INVESTIGASI FORENSIK PERBANDINGAN KECEPATAN SISTEM OPERASI *PROPRIETARY* DAN *OPEN SOURCE* DALAM MENANGKAP SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (*DDOS*)

Skripsi

untuk memnuhi sebagian persyaratan mencapai derajat S-1

Program Studi Teknik Informatika

Disusun oleh :

Rizky

12651054

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2016

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : B-4475 /Un.02/DST/PP.05.3/12/2016

Skripsi/Tugas Akhir dengan judul	:	Investigasi Forensik Perbandingan Kecepatan Sistem Operasi *Proprietary* dan *Open Source* dalam Menangkap Serangan *Distributed Denial of Service* (DDoS)
Yang dipersiapkan dan disusun oleh	:	
Nama	:	Rizky
NIM	:	12651054
Telah dimunaqasyahkan pada	:	6 Desember 2016
Nilai Munaqasyah	:	A / B

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Dr. H. Iwan Riadi, M.Kom
NIY.60020397

Penguji I

M. Mustaqim, M.T
NIP.19790331 200501 1 004

Penguji II

Anik Fajih Rifa'i, M. Kom
NIP.19860306 201101 1 009

Yogyakarta, 14 Desember 2016
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. [illegible], M.Si
NIP. 19681212 200003 1 001

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Permohonan
Lamp : 1 Bandel

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Rizky
NIM : 12651054
Judul Skripsi: Investigasi Forensik Perbandingan Kecepatan Sistem Operasi *Proprietary* dan *Open Source* dalam Menangkap serangan *Distributed Denial of Service (DDoS)*

sudah dapat dinjukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 21 November 2016
Pembimbing

Dr. H. Imam Riadi, M.Kom
NIY. 60020397

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama : Rizky

NIM : 12651054

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **"Investigasi Forensik Perbandingan Kecepatan Sistem Operasi *Proprietary* dan *Open Source* dalam Menangkap Serangan *Distributed Denial of Service (DDoS)*"** tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 18 November 2016

Hormat saya,

Rizky

12651054

MOTTO

Barang siapa ingin mutiara, harus berani terjun kelautan yang dalam (Ir. Soekarno)

PERSEMBAHAN

Kupersembahkan karya ini untuk orang-orang tercinta, yang menyemangati.

1. Untuk kedua orang tua mamah (almh) Nurlaela Siregar, untuk abi Ahmad Rizq terimakasih atas pengorbanannya.
2. Untuk abangku Zakky Ahmad terimakasih untuk motivasi yang diberikan dan rejeki yang dibagi ketika skak.
3. Untuk Bapak-Ibu dosen Teknik Informatika UIN Sunan Kalijaga Pak Bambang, Pak Imam Riadi, Pak Nasirudin, Pak Awick, Pak mustakim, Pak Taufik, Pak Sumarsono, Pak Didik, Pak Aulia, Pak Agus, Ibu Uyun, Ibu ade, dan Ibu Maria Ulfa terimakasih atas ilmu yang telah ditularkan.
4. Untuk teman-teman seperjuangan Ulfa Septi Muslimah, Bayu Resi Indrawan, Nur Rohman terimakasih telah meminjamkan laptop-laptop kalian untuk penelitian ini.
5. Untuk Indah Permatasari dan teman-teman Kerja Praktik yang selalu membagi ilmu.
6. Untuk teman-teman Teknik Informatika 2012 Mandiri khususnya dan teman-teman sejurusan yang tak bisa disebutkan satupersatu terimakasih.
7. Untuk teman-teman Kuliah Kerja Nyata, Abdi Wisnu, Eko, Muktafin, Desriani, Hairunnisa, Kurnia, Oktina, dan Intan.

KATA PENGANTAR

Alhamdulillahhirobbil'aalamiin puji syukur kehadirat Allah SWT karena atas limpahan rahmat, hidayah, serta petunjuk-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul *Investigasi Forensik Perbandingan Kecepatan Sistem Operasi Proprietary dan Open Source Dalam Menghadapi Serangan Distributed Denial of Service*. Shalawat serta salam semoga tercurah kepada Nabi Muhammad SAW. Dengan kerendahan hati penulis mengucapkan terimakasih kepada:

1. Bapak Prof. Drs. Yudian Wahyudi, M.A., Ph.D. Selaku rektor Universitas Islam Negeri Sunan Kalijaga.
2. Orang Tua Penulis Ibu (almh) Nurlaela Siregar, dan Bapak Ahmad Rizq, yang selalu menyayangi, dan mendoakan.
3. Bapak Dr. Murtono, M.Si. Selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
4. Bapak Dr. Bambang Sugiantoro, MT. Selaku Kepala Program Studi Teknik Informatika Universitas Islam Negeri Sunan Kalijaga.
5. Bapak Agus Mulyanto, S.Si, M.Kom. Selaku Pembimbing Akademik.
6. Bapak Dr. H. Imam Riadi, M.Kom. Selaku dosen pembimbing tugas akhir yang rela mengoreksi, memotivasi penulis.
7. Kepada seluruh dosen dan karyawan Program Studi Teknik Informatika.

Penulis menyadari masih banyak kekurangan dalam penelitian ini, oleh karena itu segala kritik dan saran selalu diharapkan. Akhir kata semoga penelitian ini bermanfaat.

Yogyakarta, 1 November 2016

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INVESTIGASI FORENSIK PERBANDINGAN KECEPATAN SISTEM OPERASI *PROPRIETARY* DAN *OPEN SOURCE* DALAM MENANGKAP SERANGAN *DISTRIBUTED DENIAL OF SERVICE* (*DDOS*)

Rizky
12651054
Universitas Islam Negeri Sunan Kalijaga
Email : rizkyuin@gmail.com

INTISARI

Sistem informasi dirancang untuk mendukung apa yang ingin diselesaikan pengguna, sistem operasi harus mendukung jaringan sampai tingkatan tertentu. Hasilnya adalah port yang semakin terbuka dan layanan yang aktif menjadi tersedia dan visibel. Karenanya, penyerang memiliki banyak kesempatan untuk memilih sebuah serangan hasilnya adalah dalam akses seperti yang mereka inginkan.

Tahapan penelitian mengidentifikasi sumber-sumber potensial dan kemudian dikumpulkan, mengumpulkan kepingan informasi yang relevan, melakukan analisa dan mendokumentasikan sehingga menjadi sebuah kesimpulan. Perhitungan yang digunakan menggunakan *Naïve Bayes* dengan variabel perhitungan jumlah paket yang dikirim, sistem operasi yang diguanakan, waktu serangan, dan klasifikasi serangan sesuai perhitungan standar deviasi.

