Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 6, No. 9, September 2022, hlm. 4562-4570 http://j-ptiik.ub.ac.id

Penerapan Platform Visualisasi dan Analisis Trafik Jaringan menggunakan *Elastic Stack*

Shafira Aulia Indrarto[1], Achmad Basuki[2]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]firaulia@student.ub.ac.id, [2]abazh@ub.ac.id

Abstrak

Sistem monitoring merupakan sebuah sistem yang bertujuan untuk memantau aktivitas-aktivitas pada perangkat jaringan. Monitoring diperlukan guna memantau permasalahan apa saja yang berpotensi mengganggu jaringan internet. Salah satu metode yang dapat digunakan untuk melakukan monitoring jaringan adalah dengan memanfaatkan *platform Elastic Stack*. Pada tugas akhir ini, *Elastic Stack* akan diterapkan untuk memonitoring trafik jaringan dengan cara memberikan visualisasi dari data trafik jaringan yang ada kemudia selanjutnya dilakukan analisis dari data trafik tersebut. Komponen utama penyusun sistem ini adalah sebuah server yang di dalamnya sudah dikonfigurasi oleh komponen *Elastic Stack* yaitu *Packetbeat, Elasticsearch* dan *Kibana*. Proses yang dilakukan untuk melakukan visualisasi dan analisis trafik jaringan adalah dimulai dengan pengambilan data, pengiriman data, pemrosesan data dan visualisasi data pada *dashboard*. Pada proses pengambilan data, data yang dipakai merupakan data sampel yang berasal dari trafik jaringan di Universitas Brawijaya yang didapat menggunakan TCPdump. Selanjutnya, data sampel tersebut akan dikirim ke Elasticsearch oleh *Packetbeat* untuk disimpan di dalam *database* dan dilakukan proses pengindeksan. Data yang sudah diindeks selanjutnya akan dikelompokkan menjadi *field-field* tertentu untuk mengindikasi informasi apa saja yang terdapat pada data sampel tersebut. Pada *field-field* tersebut selanjutnya akan ditampilkan visualisasi dalam bentuk *pie, chart* maupun grafik pada *Dashboard Kibana.*

Kata kunci: sistem monitoring, *Elastic Stack*, visualisasi

Abstract

Monitoring system is a system that aims to monitor activities on network devices. Monitoring is needed to monitor any problems that have the potential indication to disrupt the internet network. A method that can be used to monitor the network is to use the Elastic Stack. In this final project, Elastic Stack will be applied to monitor network traffic by providing a visualization of the existing network traffic data and then analyzing the traffic data. The main component of this system is a server in which the Elastic Stack components have been configured, there are Packetbeat, Elasticsearch and Kibana. The process for visualizing and analyzing network traffic begins with data collection, data transmission, data processing and data visualization on the dashboard. In the data collection process, the data used is sample data from network traffic at Brawijaya University which is obtained using TCPdump. Next, the sample data will be sent to Elasticsearch by Packetbeat to be stored in the database and indexed. The indexed data will be grouped then into certain fields to indicate what information is contained in the sample data. In these fields, visualizations in the form of pies, charts and graphs will be displayed on the Kibana Dashboard based on data stored.

Keywords*: monitoring system, Elastic Stack, vizualizing*

1. PENDAHULUAN

Jaringan dan perangkat teknologi informasi semakin berkembang di kehidupan sehari-hari. Penggunaan internet di Indonesia sendiri merupakan salah satu negara dengan populasi penggunaan internet terbesar di dunia. Tercatat pada tahun 2022 mencapai 204,7 juta pengguna internet di Indonesia terhitung sejak bulan Januari lalu (Annur, 2022). Adanya pertambahan jumlah pengguna yang terkoneksi ke internet berdampak pada meningkatnya trafik jaringan

sehingga kinerjanya akan mengalami penurunan (Fathoni, Sandra, 2016).

Trafik jaringan adalah pergerakan jumlah data yang melintasi jaringan komputer pada waktu tertentu (Fortinet, 2022). Peningkatan trafik jaringan memengaruhi kualitas jaringan karena dapat menyebabkan terjadinya beberapa permasalahan seperti kecepatan jaringan (*throughput*), *delay*, *packet loss*, serta meningkatnya nilai *jitter*. Adanya peningkatan trafik jaringan yang terjadi maka diperlukan sebuah perangkat monitoring jaringan. Monitoring jaringan diperlukan guna memaksimalkan seluruh sumber daya yang ada pada jaringan komputer, mendeteksi kesalahan pada jaringan maupun *user* ataupun *client* serta mengawasi jaringan komputer dengan *host* dalam jumlah besar. Perangkat monitoring jaringan yang dapat digunakan yaitu dengan protokol berbasis SNMP menggunakan Cacti atau MUNIN (B & Rifqi, 2019).

