# NETWORK FORENSIK UNTUK MENGANALISA TRAFIK DATA GAME ONLINE

Tasmi Tasmi[1], Fery Antony[1], Ubaidillah Ubaidillah[2]
[1]Program Studi Sistem Komputer Universitas Indo Global Mandiri
[2]Program Studi Ilmu Komputer Universitas Sumatera Selatan
E-Mail: tasmi@uigm.ac.id[1], feryantony@uigm.ac.id[1], ubai@uss.ac.id[2]

**Abstrak**

*Network forensics* adalah salah satu cara dalam menganalisi jenis trafik dalam sebuah jaringan adalah dengan menggunakan file log dengan merecord aktifitas pada jaringan. File log disetiap sistem sering dipakai untuk media melihat aktifitas pada sebuah sistem, terkhusus pada sebuah router dan server file ini sangat diperlukan proses investigasi analisis forensik jaringan dengan menggunakan metode Generic Network Forensics Process Model yang merupakan ilmu digital forensik yang berkaitan dengan tahap-tahap untuk menemukan sumber serangan dan mendapatkan bukti-bukti serangan yang bersumber dari file log. Tujuan dari penelitian ini dapat menerapkan model *network forensic* dalam memonitoring trafik games-online dan dapat menghasil satu sistem yang dapat menentukan prioritas memberian bandwidth, dan juga dapat dijadikan sebagai salah satu dasar pengambilan keputusan dalam membagian bandwidth. Hasil penelitian yang telah dilakukan telah mampu menganalisi jenis trafik game online dengan menggunakn tool wireshark untuk sniffing packet data serta membaguan sebuah sistem autentikasi untuk memvalidasin user pengguna jaringan. Pada tahap awal penelitian ini hasil investigasi forensik jaringan. Berdasarkan hasil pengujian tersebut dapat dinyatakan hasil sudah sesuai dengan tujuan yang diharapkan, sehingga dapat disimpulkan penelitian ini berhasil berjalan dengan baik

**Kata kunci**: *Network Forensics, Digital Investigations, Game Online*

## 1. Pendahuluan

*Game online* berkembang yang cukup pesat, ini nampak dari banyak muncul *game online* seperti *Counter Strike, mobile legends, pubg mobile* dan lain-lain. Telah banyak penelitian yang membahas tentang game online, seperti penelitian yang dilakukan [1] memahami perilaku server CounterStrike dan penelitian dan penelitian [2] pengukuran menunjukkan bahwa aplikasi menghasilkan persentase besar dari semua UDP yang diamati

Trafik adalah kemampuan dalam melakukan pengiriman data atau transmisi data yang bermacam-macam, akibatnya administrator harus mampu menjamin kualitas layanan berjalan dengan baik. Salah satu aplikasi yang banyak menggunakan bandwith adalah *Game-online* karena aplikasi ini bisa dimainkan secara bersama sehingga membutuhkan bandwidth yang besar. Selain itu setiap Game-online menggunakan protocol komunikasi yang berbeda, ada yang menggunakan UDP dan adapula yang menggunakan TCP. Dengan kasus diatas dapat mengakibatkan terjadi *hange* dan jaringan terasa lambat.

Seorang administrator harus mampu membuat sebuah sistem yang mengawasi menggunaan bandwidth agar memonitoring penggunaannya. Salah satu cara yang lagi trend adalah *forensik* yang dapat digunakan sabagai dasar awal dalam menentukan kebijakan penggunaan bandwidth. *Network Forensics* merupakan bagian dari sekian banyak model forensik yang digunakan

dalam menganalisis data. Mekanisme ini digunakan untuk menyimpan dan menampilkan kembali aktivitas yang terjadi dalam sebuah *network* sehingga seorang administrator dapat melakukan analisis kejadian yang tersimpan pada sebuah file *log system.*

Salah satu forensic digital adalah forensic jaringan yang menggunakan Framework *Generic Network Forensics* yang digunakan unutk menggabungkan keamanan dengan fungsi forensic digital dalam setiap bagiannya. Mengumpulkan banyak fase yang tersedia dalam model forensik digital tetapi dibangun pada fase-fase yang khusus untuk forensik jaringan

Pada penelitian yang dilakukan oleh [3] dan [4] menyatakan network forensic adalah bagian dari *Digital forensics* yang dipakai unutk melakukan monitoring trafik pada sebuah jaringan dengan tujuan untuk mendapatkan informasi dan deteksi jaringan. Network forensic digunakan unutk melakukan pencarian data kejahatan yang berhubungan dengan jaringan komputer.

