

**RANCANG BANGUN APLIKASI DETEKSI MALWARE BERBASIS  
*COLLECTIVE INTELLIGENCE FRAMEWORK (CIF)*  
PADA *HONEYPOT***

**SKRIPSI**



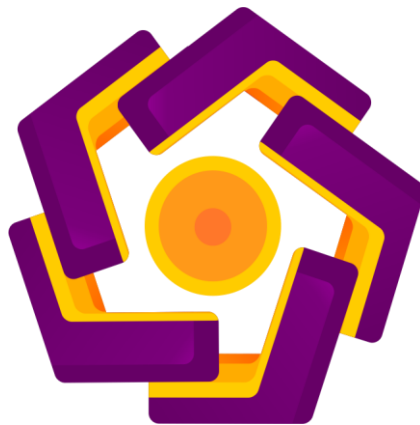
disusun oleh  
**Restu Pratama**  
**14.11.7976**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2018**

**RANCANG BANGUN APLIKASI DETEKSI MALWARE BERBASIS  
*COLLECTIVE INTELLIGENCE FRAMEWORK (CIF)*  
PADA *HONEYPOT***

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



disusun oleh  
**Restu Pratama**  
**14.11.7976**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2018**

**PERSETUJUAN**

**SKRIPSI**

**RANCANG BANGUN APLIKASI DETEKSI *MALWARE* BERBASIS  
*COLLECTIVE INTELLIGENCE FRAMEWORK (CIF)*  
PADA *HONEYPOT***


yang dipersiapkan dan disusun oleh

**Restu Pratama**

**14.11.7976**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 8 Februari 2018

**Dosen Pembimbing,**



**Nila Feby Puspitasari, S.Kom., M.Cs**  
**NIK. 190302161**

**PENGESAHAN**

**SKRIPSI**

**RANCANG BANGUN APLIKASI DETEKSI *MALWARE* BERBASIS  
*COLLECTIVE INTELLIGENCE FRAMEWORK (CIF)*  
PADA *HONEYPOT***

yang dipersiapkan dan disusun oleh

**Restu Pratama**

**14.11.7976**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 21 Februari 2018

**Susunan Dewan Penguji**

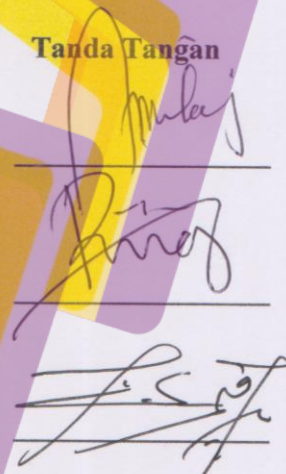
