Turnitin Originality Report

Processed on: 24-Jan-2020 12:03 AM WIB
ID: 1245449975
Word Count: 2824
Submitted: 1

Similarity Index	Similarity by Source	
17%	Internet Sources:	15%
	Publications:	5%
	Student Papers:	9%

Anilisis Log Snort Menggunakan Network Forensic By Patmi Kasih

3% match (Internet from 21-Jul-2018)
http://jurnal.stkippgritulungagung.ac.id/index.php/jipi/article/download/348/217

2% match (Internet from 21-Jul-2018)
http://jurnal.stkippgritulungagung.ac.id/index.php/jipi/article/download/344/216

1% match (Internet from 01-Jan-2020)
http://library.binus.ac.id/eColls/eThesisdoc/Bab2HTML/2013101345IFBab2001/page15.html

1% match (Internet from 12-Jun-2019)
https://classoff.wordpress.com/author/zhathy1/

1% match (Internet from 06-Dec-2019)
https://mtikel.blogspot.com/2017/12/

1% match (Internet from 18-Dec-2014)
http://infopraktis.com/category/tekno/page/6/?wpmp_switcher=desktop

1% match (Internet from 14-Jul-2019)
http://repository.umy.ac.id/bitstream/handle/123456789/7445/BAB%20IV.pdf?isAllowed=&sequence=4

1% match (student papers from 05-Apr-2018)
Submitted to University of Westminster on 2018-04-05

1% match (Internet from 19-Oct-2019)
https://dspace5.zcu.cz/bitstream/11025/35527/1/Niedermaier.pdf

1% match (Internet from 21-Jul-2018)
http://jurnal.stkippgritulungagung.ac.id/index.php/jipi/article/download/390/227

1% match (publications)
Risky Frahmatika Dewi, Khususiyah Khususiyah, Galang Surya Gumilang. "Brief group counseling focuses on the solution to improve the independence of decision making students in class XI at SMKN 2 Kediri", TERAPUTIK: Jurnal Bimbingan dan Konseling, 2017

1% match (student papers from 01-Oct-2014)
Submitted to Laureate Higher Education Group on 2014-10-01

1% match (student papers from 07-Jan-2018)
Submitted to Institute of Technology Blanchardstown on 2018-01-07

1% match (student papers from 10-Jul-2014)
Submitted to Universiti Teknologi MARA on 2014-07-10

< 1% match (publications)
Rina Firliana, Dwi Harini, Anas Rahmat A. "Sistem Informasi Layanan Kredit UKM Berbasis SMS Gateway", INTENSIF, 2017

< 1% match (Internet from 02-Feb-2015)
http://digilib.itb.ac.id/files/disk1/633/jbptitbpp-gdl-udionohari-31634-2-2008ts-1.pdf

< 1% match (Internet from 30-Jan-2019)
http://n0systemissafe.blogspot.com/2015/08/infographis-seputar-malware-di-asean.html

< 1% match (Internet from 06-Aug-2019)
https://ddd.uab.cat/search?f=keyword&ln=ca&p=Country+of+origin&sc=1

< 1% match (student papers from 20-Sep-2017)
Submitted to Colorado Technical University Online on 2017-09-20

< 1% match (Internet from 13-Jan-2020)
https://scitepress.org/Papers/2018/88202/pdf/index.html

< 1% match (Internet from 21-Jan-2020)
https://intranet.royalholloway.ac.uk/isg/documents/pdf/technicalreports/2017/rhul-isg-2017-8-machas.pdf

< 1% match (student papers from 08-May-2013)
Submitted to Napier University on 2013-05-08