Hasil penelitian menunjukan bahwa dari 12 sample yang diambil dari sistem operasi *Proprietary* dan *Open Source* dinyatakan bahwa 2 data sistem operasi *Proprietary* dinilai cepat mendapat serangan dan 4 dinilai lambat. Sementara sistem operasi *Open Source* dinyatakan 4 data dinilai cepat mendapat serangan, dan 2 data dinilai lambat mendapat serangan *DDoS*. Penelitian investigasi ini berjalan berhasil dan lancar.

Kata Kunci: Investigasi, Forensik, Jaringan, *Proprietary*, *Open Source*.

FORENSIC INVESTIGATION SPEED COMPARISON OF OPERATING SYSTEM PROPRIETARY AND OPEN SOURCE IN DEALING WITH DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS)

Rizky
12651054
Universitas Islam Negeri Sunan Kalijaga
Email : rizkyuin@gmail.com

ABSTRACT

The information system is designed to support what you want users completed, the operating system must support the network to a certain extent. The result is an increasingly open ports and active services become available and visible. Therefore, attackers have many opportunities to choose an attack result is within the access as they wish.

Stages of research to identify potential sources and then collected, collecting pieces of relevant information, analyzing and documenting it becomes a conclusion. Calculations used using Naïve Bayes with variable calculation of the number of packets sent, the operating system that is primarily used, time attacks and classification of attacks as calculated by the standard deviation.

The results showed that of the 12 samples taken from the operating system Proprietary and Open Source stated that 2 operating system data Proprietary rated fast under attack and 4 rated slow. While the Open Source operating system declared 4 Data rated quickly came under attack, and 2 data assessed later got a DDoS attack. The study of this investigation runs successfully and smoothly.

Keyword: Investigation, Forensics, Network, Proprietary, Open Source.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Sistem informasi dirancang untuk mendukung apa yang ingin diselesaikan pengguna, dalam konteks bahasan ini, sistem operasi harus mendukung jaringan sampai tingkatan tertentu. Semakin banyak jaringan yang didukung oleh sebuah sistem, semakin banyak pula layanan yang diaktifkan untuk mendukung kebutuhan-kebutuhan tersebut. Hasilnya adalah *port* yang semakin terbuka dan layanan yang aktif menjadi tersedia dan visibel. Karenanya, penyerang memiliki banyak kesempatan untuk memilih sebuah serangan hasilnya adalah dalam akses seperti yang mereka inginkan.

Selain itu, pengguna dan administrator mengira bahwa pekerjaan ini selesai saat sebuah server memiliki sistem operasi yang telah terinstall dan layanannya telah dikonfigurasi, ini merupakan kesalahan yang akan mejadikan Anda target sempurna bagi seorang penyerang jika menemukan server yang memiliki sistem operasi asli yang diinstal tanpa patch dengan semua layanan default telah diaktivasi. Server tersebut akan terkontaminasi dalam hitungan jam.

Sekarang sudah jelas bahwa penyerang yang berkeliaran di Internet menggunakan semua jenis piranti, dari yang terotomastisasi sampai yang khusus ditujukan bagi korban. Tiap orang mengetahui bahwa dibutuhkan alamat IP publik untuk terkoneksi ke Internet. Alamat-alamat ini disebarkan keseluruh dunia sehingga kita seharunsnya dapat mencari kemana serangan-serangan ditujukan.

Menurut perusahaan keamanan ISS , dari 5052 insiden keamanan yang telah direkam antara 1 april 2003 hingga 20 juni 2003, mereka mencatat 86,3% serangan dari Amerika Utara, 7,16% dari Eropa, 5,18% dari Asia, 0,72% dari Asia Pasifik, 0,39% dari Amerika Selatan, 0,21% tidak diketahui asalnya, dan 0,04% dari Afrika.

Selain itu perusahaan keamanan ISS juga mencatat sektor mana saja yang diserang diantaranya yaitu: Layanan 24,23% , Keuangan dan Asuransi 19,43 %, Eceran 15,69%, Manufakturing 10,6%, Pemerintah negara bagian, Lokal, dan Federal 7,56%, Makanan dan Obat-obatan 5,16%, Teknologi Informasi 4,26%, Bidang kesehatan 2,86%, Transportasi 2,68%, Konsultasi 2,59%, Pendidikan 1,26%, Utilitas 1,13%, Telekomunikasi 1,09%, Hiburan 0,64%, Layanan formal 0,01%.

Observasi menarik adalah dari 86,3% serangan yang berasal dari Amerika Utara, 82%-nya berasal dari Amerika Serikat, angka ini mungkin ada benarnya karena penetrasi Internet yang paling besar di Amerika Serikat, angka ini juga bisa jadi adalah keliru karena penyerang sebelumnya telah menyerang sistem di Amerika Serikat dari negara lain dan selanjutnya menggunakan sistem tersebut untuk menyerang sistem lainnya.

Distributed Denial Of Service (*DDoS*) adalah serangan yang sering kita jumpai diantara serangan serangan lainnya. *DDoS* adalah serangan yang dapat dikatakan terstrukur. *DDoS* memiliki dampak yang besar bagi sebuah server, mengingat banyaknya serangan menggunakan metode ini.

Penelitian ini bertujuan membandingkan, menganalisa dan mengidentifikasi bentuk serangan *DDoS* terhadap server yang menggunakan sistem operasi *Proprietary* dan *Open Source* dengan mengumpulkan semua *log* data dan mengkalsifikasikan waktu serangan.

Algoritma *Naïve Bayes* merupakan salah satu algoritma yang terdapat pada teknik klasifikasi *Naïve Bayes* merupakan pengklasifikasikan dengan metode probabilitas dan statistic yang dikemukakan oleh ilmuwan Inggris *Thomas Bayes*, yaitu memprediksi peluang di masa depan berdasarkan pengalaman di masa sebelumnya sehingga di kenal sebagai *Teorema Bayes*. Teorema tersebut dikombinasikan dengan *Naïve* dimana diasumsikan kondisi antar atribut saling bebas. Klasifikasi *Naïve Bayes* diasumsikan bahwa ada atau tidak ciri tertentu dari sebuah kelas tidak ada hubungannya dengan ciri dari kelas lainnya. Penelitian ini menggunakan metode *Naïve Bayes* karena mampu mengklasifikasikan data sesuai skema penelitian.

Berdasarkan kenyataan tersebut penulis ingin meneliti perbandingan sistem operasi *Proprietary* dan *Open Source* dalam menangkap serangan DDoS menggunakan metode *Naïve Bayes*.