Berdasarkan uraian di atas, untuk mengetahui apakah jensi protocol yang digunakan dan besaranya traffic yang digunakan pada saat nermain game-online, maka penelitian membahas topik (i) Bagaimana menguji model *network forensic* dalam menganalisa traffic, (ii) Bagaimana mmbuat Segementasi traffic untuk menghasilkan layanan yang baik

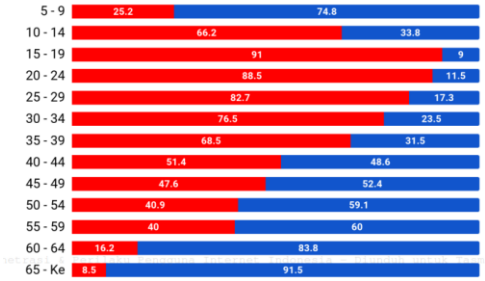
## 2. Kajian Pustaka

Sekarang ini internet sudah menjadi trend kehidupan manusia dan sudah mencakup semua sendi-sendi kehidupan. Berbagai macam pekerjaan seperti pendidikan, bisnis dan pemerintahan sudah memanfaat layanan ini dalam melakukan proses bisnisnya. Semua kebutuhan dapat didapat melalui internet, dari mencari informasi (*browsing*), *chatting*, proses belajar mengajar (*e-learning*) dan juga sampai dengan proses bisnis (*commerce*). Kebutuhan dalam mencari informasi yang cepat dan update merupakan salah satu tantangan dari suatu institusi khususnya di perguruan tinggi, oleh karena itu layanan internet menjadi bagian penting bagi proses belajar mengajar baik dalam bidang penelitian maupun dalam mencari informasi tentang satu materi. Kebutuhan layanan internet menjadi semakin meningkat dan semakin kompleks, oleh sebab diperlukan satu sistem handal yang bisa mengatur lalu lintas trafik agar semua civitas mendapatkan layanan yang baik.

[5] pada surveynya menyebutkan pada tahun 2018 pengguna internet di Indonesia pada tahun 2018 sebanyak 171,17 (64,8%) juta jiwa dari total populasi jumlah penduduk Indonesia sebesar 264,26 juta jiwa, sedangkan pada tahun 2017 pengguna internet sebanyak 143,26 (54,68%) juta jiwa seperti yang disajikan pada gambar 3.1

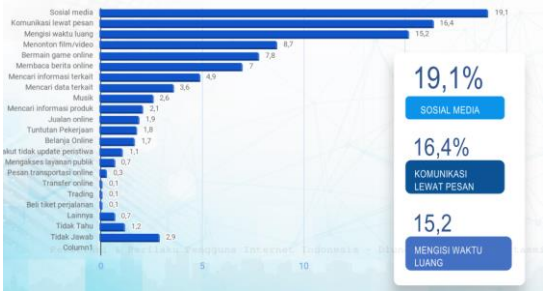

**Gambar 3.1** Data Pengguna Internet di Indonesia [5]

Pada gambar 3.2 menampilkan data pengguna internet berdasarkan usia, dimana umur 15 – 19 tahun merupakan pengguna layanan internet paling banyak sebesar 91 persen disusul usia antara 20 – 24 tahun sebanyak 88,5 persen, artinya bisa disimpulkan pengguna internet di Indonesia adalah golongan pelajar dan mahasiswa




**Gambar 3.2** Data Pengguna Internet di Indonesia berdasarkan usia [5]

Jenis peralatan elektronik yang paling sering digunakan pada tiap hari adalah smartphone sebesar 93.9 persen disusul oleh tablet sebesar 85,2 persen, desktop sebesar 68,9 persen dan laptop 56,5 persen. Ada beberapa alasan orang menggunakan layanan internet seperti social media, nonton , main game dan lain-lain




**Gambar 3.3** Alasan pengguna Internet di Indonesia [5]

## 2.1. Trafik Internet

Internet sudah menjadikan kebutuhan dan juga gaya hidup manusia termasuk juga didalam lingkungan kampus internet sduah menjadi kebutuhan dalam proses belajar mengajar. Tetapi tidak semua orang khususnya civitas dalam kampus menggunakan internet sebagai alat bantu dalam proses belajar mengajar tetapi juga digunakan untuk kesenangan pribadi seperti main Game-Online.

