Journal of SAKIRA (*Secure And Knowledge-Intelligent Research in Cybersecurity And Multimedia*) e-ISSN 3046-773X

Vol.1, No.2, Desember 2023, pp. 39~51

Forensic Network Analysis of Metarouter Using NIST SP800-86 Framework

Koresy Butarbutar[1]
[1]Sistem Informasi, Sekolah Tinggi Manajemen Informatika Dan Komputer Amikom Yogyakarta

koresybutarbutar@gmail.com[1]

Article Info

Article history:

Received November 6, 2023
Revised November 10, 2023
Accepted November 17, 2023

Keyword:

Protocol TCP / IP, NIST, ARP.

ABSTRACT

Computer networks are developing very rapidly, both in commercial institutions, in the academic world, and even in people's homes that need internet access. Internet is an acronym for Interconnection Networking, or which means a network that is widely connected. The Internet is a computer network linkage through a standard called the global Transmission Control Protocol or Internet Protocol TCP / IP, which has a system of exchanging communication packets originating through data. This study implements a virtual router network as an object for reviewing network traffic running on router hardware by utilizing network analysis tools on the Windows operating system. The framework used in the research is the National Institute of Standards and Technology (NIST). The research will end with the discovery of unusual traffic evidence using the Wireshark forensic analysis tool and Microsoft Network Monitor. The disclosure aims to be able to find the intruder's IP address from the Wireshark application and Microsoft Network Monitor, by analyzing evidence of network packets that have been prepared. Network traffic has been recorded directly using the Wireshrak tool, followed by validating the evidence between the Wireshark analysis tool and the Microsoft Network Monitor. The results of the virtual router network forensic analysis using the nist SP800-86 framework are true attacks, proven by the ARP protocol, that communication is lost between 192.168.10.5 as a client and 192.168.10.254 as a server as a result of continuous broadcast which is also proven in the ICMP protocol. Based on this research, the NIST framework uses a system that has been built with a virtual router object that analysts can use to detect cyber-attacks consistently.

I. PENDAHULUAN

Jaringan komputer berkembang dengan sangat pesat, baik di instansi-instansi komersil, dunia akademik, bahkan rumah-rumah penduduk yang membutuhkan akses internet. Internet merupakan sebuah singkatan dari Interconnection Networking, atau yang berarti jaringan yang terhubung secara luas. Internet merupakan keterkaitan jaringan komputer melalui standard yang disebut global Transmission Control Protocol atau Internet Protocol TCP/IP yang terdapat sistem pertukaran paket komunikasi yang berasal melalui data. Dengan jaringan inilah semua orang bisa berkomunikasi dengan mudah dan dalam waktu yang singkat dari seluruh dunia tanpa batas.

Internet telah diakses oleh sebagian besar masyarakat yang ada di dunia dan memanfaatkannya untuk kegiatan masing-masing. Namun pemanfaatan jaringan internet tersebut tidak hanya pada kegiatan positif saja akan tetapi banyak juga yang memanfaatkannya pada perilaku tindak kejahatan atau sering disebut dengan kejahatan dunia cyber (cybercrime). Pelaku tindakan cybercrime ini biasa disebut dengan hacker atau

e-ISSN 3046-773X

cracker, dengan alasan tertentu mereka melakukan penyusupan yang dapat merugikan para pemilik server dan jaringan komputer. Mereka menggunakan berbagai macam serangan jaringan komputer dengan tools yang dibuat secara mandiri ataupun yang telah ada di pasar.

Tindakan cybercrime yang memanfaatkan jaringan internet ini merupakan salah satu isu yang sangat penting dalam dunia teknologi dimana isu tersebut dianggap merugikan bagi para pengguna. Menurut berita yang dikeluarkan oleh

Kementrian Komunikasi dan Informatika Republik Indoensia (www.kominfo.go.id) menjelaskan bahwa angka serangan jaringan internet di Indonesia mengalami peningkatan dari tahun 2019 yang masih 1,25 juta kali menjadi 1,5 juta kali pada tahun 2020. Hal tersebut membuktikan bahwa nilai kegentingan dari tindakan cybercrime yang memanfaatkan jaringan internet ini sangat serius untuk dilakukan proses pengkajian yang mendalam. Berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor : 16 /Per/M.Kominfo/ 10 /2010 menjelaskan bahwa pengamanan jaringan telekomunikasi berbasis protokol internet bertujuan untuk menjamin keamanan dan menciptakan lingkungan serta pemanfaatan jaringan telekomunikasi berbasis protokol internet yang aman dari berbagai macam potensi ancaman dan gangguan (Pemerintah Indonesia, 2010).

