Research : *Journal of Computer, information system, & technology management* **Online** ISSN: 2615-7357
Vol. 2, **No. 02**. **Oktober 2019, Pages 59-63** **Print** ISSN: 2615-7233

APLIKASI ANALISIS NETWORK FORENSIC UNTUK ANALISIS SERANGAN PADA SYSLOG SERVER

I Wayan Ardiyasa
Institut Teknologi dan Bisnis STIKOM Bali/Sistem Informasi; Jl. Raya Puputan, No.86 Renon Denpasar Bali, (0361) 244445
Jurusan Sistem Informasi, Fakultas Informatika dan Komputer, ITB STIKOM Bali, Bali.
e-mail: **ardi@stikom-bali.ac.id**

***Abstrak*— Perkembangan internet saat ini tidak lepas dari perkembangan teknologi yang semakin canggih sehingga menjadikan akses informasi semakin mudah dan cepat. Informasi yang diakses oleh pengguna disediakan oleh layanan komputer server yang bisa memberikan layanan secara *full time*. Aktivitas pengguna yang mengkases informasi pada suatu server akan dicatat kedalam sebuah file atau disebut dengan *Syslog*. *Syslog* adalah perangkat lunak untuk menghasilkan berkas log yang disebabkan adanya aktivitas dari Inetd dan aktivitas lain. Tujuan dicatatnya aktivitas dari pengguna yang mengakses sistem informasi yang tersimpan pada komputer server adalah untuk mengetahui apabila ada aktivitas yang tidak sesuai atau kejahatan cyber seperti DDoS, *SQL Injection*, Serangan *LFI*, *RFI*. *Network Forensic Process* merupakan suatu metode yang dapat digunakan untuk kegiatan investigasi dan analisa aktivitas *cyber crime*. Dimana bukti ditangkap dari jaringan dan diinterpretasikan berdasarkan pengamatan. Didalam melakukan investigasi terhadap *Syslog file* dilakukan secara manual sehingga memerlukan waktu yang sangat lama dan tidak efisien. Untuk membantu didalam melakukan analisa dan investigasi terhadap *Syslog file* dari kejahatan *cyber*, diperlukan aplikasi yang bisa membantu dalam hal investigasi *Syslog file* untuk mempercepat proses investigasi dan memberikan informasi yang diperlukan dan akurat. Hasil dari penelitian ini adalah aplikasi analisa serangan pada *file Syslog* dengan metode *Network Forensic* Proses. Untuk pengujian pada aplikasi menggunakan metode *Blackbox testing.*

Kata kunci—Network Forensic, Syslog, Cyber crime, Investigasi.

I. PENDAHULUAN

Perkembangan internet saat ini tidak lepas dari perkembangan teknologi yang semakin canggih sehingga menjadikan akses informasi semakin mudah dan cepat. Informasi yang diakses oleh pengguna melalui media internet dengan penyedia layanan dari komputer server yang mampu memberikan layanan secara *real time* dan *full time*. Aktivitas dari pengguna yang mengakses informasi pada suatu server akan dicatat kedalam sebuah layanan atau disebut dengan File *Syslog*. *Syslog* adalah perangkat lunak untuk menghasilkan berkas log yang disebabkan adanya aktivitas dari Inetd dan aktivitas lain [1]. *Syslog* server adalah sebuah server yang menyimpan data *Syslog* berbagai macam perangkat komputer dan jaringan secara terpusat[2]. *Syslog* server harus memiliki ketersediaan tinggi untuk melayani penyimpanan syslog setiap perangkat komputer dan jaringan [3][4]. Tujuan dicatatnya aktivitas dari pengguna yang mengakses informasi yang tersimpan pada komputer server adalah untuk mengetahui apabila ada aktivitas atau kegiatan yang tidak sesuai atau kejahatan *cyber* seperti serangan *DDoS*, *SQL Injection*, Serangan *LFI*, *XSS*. Data syslog tersebut digunakan sebagai barang bukti apabila adanya insiden yang dapat merugikan dari sisi penyedia. Adapun informasi yang dapat dianalisa seperti informasi tentang jenis serangan yaitu informasi *IP Address*, informasi Waktu dan tanggal akses dan informasi url yang diakses serta kegiatan yang dilakukan didalam komputer server.