Telah banyak solusi yang sudah ditawarkan dalam menganalisi penggunaan internet baik yang offline maupun online. [6] berhasil mengenali pola-pola paket dengan baik, namun sistem masih bersifat pasif sehingga sulit untuk membedakan traffic masuk dan keluar. Penelitian yang dilakukan oleh [7] mengatur dan optimilisasi bandwith dalam melihat jenis traffic. Peneltian yang dilakukan oleh [8] medeteksi jenis traffic dengan menggunakan DPI pada jaringan nirkabel. Selain itu DPI juga dapat digunakan mendeteksi paket jenis data yang masuk dan keluar[9]

## 2.2 Network Forensic

Menurut [10] *Network Forensis* adalah mekanisme ini digunakan untuk menyimpan dan menampilkan kembali aktivitas yang terjadi dalam sebuah *network* yang digunakan sebagai bukti digital baik dari serangan maupun aktifitas dari sebuah network.

Sudah banyak penelitian menggunakan metode ini dalam menganalisi serangan di jaringan seperti peneltian yang dilakukan oleh [11] dan [12] menganalisi serang DDOS dan flooding dijaringan Komputer. Dibidang Internet sudah banyak penelitian dilakukan menggunakan network forensic yang digunakan sebagai alat bukti digital dalam mengunggap kejahatan dimedia social. seperti penelitian yang dilakukan oleh [13] melakukan forensic di whatsapp di smartphone (android) yang telah dilakuakn proses root ulang [14] menyatakan sangat pentingnya bukti log percakapan sebagai bukti kejahatan di media social, dalam penelitian ini media yang digunakan adalah Telegram, Line, dan KakaoTalk. sedangkan penelitian yang dilakukan oleh [15] berhasil mengextrak file enskripsi database whatsapp

## 2.3. Game Online

Salah cara orang untuk mengisi waktu luang adalah dengan bermain game, pada awalnya orang khususnya anak-anak masih menggunakan permainan secara tradisional. Perkembangan media yang cukup cepat dan jaringan global (internet) merupaka faktor muculnya permainan modern yang menggubah pola permainan dengan alat sederhana menjadi menggunakan computer atau handpone, yang berakibatnya permainan tradisional hilang dikarena kurang menarik dan modern khusunya dalam sisi tampilan.

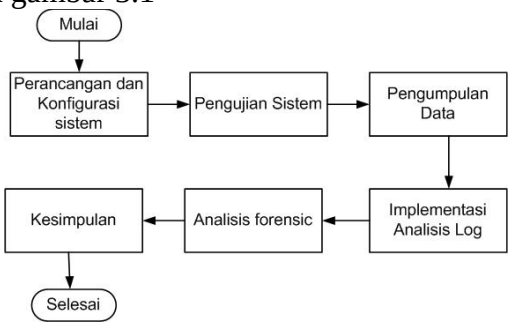
Game online adalah sebuah pemainan dalam sebuah jaringan computer, pada permainan ini memanfaat jaringan global (internet) sehingga seseorang dapat bermain secara bersama-sama, atau melawan satu sama yang lain nya. Bentuk game yang banyak digemari oleh anak-

anak dan remaja adalah *Player Unknown"s Battle Ground* (PUBG), game ini menjadi menarik diteliti karena mengadung pro dan kontrak dalam masyarakat. Pada penelitian yang dilakuakn oleh [16] menyatakan bahwa prilaku jahat (teroris) tidak bisa dikaitkan dengan seseorang yang kencanduan game PUBG. Game ini merupakan game yang mengandung banyak kekerasn, maka pada penelitian oleh [17] semakin sering orang bermain gamun PUBG maka semakin tinggi pula sikap kasar yang sering timbul pada pemainnya.

Pada survey yag dilakukan oleh APJJI pada tahun 2018 menyatakan bahwa game online mendapati urutan ke-6 orang menggunakan internet sebanyak 5,7 %, uratan pertama pengguna internet digunakan orang berkomunikasi sebesar 24,7 %.