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 (tindakan cybercrime) 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 digital forensik yaitu forensik jaringan (Dewi et al., 2017).

Mekanisme forensik jaringan dapat digunakan untuk mengkonstruksi sebuah kejadian dengan memanfaatkan sebuah sistem yang menyimpan dan melihat kembali segala aktivitas lalu lintas data sehingga administrator dapat melakukan investigasi melalui peristiwa ataupun kejadian yang tersimpan pada log system. Terdapat beberapa proses pada forensik jarigan seperti, monitoring, koleksi data, analisa data serta source traceback untuk mengetahui apa yang sebenarnya terjadi, untuk mengetahui detail koneksi, serta untuk mengetahui alamat asal dan tujuan, yang mungkin dapat mencegah dari adanya serangan terhadap sistem keamanan jaringan (Ridho et al., 2016).

Implementasi forensik jaringan pada dasarnya menggunakan standar kerangka kerja diantaranya National Institute of Justice (NIJ), Digital Forensics Research Workshop (DFRWS), National Institute of Standards and Technology (NIST) dan lainnya (Yudhana et al., 2019). Penelitian yang dilakukan menggunakan framework National Institute of Standards and Technology (NIST). National Institute of Standards and Technology (NIST) merupakan metode yang digunakan untuk melakukan forensik analisis. Metode ini sudah banyak digunakan sebagai acuan analisis forensik (Mustafa et al., 2018).

Salah satu perangkat yang paling penting pada suatu jaringan dengan cakupan yang luas adalah router. Router dapat menyimpan identitas lalu lintas data berdasarkan tabel-tabel yang tersedia melalui Router (Firmansyah et al., 2019). Perpindahan sumber informasi antar jaringan pada router menjadi perhatian utama untuk memonitor lalu lintas data yang menjadi sasaran para intruder untuk masuk kedalam sistem utama utuk merusak, menghapus, bahkan mencuri data penting yang tersimpan pada sistem utama, yang dapat merugikan baik bagi perorangan, perusahaan, maupun instansi terkait.

Pentingnya peran router dalam suatu jaringan menjadikan perangkat keras tersebut wajib ada dalam suatu topologi jaringan. Akan tetapi topologi jaringan memiliki kebutuhan dan Access Control Lists (ACLs) berbeda. ACLs yang banyak dan terpusat dapat menyebabkan traffic padat. Pemisahan ACLs berdampak pada penggunaan router yang lebih banyak dan menyebabkan biaya berlebih untuk pembelian router, pemakaian listrik dan penggunaan ruang penyimpanan. Permasalahan tersebut dapat diatasi dengan virtualisasi router sehingga dapat menghemat biaya pembuatan jaringan komputer, pemakaian energi listrik dan penggunaan tempat dibandingkan router non-virtualisasi (Galang dkk, 2017).

Router yang merupakan perangkat penting dalam sebuah jaringan, banyak bukti-bukti yang dapat diambil dari aktivitas jaringan, selain itu router juga secara cerdas mampu. mengetahui kemana alur tujuan informasi (quota) yang akan dilaluinya. Bukti-bukti yang dapat diambil dari router antara lain konfigurasi firewall, mac address, daftar ip address client, aktivitas logging admin dan lain-lain. Untuk mendapatkan bukti-bukti dari tindak cybercrime tersebut perlu dilakukannya proses investigasi jaringan forensik dengan tujuan untuk mengetahui pelaku serta dari bukti yang telah didapatkan dapat dijadikan sebagai bahan pembuktian didalam proses persidangan.