ANALISIS LOG SNORT MENGGUNAKAN NETWORK FORENSIC Ervin Kusuma Dewi1), Patmi Kasih2) 1)Sistem Informasi Universitas Nusantara PGRI Kediri 2)Teknik Informatika Universitas Nusantara PGRI Kediri 1,2) Jl. KH. Ahmad Dahlan No.76, Mojoroto, Kota Kediri, Jawa Timur 64112 e-mail: ervin @unpkediri.ac. id1), Fatkasih@gmail.com2) ABSTRAK Keamanan yang terjamin dapat meminimalisir kerugian yang disebabkan oleh serangan keamanan jaringan. Sistem keamanan jaringan merupakan faktor penting untuk menjamin stabilitas,integritas dan validitas data. Keamanan tersebut dapat dibangun dengan menggunakan Pendekatan Forensik Jaringan. Forensik Jaringan memfokuskan pada data yang diperoleh berdasarkan pengamatan pada jaringan. Sistem pengamatan serangan dapat menggunakan tools Instrusion Detection System (IDS) Snort. Snort adalah perangkat lunak IDS dan NIDS berbasis opensource dan banyak digunakan untuk untuk mengamankan sebuah jaringan dari aktifitas yang ber- bahaya. Cara kerja Snort mirip dengan TcpDump, tetapi fokus sebagai security packet sniffing. Tujuan dari pe- nelitian ini yaitu menganalisis Log snort sebagai hasil Forensik Jaringan. Pada eksperimen menggunakan topol- ogy star. Terdapat 1 PC sebagai snort, 3 PC client yang melakukan serangan, 7 PC sebagai client biasa. Dari hasil uji coba,

dilakukan set rules sebagai kecerdasan. Hasil eksperimen menunjukaan bahwa snort yang diban- gun mampu memantau lalu lintas jaringan, sehingga ketika terjadi packet mencurigakan yang mengandung se- rangan maka snort akan mengirimkan alert, selain itu juga menyimpan data serangan pada Log snort. Log ter- sebut dapat di investigasi dengan menggunakan Model Proses Forensik. Hasil investigasi menunjukkan bahwa terdapat 3 IP menyerang serta menujukkan data serangan yaitu tanggal melakukan serangan, IP penyerang, waktu serangan, dan jenis serangan.. . Kata Kunci: Network Forensik, Snort, Model Proses Forensik. ABSTRACT Security is assured to minimize losses caused by network security attack. Network security system is an impor- tant factor to ensure the ability, integrity and validity of data. Such security can be built using the Network Fo- rensic Approach. Network forensic focuses on data obtained based on observation on the network. Observing attacks can use Snort Intrusion Detection System (IDS) tool. Snort is an open source-based NIDS software, wide- ly used to secure a network from malicious activity. The working of snort similar to tcpdump, but focus as a secu- rity packet sniffing. The aim of this study is to analyze the log snort as a result of network forensic. In the experi- ment using topology star. There is 1 PC as a snort, 3 PC client that perform attacks, 7 PC as a client too. In the test conducted set as rules as intelegence. The experimental results show that snort is able to monitor network traffic, so that when the suspicious packet containing the attack will send alerts snort, but it also stores the data in the log. The logs can be investigated using the forensic process model. The results of the investigation indicate there are 3 IP attack, as well as showing the attack data are the date of the attack, attacker IP, attack time, and type of attack. Keywords: Network Forensic, Snort, Forensic Process Model. K I. LATAR BELAKANG Keamanan yang terjamin dapat meminimalisir kerugian yang disebabkan oleh serangan keamanan jarin- gan. Berdasarkan data dari direktur lembaga riset Telematika Sharing Vision yang melakukan penelitian pada Tahun 2013, indonesia mendapatkan 42.000 serangan di dunia maya per hari [1]. Begitu juga den- gan Akamai yang melaporkan indonesia menjadi Negara nomor 1 sumber serangan internet (malicious traffic) [2]. Banyaknya pengguna internet dapat menimbulkan masalah, mulai dari kasus perbuatan yang tidak menyenang- kan hingga terjadi kejahatan (fraud). Berdasarkan statistic yang dikeluarkan oleh ID-CERT menunjukkan masa- lah keamanan (security) berupa serangan melalui jaringan (network attack) termasuk perusakan situs web (de- face) dan penerobosan hak akses, virus atau malware, phising, dan fraud [3]. Sistem keamanan jaringan merupakan faktor penting untuk menjamin stabilitas, integritas dan validitas data. Keamanan tersebut dapat dibangun dengan menggunakan. Pendekatan Network Forensic. Forensik Jaringan memfokuskan pada data yang diperoleh berdasarkan pengamatan pada jaringan [4]. Kelebihan dari Network Fo- rensic yaitu mampu manganilisis trafik pada jaringan dan mengobservasi jaringan yang merupakan bagian dari inverstigasi. Pengumpulan data Network Forensic menggunakan sebuah tool yang bisa menyimpan semua kejadian data- data lalu lintas jaringa. Salah satu tool yang mampu memenuhi kebutuhan Network Forensic yaitu Snort. Snort merupakan tool cross platform yang mampu diinstall pada Windows, Mac OS, dan Linux. Snort merupakan tool yang opernsource dan update dari Snort dapat diakses oleh semua pengguna. Snort merupakan tool yang berbasis Intrusion Detection System (IDS) yang dapat memonitor jaringan yang berdampak serangan, selain itu juga me- nyimpan serangan tersebut pada Log. Tujuan dari penelitian ini yaitu mengimplementasikan snort serta

