

## SNORT IDS SEBAGAI TOOLS FORENSIK JARINGAN UNIVERSITAS NUSANTARA PGRI KEDIRI

Ervin Kusuma Dewi<sup>1</sup>, Dwi Harini<sup>2</sup>, Nisa Miftachurohmah<sup>3</sup>

<sup>1,2,3</sup>Sistem Informasi Universitas Nusantara PGRI Kediri

E-mail: <sup>1</sup>ervin@unpkediri.ac.id, <sup>2</sup>dwiharini1970@yahoo.com,

<sup>3</sup>[nisa.informatics@gmail.com](mailto:nisa.informatics@gmail.com)

*Abstrak*—Keamanan jaringan merupakan faktor yang penting dalam menjamin data. Keamanan yang terjamin dapat menghindari kerugian yang disebabkan oleh serangan di dalam jaringan. Terdapat beberapa metode yang dapat digunakan untuk melakukan keamanan suatu jaringan, yaitu dengan menggunakan Forensic Jaringan. Forensic jaringan merupakan turunan dari forensic digital. Forensic jaringan memfokuskan pada data yang diperoleh. Tools yang bisa dimanfaatkan untuk Forensic Jaringan adalah Snort. Snort merupakan perangkat lunak IDS yang cara kerjanya lebih fokus sebagai sekuriti packet sniffing, fitur utama snort yaitu payload inspection, sehingga IDS Snort cocok digunakan sebagai tools Forensic Jaringan. Tujuan dari penelitian ini adalah membuat keamanan jaringan dengan menggunakan menggunakan Forensic Jaringan. Hasil dari penelitian menunjukkan sistem yang dibangun dengan tools IDS Snort berjalan baik pada sistem operasi Windows serta mampu menampilkan alert ketika terjadi serangan ping of death.

*Kata Kunci*— *Forensic Jaringan, IDS Snort, Keamanan Jaringan.*

*Abstract* – bstrak-Keamanan Jaringan merupakan faktor Yang Penting Data hearts menjamin. Keamanan Yang Terjamin can be menghindari Kerugian Yang disebabkan Oleh Serangan di hearts Jaringan. Terdapat beberapa Metode Yang can be digunakan untuk review melakukan Keamanan Suatu Jaringan, Yaitu DENGAN using Forensic Jaringan. Forensic Jaringan merupakan turunan Dari digital forensic. Forensic Jaringan memfokuskan PADA Data Yang TIMAH. Alat Yang Bisa dimanfaatkan untuk review Forensic Jaringan Adalah

Snort. Snort merupakan Perangkat Lunak IDS Yang Cara kerjanya LEBIH Fokus sebagai sekuriti packet sniffing, fitur Utama mendengus Yaitu pemeriksaan muatan, sehingga IDS Snort Cocok digunakan alat sebagai Forensic Jaringan. Tujuan Dari Penelitian Penyanyi Adalah MEMBUAT Keamanan Jaringan DENGAN using Forensic Jaringan. Hasil Dari Penelitian menunjukkan Sistem Yang dibangun alat DENGAN IDS Snort Berjalan Baik PADA Sistem Operasi Windows Serta Mampu menampilkan peringatan ketika Terjadi Serangan ping kematian.

*Keywords* — Forensic Network, Snort IDS, Network Security.

### 1. PENDAHULUAN

Ketersediaan layanan (availability) merupakan salah satu aspek keamanan yang diperlukan dalam membuat sistem keamanan jaringan komputer atau internet. Keamanan jaringan merupakan faktor penting untuk menjamin data dari pencurian atau pengrusakan data. Dengan meningkatnya pengetahuan tentang hacking dan cracking serta di dukung banyak tool yang bisa digunakan secara mudah untuk melakukan serangan atau penyusupan. Ketika serangan terjadi, maka perlu dilakukan investigasi. Investigasi jaringan bisa dilakukan dengan menggunakan suatu cabang ilmu forensik yaitu forensik jaringan.