Berdasarkan latar belakang yang telah dipaparkan maka ranah dalam penelitian ini adalah melakukan perancangan virtual router dan menguji penyerangan terhadap virtual router tersebut, kemudian melakukan analisa investigasi forensik untuk mendapatkan aktifitas lalu lintas yang mencurigakan setelah serangan yang dilakukan. Berdasarkan penelitian yang dilakukan oleh (Fadlil et al., 2017) mengemukakan bahwa forensik jaringan merupakan cabang dari forensik digital yang terkait dengan penyelidikan untuk menentukan sumber serangan jaringan berdasarkan data log bukti, identifikasi, analisis, dan rekonstruksi kejadian. Jenis serangan terhadap suatu komputer atau server di dalam jaringan dengan cara menghabiskan sumber daya (resources) yang dimiliki oleh komputer sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses dari layanan jaringan yang diserang disebut dengan

e-ISSN 3046-773X

serangan Distributed Denial of Service (DDoS). Riset Forensik Jaringan dilakukan dalam Laboratorium Riset Magister Teknik Informatika Universitas Ahmad Dahlan Yogyakarta. Metode yang digunakan dalam penelitian ini adalah model proses forensik (The Forensic Process Model). Deteksi serangan dilakukan oleh Winbox RouterOS v3,6 dimana software tersebut menunjukan resources, data penyerang (IP Address), jumlah paket data, dan kapan terjadi serangan. Simulasi serangan dilakukan dengan software LOIC untuk mengetahui kinerja sistem pengaman jaringan komputer, sedangkan sistem pengaman jaringan komputer berupa antisipasi terhadap bentuk serangan DDoS.

Penelitian yang dilakukan oleh (Yudhana et al., 2019) menjelaskan bahwa penelitian ini menerapkan metode mobile forensik berdasarkan pedoman yang dikeluarkan oleh National Institute of Standards of Technology (NIST). Metode NIST dalam proses forensik digital dapat diterapkan pada studi kasus media penyimpanan cloud menggunakan bantuan software Axiom Magnet. Hasil penelitian ini disajikan dalam bentuk pemulihan data pada media penyimpanan Google Drive yang terhapus, yang hasilnya berupa tajuk jenis data berupa penghapusan nama akun, jenis file yang terhapus, dan stempel waktu file yang terhapus. Bukti digital yang diperoleh dengan 59 software Axiom Magnet ditemukan di file Entry227, dengan 46 file, 8 file gambar, video 3, zip 2, rar 4, pdf, 20, docx 4, pptx 2, Aplikasi 1, Database 2 dan 15 file adalah hanya nama folder yang tidak memiliki data.

Penelitian yang dilakukan oleh (Helmi et al., 2019) menjelaskan bahwa fitur layanan cloud yang dirancang untuk menyimpan data guna mendukung kelancaran proses bisnis, dapat disalahdigunakan oleh pelaku kriminal untuk menyimpan data hasil kejahatan. Penelitian ini bertujuan untuk melakukan simulasi analisis terhadap bukti digital dari suatu layanan cloud. Proses analisis menggunakan metode NIST 800-86 dilakukan pada bukti digital dari 5 skenario yang dipersiapkan sebelumnya berkaitan dengan penggunaan fitur layanan cloud yang berpotensi disalahgunakan. Teknik akuisisi data menggunakan metode live acquisition dan physical imaging untuk mendapatkan bukti digital. Hasil percobaan pada penelitian menunjukan bahwa, setelah dilakukan skenario 1 dan skenario 3, berhasil didapatkan informasi nama file dan direktori path yang diunduh oleh client 1 dan client 2 dilengkapi dengan informasi ip address, mac address, username, password dan timestamp. Setelah dilakukan skenario 2, berhasil didapatkan bukti digital berupa informasi nama dan lokasi folder di server cloud. Setelah dilakukan skenario 4, berhasil didapatkan informasi nama file dan shared folder dilengkapi dengan informasi client yang mendapatkan hak untuk mengakses file dan folder tersebut. Setelah dilakukan skenario 5, berhasil didapatkan informasi nama file dan direktori path file yang dihapus.

Penelitian yang dilakukan oleh (Ridho et al., 2016) menjelaskan bahwa router adalah salah satu perangkat yang paling dibutuhkan dalam setiap lembaga yang terhubung dengan jaringan intranet maupun internet, khususnya pada penyedia jasa internet dalam membangun sebuah jaringan dengan keamanannya. Target utama attacker sebelum masuk pada sistem utama atau pusat data adalah dengan mematikan kinerja router. Intrusion Detection System dapat dimanfaatkan sebagai sistem monitoring untuk mendeteksi serangan distributed denial of service (DDoS) secara real time. Kemampuan forensik terhadap router sangat diperlukan untuk menemukan bukti serangan yang di lakukan oleh intruder agar pelaku dapat dijerat hukum. Hasil yang harapkan melalui penelitian ini adalah proses analisa berjalan dengan baik melalui pemanfaatan intrusion detection system (IDS), administrator dapat menemukan bukti digital serta pelaku serangan melalui perangkat router yang digunakan sebagai objek penelitian.