menganalisis Log snort dengan menggunakan Network Forensik, yaitu melakukan inverstigasi dari data serangan yang tersimpan pada Log snort. Pada imple- mentasi akan dibangun sebuah topology star. II. NETWORK FORENSIK Forensik sebagian besar menangani kejahatan yang dilakukan sebelumnya, fokusnya untuk mencegah kejaha- tan di masa depan [5]. Forensik jaringan merupakan salah satu ilmu forensik digital yang melingkupi penemuan dan invesitgasi materi (data) yang ditemukan pada perangkat digital. Menurut Lazzez [6] tahapan Model Proses Forensik (The Forensic Process Model) pada ditunjukkan pada diagram alir Gambar 1. Gambar 1. Diagram Alir Penelitian [6] 1. Preparation And Authorization (Persiapan dan Otorisasi) Network Forensik bisa diterapkan jika dimana network security tools seperi system deteksi instrusi, packet analyzer, dan firewall ditempatkan di beberapa titik jaringan. Otorisasi sangat diperlukan untuk memantau lalu lintas jaringan, selain itu aturan keamanan diterapkan dengan baik sehingga tidak menya- lahi privasi individu dan organisasi. 2. Detection and Incident/Crime (Deteksi insiden / kejahatan) Alert yang disinyalkan oleh security tools menunjukkan serangan dan tahap selanjutnya akan di analisis. Sifat serangan ditentukan dari berbagai parameter. Validasi dilakukan untuk menilai dan mengkonfirmasi dugaan penyerangan. Hal ini dilakukan untuk menentukan apakah penyelidikan dilanjutkan atau menga- baikan alert sebagai false alarm. 3. Incident Response (Penanganan Insiden) Respon terhadap serangan keamanan terdeteksi berdasarkan informasi yang dikumpulkan untuk memva- lidasi dan mengevaluasi kejadian. Respon dimulai tergantung pada jenis serangan dan diarahkan oleh or- ganisasi atau kebijakan hokum yaitu rencana untuk mencegah serangan dan recover kerusakan, pada saat yang bersamaan keputusan apakah penyelidikan dilanjutkan atau tidak. Fase ini berlaku untuk kasus- kasus dimana investigasi dimulai pada saat serangan berlangsung dan tidak dapat dilakukan setelah noti- fikasi serangan. 4. Collection of Network Traces (Koleksi Jejak Jaringan) Network trace dikumpulkan oleh security tools. Pada tahap ini melakukan pencarian bukti dan pengum- pulan bukti, pengenalan terhadap bukti-bukti penyerangan dan pengumpulan bukti. 5. Preservation and Protection (Presentasi dan Ulasan) Data asli yang diperoleh dan log disimpan pada perangakat backup. Memastikan akurasi data, salinan da- ri data yang akan di analisis. Hal ini dilakukan agar penyelidikan dilakukan dapat dibuktikan lagi sehing- ga memenuhi persyaratan hukum. 6. Examination (Pemeriksaan) Data yang diperoleh membentuk dataset dan dapat dianalisis serta dipetakan. Pemeriksaan dilakukan agar informasi penting tidak hilang atau tercampur dengan data lain. Data akan diklasifikasikan, informasi dan data yang tidak penting dihapus. 7. Analysis (Analisis) Bukti-bukti dikumpulkan dan dianalisis pola serangan yang digunakan penyerang. Beberapa parameter penting yang berhubungan dengan pembentukan koneksi, protokol, sistem operasi, fragmentasi paket semua dianalisis untuk mengetahui cara penyeranh. Hasil dari tahap ini adalah validasi dari aktivitas yang mencurigakan. 8. Investigation and Attribution (Investigasi dan Atribusi) Bukti informasi yang diperoleh dari hasil analisis digunakan untuk mengidentifikasi : 1) Serangan apa yang terjadi? 2) IP siapa yang melakukan serangan? 3) Kapan serangan terjadi? 4) Dimana serangan itu terjadi? 5) Bagaimana serangan tersebut bisa terjadi? 6) Mengapa itu terjadi? 9. Presentation (Presentasi dan Review) Semua hasil di sajikan dengan bahasa yang dimengerti serta menjelaskan berbagai prosedur yang digu- nakan sampai pada kesimpulan dari proses penyidikan. Dokumentasi penyidikan juga disertakan agar bi- sa digunakan untuk mencegah kejadian serangan yang sama di masa yang akan datang. III.