Cacti merupakan sebuah platform monitoring jaringan untuk mendeteksi kinerja CPU dan *bandwidth* serta menampilkannya dalam bentuk data grafik. Perangkat khusus yang biasa digunakan yaitu *router* dan *switch*. Sedangkan MUNIN merupakan perangkat monitoring sumber daya jaringan dengan sistem *plug and play* yang hanya menampilkan data dalam bentuk metrik. Biasanya grafik kinerja yang ditampilkan meliputi *memory,* penggunaan CPU, serta sumber daya aplikasi *server*. Namun dalam penerapannya, baik Cacti maupun MUNIN sama-sama belum dapat menampilkan hasil visualisasi trafik jaringan yang lebih interaktif. Perlunya penambahan baris kode untuk memantau sumber daya jaringan pada MUNIN serta masih belum adanya perintah visualisasi pada Cacti juga menjadi kekurangan pada aplikasi monitoring jaringan tersebut.

Beberapa penelitian yang sudah dilakukan mengusulkan platform monitoring jaringan yang juga bisa menampilkan visualisasi dari trafik jaringan. Salah satu metode yang digunakan yaitu penerapan *Elastic Stack* sebagai *tools* alternatif pemantauan jaringan (Admi & Maulana, 2020). Penggunaan *Elastic Stack* bertujuan untuk memonitoring trafik, *host* serta menganalisis log yang bersifat *open source*. Monitoring trafik yang ditampilkan merupakan data yang berasal dari pengolahan *log* yang selanjutnya divisualisasikan untuk dilakukan analisis sesuai kebutuhan yang diperlukan.

Elastic Stack merupakan sekumpulan produk *open source* yang berasal dari *Elastic* yang didesain untuk membantu pengguna dalam pengambilan data dari berbagai sumber data dan format serta digunakan untuk mencari, menganalisis serts memvisualisasikan data dengan didukung berbagai layanan platform seperti *Amazon Web Service* (AWS), *Google Cloud Platform* dan *Microsoft Azure* (Yasar, 2022). *Elasticsearch* merupakan komponen utama dari *Elastic Stack* yaitu komponen yang berfungsi sebagai penyerapan data, penyimpanan serta analisis dan visualisasi (Elasticsearch, 2022). *Elasticsearch* juga merupakan mesin pencari distribusi yang bersifat *open source* untuk semua jenis data termasuk numerik, geospasial, terstruktur dan tidak terstruktur. *Packetbeat* adalah penganalisa paket jaringan yang dapat digunakan dengan *Elasticsearch* untuk menyediakan pemantauan aplikasi dan sistem analis (Elasticsearch, 2022). Sedangkan *Kibana* adalah komponen *Elastic Stack* yang berfungsi sebagai mesin visualisasi serta menganalisis data dari bagan, peta, grafik yang ditampilkan pada *dashboard* (Elasticsearch, 2022).

2. LANDASAN KEPUSTAKAAN

Penelitian pertama berjudul "*Pemanfaatan Elasticsearch untuk Temu kembali info Tugas Akhir*" (Atmaja, Ardian Prima, et al., 2018). Paper tersebut menjelaskan bahwa data-data digital yang terkumpul pada sentra data dapat dimanfaatkan kembali sehingga dapat bermanfaat bagi siapa saja yang membutuhkan. Salah satu data yang dimanfaatkan merupakan pencarian informasi tugas akhir mahasiswa dari tahun ke tahun. Hal ini membuka peluang untuk dilakukan *big data analytic* pada perguruan tinggi. Makalah ini dibangun sebuah sentra data tugas akhir yang dapat dilakukan pencarian kembali (*information retrieval*) oleh pengguna. Sistem temu kembali informasi atau mesin pencari dokumen tugas akhir ini dikembangkan menggunakan *Elasticsearch* serta *framework PHP Laravel*. Sistem ini pula akan diintegrasikan menggunakan Single Sign On (SSO) dan Student Portal yang ada sehingga untuk mengakses informasi seperti makalah publikasi ilmiah hanya memakai otentifikasi satu akun yang dimiliki civitas akademika saja.