Forensik jaringan merupakan turunan dari forensik digital yang merupakan salah satu ilmu forensik. Istilah forensik adalah

proses ilmiah (di dasari ilmu pengetahuan) dalam mengumpulkan, menganalisis dan menghadirkan berbagai bukti dalam bidang pengadilan terkaiti adanya suatu kasus hukum [1]. Forensik jaringan memfokuskan pada data yang diperoleh. Sebagai contoh mengamati traffic pada server yang diakses oleh pengguna yang diduga sebagai penyusupan server [2] sehingga forensik jaringan dapat meneliti log yang dilewati jaringan melalui Intrusion Detection System (IDS).

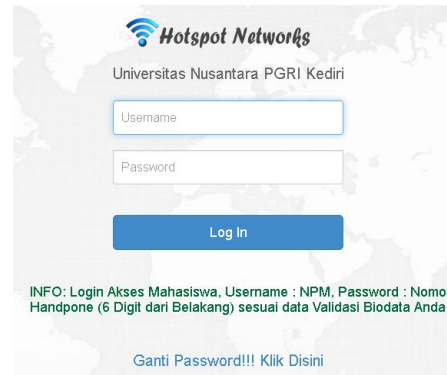
Putri dan Istiyanto [6] meneliti serangan SQL Injection dengan menggunakan Model Proses Forensik (The Forensic Process Model). Pengambilan data dengan menggunakan IDS (Instruction Detection System) Snort. Dari hasil analisis data log serangan SQL Injection yang menuju ke server Universitas Gadjah Mada ([www.ugm.ac.id](http://www.ugm.ac.id)). Mahrouqi dkk [7] membuat simulasi serangan SQL Injection dengan menggunakan GNS3(Graphic Network Simulator). Tujuan utama penelitiannya adalah merancang serangan virtual network untuk membuat sandbox yang memungkinkan untuk melakukan eksperimen yang tidak mengeluarkan biaya besar. Hasil dari penelitiannya digunakan sebagai rekomendasi dalam infrastruktur TI yang menguji website dengan menggunakan serangan SQL Injection. Untuk mensimulasikan skenario serangan dengan menggunakan tools open source GNS3, Oracle VM Virtual Box, VMWare Workstation. Selain itu juga menggunakan tools Whireshark untuk menganalisis aktifitas jaringan.

## 2. METODE PENELITIAN

### *Analisa Sistem Lama*

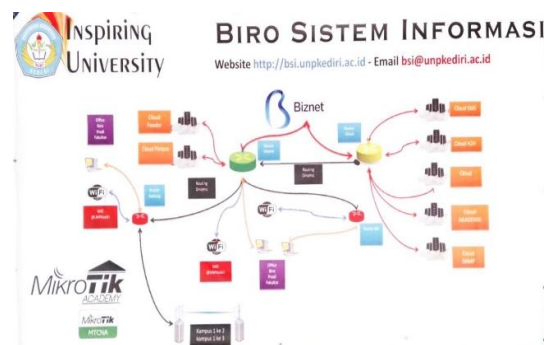
Universitas Nusantara PGRI memiliki 5 kampus, semua tersebar di wilayah kota Kediri. Jaringan UN PGRI dikelola oleh Biro Sarana Informasi (BSI). Pembagian jaringan dengan menggunakan router network. Router yang digunakan adalah Mikrotik karena mikrotik merupakan perangkat lunak sekaligus sistem operasi yang dapat digunakan sebagai router. Keamanan jaringan yang digunakan adalah

dengan menggunakan sistem log in yang sudah di sediakan oleh Mikrotik seperti Gambar. 1



GAMBAR I. LOGIN HOTSPOT UN  
PGRI KEDIRI

Topologi jaringan Universitas Nusantara PGRI Kediri adalah pengembangan dari topologi star. Server, berada di Gedung G, dimana beban kinerja dari server sebagai penyedia layanan tersebar sehingga dapat diakses oleh seluruh kampus. Biro Sistem Informasi menjadi pusat jaringan sekaligus pembagi bandwidth dari tiap-tiap Lab, kantor, dan fakultas-fakultas. Pembagian bandwidth per gedung berdasarkan jumlah user (Dosen dan Mahasiswa).