## 3. Metode Penelitian

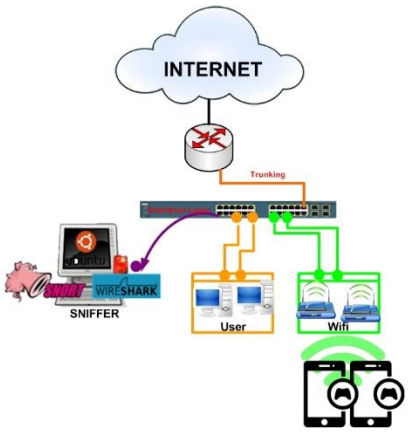
Bab ini akan menjelaskan Metode yang digunakan dalam penelitian untuk menghasilkan data yang lengkap dan akurat untuk menyelesaikan permsalahan, adapun tahapan dalam penelitian ini ditampilkan pada gambar 3.1




**Gambar 3.1** Metodelogi Penelitian

### 3.1 Perancangan Sistem

Penelitian dilakukan di Universitas Indo Global Mandiri. Topologi yang diterapkan dalam penelitian ini adalah menggunakan topologi jenis *star*, yang mana sebagai pusat dari topologi tersebut adalah *Router*, *switch* dan 2 buah komputer PC serta 2 Smartphone, dan Sebuah pc untuk mengumpulkan data/*logging*. Gambar 3.2 adalah topoli yang akan digunakan dalam penelitian ini yang berfungsi untuk men-capture traffic user.




**Gambar 3.2** Topologi Penelitian

### 3.2 DataSet

Untuk mendapatkan raw data pada penelitian ini menggunakan aplikasi sniffing yang akan dipasang pada sebuah router seperti pada gambar 3.2. Raw data yang diambil secara *real-time* dibagian router. Data yang akan difilter atau yang akan di sniffing adalah jenis paket data game online (IP, Port dan Protokol yang digunakan)

### 3.3 Implementasi Analisis Log

Tahap implementasi adalah bagian untuk mengimplementasikan hasil racangan topologi, aplikasi dan sistem perangkat lunak. Pada proses implementasi ini dibuat dalam sebuah *source code* program. Proses pemograman menggunakan Bahasa pemograman tingkat tinggi untuk menarik file log di router ke (*Database Management System*/DBMS) dengan menggunakan aplikasi API (*Application Programming Interface*).

### 3.4 Analisis Forensik

Digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum, yang dalam hal ini adalah untuk membuktikan kejahatan dalam dunia cyber, sehingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut.

Ada Sembilan tahapan dalam metode *Generic Framework for Network Forensics* yaitu : *Preparation*, *Detection*, *Incident Respone*, *Collection*, *Preservation*,

*Examination*, *Investigation*, dan *Presentation*.

Pada penelitin ini bertujuan untuk menyakinkan bahwa sistem yang dibangun telah sesuai dengan kebutuhan, maka dalam awal penelitian forensic network ini penulis focus pada tahap 1 sampai dengan 4 yaitu tahap 1) *Preparation* adalah persiapan dalam melakukan investigasi. Persiapan ini meliputi alat yang berupa hardware dan software, serta sumber daya manusia yang akan melakukan kegiatan investigasi, 2) *Detection* merupakan tahap memastikan adanya trafik game online, 3) *Incident* melakukan tindakan awal dalam proses investigasi setelah terkonfirmasi adanya pengguna Game Online, dan 4) *Collection* pengumpulan data hasil penelusuran jejak pada jaringan.

Model foreksi yang digunakan untuk meng-klasifikasi jenis game yang dimain oleh user berupa IP Sumber, IP Tujuan, Port dan Protokol yang digunakan, berikut ini adalah tabel analisi forensic yang akan digunakan untuk proses klasifikasi

**Tabel 3.1**. Klasifikasi Forensik Game-Online

| IP Sumber | Lokasi | TX | RX |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## 4. Hasil dan Pembahasan

Pada bagian ini berisi pembahasan tentang tahapan pengujian dan analisa hasil pengujian yang dilakukan. Terdapat beberapa tahapan pengujian yang dilakukan, yaitu *Preparation*, *Detection*, *Incident Respone*, *Collection*

### 4.1. Peracangan Sistem

Tahap ini adalah persiapan sistem baik dari sisi hardware dan software dalam forensic trafik game online pada jaringan di kampus UIGM

1. **Kebutuhan Perangkat Keras**

   Kebutuhan perangkat keras dalam penelitian ini menggunakan beberapa komponen jaringan berupa :

   - Router Mikrotik yang digunakan sebagai forwader packet data
   - Wifi sebagai AP untuk memperkuat sinyal
   - Handpone yang digunakan untuk user permain game online