Untuk mendapatkan informasi serangan pada sebuah komputer server perlu dilakukannya analisis terhadap file *syslog*. Metode yang digunakan didalam melakulan analisis adalah metode *Network forensic process*[5]. *Network Forensic Process* merupakan suatu metode yang dapat digunakan untuk kegiatan investigasi dan analisa aktivitas *cyber crime*. Dimana bukti ditangkap dari jaringan dan diinterpretasikan berdasarkan pengamatan [6][7]. Kebanyakan tim investigasi *digital forensic* didalam melakukan investigasi terhadap *file syslog* dilakukan secara manual dengan memeriksa isi *file syslog* perbaris kode, sehingga memerlukan waktu yang sangat lama untuk menemukan sumber dan informasi serangan dari file *syslog* tersebut. Untuk membantu investigator didalam melakukan analisa dan investigasi terhadap *file syslog* dari kejahatan *cyber*, perlu adanya aplikasi yang bisa membantu dalam kegiatan investigasi terhadap *file syslog* yang bertujuan untuk membantu mempercepat

proses investigasi dan memberikan informasi yang diperlukan secara baik dan akurat.

Penelitian ini menghasilkan aplikasi untuk melakukan analisa serangan *cyber* terhadap suatu komputer sistem pada file *syslog*.

II. LANDASAN TEORI

2.1 Syslog

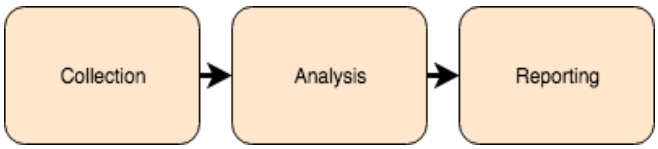
Syslog adalah mekanisme audit gabungan yang digunakan oleh sistem operasi Linux. Ini memungkinkan pengumpulan log lokal dan jarak jauh. Syslog memungkinkan administrator sistem untuk mengumpulkan dan mendistribusikan data audit dengan satu titik manajemen. Syslog dikendalikan berdasarkan per-mesin dengan file /etc/syslog.conf [8]. Syslog adalah perangkat lunak untuk menghasilkan berkas log yang disebabkan adanya aktivitas dari Inetd dan aktivitas lain [1]. Syslog server adalah sebuah server yang menyimpan data syslog berbagai macam perangkat komputer dan jaringan secara terpusat. Syslog server harus memiliki ketersediaan tinggi untuk melayani penyimpanan syslog setiap perangkat komputer dan jaringan [3].

2.2 Network Forensic

Network forensics adalah meng-*capture*, merekam, dan menganalisis kejadian didalam jaringan untuk menemukan sumber serangan keamanan. Menangkap lalu lintas jaringan melalui jaringan itu sederhana secara teori, tetapi dalam praktiknya relatif kompleks. Ini dikarenakan besarnya jumlah data yang mengalir melalui jaringan dan sifat kompleks dari protokol Internet[8] atau Network Forensic Process merupakan suatu metode yang dapat digunakan untuk kegiatan investigasi dan analisa aktivitas cyber crime. Dimana bukti ditangkap dari jaringan dan diinterpretasikan berdasarkan pengamatan[6]

III. METODE

Pada penelitian ini mengadopsi dan menggunakan metode *Network Forensic Process*. *Network Forensic* adalah meng-*capture*, merekam, dan menganalisis kejadian didalam jaringan untuk menemukan sumber serangan keamanan. Menangkap lalu lintas jaringan melalui jaringan itu sederhana secara teori, tetapi dalam praktiknya relatif kompleks. Ini dikarenakan besarnya jumlah data yang mengalir melalui jaringan dan sifat kompleks dari protokol Internet[8] atau Network Forensic Process merupakan suatu metode yang dapat digunakan untuk kegiatan investigasi dan analisa aktivitas cyber crime. Dimana bukti ditangkap dari jaringan dan diinterpretasikan berdasarkan pengamatan[6]. Ada beberapa langkah didalam melakukan investgasi. Metode ini digunakan untuk mendapatkan informasi dan mengambil keputusan[9]. Tahapan pada penelitian ini dapat digambarkan seperti pada Gambar 1.