GAMBAR II. TOPOLOGI JARINGAN UN  
PGRI KEDIRI

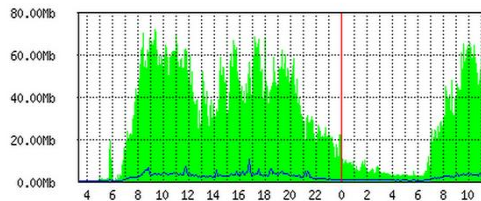
Layanan Internet Service Provider (ISP) menggunakan Biznet. Layanan tersebut dipilih karena Biznet fiber menyediakan konektivitas di dalam kota. Seluruh jaringan terhubung dengan kabel Fiber Optik dengan

kapasitas tinggi untuk mendukung transmisi data, suara dan audio. Jaringan Biznett menerapkan Multi Protocol Labeling Switching (MPLS) beroperasi pada model OSI Layer 2.5 yang dapat digunakan untuk membawa berbagai macam traffic seperti IP, ATM, SONET, dan Frame Ethernet. Hal itulah yang mendasari Biro Sistem Informas memilih ISP Biznett.

Sedangkan router yang digunakan merupakan router Mikrotik, alasan BSI menggunakan router ini yaitu manajemen administrator mudah karena disediakan winbox agar memudahkan admin untuk melakukan setting jaringan. Mikrotik juga memiliki sistem operasi yang berfungsi sebagai router network yang bisa digunakan untuk manajemen bandwidth, firewall, dan sistem hotspot.

Statistik pemakaian bandwidth internet Kampus UN PGRI Kediri pada bulan September 2005 dapat dilihat pada Gambar 3. Terlihat pada gambar bahwa yang paling banyak penggunaan jaringan pada pukul 08.00 sampai pukul 20.00.

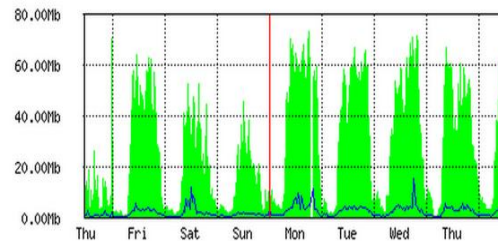
"Daily" Graph (5 Minute Average)



GAMBAR III. TRAFFIC PEMAKAIAN  
JARINGAN PER HARI

Sedangkan traffic pemakaian jaringan perminggu dapat dilihat pada Gambar 4, terlihat traffic pemakaian tertinggi pada hari senin, selasa, rabu dan kamis, karena pada hari-hari tersebut merupakan hari aktif kuliah. Sehingga banyak pemakaian jaringan dari mahasiswa,

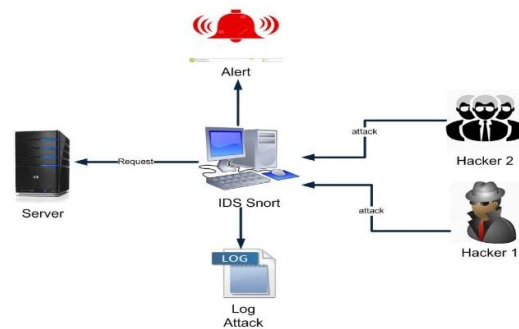
"Weekly" Graph (30 Minute Average)



GAMBAR IV. TRAFFIC PEMAKAIAN  
JARINGAN PER MINGGU

### Arsitektur Ids Snort

Gambar 5 merupakan arsitektur IDS Snort. Snort diletakkan satu switch core dengan Server, sehingga user yang mengakses server akan melewati switch core maka dapat dipantau oleh server IDS Snort. Snort melakukan decode terhadap paket layer aplikasi dan diberika rule untuk mengumpulkan traffic tertentu yang mengandung isi terkait dengan aplikasi yang mengeluarkan paket tersebut. Snort bekerja dengan beberapa bagian yang bertugas melakukan proses tertentu antara lain paket capture block, decoder block, dan preprosesor block. Rule snort di buat terlebih dahulu sehingga ketika terjadi serangan yang sama dengan rule, maka akan muncul alert, dan serangan tersimpan di log database. Log yang tersimpan di database berfungsi sebagai alat bukti pelaporan.