2. **Kebutuhan Perangkat Lunak**

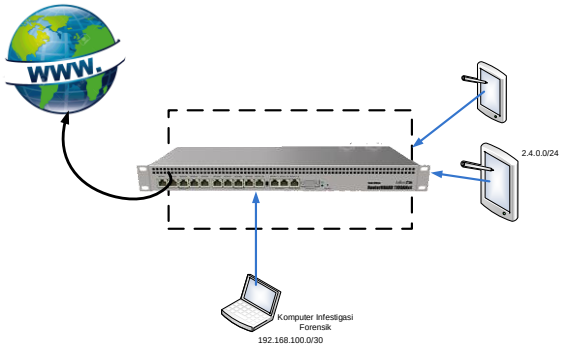
   Kebutuhan perangkat lunak yang digunakan untuk kebutuhan forensic jaringan dalam penelitian ini adalah :

   - Android
   - Linux (mikrotik)
   - PHP
   - API
   - Mysql Server

Penelitian forensic jaringan ini menggunakan perangkat router yang bertindak sebagai monitoring dan php pada saat implementasi. *Handpone* (PC) menggunakan IP yang diakses melalui jaringan lokal dengan koneksi jaringan WIFI Melakukan pairing user dan password serta SSID supaya antar perangkat terhubung sebelum dilakukan simulasi.

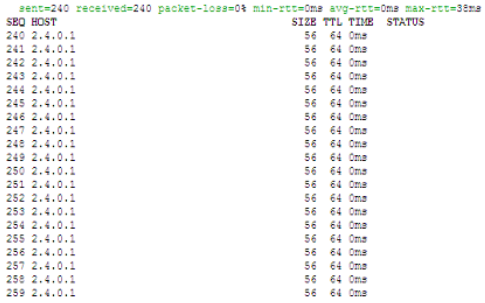
### 4.2 Pengujian Sistem

Tahap ini dibagi dalam dua bagian yaitu mendesain topologi, installasi dan konfigurasi seperti ditunjukan pada gambar 4.2 Hasil dari tahap ini adalah untuk menghasilkan trafik jaringan baik dari sisi Inbound ataupun Outbund. Letak dari implementassi forensik jaringan pada penelitian ini dapat dilihat di gambar 4.1 yaitu artsitektur dari forensik jaringan serangan pada perangkat router sebagai media forwading *Internet of Thigs* (IoT).




**Gambar 4.1** Arsitetur network forensic

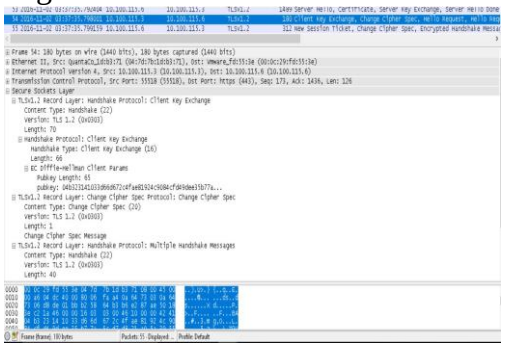
Setelah dilakukan konfigurasi dilakukan tes koneksi dari sisi user ke router dengan menggunakan PING yang ditunjukan gambar 4.2 dibawah ini




**Gambar 4.2** Tes koneksi ke router

### 5.3 Pengumpulan Data

*Packet capture* (Pcap) adalah program yang digunakan untuk meng-*capture* trafik di *network*. Pada OS *windows* dikenal dengan nama wincap dan di OS linux dikenal dengan lipcap. Pada penelitian ini menggunakan tool wireshask untuk mendapatkan data (raw data), dimana proses ini akan menghasilakn proses transaksi komunikasi antara router dan user, hasil capture data akan menjadi validasi data yang lewat pada jaringan yang sepeti ditampilkan pada gambar dibawah ini



**Gambar 4.3** Capture Packet

### 5.4.Analisi Forensik

Forensik jaringan dipakai untuk mendapatkan hasil Analisa trafik dalam sebuah jaringan. Pada perangkat yang digunakan akan menghasilkan data yang banyak, mulai dari wakru akses, ip yang digunakan client serta posisi client tekoneksi dan yang paling terpenting adalah alamat ip dari game dan port yang digunakan dalm proses transksi game online.