Penelitian kedua berjudul "*Sistem manajemen dan Visualisasi Syslog Perangkat Jaringan komputer pada ICT Universitas*

Diponegoro Berbasi ELK Stack" (Fauzi, Adnan, 2020). Paper tersebut menyebutkan bahwa jaringan komputer merupakan himpunan interkoneksi antara 2 komputer *autonomous* atau lebih yang terhubung menggunakan transmisi kabel atau tanpa kabel. Administrator jaringan bertanggung jawab atas mendesain, mengonfigurasi perangkat jaringan dan menjaga stabilitas trafik. Perangkat jaringan, selaku objek yang dikelola administrator tidak jarang mengalami hambatan atau problem. Masing-masing persoalan mempunyai penyebab yang beragam, bisa dikarenakan kesalahan administrator, tidak adanya dokumentasi atau pendayagunaan perangkat oleh pihak yang tidak berwenang. Masing-masing persoalan menjadi sebuah *event* dari perangkat jaringan yang semua event tersebut terekam pada *system log* (*syslog*). Berdasarkan permasalahan tersebut, penulis bermaksud mengimplementasikan sistem manajemen dan visualisasi syslog perangkat jaringan berbasis *ELK Stack*. Pengimplementasian tersebut guna memudahkan administrator jaringan untuk menganalisa serta mengambil tindakan dari persoalan pada perangkat jaringan yang dikelola.

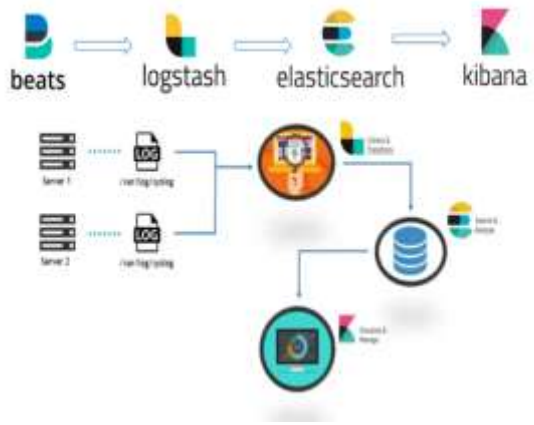
Penelitian ketiga berjudul "*Penerapan Elastic Stack sebagai Tools alternatif Pemantauan Traffic Jaringan dan Host pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia*" (Admi, Adrian. 2020). Paper ini menjelaskan tentang meningkatnya pemanfaatan teknologi informasi dan komunikasi untuk pengelolaan informasi berbanding lurus dengan meningkatnya kebutuhan keamanan terhadap *database*, sistem serta aplikasinya. Selain kebutuhan keamanan yang semakin tinggi, kecenderungan resiko seperti aktivitas *malware data leakage and manipulation, web hacking incident, denial of service* (DOS) yang semakin tinggi juga sebagai konsekuensi dari kemudahan akses informasi. Untuk memecahkan persoalan tersebut maka pemerintah wajib menciptakan pola koordinasi antara pemerintah pusat dan wilayah. Dalam melakukan aktivitas tersebut, perlu adanya pemantauan atau monitoring infrastruktur jaringan menggunakan sebuah *tools* untuk membantu menemukan ancaman pada *traffic* jaringan serta *host*. Pada hal ini, penulis merekomendasikan alternative tools yaitu *Surricata*, *OSSEC* serta *Elastic Stack* untuk memonitoring lalu lintas jaringan dan *host* serta analisis *log* yang praktis untuk diimplementasikan.

2.1 Monitoring Jaringan

Monitoring jaringan adalah proses penting untuk memantau kinerja dan permasalahan pada komponen jaringan seperti *router*, *switch*, *firewall*, *server* dan *VM* untuk selanjutnya dievaluasi secara terus-menerus untuk mengoptimalkan dan mempertahankan kinerjanya (Zoho Corp, 2022). Beberapa aspek penting dalam monitoring jaringan antara lain memantau hal-hal penting dalam jaringan, mengoptimalkan interval pemantauan, serta melihat protokol yang tepat. Pada monitoring jaringan juga diperlukan bantuan perangkat lunak monitoring jaringan beserta perangkat yang mendukung. Berdasarkan permasalahan yang ada, pemilihan sistem monitoing jaringan yang efektif juga diperlukan guna mengatasi permasalahan jaringan yang berdampak pada kinerja komponen-komponen yang ada.