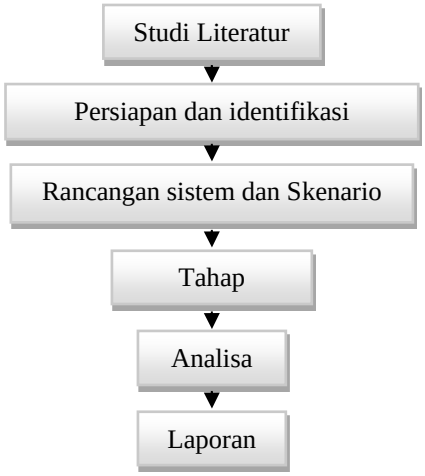
Penelitian yang dilakukan oleh (Firmansyah et al., 2019) menjelaskan bahwa virtual router sangat berguna untuk tujuan memecah jaringan jika router yang dimiliki hanya 1 (satu) unit. Tujuan dari penelitian ini adalah menemukan serangan yang terjadi melalui protokol yang diserang oleh penyusup dan metode yang digunakan dalam penenlitian ini yaitu metode live forensic. Tools yang digunakan yaitu Wireshark, tools tersebut digunakan untuk menganalisis lalu lintas jaringan jika terjadinya penyusupan, dan sangat mendukung banyak protokol, namun penelitian ini hanya membahas tentang protokol ARP dan ICMP. Serangan badai ARP dapat diketahui dengan cara melihat tujuan protokol ARP, jika pancaran terjadi dalam rentan waktu lebih dari 10s, maka dapat disimpulkan terjadinya serangan badai ARP. Protokol ICMP pada aplikasi wireshark juga membuktikan bahwa laptop dengan IP address 192.168.10.252 dan 192.168.20.253 tidak dapat melakukan permintaan tujuan selanjutnya yang artinya koneksi internet saat itu terputus.

Penelitian yang dilakukan oleh (Mustafa et al., 2018) menjelaskan bahwa ilmu forensik merupakan ilmu yang relatif baru dan bahkan belum banyak dikenal di kalangan masyarakat. Permasalahan yang timbul pada saat ini adalah sangat jarang penelitian yang dilakukan dalam hal investigasi forensik dalam menghadapi kejahatan dalam dunia cyber, khususnya dalam email spam tersebut. Metode yang digunakan adalah National Institute of Standards and Technology (NIST) dengan tahapan Collection, Examination, Analisys dan Reporting. Hasil penelitian yang dilakukan yaitu terdapat pola pemalsuan email yang berupa subjek, alamat dan tanggal email yang palsu. Selain itu investigasi email forensik ini juga menghasilkan: 1) Alamat email pengirim email palsu; 2) memeriksa protokol inisiasi pesan (HTTP, SMTP); 3) memeriksa ID pesan; 4) alamat IP pengirim. Aspek lain yang dapat mengontrol analisis forensik meliputi format penyimpanan alamat email, ketersiadaan cadangan email ketika email tersebut dipindah dan protokol yang digunakan dalam menganalisis email.

II. METODE

e-ISSN 3046-773X

Proses penelitian dibagi menjadi 6 tahapan secara garis besar penelitian ini dari awal hingga akhir. Alur penelitian ditunjukkan pada Gambar 1.



Gambar 1. Alur Penelitian

1.Studi Literatur

Studi literatur digunakan untuk memahami tentang konsep, teori, dan hasil temuan penelitian lain yang serumpun dan dijadikan acuan sebagai landasan penelitian. Pada studi literatur berisi rangkuman dan hasil penelitian sebelumnya dengan topik yang berhubungan

2.Persiapan dan identifikasi kebutuhan

Tahapan ini merupakan suatu proses persiapan alat dan bahan yang digunakan dalam melakukan penelitian untuk keperluan simulasi sampai dengan investigasi forensik akan dilakukan, seperti tools bantuan, hardware maupun software.