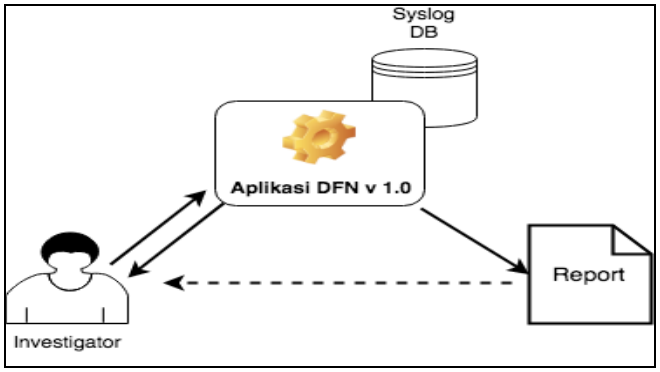
Gambar 1. *Network Forensic Process*

Tahapan Network Forensic *Process* dibagi menjadi tiga proses diantaranya *Collection*, *Analysis* dan *Reporting*. Pada Gambar 1, tahap *network forensic Process* dapat dijelaskan bahwa metode tahap *Network Forensic* dimulai dengan *Collection* atau disebut pengumpulan paket data di jaringan internet[10]. Pada tahap ini pengumpulan data dilakukan secara *online* (data bersifat *volatile*) data yang diambil adalah file *syslog* yang diambil pada *webserver* komputer server dengan file type .log. Tahap berikutnya adalah *Analysis*, pada tahap *analysis investigator* melakukan analisa terhadap file *syslog* untuk mencari informasi serangan *cyber* terhadap komputer server yang tercatat oleh syslog. Jenis serangan yang dianalisa adalah serangan SQL Injection, XSS dan LFI. Tahap akhir adalah *Reporting*. *Reporting* adalah tahap pelaporan dari hasil analisis dari file *syslog* dengan format file .pdf.

IV. HASIL

4.1 Arsitektur Sistem

Aplikasi ini merupakan aplikasi berbasis web dengan arsitektur sistem menggunakan *localhost* untuk menjalankan proses aplikasi ini selain itu, penggunaan *report* dan database digunakan sebagai media untuk menyimpan proses analisa yang dilakukan oleh *investigator* dan modul report untuk menampilkan hasil dari analisa tersebut. Berikut ini merupakan arsitektur sistem pada aplikasi analisa file syslog menggunakan metode *Network forensic* proses pada gambar 2.



Gambar 2. Arsitektur Sistem Aplikasi analisis file *syslog*

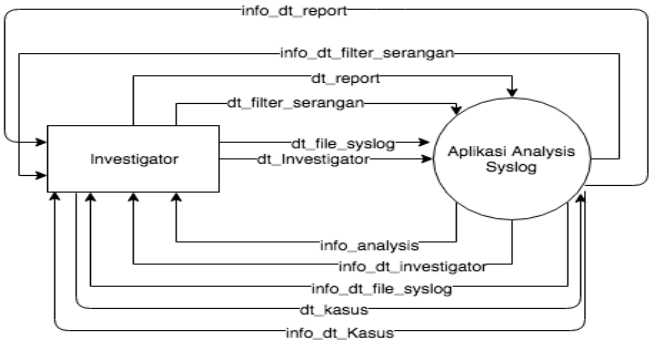
Arsitektur sistem pada gambar 2. Merupakan gambaran umum dari aplikasi analisa file Syslog berbasis web. Pada aplikasi terdapat satu pengguna yaitu pengguna