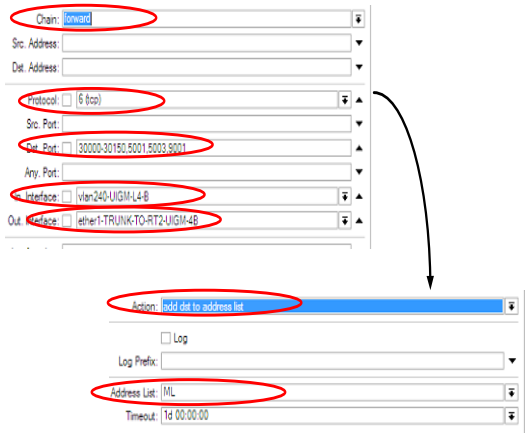
Dalam setiap menit nya akan menghasilkan data yang besar dan sangat sulit untuk dianalisa menjadi barang bukti ada user yang menggunakan jaringan sebagai media bermain game online. Penelitian ini adalah tahap awal dalam proses forensik jaringan yang baru dilakukan empat tahapan dari sembilan tahap pada porses forensic dalam mencari barang bukti user menggunakan jaringan sebagai alat untuk bermain game online.

1. **Tahap *Preparation***

   Tahap ini adalah bagaian dalam menggunak tool dalam menganalisai paket data, perangkat lunak untuk digunakan untuk memonitoring trafik sebagai media yang akan menggunakan memantau penggunaan game online dalam jaringan. Pada bagian ini harus dapat memastikan bahwa bukti maksimal dan kualitas dapat dikumpulkan untuk membuktikan penggunaan jaringan sebgai alata bukti kejahatan. Otorisasi yang diperlukan untuk memantau lalu lintas jaringan diperoleh dan kebijakan keamanan yang ditetapkan dengan baik di tempat sehingga privasi individu dan organisasi tidak dilanggar

2. **Tahap *Detection***

   Pada bagian ini bagian yang penting kerena pembuatan rule sebagai deteksi trafik game online. Tahap ini diawali oleh capture paket yang digunakan sebagai media untuk mendapatkan informasi dari game online khususnya PUBG. Dari hasil capture awal maka dijadikan modal awal dalam membuat rule untuk mendeteksi adanya trafik game online. Adapun rule yang digunakan dalam penelitian ini adalah :

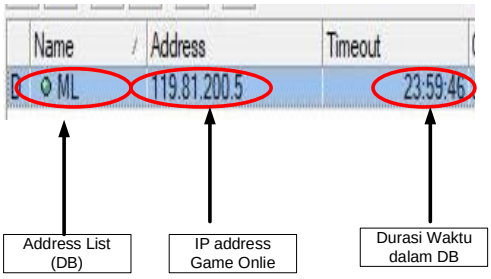



**Gambar 4.4** .Rule deteksi game online (PUBG)

Keterangan

- Chain = Forward digunakan sebagai rule yang dipakai untuk memantau trafik yang lewat router, dari public ke local
- Protokol = 6 (TCP) adalah membuktikan bahwa game online PUBG mengunakan komunikasi TCP
- DST-Port digunakan untuk jalur keluar masuk traffic game online
- In-Intreface = media (interface) yang mengarah ke user
- Out-Interface = media (interface) router yang terhubung ke public
- Action = add dst address list ini dipakai untuk merecord jenis traffic game online yang di akses oleh user
- Address List =ML nama db untuk menampung list pengguna game online

Setelah tahap pembuatan rule dimasukan dalam mesin (router) selanjutnya menampilkan hasil rule yang dikembangkan. Hasil pada tahap ini menunjukkan rule yang dibagun dapat menghasilkan deteksi traffic game online secara real time. Gambar 5.5 dibawah ini menampilkan hasil deteksi paket game online



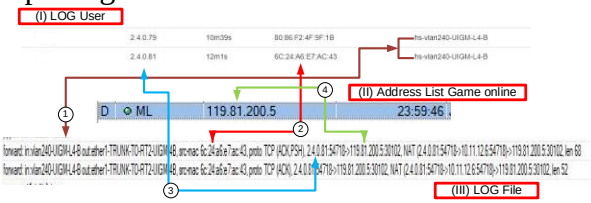

**Gambar 4.5**. Hasil deteksi trafik game online

3. **Tahap *Incident Response***

Tahap ini adalah tahap untuk menentukan keputusan atau kebijakan yang akan dilakukan berdasarkan hasil deteksi yang dimulai dari informaso tentang jenis trafik yang nanti akan digunakan untuk memvalidasi jenis data yang sudah di amati. Fase ini hanya berlaku untuk kasus di mana penyelidikan dimulai ketika trafik sudah aktif sedang berlangsung. Tahap ini kan menjadi input pada tahap terakhir pada penelitian ini yaitu menentukan kebijakan yang akan dibuat dalam menanggulangi game online

