         | 36 |
| Tabel 3.4 Bahan Pendukung.....                           | 36 |
| Tabel 4.1 Hasil Pengujian Deteksi Normal .....           | 59 |
| Tabel 4.2 Tabel perbandingan durasi transmisi data ..... | 67 |



## DAFTAR GAMBAR

|                                                                                                    |    |
|----------------------------------------------------------------------------------------------------|----|
| Gambar 2.1 Alur Kerja IoT .....                                                                    | 27 |
| Gambar 2.2 <i>Virtual Private Server</i> .....                                                     | 29 |
| Gambar 2.3 <i>Snort workflow diagram</i> .....                                                     | 30 |
| Gambar 2.4 <i>ICMP Flood Attack Diagram</i> .....                                                  | 31 |
| Gambar 2.5 <i>SYN Flood Diagram</i> .....                                                          | 32 |
| Gambar 2.6 <i>UDP Flood Architecture</i> .....                                                     | 32 |
| Gambar 2.7 Skema Pin ESP32-CAM.....                                                                | 33 |
| Gambar 2.8 Sensor PIR .....                                                                        | 33 |
| Gambar 3.1 Kerangka penelitian .....                                                               | 37 |
| Gambar 3.2 Topologi Arsitektur Jaringan.....                                                       | 38 |
| Gambar 3.3 Flowchart alur kerja integrasi sistem .....                                             | 39 |
| Gambar 3.4 Tampilan rangkaian awal.....                                                            | 41 |
| Gambar 3.5 <i>Library UniversalTelegramBot</i> .....                                               | 41 |
| Gambar 3.6 <i>Library ESP32</i> .....                                                              | 42 |
| Gambar 3.7 Konfigurasi SSID dan <i>Password</i> .....                                              | 42 |
| Gambar 3.8 Konfigurasi awal VPS .....                                                              | 43 |
| Gambar 3.9 Tampilan versi <i>snort</i> yang sudah terinstal .....                                  | 43 |
| Gambar 3.10 Tampilan versi python3 dan flask yang berhasil terinstal .....                         | 44 |
| Gambar 3.11 Konfigurasi <i>Uncomplicated Firewall</i> (UFW) pada VPS.....                          | 45 |
| Gambar 3.12 Instalasi Ubuntu di komputer penyerang .....                                           | 45 |
| Gambar 3.13 Tampilan versi hping3 yang berhasil diinstal .....                                     | 46 |
| Gambar 3.14 Alur Komunikasi bot Telegram .....                                                     | 47 |
| Gambar 4.1 Tampilan perangkat ESP32-CAM.....                                                       | 51 |
| Gambar 4.2 Tampilan isi program ESP32-CAM di arduino IDE .....                                     | 51 |
| Gambar 4.3 Tampilan program berhasil dimasukkan ke dalam perangkat dan terhubung ke internet ..... | 52 |
| Gambar 4.4 Tampilan isi <i>script middleware</i> monitoring_snort.py .....                         | 52 |
| Gambar 4.5 Tampilan status <i>Running</i> server pada VPS Vultr .....                              | 53 |
| Gambar 4.6 Tampilan <i>running services</i> layanan <i>snort</i> .....                             | 53 |
| Gambar 4.7 Tampilan <i>script python</i> sedang berjalan .....                                     | 53 |
| Gambar 4.8 Tampilan log <i>snort</i> IDS sedang berjalan .....                                     | 54 |

|                                                                                                                           |    |
|---------------------------------------------------------------------------------------------------------------------------|----|
| Gambar 4.9 Tampilan versi ubuntu di komputer penyerang .....                                                              | 54 |
| Gambar 4.10 Tampilan versi Hping3 di komputer penyerang .....                                                             | 54 |
| Gambar 4.11 Pengambilan API Token bot Telegram pada @BotFather .....                                                      | 54 |
| Gambar 4.12 Pengambilan chatID pengguna .....                                                                             | 55 |
| Gambar 4.13 <i>User Interface</i> bot telegram .....                                                                      | 55 |
| Gambar 4.14 Sinkronisasi chatID pengguna ke dalam skrip otomasi di VPS.....                                               | 56 |
| Gambar 4.15 Tampilan isi file konfigurasi <i>rules snort</i> pada server VPS .....                                        | 57 |
| Gambar 4.16 Perangkat sudah menyala dan dalam keadaan <i>standby</i> .....                                                | 57 |
| Gambar 4.17 Tampilan serial monitor menunjukkan perangkat sudah terhubung ke<br><i>Wi-Fi</i> .....                        | 57 |
| Gambar 4.18 Mode deteksi <i>Snort</i> IDS .....                                                                           | 58 |
| Gambar 4.19 Menjalankan skrip python3 .....                                                                               | 58 |
| Gambar 4.20 Tampilan antarmuka log <i>snort</i> .....                                                                     | 58 |
| Gambar 4.21 Perintah hping3 untuk simulasi TCP <i>Syn</i> yang berjalan di komputer<br>penyerang.....                     | 60 |
| Gambar 4.22 Perintah hping3 untuk simulasi UDP <i>Flood</i> yang berjalan di komputer<br>penyerang.....                   | 60 |
| Gambar 4.23 Perintah hping3 untuk simulasi ICMP <i>Ping Flood</i> yang berjalan di<br>komputer penyerang .....            | 60 |
| Gambar 4.24 Notifikasi deteksi gerakan dan foto pada telegram .....                                                       | 61 |
| Gambar 4.25 Log <i>alert</i> deteksi serangan TCP <i>Syn Flood</i> pada python3 (flask) ...                               | 62 |
| Gambar 4.26 Log <i>alert</i> deteksi serangan TCP <i>Syn Flood</i> pada VPS .....                                         | 63 |
| Gambar 4.27 Notifikasi pada telegram saat terjadinya serangan TCP <i>Syn Flood</i><br>bersamaan dengan deteksi fisik..... | 63 |
| Gambar 4.28 Log <i>alert</i> deteksi serangan UDP <i>Flood</i> pada python3 (flask) .....                                 | 64 |
| Gambar 4.29 Log <i>alert</i> deteksi serangan UDP <i>Flood</i> pada VPS .....                                             | 64 |
| Gambar 4.30 Notifikasi Alert UDP Flood pada Aplikasi Telegram.....                                                        | 65 |
| Gambar 4.31 Log <i>alert</i> deteksi serangan ICMP <i>Ping Flood</i> pada VPS .....                                       | 66 |
| Gambar 4.32 Log <i>alert</i> deteksi serangan ICMP <i>Ping Flood</i> pada python3 (flask).<br>.....                       | 66 |
| Gambar 4.33 Notifikasi Serangan ICMP Flood dan Foto Deteksi Fisik Secara<br>Bersamaan.....                                | 66 |