sebagai investigator. *Investigator* merupakan sebutan untuk ahli dibidang digital *forensic*. Untuk melakukan analisa file *Syslog*, *investigator* mengakses aplikasi dengan membuat dan menginputkan terlebih dahulu nama investigator dan kasus yang terjadi pada file syslog. File syslog diupload dan dilakukan analisis dengan cara mengupload dan membuka file syslog serta ditampilkan pada halaman aplikasi analisis tersebut. Untuk melakukan analisis, *investigator* menggunaka sistem *filtering* dengan cara menginputkan jenis serangan yang terjadi pada file *syslog* tersebut. Jenis serangan tersebut seperti *SQL Injection* (*sqli*), *Cross Site Srcipting* (*XSS*) dan *Local File Inclusion* (*lfi*). Dengan menggunakan sistem filter, *investigator* langsung dapat mengetahui informasi jenis serangan, sumber serangan berupa IP Address, waktu serangan dan titik kelemahan dari sistem tersebut. Setelah melakukan analisis file syslog dan apabila didapatkan informasi serangannya langkah berikutnya adalah dilakukan proses cetak. Proses cetak akan menghasilkan *report* dari informasi *investigator* dan informasi serangannya secara detail dan *report* yang dihasilkan dari aplikasi ini bisa digunakan sebagai barang bukti di pengadilan untuk kasus kejahatan komputer.

4.2 Perancangan Sistem

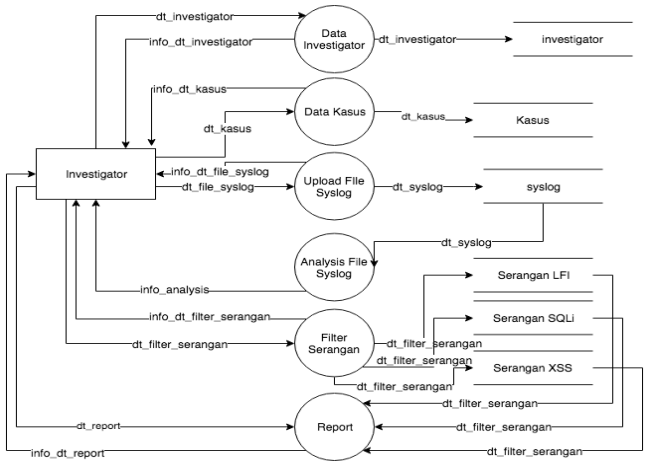
Didalam membangun dan merancang aplikasi analisis *network forensic file syslog* menggunakan Diagram konteks, Data Flow Diagram serta menggunakan konseptual database dan ERD untuk menggambarkan struktur rancangan databasenya. Berikut ini adalah rancangan dan aliran data pada aplikasi *network forensic file syslog* adalah sebagai berikut :

4.2.1 Diagram Konteks



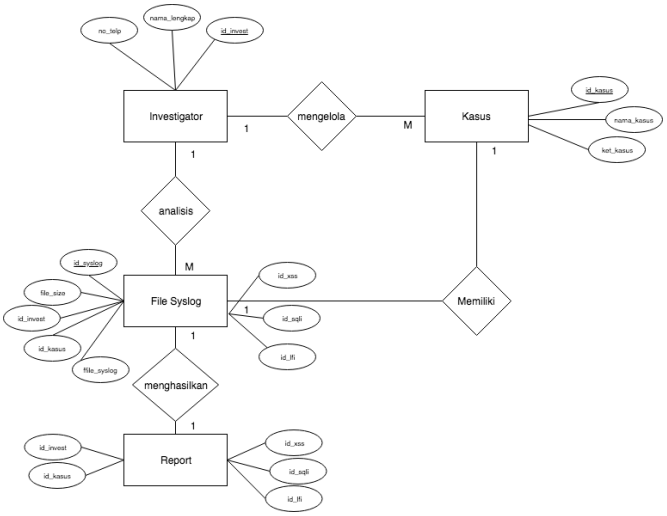
Gambar 3. Diagram Konteks Aplikasi analisis *syslog*