1.2 Rumusan Masalah

Berdasarkan penjelasan diatas, penulis merumuskan masalah sebagai berikut:

1. Bagaimana menemukan alamat penyerang server yang telah melakukan penyerangan *DDoS*?

2. Bagaimana menganalisa kecepatan serangan *DDoS* terhadap sistem operasi *Proprietary* dan sistem operasi *Open Source*?
3. Bagaimana menemukan sistem operasi yang lebih rentan dan lebih kuat dalam menghadapi serangan *DDoS*?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini antara lain yaitu:

1. Serangan yang dilakukan adalah simulasi,
2. Skenario simulasi dilakukan tidak *live attack*,
3. Skenario serangan ini menggunakan server bersistem operasi *Windows 10 Education* dan Ubuntu 15.10 *Desktop*.

1.4 Tujuan Penelitian

Tujuan penelitian ini yaitu:

1. Menemukan IP *Address* yang melakukan serangan *DDoS*.
2. Melakukan analisa terhadap kecepatan serangan *DDoS*.
3. Mengetahui sistem operasi mana yang lebih rentan dan kuat terhadap serangan *DDoS*.

1.5 Manfaat Penelitian

Sebagai penelitian ini penulis menginginkan sebagai pembelajaran bagi penulis dan pembaca untuk tindakan pencegahan terhadap serangan *DDos*, serta dapat mempelajari pencegahan dari serangan *DDoS* ini.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang dapat dari penelitian ini yaitu sebagai berikut:

1. *Tools* snort yang digunakan pada Ubuntu 15.10 *Desktop* menunjukan *ip address* penyerang dan protokol yang diserangan, sehingga investigasi mendapatkan penyerang. *Tools* wireshark yang digunakan pada *Windows 10 Education* menunjukan *ip address* penyerang dan protokol yang diserang.
2. Perhitungan menggunakan *Naïve Bayes* dari 12 sample yang dihitung, sistem operasi Ubuntu 15.10 Desktop dinilai lebih cepat karena 4 dari 12 sampel dinilai cepat sementara sistem operasi Windows 10 Education 2 dari 12 sampel dinilai cepat. Sementara nilai lambat dari sistem operasi Ubuntu 15.10 Desktop yaitu 2 dari 12 sample, sementara untuk sistem operasi Windows 10 Education 4 dari 12 sampel.
3. *Windows 10 Education* memiliki kelebihan dalam menghadapi serangan *DDoS* karena lebih lambat dalam menangkap serangan tersebut. Sampel menunjukan 4 dari 12 sampel Windows 10 Education dinilai lambat dalam menghadapi serangan *DDoS*.

5.2 Saran

Penelitian ini tentunya masih banyak kekurangan, saran untuk penelitian selanjutnya perlu diperhatikan beberapa hal diantaranya:

1. Penelitian selanjutnya dapat menggunakan spesifikasi server dan sistem operasi yang memadai untuk sebuah server agar bisa digunakan analisis pada server sesungguhnya.
2. Penelitian dapat membuat *tools* pemfilter spam serangan *Distributed Denial of Service.*
3. Mencoba analisis pada server sesungguhnya.
4. Penelitian mencoba menggunakan UDP dalam serangan.

DAFTAR PUSTAKA

Abbas, Sri, P. U. & Herika, H., 2014. *Modul Workshop Keamanan Jaringan dengan Backtrack: Wififu, MITM, Stress Testing dan Web Attack*.

Abdillah, F., 2015. *Konsep DoS dan DDoS (Distributed Denial of Service), serta Mekanisme Serangan DoS dan DdoS dan cara penanggulangannya.*

Ahmad, S., 2013. *DDoS Attack Detection Simulation and Handling Mechanism*.

Anon., 2016. [Online] Available at: https://www.snort.org [Diakses 19 Agustus 2016].

Baskoro, A. P., Supeno, D. & Wahyu, S., 2011. *Linux Virtual Server Untuk Mengatasi Serangan Ddos*.

Faris, M., 2010. *Analisa Serangan DDoS Pada Server Ubuntu yang Beroperasi Dalam Wireless Local Area Network*.

Masidan., 2012. *Implementasi dan Analisa HIDS (Host Based Intrusion Detection System) Dengan Snort Untuk Mencegah DDoS (Distributed Denial of System).*

Noah, D., 2015. *Snort 2.9.8.x on Ubuntu 12, 14, and 15*.

Rudi, H,. 2012. *Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denial of Service*.

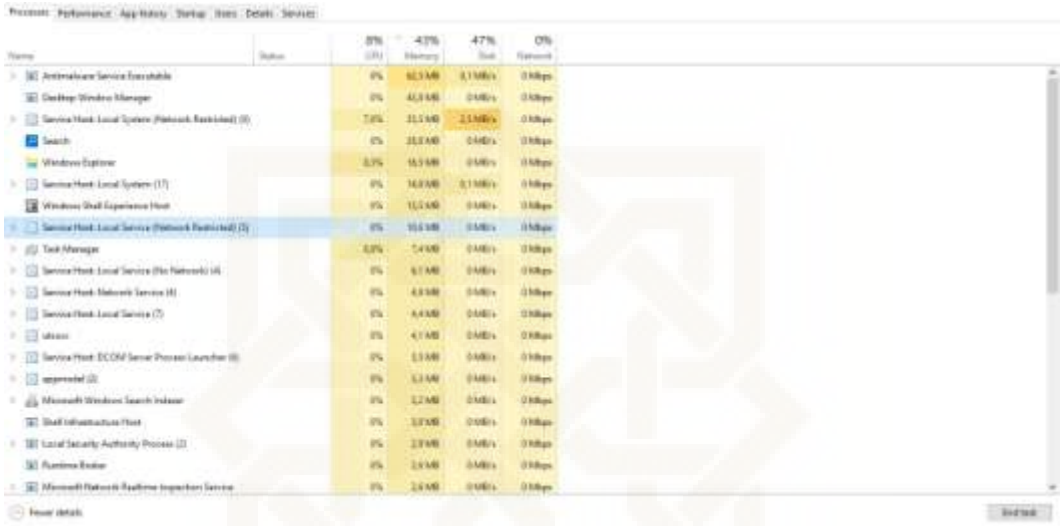
Wendell, O., 2008. *Computer Networking First-Step*. Yogyakarta: Andi Publisher.

Yogi, S, N., 2012. *Investigasi Forensik Jaringan Dari Serangan Distributed Denial of Service(DDoS) Menggunakan Metode* Naïve *Bayes*.