IMPLEMENTASI Snort [7] adalah perangkat lunak IDS dan NIDS berbasis opensource dan banyak digunakan untuk untuk mengamankan sebuah jaringan dari aktifitas yang berbahaya. Cara kerja Snort mirip dengan TcpDump, tetapi fokus sebagai security packet sniffing. Fitur utama Snort yang membedakan dengan TcpDump adalah payload inspection, dimana Snort melakukan analisis payload rule set yang disediakan [8]. Snort mempunyai tiga komponen : 1) Sesor yang dapat mengenali adanya security events. 2) Console yang dapat memonitor event dan alerts dan mengontrol sensor 3) Central Engine yang berguna untuk menyimpan event logged yang dilakukan oleh sensor kedalam database dan menggunakan aturanaturan keamanan yang berguna untuk menangani event yang terjadi. Snort di install pada Linux Ubuntu versi 16.04, versi Snort yang di install adalah versi 2.9.9.0 yang dapat di download pada https://www.snort.org/ [9]. Gambar 2 merupakan Snort yang sudah berhasil di install. Gambar 2. SNORT Pada Gambar 3 merupakan cara kerja Snort detection engine dengan IDS mode. Ketika terdapat packet datang melalui switch maka akan terdeteksi oleh detection engine yang sudah terinstall Snort sebagai IDS di cocokan dengan rules yang sudah di set. Packet tersebut dicek apakah packet sesuai dengan rules. Ketika packet tersebut mengandung konten serangan maka akan tersimpan di Log Snort dan akan memunculkan alarm. Namun ketika packet tersebut tidak mengandung konten serangan maka packet tersebut di discard (diabaikan) dan langsung dikirimkan. Detection Engine Logging/Alert Rules Jika Iya, mengirimkan Logging/Alerting Apakah packet sesuai dengan Rules Tidak Discard Gambar 3. Snort detection engine [10] Pada Snort terdapat rule sebagai kecerdasaan Snort. Pengambilan dan penandaan packet dilakukan dengan cara sniffing pada lalu lintas packet pada transport protokol TCP baik packet yang dikirim maupun yang diterima. Rules yang di set memberikan kecerdasan pada saat proteksi, sehingga proses investigasi sangat tergantung dari kecerdasan rule. Gambar 4 merupakan konfigurasi dari penyimpanan rules, ketika terdapat serangan pada server maka log dari serangan tersebut akan tersimpan pada rule. Rules yang diterapkan yaitu : 1) Ping of death. Snort melakukan pencatatan untuk semua paket ICMP yang masuk ke jaringan. Ketika ada paket yang di curigai maka akan muncul pesan “ping of death”, 2) Ketika terjadi serangan pada FTP maka akan muncul notifikasi “FTP connection attempt” 75 Rule 1 alert icmp any any -> $HOME_NET any (msg:"ping of death"; sid:1000001;rev:1; classtype:icmp-event;) Rule 2 alert tcp 192.168.0. 69 any -> $HOME_NET 23 (msg:" FTP connection attempt"; sid:1000002; rev:1;) Gambar 4. Rules Implementasi dilakukan pada server SNORT, log yang tersimpan akan di analisis mengikuti alur Model Proses Forensik. Log akan di parsing untuk melihat isi dari SNORT log, apakah serangan itu bentuk berbahaya atau ti- dak. Snort –dvr snort.log 1494909748 Gambar 5. Membuka Log SNORT Salah satu cara untuk membuka Log Snort dengan menggunakan fungsi -r baik dari Snort, TCPDump, Ethereal atau program lain yang membuat file format libpcap. Gambar 5 merupakan perintah untuk membaca Log Snort. IV. EKSPERIMENT DAN ANALISIS Topologi yang digunakan untuk eksperimen adalah topologi star. Terdapat 1 PC sebagai Snort, 10 PC sebagai client dan semuanya terhubung dengan Switch. Gambar 6 merupakan desain topologi yang digunakan untuk eks- perimen. PC1 PC2 PC3 PC4 SNORT PC5 Switch PC7 PC6 PC10 PC9 PC8 Gambar 6. Topologi Pada eksperimen ini 3 PC akan melakukan serangan kepada server Snort, selain itu 3 PC lainya hanya sebagai client biasa yang mengirimkan packet data ke PC Snort dan ke PC lainya. Lalu lintas tersebut akan di analisis. Konfigurasi dari eksperimen ini seperti Tabel 1.