3.Rancangan Sistem dan Skenario Kasus

Perancangan sistem pada penelitian ini merupakan kerangka kerja (framework) berupa rancangan virtual router yang akan digunakan sebagai abjek penelitian. Tahap selanjutnya yaitu proses perancangan skenario kasus penyerangan terhadap virtual router tersebut dan kemudian dilakukan proses analisis forensik.

4.Tahap Forensik

Tahap ini dilakukan proses Analisa bukti digital pada virtual router yang telah diimplementasikan skenario kasus penyerangan. Proses analisa tersebut dilakukan berdasarkan metode NIST 800-86 yang terdiri dari 4 bagian, yaitu collection, examination, analysis dan reporting.

5.Analisa

Proses analisa merupakan proses validasi terhadap bukti digital yang ditemukan pada proses forensik jaringan hingga pada akhirnya bukti digital tersebut dapat ditunjukkan pada proses persidangan.

6.Laporan

Tahap terakhir adalah melakukan dokumentasi terhadap penelitian yang dilakukan agar bias menjadi karya ilmiah dan memungkinkan sebagai referensi penelitian yang berkaitan di topik yang dibahas.

Alat dan bahan yang diperlukan untuk menunjang penelitian ini dapat dilihat seperti pada Tabel 1.

Tabel 1. Alat dan Bahan Penelitian

No.	Alat dan Bahan	Jumlah	Deskripsi	Keterangan
1	Mikrotik RB951Ui-2HnD	1	RouterOS versi 6	Router Fisik
2	Modem ADSL	2	ZTE dan Huawei	Switch
3	*Notebook*	4	Prosesor Intel Core i5	Perangkat keras analisis/investigator
4	*Wireshark*	1	*Live sniffing* dan *Static Forensic*	Alat akan diinstall pada Microsoft Windows 10
5	*Smartphone*	2	Sony Z5 dan Sony C3	Perangkat Penyerang
6	*Winbox*	1	v3.19	Antar muka router
7	*Termux*	1	Android	Alat penyerang
8	*Microsoft Windows 10*	1	Windows 10 Pro File sistem NTFS	Perangkat lunak sistem operasi
9	*Microsoft Network Monitor 3.4*	1	*Live sniffing* dan *Static Forensic*	Alat akan diinstall pada Microsoft Windows 10

3.1. Rancangan Sistem

Forensik sebagian besar menangani kejahatan yang dilakukan sebelumnya, fokusnya untuk mencegah kejahatan di masa depan. Forensik jaringan merupakan salah satu ilmu forensik digital yang melingkupi penemuan dan invesitgasi materi yang ditemukan pada perangkat digital. Model Proses Evaluasi Forensik yang digunakan oleh peneliti ditunjukkan pada Gambar 2.

e-ISSN 3046-773X

Gambar 2. Perancangan Sistem

Perancangan *virtual router* artinya bahwa penentuan topologi jaringan virtual router dan rancangan interface agar virtual router dapat diterima sesuai konfigurasi dengan perancangan yang diinginkan. *Interface* setiap virtual router akan dibuat secara manual, pemanfaatan terminal atau *Command Line Interpreter* (CLI) dan atau sering disebut *console* maupun tatap muka grafis atau *Graphical User Interface* (GUI) pada aplikasi winbox, sehingga langkah ini sangat penting untuk diingat. Virtual router pada vitual router akan dibuat sebanyak 2(dua), masing-masing akan diberi nama Meta1 dan Meta2, sedangkan router asli diberi nama SKALAPETA. Perancangan serangan dibuat agar dapat dipastikan bahwa lalu lintas paket jaringan terhambat dengan pemanfaatan aplikasi *termux* dari android. Tahapan pengujian dan analisis merupakan tahapan akhir untuk pengujian sitem yang dibuat. Langkah ini merupakan pengungkapan adanya serangan yang terjadi pada sistem yang dibuat, dengan pemanfaatan kerangka kerja NIST. Jika dalam pengujian sistem tidak bekerja sesuai dengan harapan, maka akan kembali pada proses pengaturan. Pengungkapan bertujuan agar bukti penemuan dapat dianalisis dan dilaporkan sebagai tindak kejahatan. IP address maupun protokol-protokol digunakan penyusup atau penyerang terdeteksi dari aplikasi *Microsoft Network Monitor 3.4* dapat dijadikan sebuah bukti.