4.2.2 DFD Level 0



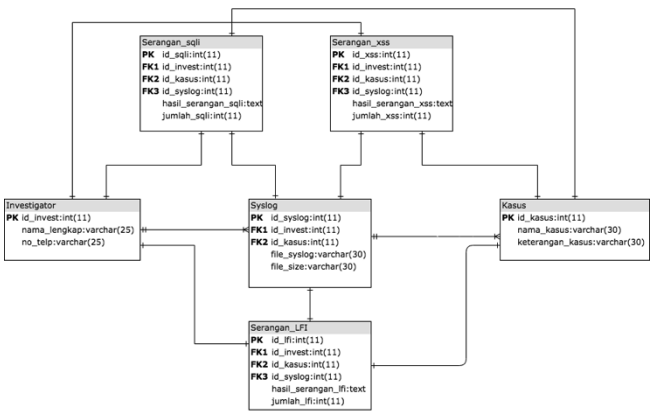
Gambar 4. DFD level 0 Aplikasi analisis file *syslog*

4.2.3 Konseptual Database



Gambar 5. Konseptual Database

4.2.4 ERD

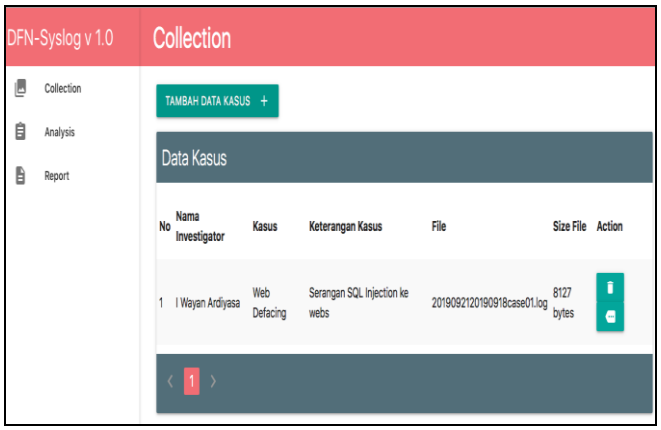


Gambar 6. Entity Relationship Diagram (ERD)

Online ISSN: 2615-7357
Print ISSN: 2615-7233

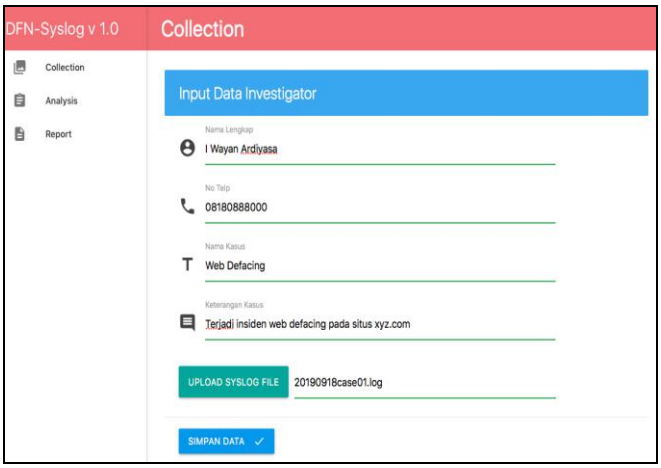
4.3 Implementasi Sistem

4.3.1 Antarmuka aplikasi halaman home



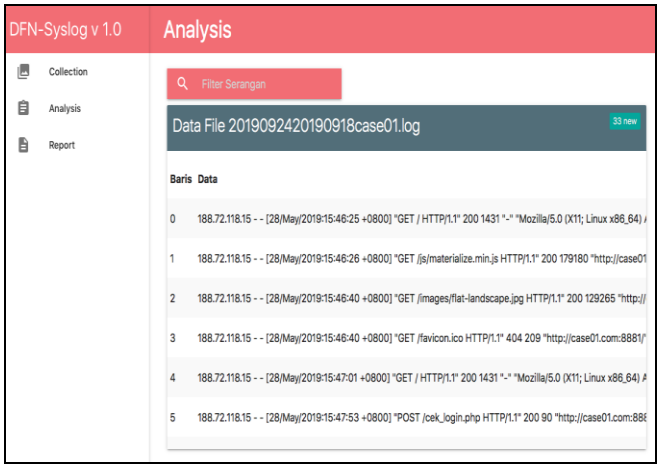
Gambar 7. Halaman *home* aplikasi *analysis file syslog*