Tabel 1. Konfigurasi ekperimen Nama PC dan IP Sistem Operasi Toosl pendu- Konfigurasi Aplica- Address kung tion PC 0 Ubuntu versi 16.04 LTS SNORT versi NIDS with alert IP : 192.168.0.69 2.9.9.9 SNORT Rules, TCP. PC 1 Microsoft Windows 7 Command Ping flood & ftp attack IP : 192.168.0.70 Prompt PC 2 Microsoft Windows 7 Command - IP : 192.168.0.71 Prompt PC 3 Microsoft Windows 7 Command Ping flood & ftp attack IP : 192.168.0.72 Prompt PC 4 Microsoft Windows 7 Command - IP : 192.168.0.73 Prompt PC 5 Microsoft Windows 7 Command - IP : 192.168.0.75 Prompt PC 6 Microsoft Windows 7 Command - IP : 192.168.0.76 Prompt PC 7 Microsoft Windows 7 Command - IP : 192.168.0.77 Prompt PC 8 Microsoft Windows 7 Command - IP : 192.168.0.78 Prompt PC 9 Microsoft Windows 7 Command Ping flood & ftp attack IP : 192.168.0.96 Prompt PC 10 Microsoft Windows 7 Command - IP : 192.168.0.80 Prompt Pengujian dilakukan dengan melakukan serangan dengan menggunakan ping flood dan FTP attack. IP yang akan melakukan serangan adalah IP : 192.168.0.70, IP : 192.168.0.72 dan IP : 192.168.0.96. Dari hasil pengujian ketika dilakukan serangan, Snort mempu mendeteksi serangan tersebut berdasarkan kecerdasarn rules yang dibe- rikan. Snort akan memberikan alert, selain itu menyimpan file data serangan pada Log Snort /var/log/snort. Gam- bar 7 adalah salah satu contoh file Log Snort yang di parsing. Gambar 7. Parsing Log Snort 1 Dari Gambar 7 dapat diketehui serangan terjadi pada bulan Agustus dan tanggal 28 , waktu serangan 16:07:09, IP penyerang yaitu 192.168.0.70, dan jenis serangan ICMP (Internet Control Message Protocol) dengan TTL (Time to Live) 128, ID 512. Gambar 8. Parsing SNORT Log 2 Selain itu pada Gambar 8 juga merupakan hasil dari parsing Log Snort yang diketahui bahwa runtime untuk proses packet adalah 0.102570 second dengan total packet 992 packet. Memory sebesar 610.304 bytes. Informasi dari packet log merupakan bahan investigasi forensik jaringan. Dari informasi tersebut administrator jaringan mengetahui apa saja yang terjadi pada jaringan sehingga dapat menelusuri data serangan. Pada file log memung- kinkan semua trafik jaringan di capture dan dilakukan analisis. File log yang berasal dari Snort IDS digunakan sebagai bukti kejadian yang terjadi pada jaringan dan digunakan sebagai bukti. Untuk memudahkan dalam mem- baca hasil serangan, maka disajikan dalam bentuk tabel. Tabel 2 merupakan hasil invertigasi. Tabel 2. Hasil investigasi No Log IP penye- rang Time ID Seq Total (WIB) Packet (pkt/sec) Packet Processing (seconds) 1 1494910751 192.168.0.70 16:10:29 384 27905 78 0.38063 2 1503910699 192.168.0.96 15:58:20 369 4096 19 0.490 3 1501040067 192.168.0.72 16:10:00 512 62976 655 0.91552 4 1503911199 192.168.0.70 16:07:09 512 42496 992 0.102570 V. KESIMPULAN Berdasarkan implementasi dengan menggunakan tools keamanan jaringan Snort maka dapat disimpulkan Snort yang dibangun dapat memantau lalu lintas packet di dalam jaringan serta mampu mendeteksi serangan berdasar- kan rule yang diset, sehingga serangan jaringan komputer tersebut dapat segera ditangani segera mungkin oleh administrator karena terdapat alert. Dari hasil uji coba serangan, total serangan sebanyak 4 (empat) kali. Serangan 2 (dua) kali dilakukan oleh IP yang sama yaitu 192.168.0.70 namun waktu serangan yang berbeda. Dengan menggunakan Network Forensic dapat di kumpulkan bukti-bukti serangan dan dilakukan investigasu untuk men- dapatkan Bukti. Bukti serangan yang didapat meliputi tanggal dan bulan pada saat menyerang, IP penyerang, je- nis serangan, waktu serangan dan jumlah packet yang dikirimkan. DAFTAR PUSTAKA [1] R. Wahyudi. (Oktober, 2014). Kejahatan Dunia Maya di Indonesia Mengkhawatirkan. Kompas Tekno. [Online].