**Nama Penguji**

**Nila Feby Puspitasari, S.Kom., M.Cs.**  
**NIK. 190302161**

**M. Rudyanto Arief, M.T.**  
**NIK. 190302098**


**Ferry Wahyu Wibowo, S.Si., M.Cs.**  
**NIK. 190302235**

**Tanda Tangan**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 12 Maret 2018

**DEKAN FAKULTAS ILMU KOMPUTER**



**Krisnawati, S.Si., M.T.**  
**NIK. 190302038**

## PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 12 Maret 2018



Restu Pratama

NIM. 14.11.7976

## MOTTO

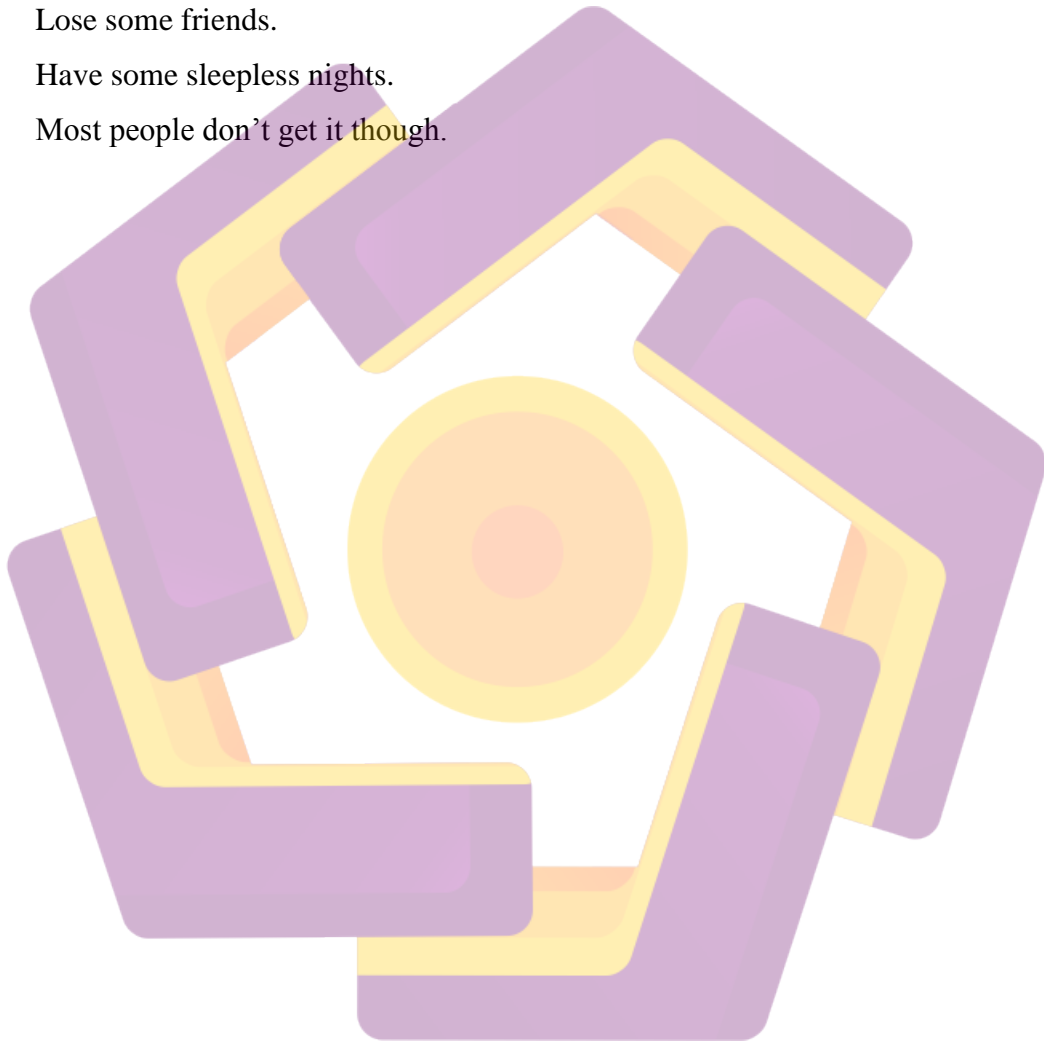
You gotta step out of your comfort zone.

Be broke for a while.

Lose some friends.

Have some sleepless nights.

Most people don't get it though.



## PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Alhamdulillah rabbil'alamin puji syukur atas kehadiran Allah SWT berkat rahmat dan karunia-Nya lah penulis dapat menyelesaikan skripsi ini sebagai salah satu persyaratan untuk mencapai gelar Sarjana Komputer. Skripsi ini saya persembahkan kepada :

1. Kedua Orang Tua, Bapak Suroto dan Ibu Maryati serta seluruh keluarga besar yang senantiasa memberikan semangat, doa, serta motivasi yang tiada henti.
2. Ibu Nila Feby Puspitasari, S.Kom., M.Cs selaku dosen pembimbing yang selalu mengarahkan dan memberikan masukan dalam proses penyusunan skripsi ini.
3. Keluarga besar 14-S1TI-06 atas segala bentuk dukungan yang telah diberikan.
4. Teman – teman Universitas Amikom Yogyakarta yang senantiasa memberikan semangat dan dukungan selama penelitian dan penyusunan skripsi.

## KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan kasih sayang dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Rancang Bangun Aplikasi Deteksi *Malware* Berbasis *Collective Intelligence Framework (CIF)* Pada *Honeypot*”.

Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat untuk mendapatkan gelar sarjana pada Program Studi Informatika di Universitas Amikom Yogyakarta.

Dalam penyusunan skripsi ini, banyak pihak yang membantu dalam berbagai hal. Oleh karena itu, penulis menyampaikan rasa terima kasih kepada :

1. Ibu Nila Feby Puspitasari, S.Kom., M.Cs. selaku pembimbing.
2. Seluruh dosen Program Studi Informatika Universitas Amikom Yogyakarta.
3. Orang tua dan keluarga tercinta yang telah memberikan banyak dukungan baik secara moril maupun materiil.
4. Sahabat dan rekan yang selalu memberikan dukungan yang selalu memberikan dukungan dan motivasi.
5. Semua pihak yang telah membantu dalam penyusunan skripsi ini.

Yogyakarta, Februari 2018

Penulis

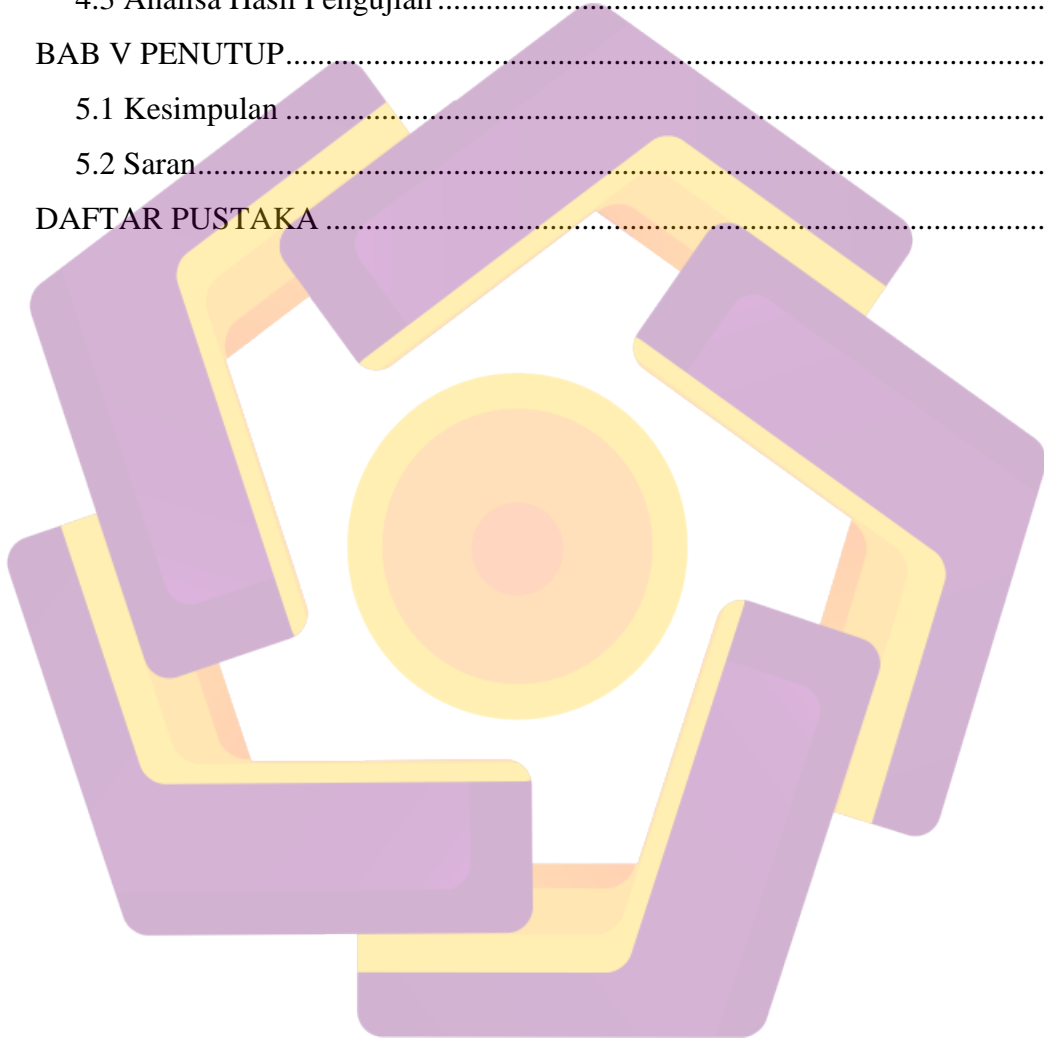


## DAFTAR ISI

JUDUL .....	I
PERSETUJUAN .....	III
PENGESAHAN .....	IV
PERNYATAAN.....	V
MOTTO .....	VI
PERSEMBAHAN.....	VII
KATA PENGANTAR .....	VIII
DAFTAR ISI.....	IX
DAFTAR TABEL.....	XII
DAFTAR GAMBAR .....	XIII
INTISARI.....	XV
ABSTRACT .....	XVI
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Maksud dan Tujuan Penelitian.....	5
1.5 Metode Penelitian.....	5
1.5.1 Pengumpulan Data .....	5
1.5.1.1 Observasi.....	5
1.5.1.1 Deskriptif.....	5
1.5.1.1 Studi Pustaka.....	6
1.5.2 Metode Pengembangan Aplikasi .....	6
1.6 Sistematika Penulisan.....	7
BAB II LANDASAN TEORI.....	9
2.1 Kajian Pustaka.....	9