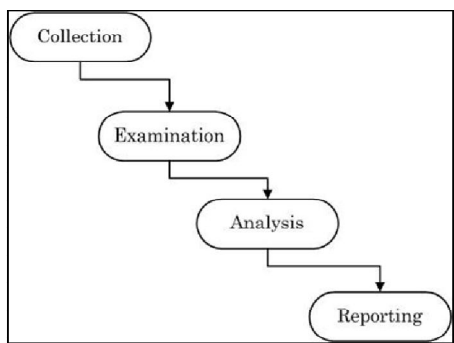


GAMBAR V. ARSITEKTUR IDS SNORT

### Pendekatan Forensik

Pendekatan yang digunakan untuk melakukan analisis serangan yaitu dengan

menggunakan pendekatan Model Proses Forensic (The Forensic Process Model) seperti Gambar 6.



GAMBAR VI. MODEL PROSES FORENSIK [8]

Tahapan-tahapan yang digunakan dalam proses forensik antara lain [8] :

1. *Collecting* : Pada tahap ini meliputi pencarian, mengakui, pengumpulan, dan dokumentasi alat bukti. Pengumpulan barang bukti dengan menggunakan tools IDS Snort karena snort mampu melakukan pendeteksian serangan karena terdapat rule, sehingga jika paket yang melewati jaringan mencurigakan sesuai dengan rule maka mengirimkan alert dan menyimpan pada *log*.
2. *Examination* : Proses pemeriksaan informasi dan mengungkap dokumentasi untuk pembuktian. Pemeriksaan dilakukan dengan menganalisa *file log* yang di tangkap oleh IDS Snort.
3. *Analysis*: Mempelajari hasil dari pemeriksaan dan pembuktian kasus untuk mengidentifikasi :
  - a. Serangan apa yang terjadi ?
  - b. IP siapa yang melakukan serangan?
  - c. Kapan serangan terjadi?
  - d. Dimana serangan itu terjadi?
  - e. Bagaimana serangan tersebut bias terjadi?

f. Mengapa itu terjadi?

4. *Reporting* : Menulis laporan mengenai proses pemeriksaan dan informasi yang di dapat dari seluruh penyelidikan. Laporan ini digunakan untuk bukti dari hasil penyelidikan.

#### **Rule Snort**

*Rule* digunakan sebagai knowledge base dalam proses deteksi. Pada snort ada tiga tipe rule yang digunakan ketika ada paket data yang cocok dengan pola yang ada, antara lain :

1. *Pass*, rule ini akan melakukan drop terhadap paket yang cocok dengan pola deteksi.
2. *Log*, menulis paket secara penuh pada rutin pencatatan *log* yang telah didefinisikan oleh user di awal run time.
3. *Alert*, menghasilkan sebuah even notifikasi menggunakan metode yang telah ditentukan oleh pengguna pada command line, dan kemudian mencatat *log* dari paket secara keseluruhan dengan menggunakan mekanisme *log* proses analisa lebih lanjut.