4.3.2 Antarmuka aplikasi halaman data kasus dan *input* data *investigator*



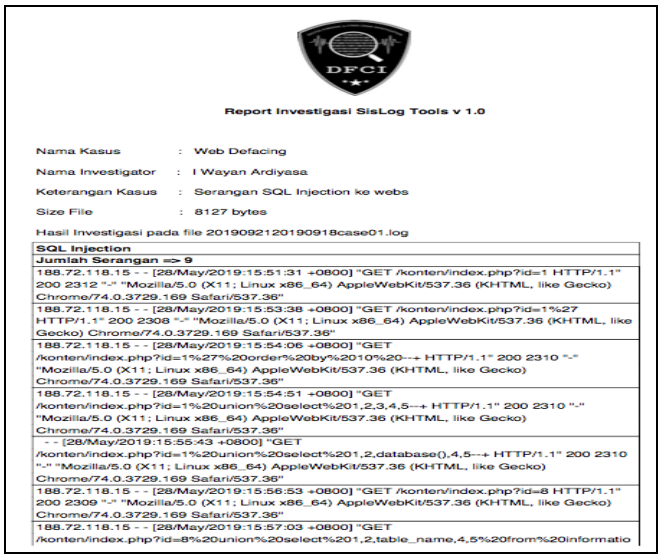
Gambar 8. Halaman *input* data *investigator*

4.3.3 Antarmuka aplikasi halaman *analysis* kasus



Gambar 9. Halaman analysis serangan *cyber*

4.3.4 Antarmuka halaman *report*



Gambar 10. *Report* hasil analisis serangan

4.4 Pengujian

Pengujian dilakukan untuk mengukur kesesuaian rancangan dan implementasi serta untuk mengetahui kesalahan atau *error* yang mungkin terjadi pada aplikasi. Pengujian dilakukan dengan menggunakan metode *blackbox testing*. Metode *blackbox testing* merupakan pengujian yang berfokus terhadap fungsionalitas dari aplikasi analisa *network forensic* file *syslog*. Berikut tabel hasil pengujian metode *blackbox testing* pada aplikasi analisis *network forensic* file *syslog* adalah sebagai berikut :

Tabel 1. Tabel hasil pengujian *blackbox testing* pada aplikasi

No.	Skenario Testing	Hasil yang diharapkan	Hasil Pengujian	Keterangan
1.	Menginputkan semua isian data kasus dan isian data investigator, lalu pilih file *syslog* dan klik button 'simpan'	Sistem menampilkan *messagebox* data sudah disimpan	Sesuai harapan	Valid
2.	Mengosongkan semua isian data pada halaman tambah data kasus dan data *investigator*, lalu kilk button 'simpan'	Sistem menampilkan 'gagal!tipe file tidak sesuai'	Sesuai harapan	Valid
3.	Menghapus data kasus	Sistem menampilkan	Sesuai harapan	Valid

No.	Skenario Testing	Hasil yang diharapkan	Hasil Pengujian	Keterangan
	dengan cara klik *button* '*delete'*	*messagebox* 'Yakin mau dihapus?' klik OK data terhapus		
4.	Melakukan analisa file *syslog*, dengan cara klik *button* analisis file	Sistem menampilkan halaman analisa file *syslog*	Sesuai harapan	Valid
5.	Melakukan *filtering* serangan untuk mengetahui jenis serangan yang ada pada file *syslog*, langkahnya menggunakan *keyword* sqli, lfi, xss pada filter pencarian lalu lanjutkan dengan enter.	Sistem menampilkan infornasi yang dicari oleh *investigator*	Sesuai harapan	Valid
6.	Mencetak hasil analisa kasus dalam bentuk *report*, langkahnya klik *button* '*report'*	Sistem menampilkan *report* dalam bentuk pdf	Sesuai harapan	Valid