2.2 Landasan Teori.....	11
2.2.1. <i>Malware</i> .....	11
2.2.1.1 Jenis – jenis <i>malware</i> .....	11

2.2.1.2 Analisis <i>malware</i> .....	16
2.2.2 <i>Threat Intelligence</i> .....	17
2.2.3 <i>Collective Intelligence Framework (CIF)</i> .....	18
2.2.4 <i>Honeypot</i> .....	22
2.2.4.1 Jenis <i>honeypot</i> .....	23
2.2.4.2 <i>Dionaea honeypot</i> .....	23
<b>BAB III ANALISIS DAN PERANCANGAN</b> .....	29
3.1 Analisis.....	29
3.1.1 Identifikasi Masalah .....	29
3.1.2 Analisis Kebutuhan Sistem .....	35
3.1.2.1 Kebutuhan Fungsional Sistem.....	35
3.1.2.2 Kebutuhan Non-Fungsional Sistem .....	36
3.2 Perancangan .....	39
3.2.1 Perancangan Jaringan dan <i>Honeypot</i> .....	40
3.2.2 Perancangan <i>Server Collective Intelligence Framework (CIF)</i> .....	41
3.2.3 Perancangan Aplikasi Deteksi <i>Malware</i> .....	41
3.2.3.1 Database dan API.....	47
3.2.3.2 Perancangan <i>Web Interface</i> .....	49
<b>BAB IV IMPLEMENTASI DAN PEMBAHASAN</b> .....	52
4.1 Implementasi .....	52
4.1.1 Implementasi dan Konfigurasi <i>Honeypot</i> .....	52
4.1.2 Implementasi dan Konfigurasi <i>Server CIF</i> .....	54
4.1.3 Pembuatan Aplikasi .....	55
4.1.3.1 Halaman Awal ( <i>index.php</i> ) .....	55
4.1.3.2 Halaman <i>Attack Summary</i> ( <i>sqpdo_new.php</i> ) .....	57
4.1.3.3 Halaman Detail Koneksi ( <i>connection_details.php</i> ).....	61
4.1.3.4 Halaman Detail <i>Malware</i> ( <i>malware_details.php</i> ) .....	62
4.1.3.5 Halaman Deteksi <i>Malware</i> ( <i>alldetect.php</i> ) .....	64
4.1.3.6 Halaman <i>Rule Creator</i> .....	65
4.1.3.7 Modul <i>Header</i> ( <i>header.php</i> ).....	70
4.1.3.8 Modul <i>Simple Check</i> ( <i>simplecheck.php</i> ).....	70