Yunan, A. P., 2014. *Penggunaan Nmap Dan Hping 3 Dalam Menganalisa Keamanan Jaringan Pada B2P2TO2T (Karanganyar, Tawangmangu).*

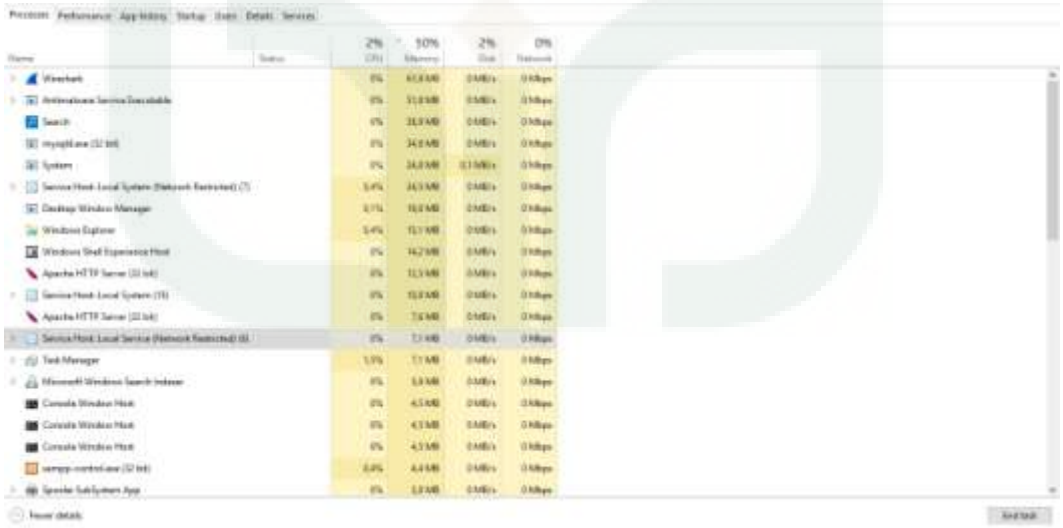
LAMPIRAN

Lampiran 1 Kondisi performa laptop sistem operasi Windows 10 sebelum *tools* digunakan:



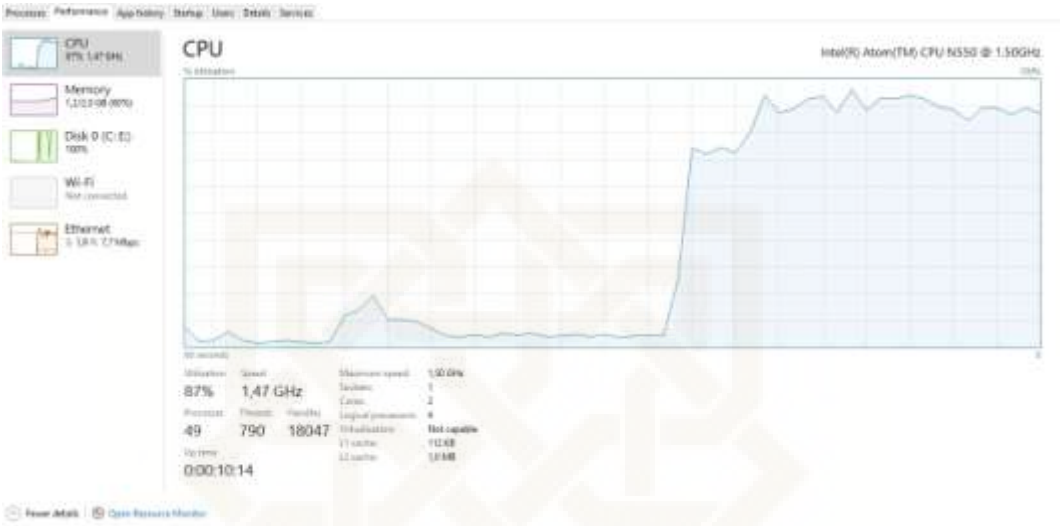
Lampiran 1 Kondisi Windows 10 Normal

Lampiran 2 Kondisi performa laptop sistem operasi Windows 10 sesudah *tools* digunakan:



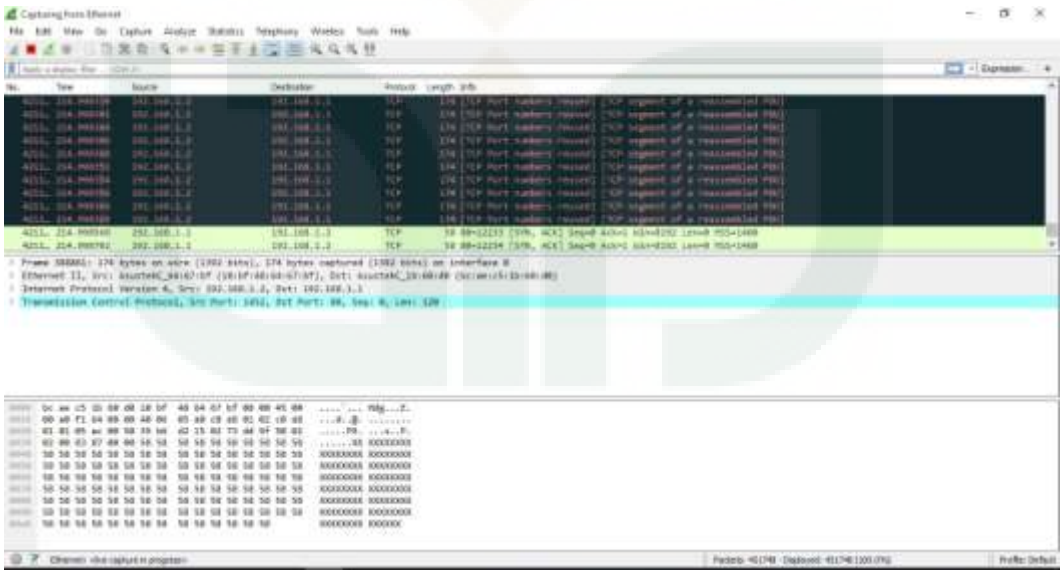
Lampiran 2 Performa Windows 10Ketika Tools Dinyalakan

Lampiran 3 Kondisi performa laptop sistem operasi Windows 10 mendapat serangan 30.000 paket:



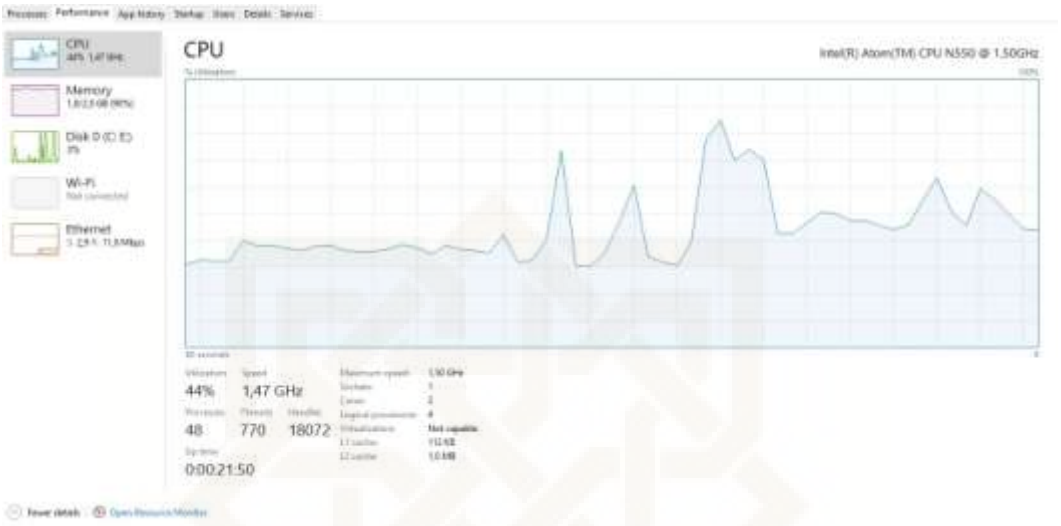
Lampiran 3 Performa Windows 10 Serangan 30.000 Paket

Lampiran 4 Kondisi wireshark pada sistem operasi Windows 10 mendapat serangan 30.000 paket:



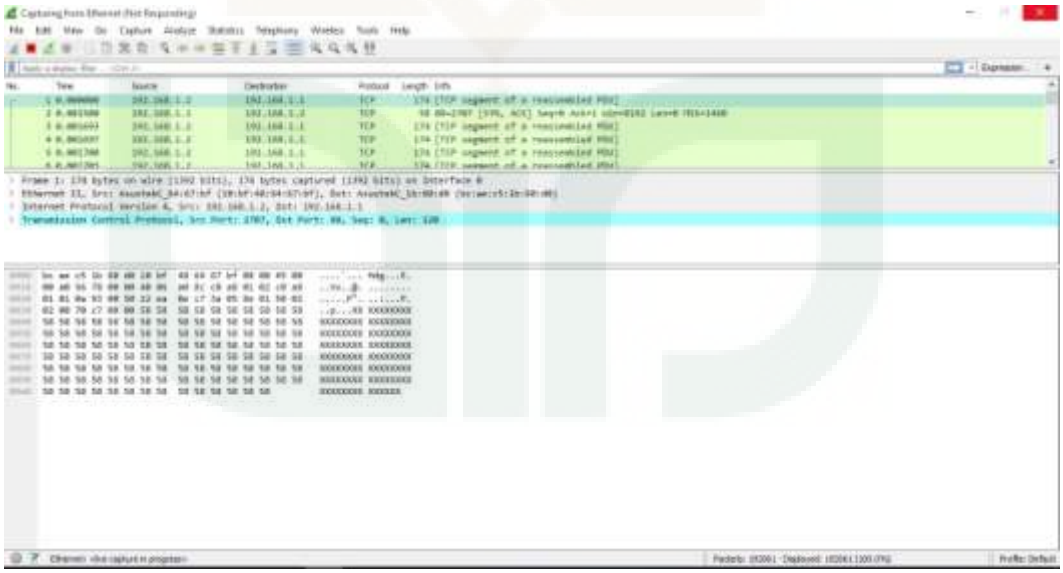
Lampiran 4 Kondisi Wireshark Serangan 30.000 Paket

Lampiran 5 Kondisi performa laptop sistem operasi Windows 10 mendapat serangan 50.000 paket:



Lampiran 5 Performa Windows 10 Serangan 50.000 Paket

Lampiran 6 Kondisi wireshark pada sistem operasi Windows 10 mendapat serangan 50.000 paket:

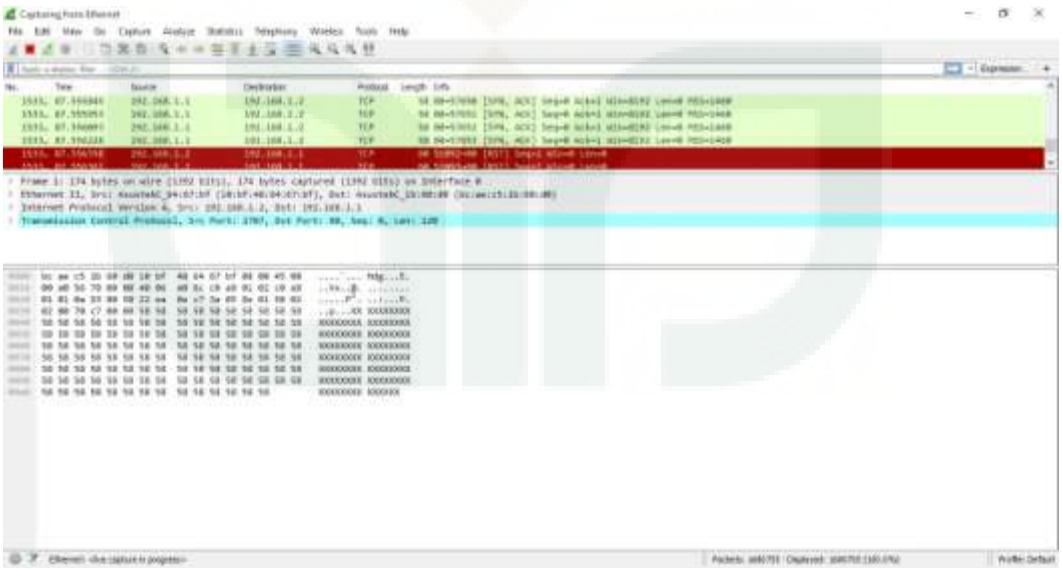


Lampiran 6 Kondisi Wireshark Serangan 50.000 Paket

Lampiran 7 Kondisi performa laptop sistem operasi Windows 10 mendapat serangan 100.000 paket:

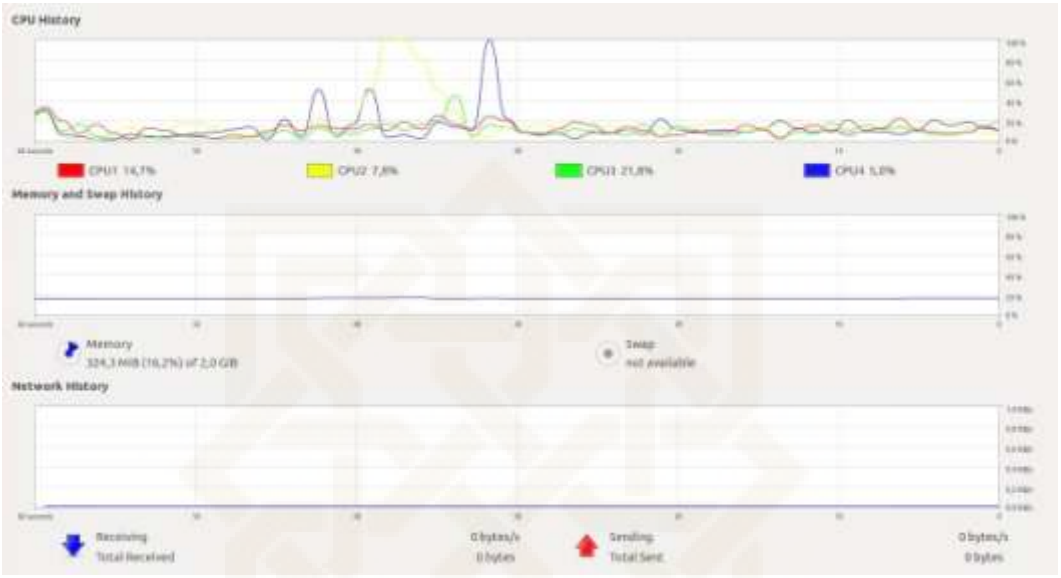
Lampiran 7 Performa Windows 10 Serangan 100.000 Paket

Lampiran 8 Kondisi wireshark pada sistem operasi Windows 10 mendapat serangan 100.000 paket:



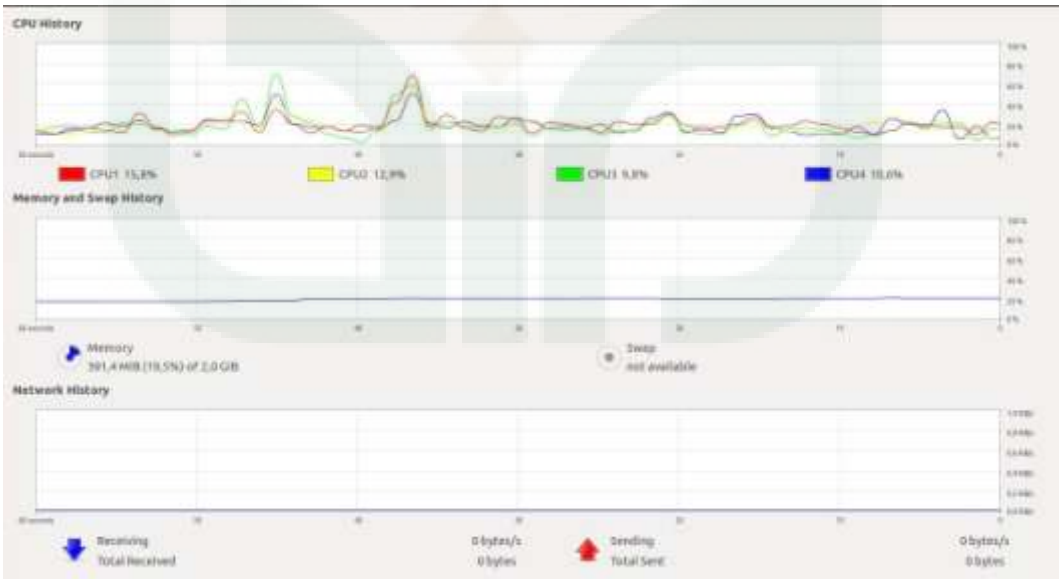
Lampiran 8 Kondisi Wireshark Serangan 50.000 Paket

Lampiran 9 Kondisi performa laptop sistem operasi Ubuntu 15.10 sebelum *tools* digunakan:



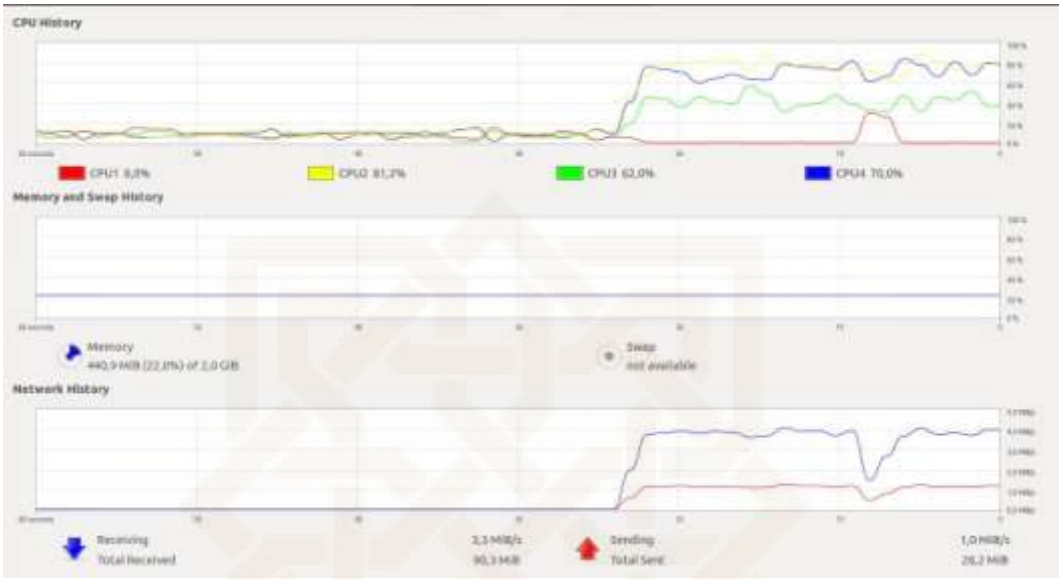
Lampiran 9 Kondisi Ubuntu 15.10 Normal

Lampiran 10 Kondisi performa laptop sistem operasi Ubuntu 15.10 sesudah *tools* digunakan:



Lampiran 10 Performa Ubuntu 15.10 Ketika Tools Dinyalakan

Lampiran 11 Kondisi performa laptop sistem operasi Ubuntu 15.10 mendapat serangan 30.000 paket:



Lampiran 11 Performa Ubuntu 15.10 Serangan 30.000 Paket

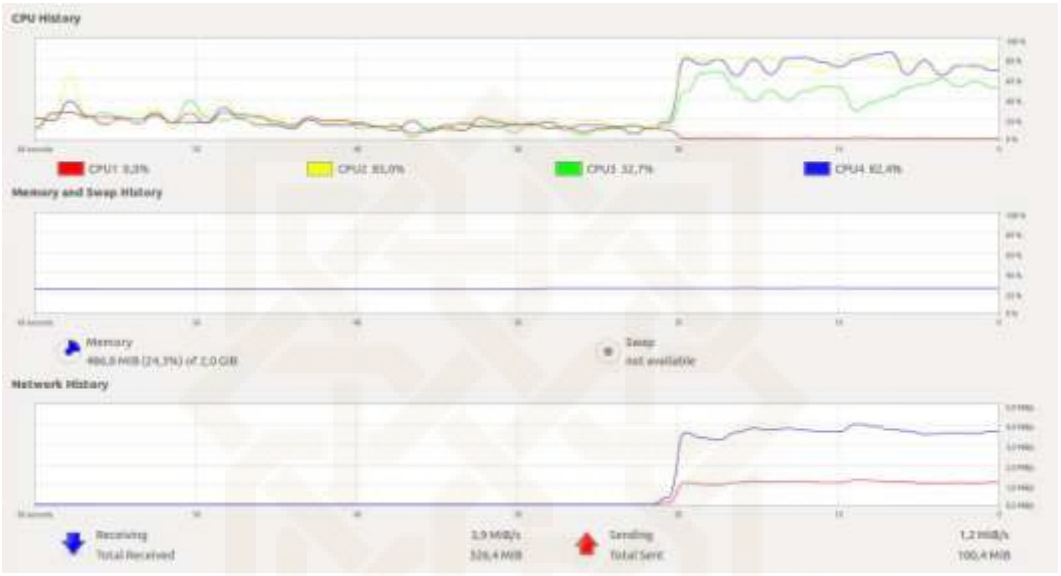
Lampiran 12 Kondisi snort pada sistem operasi Ubuntu 15.10 mendapat serangan 30.000 paket:

```
Run time for packet processing was 17.332590 seconds
Snort processed 17165 packets.
Snort ran for 0 days 0 hours 0 minutes 17 seconds
Pkts/sec:       1009
===============================================================
Memory usage summary:
Total non-mmapped bytes (arena)    : 610304
Bytes in mapped regions (hblkhd)   : 11898880
Total allocated space (uordblks)   : 487472
Total free space (fordblks)        : 122832
Topmost releasable block (keepcost) : 87296
===============================================================
Packet I/O Totals:
Received       : 2378780
Analyzed       : 48629 (  2.044%)
Dropped        : 2319939 ( 49.374%)
Filtered       : 0 (  0.000%)
Outstanding    : 2330151 ( 97.956%)
Injected       : 0
===============================================================
Breakdown by protocol (includes rebuilt packets):
```

Eth	: 48628 (100.000%)
VLAN	: 0 (0.000%)
IP4	: 48626 (99.996%)
Frag	: 0 (0.000%)
ICMP	: 0 (0.000%)
UDP	: 1 (0.002%)
TCP	: 48625 (99.994%)
IP6	: 2 (0.004%)
IP6 Ext	: 2 (0.004%)
IP6 Opts	: 0 (0.000%)
Frag6	: 0 (0.000%)
ICMP6	: 0 (0.000%)
UDP6	: 2 (0.004%)
TCP6	: 0 (0.000%)
Teredo	: 0 (0.000%)
ICMP-IP	: 0 (0.000%)
IP4/IP4	: 0 (0.000%)
IP4/IP6	: 0 (0.000%)
IP6/IP4	: 0 (0.000%)
IP6/IP6	: 0 (0.000%)
GRE	: 0 (0.000%)
GRE Eth	: 0 (0.000%)
GRE VLAN	: 0 (0.000%)
GRE IP4	: 0 (0.000%)
GRE IP6	: 0 (0.000%)
GRE IP6 Ext	: 0 (0.000%)
GRE PPTP	: 0 (0.000%)
GRE ARP	: 0 (0.000%)
GRE IPX	: 0 (0.000%)
GRE Loop	: 0 (0.000%)
MPLS	: 0 (0.000%)
ARP	: 0 (0.000%)
IPX	: 0 (0.000%)
Eth Loop	: 0 (0.000%)
Eth Disc	: 0 (0.000%)
IP4 Disc	: 0 (0.000%)
IP6 Disc	: 0 (0.000%)
TCP Disc	: 0 (0.000%)
UDP Disc	: 0 (0.000%)
ICMP Disc	: 0 (0.000%)
All Discard	: 0 (0.000%)
Other	: 0 (0.000%)
Bad Chk Sum	: 20633 (42.430%)
Bad TTL	: 0 (0.000%)
S5 G 1	: 0 (0.000%)
S5 G 2	: 0 (0.000%)

Total : 48628
==========
Snort exiting

Lampiran 13 Kondisi performa laptop sistem operasi Ubuntu 15.10 mendapat serangan 50.000 paket:



Lampiran 13 Performa Ubuntu 15.10 Serangan 50.000 Paket

Lampiran 14 Kondisi snort pada sistem operasi Ubuntu 15.10 mendapat serangan 50.000 paket:

Run time for packet processing was 18.765166 seconds
Snort processed 16251 packets.
Snort ran for 0 days 0 hours 0 minutes 18 seconds
Pkts/sec: 902
==========
Memory usage summary:
Total non-mmapped bytes (arena) : 610304
Bytes in mapped regions (hblkhd) : 11898880
Total allocated space (uordblks) : 487472
Total free space (fordblks) : 122832
Topmost releasable block (keepcost) : 87296
==========
Packet I/O Totals:
Received : 2144401
Analyzed : 50291 (2.345%)
Dropped : 2090587 (49.365%)
Filtered : 0 (0.000%)
Outstanding : 2094110 (97.655%)
Injected : 0