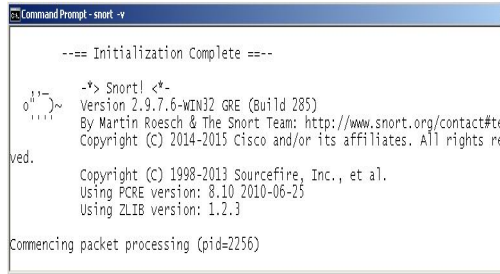
Penulisan rule menggunakan format seperti di bawah ini :

```
[tipe rule] [protokol] [alamat ip  
| any (semua)][nomor port | any  
(semua)] [-> (satu arah) | <> (dua  
arah)] [pola deteksi, penandaan,
```

#### **Implementasi**

IDS Snort adalah perangkat lunak IDS yang berbasis *open source* dan banyak digunakan untuk mengamankan sebuah jaringan dari aktifitas yang berbahaya. Snort dapat digunakan sebagai *alternative* untuk mendeteksi paket yang berorientasi serangan dalam keamanan jaringan. Snort secara kerja mirip dengan tcpdump, tetapi lebih fokus sebagai aplikasi sekuriti packet *sniffing*. Fitur utama snort yang membedakan dengan tcpdump adalah *payload inspection*, dimana memungkinkan snort melakukan analisa payload berdasarkan rule set yang disediakan.

Gambar 7 merupakan implementasi Snort yang digunakan pada penelitian ini yaitu menggunakan versi 2.9.7.6. Sedangkan spesifikasi sistem operasi yang digunakan adalah Windows 7, Win 32.



GAMBAR VII. VERSI SNORT

### 3. HASIL & PEMBAHASAN

#### Rule Snort

Rule yang di set memberikan *knowledge* pada saat proteksi, sehingga proses investigasi sangat bergantung dari *knowledge rule*. Terdapat 5 rule yang digunakan pada penelitian ini yaitu:

1.

```
alert icmp any any -> any
any (msg:"Seseorang sedang melakukan ping of death!"; sid:1000001;)
```

Rule diatas akan membuat Snort melakukan pencatatan untuk semua paket ICMP yang masuk ke jaringan. Ketika ada paket yang di curigai maka akan muncul pesan "Seseorang sedang melakukan ping of death, dengan sid 1000001.

2.

```
alert udp any any -> any
any (msg:"UDP Attack"; sid:1000002;)
```

Rule diatas akan membuat Snort melakukan pencatatan untuk semua paket UDP yang masuk ke jaringan. Ketika ada paket yang di curigai maka akan muncul pesan "UDP Attack", dengan sid 1000002.

3.

```
alert tcp any any -> any
80 (msg:"TCP attack "; sid:1000003;)
```

Rule diatas akan membuat Snort melakukan pencatatan untuk semua paket TCP yang masuk ke jaringan. Ketika ada paket yang di curigai maka akan muncul pesan "TCP Attack", dengan sid 1000003.

4.

```
alert tcp any any ->
192.168.43.74/24 80
(content: "/cgi-bin/phpf"; msg: "PHF probe!"; sid:1000004;)
```

Rule diatas akan melakukan kompleksitas pengecekan dan bisa ditambahkan sesuai dengan opsi port yang disediakan, rule diatas menggunakan port 80, dan sid 1000004.

5.

```
alert tcp any any ->
192.168.43.74/24
6000:6010 (msg: "X Traffic"; sid:1000005)
```

Rule diatas melakukan pengecekan dengan menggunakan batas atas dan batas bawah port, dengan sid 1000005.

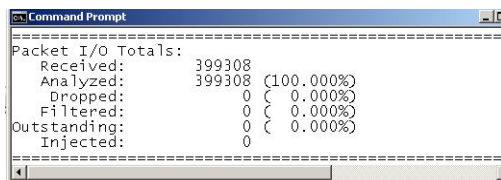


GAMBAR VIII. DETEKSI RULE SNORT  
HASIL RUN SNORT

Fungsi Snort sebagai *sniffer* node, sehingga dengan menjalankan Snort sebagai *sniffer*

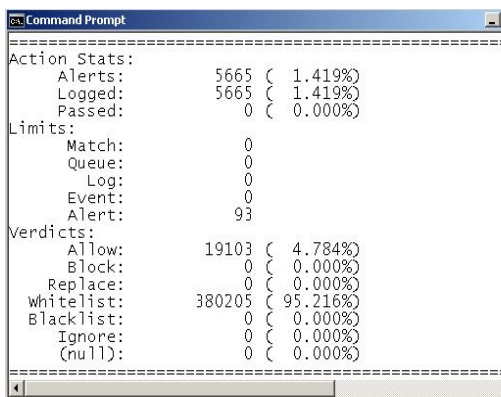


maka pada run akan memonitor secara real time. Untuk menjalankan snort pada *sniffer* node dengan menggunakan perintah `snort -v`, `snort -vd`. Pada penelitian ini menjalankan snort dengan perintah : `snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 2`