4.5 Pembahasan

Hasil pada tahap implementasi dan pengujian yang dilakukan sudah sesuai dengan yang diharapkan. Aplikasi analisis *network forensic* untuk melakukan analisa serangan *cyber* pada file *syslog* bertujuan untuk membantu khususnya *investigator digital forensic* didalam mencari informasi serangan *cyber* pada file *syslog*. Aplikasi ini dibuat berbasis web untuk bisa diakses oleh pengguna lainnya apabila ingin melakukan analisa awal terhadap kasus kejahatan *cyber*. File syslog didapakan dari teknik *collection* secara *online*, setelah didapatkan file *syslog.log* dilakukan tahap analisa dengan melakukan input data *investigator* dan file syslog.log yang akan dianalisa. Pada tahap analisa, *investigator* bisa melakukan analisa serangan dengan menggunakan sistem *filtering* untuk mencari informasi serangan pada file *syslog.log* parameter jenis serangan yang bisa dicari adalah SQLinjection, XSS dan LFI. Apabila ditemukan adanya serangan maka *investigator* bisa melakukan proses *reporting* atau pelaporan dari hasil investigasi untuk dukumentasi dan hasil pelaporan ini bisa digunakan oleh *investigator* untuk proses hukum apabila diperlukan.

V. KESIMPULAN

Adapun kesimpulan dari penelitian ini adalah :

1. Telah dihasilkannya aplikasi analisis file *syslog* untuk melakukan analisa serangan kedalam komputer server berbasis web.
2. Perancangan aplikasi analisis file *syslog* menggunakan *Data Flow Diagram*, konseptual database dan *entity relationship diagram*.
3. Pada tahap pengujian aplikasi menggunakan metode *blackbox testing* untuk mengetahui kesesuaian fungsionalitas aplikasi. Hasil dari pengujian ini sudah sesuai harapan dan valid.

DAFTAR PUSTAKA

[1] I. Mahardika, "Secure remote login pada sistem operasi slackware linux," hal. 1–7, 2003.

[2] L. B. Becker, M. Gergeleit, S. Schemmer, dan E. Nett, "Using a flexible real-time scheduling strategy in a distributed embedded application," in *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, 2003, vol. 2, no. January, hal. 652–657.

[3] T. H. Ditanaya, R. M. Ijtihadie, dan M. Husni, "Rancang Bangun Sistem Log Server Berbasis Syslog dan Cassandra untuk Monitoring Pengelolaan Jaringan di ITS," *J. Tek. ITS*, vol. 5, 2016.

[4] E. K. Dewi, "ANALISIS LOG SNORT MENGGUNAKAN NETWORK FORENSIC," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 2, no. 2, Des 2017.

[5] M. N. A. Khan, "Multi-agent Based Forensic Analysis Framework for Infrastructures Involving Storage Networks," *Proc. Natl. Acad. Sci. India Sect. A - Phys. Sci.*, vol. 89, no. 2, hal. 291–309, Jun 2019.

[6] A. Ginanjar, N. Widiyasono, dan R. Gunawan, "Analisis Serangan Web Phishing pada Layanan E-commerce dengan Metode Network Forensic Process," *JUTEI Ed. Vol. No.2 Oktober 2018*, no. 2, hal. 147–157, 2018.

[7] A. Al-murjan, "Network Forensic Investigation of Internal Misuse / Crime in Saudi Arabia : A Hacking Case," *Annu. ADFSL Conf. Digit. Forensics, Secur. Law*, no. Gollmann 2006, hal. 15–32, Okt 2008.

[8] EC-Council, *Investigating Network Intrusions and Cybercrime*. 2010.

[9] A. Lubis, A. Putera, dan U. Siahaan, "NetworkForensic Application in General Cases," *IOSR J. Comput. Eng.*, vol. 18, no. December, hal. 41–44, 2016.

[10] I. Riadi dan N. Hildayanti, "Forensics Analysis of Router On Computer Networks Using Live Forensics Method," *Int. J. Cyber-Security Digit. Forensica 8(1) 74-81*, no. May, 2019.