4.2. Pengujian.....	72
4.2.1 Pengujian <i>Honeypot</i> .....	72
4.2.2 Pengujian <i>Server CIF</i> .....	74
4.2.3 Pengujian Aplikasi .....	75
4.2.4 Pengujian <i>Rule</i> .....	77
4.3 Analisa Hasil Pengujian .....	77
BAB V PENUTUP.....	80
5.1 Kesimpulan .....	80
5.2 Saran.....	81
DAFTAR PUSTAKA .....	83



## DAFTAR TABEL

Tabel 3.1	Data hasil serangan selama Februari 2015- Februari 2016.....	30
Tabel 3.2	Rata- rata koneksi perhari .....	31
Tabel 3.3	Hasil perhitungan korelasi antara koneksi dan download .....	31
Tabel 3.4	Hasil identifikasi <i>malware</i> .....	32
Tabel 3.5	Analisis SWOT .....	33
Tabel 3.6	Perbandingan fitur virustotal API dan CIF .....	35
Tabel 3.7	Spesifikasi laptop .....	36
Tabel 3.8	Spesifikasi <i>virtual machine</i> CIF server .....	37
Tabel 3.9	Spesifikasi <i>single board computer</i> (SBC).....	37
Tabel 3.10	Aplikasi yang digunakan .....	38
Tabel 4.1	Data hasil monitoring <i>resource honeypot</i> .....	73
Tabel 4.2	Data hasil monitoring <i>resource server</i> CIF.....	74
Tabel 4.3	Rangkuman data <i>database</i> pengujian .....	76
Tabel 4.4	Hasil pengujian deteksi <i>malware</i> .....	76

## DAFTAR GAMBAR

Gambar 2.1	Arsitektur <i>collective intelligence framework</i> (CIF) .....	19
Gambar 2.2	Proses <i>fetching, parsing</i> dan <i>normalize</i> .....	20
Gambar 2.3	<i>Post processing</i> .....	21
Gambar 2.4	Proses pada CIF API .....	21
Gambar 2.5	Proses deteksi <i>malware</i> oleh <i>honeypot</i> <i>dionaea</i> .....	25
Gambar 3.1	Rancangan jaringan <i>honeypot</i> .....	40
Gambar 3.2	Cara kerja <i>collective intelligence framework</i> .....	41
Gambar 3.3	Diagram alur kerja aplikasi .....	43
Gambar 3.4	Context Diagram .....	44
Gambar 3.5	DFD level 1 .....	45
Gambar 3.6	DFD level 2 proses menampilkan info <i>malware</i> .....	46
Gambar 3.7	DFD level 2 proses menampilkan <i>rule</i> .....	46
Gambar 3.8	Struktur tabel <i>connections</i> dan <i>downloads</i> .....	47
Gambar 3.9	Struktur JSON API CIF .....	48
Gambar 3.10	Desain halaman utama (homepage) .....	49
Gambar 3.11	Desain halaman data deteksi <i>honeypot</i> .....	50
Gambar 3.12	Halaman detail koneksi dan <i>port</i> serangan .....	50
Gambar 3.13	Desain halaman detail <i>malware</i> .....	51
Gambar 3.14	Desain halaman deteksi <i>malware</i> .....	51
Gambar 4.1	Perintah linux untuk instalasi dependensi <i>dionaea</i> .....	52
Gambar 4.2	Perintah linux untuk <i>build script</i> <i>dionaea</i> .....	53
Gambar 4.3	Perintah untuk melakukan instalasi <i>dionaea honeypot</i> .....	53
Gambar 4.4	Perintah untuk menjalankan service <i>honeypot</i> .....	53
Gambar 4.5	Perintah untuk melakukan instalasi CIF <i>server</i> .....	55
Gambar 4.6	<i>Output query</i> CIF .....	55
Gambar 4.7	Kode program halaman awal .....	56
Gambar 4.8	Tampilan halaman awal .....	57
Gambar 4.9	Kode program halaman <i>attack summary</i> .....	60
Gambar 4.10	Tampilan halaman <i>attack summary</i> .....	61