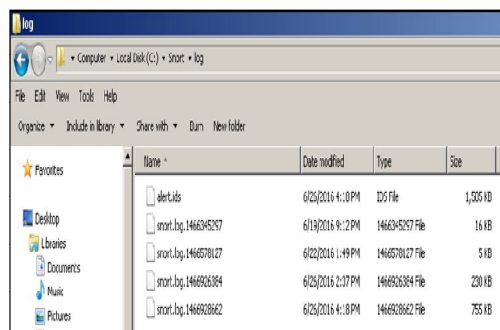
GAMBAR IX. TOTAL I/O PAKET

Gambar 9 merupakan jumlah paket yang diterima oleh IP 192.168.43.74. Paket yang diterima merupakan aktivitas dari IP 192.168.43.74 mengakses berbagai url, sehingga lalu lintas paket tersebut tercapture pada snort. Sedangkan Gambar 10 merupakan *alert* yang terjadi sebanyak 5665 alert. Munculnya alert karena dilakukan dengan melakukan serangan ping of death, yaitu menggunakan perintah `ping -l 100 192.168.43.74 -t`.



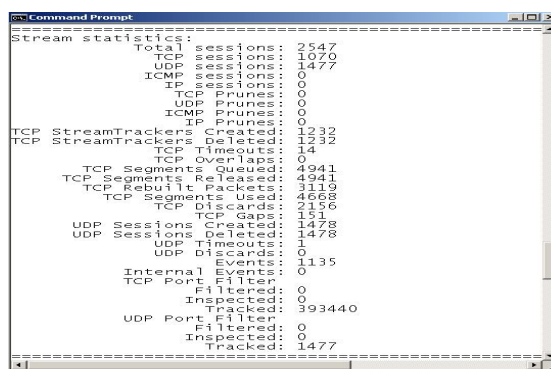
GAMBAR X. ALERT

Karena ping tersebut mencurigakan sesuai dengan *rule* yang sudah di *set*, maka muncul *alert* sebagai tanda bahwa terjadi serangan dan dicatat di *file log*. Hasil pencatatan di *file log* dapat dilihat pada Gambar 11. Dimana terjadi serangan pada tanggal 19, 22, 26 juni 2016. Skenario ini digunakan untuk menguji apakah snort bekerja berdasarkan *rule* yang sudah di *set*. Dan hasilnya adalah Snort mampu mendeteksi serangan berdasarkan *rule knowledge* yang sudah di *set*.



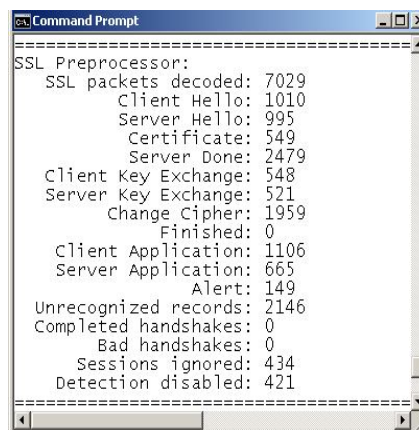
GAMBAR XI. LOG SNORT

Gambar 12 merupakan stream statistik, sehingga setiap aktifitas dari masing-masing protokol yang sudah di definikan pada rule snort yaitu TCP, ICMP, UDP dapat dilihat.



GAMBAR XII. STREAM STATISTIC

Gambar 12 merupakan SSL Preprocessor yang hasil analisa (preprocessor) atau manipulasi terhadap paket sebelum dikirim ke *detection engine*.