4. **Tahap *Collection***

Bagian ini akan menghasilkan validasi data dari rule dan log serta proses autentikasi (login) user pada sistem. Pengumpulan barang bukti dalam penelitian ini menggunakan log trafik pada router. Kegiatan ini akan memvalidasi user dan ip game online yang diakses oleh user. Untuk menguji kebenaran data, maka dalam penelitian ini dilakukan validasi data dari hasil data pengujian Log User Login pada sistem, address yang dihasilkan pada tahap 2 serta file log dalam router sebagai kunci pembuktian ada user yang menggunakan jaringan untuk bermain game online seperti yang ditampilkan pada gambar 5.6.




**Gambar 4.6** . Validasi Data

Hasil validasi antara *Log User, Address list dan Log file* sebagai berikut:

1. Point 1 adalah menampilkan logi user login menggunakan SSID wifi
2. Point 2 menunjukkan MacAddress device yang digunakan user
3. Point 3 adalah IP yang digunakan user untuk mengakses game online
4. Point 4 adalah IP address dari game online PUBG

Pada bagian akhir dalam penelitian ini adalah melakukan pengelompaan data berdasarakan ip, port dan lain-lain sebagai bahan untuk analisis untuk barang bukti terhadap user yang menggunakan jaringan sebagai media untuk bermain game online (PUBG). Table 5.1 menyajikan beberap user yang terdeksi koneksi menggunakan router

**Table 4.1** List user pengguna jaringan

| IP Sumber | MAC Address | Lokasi | TX | RX |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 2.3.0.53 | 94:39:E5:4F:C9:75 | hs-vlan230-UIGM-L3-B | 3756527 | 99012384 |
| 2.1.0.107 | CC:B0:DA:8D:51:47 | hs-vlan210-UIGM-L1-B | 2872970 | 82014652 |
| 2.1.0.75 | 70:5E:55:ED:21:8B | hs-vlan210-UIGM-L1-B | 586152 | 5761318 |
| 2.5.0.82 | 74:51:BA:33:FC:F4 | hs-vlan250-UIGM-L5-B | 594847 | 7254661 |
| 2.3.0.23 | 00:56:CD:D8:1C:61 | hs-vlan230-UIGM-L3-B | 592828 | 5042071 |
| 2.3.0.24 | 00:56:CD:D8:1C:61 | hs-vlan230-UIGM-L3-B | 421313 | 5036971 |
| 2.5.0.85 | 74:51:BA:33:FC:F4 | hs-vlan250-UIGM-L5-B | 5330220 | 54125536 |
| 2.4.0.82 | 78:02:F8:33:96:77 | hs-vlan240-UIGM-L4-B | 1029352 | 15879742 |
| 2.4.0.81 | 70:5E:55:6C:1C:93 | hs-vlan240-UIGM-L4-B | 341985 | 6498605 |
| 2.4.0.79 | 88:D5:0C:0E:86:B0 | hs-vlan240-UIGM-L4-B | 323409 | 1352161 |
| 2.4.0.80 | D4:1A:3F:47:FB:F1 | hs-vlan240-UIGM-L4-B | 738545 | 14617319 |
| 2.4.0.84 | AC:37:43:DD:01:C8 | hs-vlan240-UIGM-L4-B | 10882887 | 17527183 |
| 2.4.0.85 | 70:78:8B:C9:76:FF | hs-vlan240-UIGM-L4-B | 78909 | 219632 |
| 2.4.0.86 | 08:7F:98:C7:CD:ED | hs-vlan240-UIGM-L4-B | 75818 | 212280 |
| 2.2.0.197 | AC:37:43:DD:01:C8 | hs-vlan220-UIGM-L2-B1 | 589980 | 9940013 |
| 2.2.0.198 | 70:78:8B:C9:76:FF | hs-vlan220-UIGM-L2-B1 | 398776 | 169147 |
| 2.2.0.199 | 64:DB:43:BE:01:E2 | hs-vlan220-UIGM-L2-B1 | 545502 | 10156772 |
| 2.2.0.200 | 08:7F:98:C7:CD:ED | hs-vlan220-UIGM-L2-B1 | 672151 | 12347661 |
| 2.2.0.201 | D4:1A:3F:47:FB:F1 | hs-vlan220-UIGM-L2-B1 | 214779 | 905947 |