Gambar 4.11	Kode program halaman detail koneksi .....	61
Gambar 4.12	Tampilan halaman detail koneksi .....	62
Gambar 4.13	Kode program halaman detail <i>malware</i> .....	63
Gambar 4.14	Tampilan halaman detail <i>malware</i> .....	64
Gambar 4.15	Kode program halaman deteksi <i>malware</i> .....	64
Gambar 4.16	Tampilan halaman deteksi <i>malware</i> .....	65
Gambar 4.17	Kode program request.php .....	66
Gambar 4.18	Tampilan request.php .....	67
Gambar 4.19	Kode program alka.php .....	68
Gambar 4.20	Kode program createrule.sh .....	69
Gambar 4.21	Kode program generatelist.sh .....	70
Gambar 4.22	Kode program <i>query</i> modul <i>header</i> .....	70
Gambar 4.23	Tampilan modul header.php pada halaman aplikasi .....	70
Gambar 4.24	Kode program modul simple check .....	71
Gambar 4.25	Tampilan modul simplecheck.php .....	72
Gambar 4.26	Data hasil monitoring <i>service honeypot</i> .....	74
Gambar 4.27	Data hasil monitoring <i>service port server CIF</i> .....	75
Gambar 4.28	Hasil pengujian <i>rule</i> .....	77

## INTISARI

Perkembangan *malware* semakin meningkat dan bervariasi dari tahun ke tahun. Tidak hanya menargetkan sistem komputer sebagai korbannya, *malware* juga menyerang *smartphone* dan perangkat IoT. Menurut survey yang dilakukan oleh symantec, pada tahun 2016 terdapat 357 juta jenis *malware* baru yang secara aktif menyerang sistem komputer dan *smartphone*. Beberapa pencegahan telah dilakukan di berbagai instansi termasuk dengan memasang *honeypot* untuk menangkap *malware* yang menyerang melalui jaringan komputer.

Penggunaan *honeypot* untuk menangkap *malware* pada jaringan komputer dianggap cukup efektif karena selain mendapatkan salinan *malware*, *honeypot* juga dapat mencatat informasi tentang pengirim *malware*. Namun demikian, kemampuan *honeypot* dalam mendeteksi *malware* masih sangat sederhana sehingga dibutuhkan aplikasi untuk meningkatkan kemampuan *honeypot* dalam mendeteksi *malware*.

Aplikasi yang dibuat dalam penelitian ini mampu meningkatkan kemampuan *honeypot* dalam mendeteksi *malware* dengan memanfaatkan *collective intelligence framework (CIF)*. CIF tidak hanya mendeteksi *hash malware* melainkan juga *ip address* pengirim sehingga dapat dilakukan pencegahan. Hasil yang diperoleh adalah serangan *malware* dapat dideteksi dan dicegah walaupun dengan persentase deteksi yang masih kecil.

**Kata Kunci:** *malware, honeypot, threat intelligence, dionaea, CIF.*

## **ABSTRACT**

*The development of malware is increasing and varies from year to year. Not only targeting computer systems as a victim, malware also attacks smartphones and IoT devices. According to a survey conducted by Symantec, by 2016 there are 357 million new types of malware that actively attack computer and smartphone systems. Some precautions have been done in various instances including by installing a honeypot to capture the malware that is attacking through a computer network.*

*The use of honeypot to capture malware on computer networks is considered quite effective because in addition to getting a copy of malware, honeypot can also record information about the sender of malware. However, the ability of honeypot in detecting malware is still very simple so that the application needed to improve the ability of honeypot in detecting malware.*

*Applications created in this study are able to improve the ability of honeypot in detecting malware by utilizing collective intelligence framework (CIF). CIF not only detects malware hash but also the sender ip address so the attack can be prevented. The results obtained are malware attacks can be detected and prevented even with a small percentage of detection.*

**Keyword:** *malware, honeypot, threat intelligence, dionaea, CIF.*