GAMBAR XIII. SSL PREPROCESSOR

#### 4. KESIMPULAN & SARAN

Berdasarkan dari hasil instalasi dan konfigurasi snort menunjukkan snort bisa berjalan dengan baik di windows 7. Kejelian dalam konfigurasi mempengaruhi performa dari snort, karena jika terjadi error pada saat konfigurasi akan mempengaruhi sniffer dari snort. Karena snort merupakan tools yang bisa digunakan sebagai sniffer dan kecerdasan snort dalam menanggapi permasalahan keamanan berdasarkan rule snort, maka perlu di definisikan rule yang benar-benar memiliki knowledge dalam mendeteksi jenis serangan. Hasil pengujian dengan menggunakan ping of death menunjukkan bahwa snort mampu mendeteksi serangan tersebut dengan munculnya alert pada saat terjadi serangan. Serangan tersimpan pada file log, sehingga file log tersebut yang digunakan sebagai alat bukti forensic jaringan. Snort yang sudah di konfigurasi serta kecerdasan rule yang sudah dibuat, dapat diimplementasikan pada server UN PGRI Kediri dengan mengganti konfigurasi IP server UN PGRI Kediri guna memantau aktifitas lalu lintas server UN PGRI dari serangan.

Saran-saran untuk penelitian lebih lanjut yaitu (1) Snort yang diinstal berjalan di windows, kedepan bias di uji coba dengan menggunakan system operasi linux, karena di linux sudah menyediakan snort sebagai IDS berbeda dengan windows. (2) Bisa membuat notifikasi secara real time dengan menggunakan API jejaring social, sehingga ketika terjadi serangan, maka akan muncul notifikasi ke mobile phone administrator jaringan.

#### Ucapan Terimakasih

Penulis mengucapkan terima kasih kepada LPPM UN PGRI Kediri dan YPLPT PGRI Kediri karena memberikan dukungan financial terhadap penelitian ini, sehingga penelitian ini dapat terselesaikan dengan baik. Selain itu juga mengucapkan terima kasih kepada PUSKOM UN PGRI dan BSI UN PGRI Kediri karena memberikan fasilitas untuk mendukung penelitian penulis. Besar harapan, penelitian ini dapat memberikan kontribusi keilmuan di bidang jaringan atau keamanan jaringan komputer.

#### DAFTAR PUSTAKA

- [1] Sulianta F. 2008. Komputer Forensik. Jakarta : PT. Elex Media Komputindo.
- [2] Raharjo, B., 2013, Sekilas Mengenai Forensik Digital. Jurnal Sosioteknologi, Edisi 29 Tahun.
- [3] Ariyus, D., 2007, Intrusion Detection System: Sistem Pendeteksi Penyusup pada Jaringan Komputer, Yogyakarta: Penerbit Andi.
- [4] Dewi, E.K., 2016, Rancangan Keamanan Jaringan Dengan Menggunakan Model Proses Forensik, Jurnal Maklumatika, Vol. 2, No. 2, Januari 2016. ISSN 2407-5043
- [5] Misra, R dan Dhir, R., 2012, Cyber Crime Investigation and Network Forensic System Using Honeypot, International Journal of Latest Trends in Engineering and Technology (IJLTET).ISSN : 2278-621X
- [6] Putri R.U dan Istiyanto J.E. 2012. Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. IJCCS , Vol.6, No.2,July 2012, pp. 101-112.
- [7] Mahrouqi A.P, Tobin P, Abdalla S dan Kechadi T., 2014. Simulating SQL- Injection Cyber-attacks using GNS3, IACSIT.
- [8] Baryamureeba,V., Tushabe, F., 2004, The Enhanced Digital Investigation Process Model. Proceedings of the Fourth Digital Forensic ResearchWorkshop, May

Seminar Nasional Inovasi Teknologi  
UN PGRI Kediri, 22 Februari 2017

ISBN : 978-602-61393-0-6  
e-ISSN : 2549-7952

*Halaman ini sengaja dikosongkan*