2.2 Elastic Stack

Elastic Stack merupakan salah satu solusi log *management* yang berbasis *open-source* yang dapat mencatat sebuah log dari seluruh perangkat yang ada. Komponen-komponen dalam *Elastic Stack* bertujuan untuk memonitor serta mengamankan infrastruktur IT (Infrastructure, 2020).



Gambar 1 Elastic Stack

(Sumber: https://i-3.co.id/monitor-infrastruktur-it-anda-secara-real-time-dengan-elk-stack)

Gambar 1 menunjukan komponen dari *Elastic Stack* yaitu:

1. *Beats* : *Beats* merupakan platform *open-source* sebagai pengirim data *single purpose*. Data yang dikirm dari *beats* ke logstash dapat berupa sebuah sistem yang berjumlah ratusan maupun ribuan (Elasticsearch, 2022).
2. *Logstash* : *Logstash* merupakan platform pemrosesan data pada sisi server dan bersifat *open-source* yang dapat menyerap data dari beberapa sumber lalu mengubahnya dan mengirimkan data tersebut ke dalam *Elasticsearch* (Service, 2022)
3. *Elasticsearch* : *Elasticsearch* merupakan mesin pencarian dan analitik RESTful yang bersifat *open-source* serta menyediakan kemampuan untuk melakukan pencarian dokumen secara cepat dan *realtime* (Elasticsearch, 2022).
4. *Kibana* : *Kibana* merupakan *platform* yang berguna untuk visualisasi data dengan cara mengakses terlebih dahulu dengan REST API dan dibantu dengan kemampuan *searching* dari *Elasticsearch*. Umumnya data yang diakses berupa data (.json) (Elasticsearch, 2022).

Keempat komponen *Elastic Stack* dari gambar 2.1 yang terdiri dari *Beats, Logstash, Elasticsearch,* dan *Kibana* merupakan komponen yang saling bekerjasama untuk memonitor dan mengamankan infrastruktur IT. Seluruh data *input* yang ada pada infrastruktur dikumpulkan oleh *Beats* untuk selanjutnya dikirim ke *Logstash.* Setelah itu, data *input* yang sudah diproses selanjutnya akan diindeks ke *Elasticsearch* agar dapat disimpat disebuah *database*. Kemudian, data yang disimpan tersebut dapat divisualisasikan melalui *Kibana*.

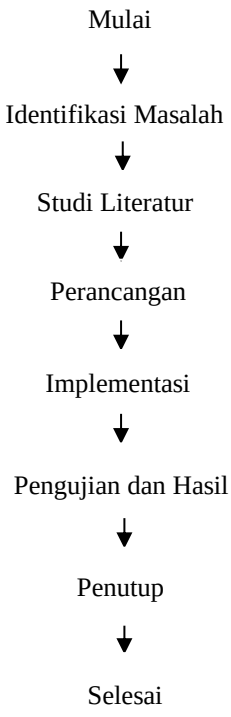
2.3 Packetbeat

Packetbeat adalah pengirim dan penganalisis data yang bersifat *open-source* serta mendukung *Elastic Common Schema* (ECS), yaitu paket jaringan yang terintegrasi dengan *Elastic Stack* (*Elasticsearch*, Logstash, dan Kibana). Sebagai bagian dari pengirim log *Elastic* (Filebeat, Topbeat, Libbeat, Winlogbeat), *packetbeat* menyediakan metrik monitoring secara *real time* berbasis web, *database*, dan protokol jaringan lainnya dengan memonitoring packet secara langsung yang disambungkan melalui kabel. *Packetbeat* juga mrupakan komponen yg mendukung beberapa protokol, mulai dari database hingga penyimpanan key value yang selanjutnya di *stores* ke HTTP dan protokol tingkat rendah (Elasticsearch, 2022).

Monitoring paket data menggunakan *Elastic Stack* membantu mendeteksi lalu lintas paket jaringan dan karakteristik paket yang tidak biasa, mengidentifikasi sumber packet dan tujuannya, mencari paket data string tertentu dan membuat dashboard yang mudah dipahami dengan statistic yang luas. Monitoring paket dapat mengimbangi tingkat keamanan dan membantu meningkatkan waktu respon terhadap berbagai serangan.

3. METODE PENELITIAN

Adapun tahapan-tahapan dalam membangun penelitian ini dapat disimpulkan pada diagram alur metodologi penelitian seperti pada Gambar 2.