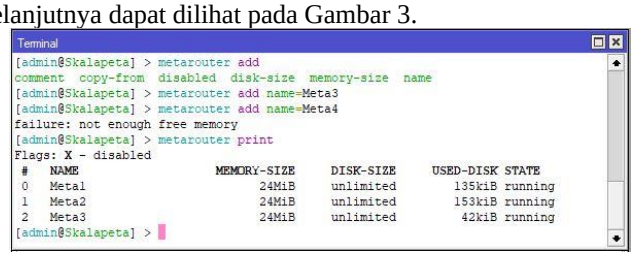
III. HASIL DAN PEMBAHASAN

3.1 Perancangan Virtual Router

Penyajian rancangan sistem virtual router, meliputi pembentukan Virtual router, pengaturan *static interface* alamat IP virtual router yang masing-masing akan digunakan sebagai alamat rekam paket lalu lintas jaringan pada *real scenario,* dan sampai pada tahap akhir perancangan yaitu terciptanya jaringan forensik virtual router dengan pemanfaatan alat rekam paket data yang bergerak pada jaringan virtual router.

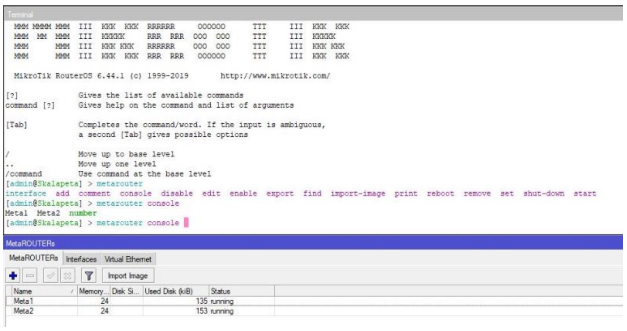
3.1.1 Pembentukan Virtual router

Pembuatan virtual router dapat dilakukan dengan 2 (dua) cara seperti yang telah dijelaskan sebelumnya, yaitu menggunakan *console* dan memanfaatkan aplikasi winbox. Penggunaan *console* akan dijelaskan pada penelitian ini yang selanjutnya dapat dilihat pada Gambar 3.



Gambar 3. Pembentukan Virtual router

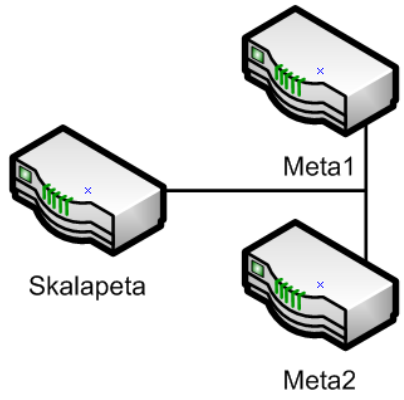
Terlihat sudah terbentuk 3 (tiga) virtual router dengan pemanfaatan *console* yaitu dengan cara penggunaan *script "virtual router add"* kemudian memberikan nama dengan "*virtual router add name=Meta1*" sampai seterusnya. Penghapusan akan menggunakan *script "virtual router delete number=2"* untuk penghapusan pada nama Meta3. Selanjutnya yaitu cara pengaksesan virtual router dapat dilihat pada Gambar 4.



Gambar 4. Akses Virtual router

Terlihat pada gambar, terdapat 2 (dua) virtual router yang artinya Virtual router lainnya berhasil terhapus. Akses virtual router dengan menggunakan *script "virtual router console"* kemudian pilih nama virtual router yang akan diakses. Router yang dimiliki saat ini berjumlah 3(tiga) buah, dapat diilusatrasikan pada Gambar 5.

e-ISSN 3046-773X

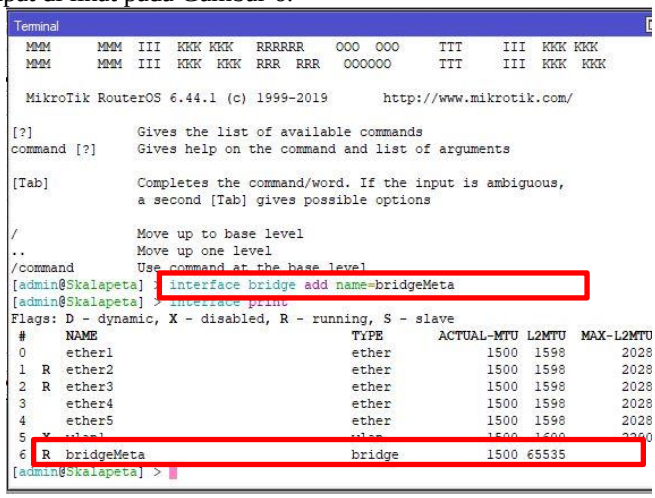


Gambar 5. Ilustrasi Router

Penggunaan virtual router pada virtual router akan sangat berguna jika hanya 1(satu) buah router fisik yang dimiliki. Virtual router dapat berfungsi sama sebagai router terlihat pada gambar di atas.