Tersedia : http://tekno.kompas.com/read/2014/10/18/0808000/Kejahatan.Dunia.Maya.di.Indonesia [2] Akamai. (Ocktober, 2013). Akamai Releases Second Quarter 2013 'State Of The Internet' Report. [Online] : http://www.akamai.com/ [3] ID-CERT.(Agustus 2013). Incident Handling Report. [Online] . Tersedia : http://www.cert.or.id/incident_handling/penelitian/3/ [4] B. Raharjo. (Agustus, 2013).Sekilas Mengenai Forensik Digital. Jurnal Sosioteknologi. [Online]. vol. 12 No. 29, p. 384. Tersedia : http://journals.itb.ac.id/index.php/sostek/article/view/ 1116/722. [5] K. Franke. (September, 2010). Digital and Computation Forensics, Forensic Lab Testimoni : NISlab. [Online]. Tersedia : https://sites.google.com/site/testimonlab/ [6] A. Lazzez .(January, 2013) . A Survey about Network Forensic Tools. Int. J. Comput. Inf. Technol. [Online]. vol. 2, no. 1, p. 74. Tersedia : https ://www.ijcit.com/archives/volume2/issue1/Paper020110.pdf [7] N. Dietrich. (Desember, 2017). Snort 2.9.8.x on Ubuntu 12, 14, 15. Document Snort. [Online]. Tersedia : https://www.snort.org/documents. [8] E. K. Dewi. (Januari, 2016). Model, ancangan Keamanan Jaringan Dengan Menggunakan Proses Forensik. Jurnal Maklumatika. [Online] vol. 2, p. 34. Tersedia : http://maklumatika.uniat.ac.id/post-152-volume-3-no-2-januari-2017.html [9] Snort. (Juni, 2017). Snort. [Online]. Tersedia: https://www.snort.org/. [10]R. R. Singh and D. S. Tomar. (Februari, 2015). Network Forensics : Detection and Analysis of Stealth Port Scanning Attack. Interantional J. Comput. Netw. Commun. Secur. [Online]. vol. 3, p. 33. Tersedia : http://www.ijcncs.org/published/volume3/issue2/p2_3-2.pdf E-ISSN : 2540 - 8984 JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Volume 02, Nomor 02, Desember 2017 : 72 - 79 E-ISSN : 2540 - 8984 JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Volume 02, Nomor 02, Desember 2017 : 72 - 79 E-ISSN : 2540 - 8984 JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Volume 02, Nomor 02, Desember 2017 : 72 - 79 E-ISSN : 2540 - 8984 JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Volume 02, Nomor 02, Desember 2017 : 72 - 79 E-ISSN : 2540 - 8984 JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Volume 02, Nomor 02, Desember 2017 : 72 - 79 E-ISSN : 2540 - 8984 JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Volume 02, Nomor 02, Desember 2017 : 72 - 79 E-ISSN : 2540 - 8984 JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Volume 02, Nomor 02, Desember 2017 : 72 - 79 E-ISSN : 2540 - 8984 JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika) Volume 02, Nomor 02, Desember 2017 : 72 - 79 72 73 74 76 77 78 79