Gambar 2 Diagram alur penelitian

Identifikasi Masalah merupakan permasalahan yang diangkat dalam tugas akhir ini yaitu untuk melihat aktivitas dari trafik jaringan yang sudag divisualisasi serta diterapkan menggunakan *Elastic Stack.* Penggunaan *Elastic Stack* bertujuan untuk memonitoring sebuah paket jaringan yang masuk serta dilakukan analisis. Pada tugas akhir

ini akan dilakukan penerapan sistem trafik jaringan dalam bentuk visualisasi serta akan dilakukan analisis guna melihat aktivitas apa saja yang ada pada trafik jaringan.

Studi literature yaitu untuk melakukan pencarian literature/referensi terkait judul yang sedang dikerjakan. Referensi tersebut digunakan untuk membantu dalam proses pengerjaan skripsi serta mempermudah dalam melakukan implementasi sistem. Literatur yang digunakan berasal dari buku, jurnal, maupun bacaan yang berkaitan dengan topik yang sedang dikerjakan *Packetbeat, Elasticsearch, Kibana* dan sebagainya.

Pada perancangan yang dilakukan pada penelitian ini dimulai dengan melakukan perancangan perancangan lingkungan lalu perancangan sistem. Implementasi dilakukan berdasarkan perancangan yang telah dibuat sebelumnya. Tahapan dalam melakuakn impelementasi ini antara lain gambaran umum sistem, implementasi pengiriman data, implementasi pengolahan data, serta implementasi visualisasi data. Pada bagian gambaran umum sistem akan dijelaskan mengenai lingkungan apa saja yang dibutuhkan maupun digunakan untuk menjalankan sistem. Hasil dari implementasi sistem ini juga akan digunakan sebagai bahan evaluasi pada sistem.

Setelah sistem diimplementasi, tahapan berikutnya adalah melakukan pengujian terhadap sistem tersebut. Tujuan dilakukan pengujian adalah untuk mengetahui apakah seluruh kebutuhan perangkat keras maupun lunak yang dibutuhkan dan digunakan sudah terpenuhi serta untuk mengetahui seberapa baik kinerja dari sistem tersebut. Pada tahap visualisasi, data yang dihasilkan akan dianalisis untuk mengetahui informasi apa saja yang terdapat dalam data trafik jaringan (data sampel) tersebut serta apakah metode yang digunakan berjalan sesuai dengan tujuan tugas akhir. Parameter yang digunakan untuk mengetahui informasi dalam data trafik jaringan antara lain isi (*field)* yang ditampilkan (*client* IP, *destination* IP, *network transportation, network type, network protocol, server domain* dan *server* IP).

4. IMPLEMENTASI

4.1 Implementasi Lingkungan

Pada subbab ini akan menjelaskan mengenai kebutuhan perangkat keras dan perangkat lunak yang akan digunakna sebagai penunjang implementasi sistem yang akan dibangun.

Tabel 1 Spesifikasi Perangkat Keras

Spesifikasi	Keterangan
Processor	Intel Core i5-8250U 1.60 GHz
Memory	12288 MB
Harddisk	HDD 1000 GB

Tabel 2 Spesifikasi Perangkat Lunak

Perangkat Lunak	Deskripsi
Sistem Operasi Ubuntu Linux 20.04 LTS	Merupakan sistem operasi yang digunakan untuk menjalankan seluruh kebutuhan perangkat lunak yang dibutuhkan dalam tugas akhir
Packetbeat	Merupakan komponen yang digunakan untuk mengirim data (.pcap)
Elasticsearch	Merupakan komponen yang digunakan untuk mengolah data (.pcap) untuk dilakukan pengindeksan (pengolahan data)
Kibana	Merupakan komponen yang digunakan untuk memvisualisasikan data

4.2 Pengambilan Data

Penerapan dalam tugas akhir ini menggunakan sebuah data sampel yang berasal dari trafik jaringan di Universitas Brawijaya yang didapat menggunakan TCPdump. Data yang digunakan merupakan data sampel yang di*capture* pada tanggal 27 Juni 2022 dengan rentang waktu 60 menit yang dimulai dari pukul 13:42 WIB. Data yang diambil merupakan data (.pcap) dengan ukuran *file* 36,05Gb. Informasi dari data sampel tersebut antara lain *time* (waktu saat paket tertangkap), *source* (sumber alamat IP dari paket yang ditangkap), *destination* (tujuan alamat IP dari paket yang ditangkap), *protocol* (tipe protokol yang dipakai dari paket yang ditangkap), *info* (informasi detail dari paket yang ditangkap),

source port (field pada TCP header yang mengidentifikasi program aplikasi pada komputer pengirim), *destination port* (nomor yang berkaitan dengan tujuan aplikasi yang terletak pada remote host).