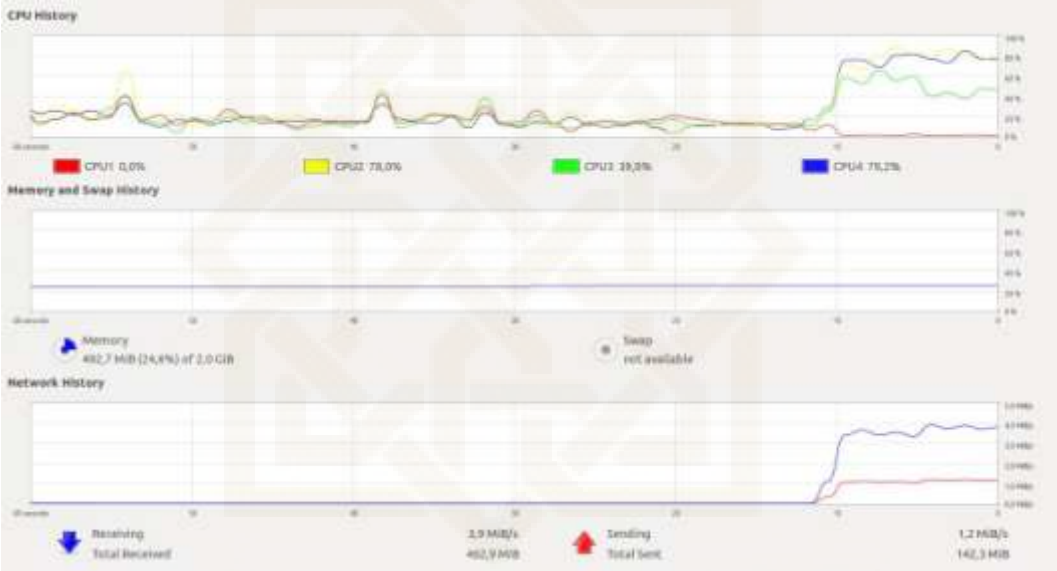
==========

Breakdown by protocol (includes rebuilt packets):

Eth	: 50290 (100.000%)
VLAN	: 0 (0.000%)
IP4	: 50284 (99.988%)
Frag	: 0 (0.000%)
ICMP	: 0 (0.000%)
UDP	: 6 (0.012%)
TCP	: 50278 (99.976%)
IP6	: 6 (0.012%)
IP6 Ext	: 6 (0.012%)
IP6 Opts	: 0 (0.000%)
Frag6	: 0 (0.000%)
ICMP6	: 0 (0.000%)
UDP6	: 6 (0.012%)
TCP6	: 0 (0.000%)
Teredo	: 0 (0.000%)
ICMP-IP	: 0 (0.000%)
IP4/IP4	: 0 (0.000%)
IP4/IP6	: 0 (0.000%)
IP6/IP4	: 0 (0.000%)
IP6/IP6	: 0 (0.000%)
GRE	: 0 (0.000%)
GRE Eth	: 0 (0.000%)
GRE VLAN	: 0 (0.000%)
GRE IP4	: 0 (0.000%)
GRE IP6	: 0 (0.000%)
GRE IP6 Ext	: 0 (0.000%)
GRE PPTP	: 0 (0.000%)
GRE ARP	: 0 (0.000%)
GRE IPX	: 0 (0.000%)
GRE Loop	: 0 (0.000%)
MPLS	: 0 (0.000%)
ARP	: 0 (0.000%)
IPX	: 0 (0.000%)
Eth Loop	: 0 (0.000%)
Eth Disc	: 0 (0.000%)
IP4 Disc	: 0 (0.000%)
IP6 Disc	: 0 (0.000%)
TCP Disc	: 0 (0.000%)
UDP Disc	: 0 (0.000%)
ICMP Disc	: 0 (0.000%)
All Discard	: 0 (0.000%)
Other	: 0 (0.000%)
Bad Chk Sum	: 21278 (42.311%)
Bad TTL	: 0 (0.000%)

S5 G 1 : 0 (0.000%)
S5 G 2 : 0 (0.000%)
Total : 50290
==========
Snort exiting

Lampiran 15 Kondisi performa laptop sistem operasi Ubuntu 15.10 mendapat serangan 100.000 paket:



Lampiran 15 Performa Ubuntu 15.10 Serangan 100.000 Paket

Lampiran 16 Kondisi snort pada sistem operasi Ubuntu 15.10 mendapat serangan 100.000 paket:

Run time for packet processing was 16.726003 seconds
Snort processed 14909 packets.
Snort ran for 0 days 0 hours 0 minutes 16 seconds
Pkts/sec: 931
==========
Memory usage summary:
Total non-mmapped bytes (arena) : 610304
Bytes in mapped regions (hblkhd) : 11898880
Total allocated space (uordblks) : 487472
Total free space (fordblks) : 122832
Topmost releasable block (keepcost) : 87296
==========
Packet I/O Totals:

```
Received        : 1477312
Analyzed        : 29504 (  1.997%)
Dropped         : 1437296 ( 49.314%)
Filtered        : 0 (  0.000%)
Outstanding     : 1447808 ( 98.003%)
Injected        : 0
==========================================================
Breakdown by protocol (includes rebuilt packets):
Eth             : 29503 (100.000%)
VLAN            : 0 (  0.000%)
IP4             : 29497 ( 99.980%)
Frag            : 0 (  0.000%)
ICMP            : 0 (  0.000%)
UDP             : 6 (  0.020%)
TCP             : 29491 ( 99.959%)
IP6             : 6 (  0.020%)
IP6 Ext         : 6 (  0.020%)
IP6 Opts        : 0 (  0.000%)
Frag6           : 0 (  0.000%)
ICMP6           : 0 (  0.000%)
UDP6            : 6 (  0.020%)
TCP6            : 0 (  0.000%)
Teredo          : 0 (  0.000%)
ICMP-IP         : 0 (  0.000%)
IP4/IP4         : 0 (  0.000%)
IP4/IP6         : 0 (  0.000%)
IP6/IP4         : 0 (  0.000%)
IP6/IP6         : 0 (  0.000%)
GRE             : 0 (  0.000%)
GRE Eth         : 0 (  0.000%)
GRE VLAN        : 0 (  0.000%)
GRE IP4         : 0 (  0.000%)
GRE IP6         : 0 (  0.000%)
GRE IP6 Ext     : 0 (  0.000%)
GRE PPTP        : 0 (  0.000%)
GRE ARP         : 0 (  0.000%)
GRE IPX         : 0 (  0.000%)
GRE Loop        : 0 (  0.000%)
MPLS            : 0 (  0.000%)
ARP             : 0 (  0.000%)
IPX             : 0 (  0.000%)
Eth Loop        : 0 (  0.000%)
Eth Disc        : 0 (  0.000%)
IP4 Disc        : 0 (  0.000%)
IP6 Disc        : 0 (  0.000%)
TCP Disc        : 0 (  0.000%)
```

```
UDP Disc      : 0 (  0.000%)
ICMP Disc     : 0 (  0.000%)
All Discard   : 0 (  0.000%)
Other         : 0 (  0.000%)
Bad Chk Sum   : 12531 ( 42.474%)
Bad TTL       : 0 (  0.000%)
S5 G 1        : 0 (  0.000%)
S5 G 2        : 0 (  0.000%)
Total         : 29503
===============================================================
Snort                                                    exiting
```