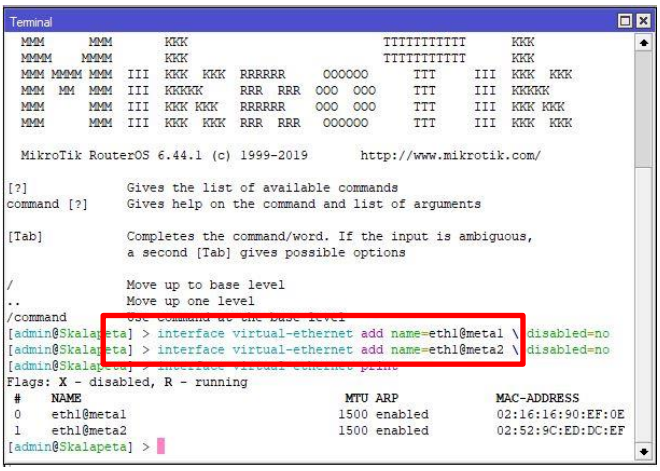
3.1.2 Pengaturan Static Interface

Interface sangat diperlukan bagi setiap router agar terjalin komunikasi antar perangkat lain seperti *switch to switch*, *switch to* komputer maupun perangkat router itu sendiri dan hubungan komunikasi dengan perangkat sesama virtual router. Menghubungkan *Interface* kepada virtual router dapat menggunakan 2(dua) pilihan yaitu menggunakan *static interface* dan *dinamic interface.* Fokus pada percobaan ini yaitu menggunakan *Static Interface.* Pengaturan *interface* dapat di lihat pada Gambar 6.



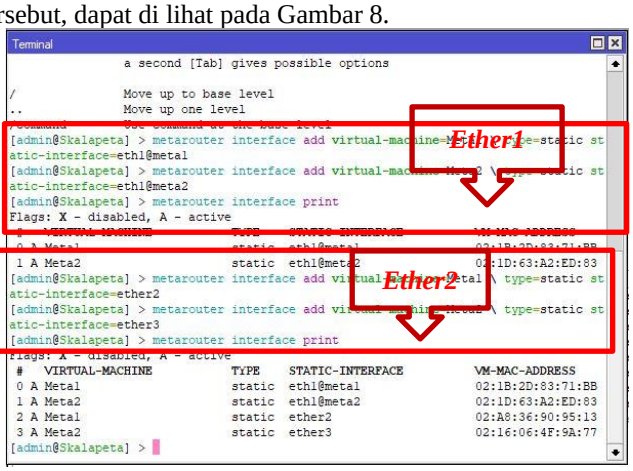
Gambar 6. *Interface Bridge*

Router Skalapeta membutuhkan *interface bridge* diutamakan agar pengaturan sesuai dengan alur, yang bertujuan untuk menghubungkan sesama virtual router. Selanjutnya akan di buat *interface virtual ethernet* dari masing-masing virtual router, adapun perintah yang dapat digunakan yaitu pada Gambar 7.