4.3 Pengiriman Data

Setelah mendapatkan data sampel, maka tahap selanjutnya adalah melakukan proses pengiriman data. Pada proses pengiriman data, komponen yang digunakan adalah *Packetbeat*. *Packetbeat* diinstal dan dikonfigurasi di sisi server, yaitu di dalam Ubuntu *Linux 20.04* LTS. Penggunaan *Packetbeat* dibutuhkan karena komponen tersebut mengirimkan paket berupa *network* trafik yang sesuai dengan sistem yang sedang dikerjakan. Sebelum melakukan pengiriman data, maka dilakukan konfigurasi terlebih dahulu pada editor *Packetbeat* dengan menggunakan perintah *sudo nano /etc/packetbeat/packetbeat.yml* .

4.5 Pengolahan Data

Data sampel yang sudah dikirim oleh *Packetbeat* selanjutnya akan diolah *Elasticsearch*. Koomponen ini juga diinstal dan dikonfigurasi pada server Ubuntu *Linux* 20.04 LTS. Pada tahap ini, data yang sudah dikirim akan disimpan di dalam *database* yang berbasis NoSQL *database.* Selain sebagai media penyimpanan, *Elasticsearch* juga berfungsi sebagai mesin pencari serta media analisis data yang berbasis *Apache Lucene*. Selama menerima data dari *Packetbeat*, *Elasticsearch* akan mengatur untuk membuat indeks baru pada saat terjadi pengiriman. Setiap data yang diindeks, selanjutnya akan dikelompokkan ke dalam masing-masing *field* secara otomatis dalam bentuk format JSON *document*.

4.4 Visualisasi Data

Pada tahap ini data sampel (.pcap) yang sudah diolah dan disimpan oleh *Elasticsearch* kemudian divisualisasikan menggunakan *Kibana*. Komponen *Kibana* yang sudah diinstal dan dikonfigurasi pada server Ubuntu *Linux* 20.04 LTS ini menyediakan fitur yang kuat dan mudah digunakan seperti histogram, grafik garis, diagram lingkaran dan lain sebagainya. Pengaksesan pada *Kibana* dapat dibuka pada *web browser* dengan *url* "*https://192.168.1.70/5601*".

Pada gambar 3, terlihat pada menu *Discover* bahwa data sampel sudah muncul. Selanjutnya juga terlihat pada *field* yaitu beberapa informasi yang tertera pada data sampel yang selanjutnya menjadi isi pembuatan *dashboard*. Data yang terlihat pada *field* antara lain *timestamp, agent.ephemeral_id, agent.hostname, agent.id, agent.name, agent.type, agent.version, bytes_in, bytes_out, client_bytes, client_ip, client_port, destination_bytes, destination_domain, dan destination_ip.*

5. PENGUJIAN

5.1 Pengujian Sistem

Gambar 5 Hasil Visualisasi Data

Gambar 3 Discover Kibana

Tahapan pertama yang dilakukan setelah melakukan semua konfigurasi sistem *Packetbeat, Elasticsearch* dan *Kibana* ke dalam Linux *Ubuntu* 20.04 LTS yaitu pengambilan data dengan menggunakan data sampel. Data sampel yang dipakai berasal dari trafik jaringan di Universitas Brawijaya yang didapat menggunakan TCPdump. Data sampel tersebut merupakan data (.pcap).

Setelah dilakukan proses pengumpulan data, maka langkah selanjutnya yaitu pengiriman data. Data sampel (.pcap) yang sudah ada selanjutnya akan dilakukan pengiriman data oleh *Packetbeat*. Pengiriman data oleh *Packetbeat* menggunakan perintah " *sudo packetbeat –I " capturedUB.pcap" ".* Selanjutnya, tahap yang akan dilakukan adalah proses pengolahan data. Pada proses pengolahan data, komponen yang bertugas yaitu *Elasticsearch*. Di dalam *Elasticsearch*, data yang dikirim dari *Packetbeat* akan secara otomatis dilakukan penyimpanan ke dalam *database* berbasis NoSQL. Data yang disimpan di dalam *database* tersebut oleh *Elasticsearch* juga akan dilakukan pengindeksan berdasarkan informasi data yang dikirim guna memudahkan pencarian