## 5. Kesimpulan dan Keterbatasan

Dari proses penelitian yang dilakukan dan berdasarkan hasil yang diperoleh, maka dapat disimpulkan bahwa Pengujian Generic Network Forensics Process Model uk dapat digunakan untuk membantu proses investigasi forensik digital. Dan menyajikan bukti digital untuk membuat kebijakan. dan Kinerja trafik game online cukup besar di sekitaran 6498605 byte ini akan mengakibatkan user lain akan terganggu akses nya. Selanjutnya penelitian ini akan dilanjutkan dan memfokuskan pada proses forensic untuk kasus di keamanan jaringan computer

## Referensi


[1] T. Henderson, "Latency and USer Behavior on a Multiplayer game Server".

[2] S. Diego and F. Directions, "Trends in Wide Area IP Traffic Patterns," no. March 2000.

[3] Yanping Zhang, Y. Xiao, M. Chen, J. Zhang, and H. Deng, "A survey of security visualization for computer network logs," *Secur. Commun. Networks*, vol. 5, no. June 2011, pp. 422–437, 2012, doi: 10.1002/sec.

[4] S. Budiharjo and F. Riyadi, "FORENSIK JARINGAN PADA LALU LINTAS DATA DALAM JARINGAN HONEYNET DI INDONESIA SECURITY INCIDENT RESPONE TEAM ON INTERNET INFRASTRUCTURE/COORDINATION CENTER," vol. 13, no. 2, pp. 125–136, 2014.

[5] Asosiasi Penyelenggara Jasa Internet Indonesia, "Penetrasi & profil perilaku pengguna internet indonesia," 2018.

[6] H. Zhang, D. Yao, N. Ramakrishnan, and Z. Zhang, "Causality reasoning about network events for detecting stealthy malware activities," *Comput. Secur.*, vol. 58, pp. 180–198, 2016, doi: 10.1016/j.cose.2016.01.002.

[7] I. G. Siqueira, L. B. Ruiz, and a. a. F. Loureiro, "Coverage area management for wireless sensor networks," *Int. J. Netw. Manag.*, no. October 2005, pp. 17–31, 2007, doi: 10.1002/nem.

[8] A. F. Oklilas and Tasmi, "Monitoring and Indentification Packet in Wireless With Deep Packet Inspection Method," *Int. Conf. Recent Trends Phys. 2016 IAES Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 365, p. 011001, 2017, doi: 10.1088/1742-6596/365/1/011001.

[9] T. J. Parvat, P. Chandra, and N. Delhi, "Performance Improvement of Deep Packet Inspection for Intrusion Detection," pp. 224–228, 2014.

[10] B. I. Riadi, "Log Analysis Techniques using Clustering in Network Forensics," 2017.

[11] I. Riadi, "Network Forensics For Detecting Flooding Attack On Web Server," no. March, 2017.

[12] S. Budiharjo and F. Riyadi, "FORENSIK JARINGAN PADA LALU LINTAS DATA DALAM JARINGAN HONEYNET DI INDONESIA SECURITY INCIDENT RESPONE TEAM ON INTERNET INFRASTRUCTURE/COORDINATION CENTER," vol. V, no. 9, pp. 26–

33, 2014.
[13] S. Ngo, “An Analysis of WhatsApp Forensics in Android Smartphones,” vol. 5013, no. 3, pp. 349–350, 2014.
[14] G. B. Satrya, P. T. Daely, and S. Y. Shin, “Android Forensics Analysis : Private Chat on Social Messenger Android,” no. June 2018, 2016, doi: 10.1109/ICUFN.2016.7537064.
[15] G. Lp and J. Ky, “Information Technology & Software Engineering WhatsApp Forensics : Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices,” *J. Inf. Technol. Softw. Eng.*, vol. 5, no. 2, pp. 2–5, 2015, doi: 10.4172/2165-7866.1000.
[16] P. Dagdee and L. Philip, “the Rise of Pubg and the Marketing Strategies Behind Its Success,” *Int. J. Sci. Res. Rev.*, 2019.
[17] A. . D. Falamartha, “PENGARUH GAME ONLINE POINT BLANK TERHADAP KEMAMPUAN BERBAHASA SANTUN DALAM BERKOMUNIKASI ANTAR SESAMA TEMAN DI LINGKUNGAN SISWA SMP YP 17 BARADATU KAB. WAY KANAN,” *Skripsi*, 2013, doi: 10.1017/CBO9781107415324.004.