Tahap selanjutnya yaitu proses visualisasi data. Proses visualisasi data pada sistem dilakukan oleh *Kibana*. Input yang digunakan untuk melakukan visualisasi adalah data yang sudanh melalui proses pengolahan oleh *Elasticsearch*

Pada gambar 5, terlihat bahwa data sampel (.pcap) sudah melalui proses visualisasi data oleh *Kibana* serta berhasil ditampilkan dalam bentuk *Dashboard*. Beberapa informasi yang ditampilkan di dalam *Dashboard* antara lain *client IP, destination IP, network transport, network protocol, network type, client and destination bytes, destination and server domain.*

5.2 Analisis Pengujian

Gambar 6 Timestamp Dashboard Kibana

Setelah dilakukan pengujian, sistem yang dibangun dapat mencapai tujuan yang diinginkan yaitu penerapan platform visualisasi dan analisis trafik menggunakan Elastic Stack.

Gambar 4 Tahapan pengujian

Dalam visualisasi yang ditampilkan oleh *Kibana*, terlihat bahwa waktu yang tertera pada *Dashboard Kibana* merupakan format waktu sesuai dengan tanggal dan jam proses tersebut dilakukan seperti pada gambar 6.

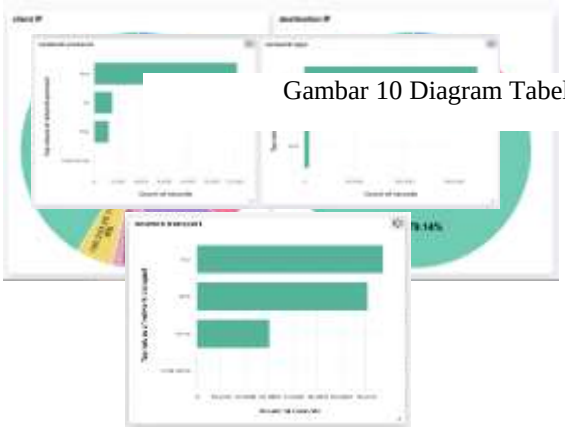
Client IP dan *destination IP* digambarkan dengan diagram donut seperti gambar 7. Presentase yang terlihat disusun berdasarkan

presentase data terbanyak hingga data terkecil. Pada *client IP*, berdasarkan rentang waktu yang tertera pada *timestamp*, IP 175.45.184.73 mendapatkan presentase terbanyak kedua yaitu

Gambar 7 Diagram Donut

sebesar 18.06%. Sedangkan pada *destination IP*, presentase 11.5% dimiliki oleh IP 175.45.184.186.

Gambar 8, *field* pada *network transport, network type, network protocol* disajikan dengan menggunakan diagram bar horizontal. Masing-masing *field* mempunya *count of records* yang berbeda-beda dalam rentang waktu yang tertera



Gambar 10 Diagram Tabel

Gambar 8 Diagram Bar Horizontal

pada *timestamp*.

Pada *network transport*, sebanyak 77.125 *records* tercatat pada *transport* UDP dari total 4 transport yang tertera. Kemudian pada *network protocol*, diantara *protocol DNS, TLS, HTTP*, *records* sebanyak 12.203 merupakan protocol terbanyak yang digunakan pada trafik jaringan ini. Sedangkan tipe IPv4 merupakan *record* terbanyak yang ditampilkan pada *field netwok type* yaitu sebanyak 173,329.

Gambar 9 Diagram Line

Pada gambar 9, ditampilkan diagram *line* dari *field client and destination bytes* dalam bentuk rata-rata *bytes*. Artinya, grafik ini menampilan besaran *file* informasi rata-rata yang tertera pada *client* dan *destination* dalam besaran *bytes.* Warna pada diagram line menunjukan warna biru mewakili median dari *destination bytes*, sedangkan warna hijau menunjukan median dari *client bytes*. Selama rentang waktu yang tertera pada *timestamp*, grafik *bytes* pada diagram menunjukan bahwa *destination bytes* cenderung naik-turun dan pada *client bytes* cenderung stabil.

Pada gambar 10, merupakan diagram *server domain* dan *destination domain*. *Server domain* merupakan sekelompok node ataupun workstation yang bertujuan untuk membagi sumber daya dan data. Pada *server domain* juga dapat menjadi bagian dari domain bersama dengan client dan server. Sedangkan *destination* domain merupakan alamat URL pada suatu halaman *website* pada saat pengguna melakukan pencarian website tertentu. Pada diagram tersebut, tabel pada *server domain* menunjukan 4 *server domain* teratas dan pada *destination domain* tertera 6 baris dengan menunjukan *blog.ub.ac.*id sebagai server domain dan *destination domain* terbanyak.

6. KESIMPULAN

Pengimplementasian sistem dilakukan sesuai dengan gambar 4. Komponen yang disiapkan pada sistem antara lain *Elastic Stack* (*Elasticsearch, Kibana, Packetbeat*) yang diinstal dan dikonfigurasi pada Ubuntu *Linux 20.04 LTS*. *Packetbeat* digunakan sebagai pengirim data (.pcap) yang sudah disiapkan sebelumnya. Dari *Packetbeat*, data akan dikirim menggunakan perintah tertentu lalu diproses oleh *Elasticsearch*. Pada *Elasticsearch* akan diatur untuk membuat indeks yang nantinya akan dikelompokkan ke dalam masing-masing *fields* secara otomatis untuk mempermudah visualisasi data. Proses visualisasi data akan ditampilkan pada *dashboard Kibana* untuk selanjutnya dianalisis *fields* yang ada pada trafik jaringan.

Visualisasi pada tugas akhir ini dilakukan menggunakan *Kibana*. Saat melakukan visualisasi, beberapa *field* akan muncul guna menunjang tampilan visualisasi. Hasil visualisasi ini ditampilkan dalam menu *dashboard* dengan menampilkan isi dari beberapa *field* yang tersedia serta ditampilkan dalam bentuk diagram yang interaktif. Selanjutnya, dari visualisasi yang sudah ditampilkan maka ditariklah sebuah analisis. Analisis yang ditampilkan merupakan hasil analisis per diagram karena isi *dashboard* bermacam-macam seperti analisis dari *destination* dan *server domain*, *client and destination bytes, client IP* dan *destination IP* serta *network transport, network type, network protocol.*

7. DAFTAR PUSTAKA

Admi, A. & Maulana, A. H. N., 2020. Penerapan Elastic Stack sebagai Tools Alternatif Pemantauan Trafik Jaringan dan Host pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia. pp. 69-77.

Annur, C. M., 2022. *Ada 204,7 Juta Pengguna Internet di Indonesia Awal 2022*. [Online] Available at: https://databoks.katadata.co.id/datapublish/2022/03/23/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022 [Accessed 14 June 2022].

B, B. & Rifqi, M., 2019. Implementasi dan Perbandingan Monitoring Jaringan Berbasis Simple Network Management Protocol (SNMP) Menggunakan Cacti dan Munin di SMK NEGERI 1 PEKANBARU. *ZONAsi: Jurnal Sistem Informasi*, 1(2), pp. 58-74.

Elasticsearch, 2022. *Kibana your window into Elastic.* [Online] Available at: https://www.elastic.co/guide/en/kibana/current/introduction.html [Accessed 14 June 2022].

Elasticsearch, 2022. *Packetbeat Overview.* [Online] Available at: https://www.elastic.co/guide/en/beats/packetbeat/current/packetbeat-overview.html [Accessed 14 June 2022].

Elasticsearch, 2022. *What is Elasticsearch.* [Online] Available at: https://www.elastic.co/what-

is/elasticsearch
[Accessed 14 June 2022].

Fathoni, Sandra, 2016. Evaluasi Kualitas dan Pengguna Jaringan Internet. *Informatika,* 4(1), pp. 51-64.

Fortinet, 2022. *Network Traffic.* [Online] Available at: https://www.fortinet.com/resources/cyberglossary/network-traffic
[Accessed 14 June 2022].

Infrastructure, I., 2020. *Monitor Infrastruktur IT Anda Secara Real-Time dengan ELK Stack.* [Online] Available at: https://i-3.co.id/monitor-infrastruktur-it-anda-secara-real-time-dengan-elk-stack
[Accessed 14 June 2022].

Service, A. W., 2022. *Logstash.* [Online] Available at: https://aws.amazon.com/opensearch-service/the-elk-stack/logstash/
[Accessed 2022 June 2022].

Yasar, K., 2022. *Elastic Stack (ELK Stack).* [Online]
Available at: https://www.techtarget.com/searchitoperations/definition/Elastic-Stack
[Accessed 14 June 2022].

Zoho Corp, 2022. *Basics of Network Monitoring.* [Online]
Available at: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html
[Accessed 14 Juni 2022].