Gambar 7. Interface Virtual Ethernet

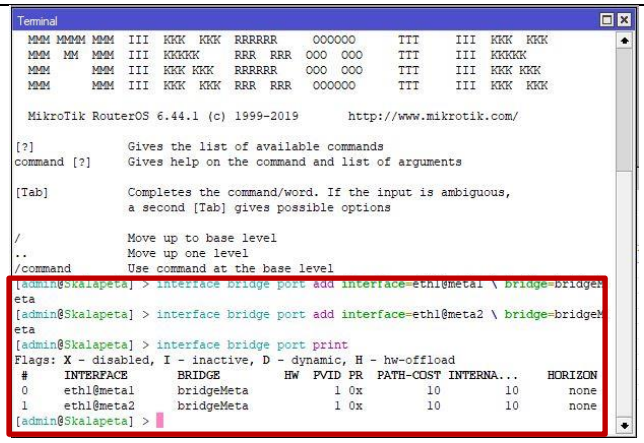
Interface Virtual Ethernet (vEth) adalah *interface* logis yang dibuat untuk memenuhi kebutuhan layanan komunikasi eksternal agar terhubung melalui port virtual. Setelah vEth berhasil dibuat, maka selanjutnya adalah mengarahkan vEth untuk menjadi *interface* ether1 pada masing-masing virtual router. Perintah yang dapat digunakan untuk pengaturan tersebut, dapat di lihat pada Gambar 8.



Gambar 8. *Virtual router Interface*

Masing-masing interface ether2 akan menghubungkan ke jaringan eksternal. *Interface* ether2 pada *Virtual Machine* (VM) Meta1 akan terhubung dengan jaringan luar menggunakan *interface* ether2 milik router Skalapeta, sedangkan Meta2 *interface* ether2, akan terhubung dengan jaringan luar menggunakan *interface* ether3 router Skalapeta. Langkah terakhir adalah menghubungkan interface dari masing-masing virtual router agar dapat terhubung dengan *interface* bridgeMeta dari router Skalapeta. Perintah yang digunakan dapat dilihat pada Gambar 9.

e-ISSN 3046-773X

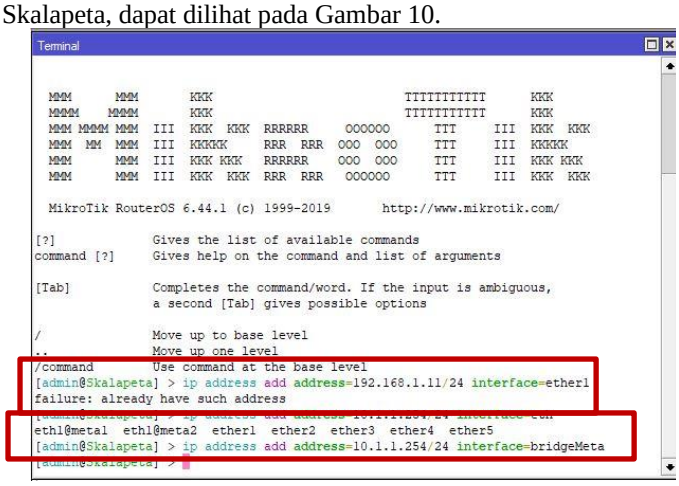


Gambar 9. *Interface Bridge Port*

Sampai pada tahap menghubungkan *interface bridge port*, pengaturan pada router Skalapeta telah selesai dilakukan. Pekerjaan akan dilanjutkan pada pengaturan IP *Address* pada router Skalapeta maupun masing-masing Virtual router.

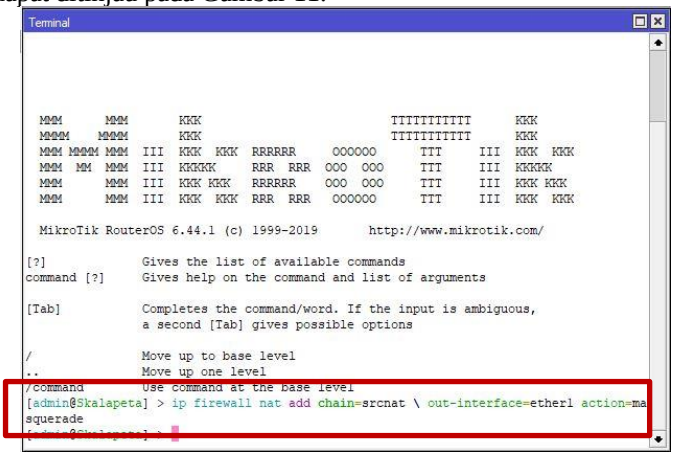
3.1.3 Pengaturan IP network

Sebelum melakukan pengaturan virtual router, pada bagian ini terlebih dahulu melakukan setting IP yang akan gunakan untuk klien yang akan terkoneksi dengan mikrotik, menentukan IP yang akan jadikan sebagi IP *public* yang berikan kepada klien. Pengaturan IP *Address* pada router Skalapeta merupakan pengaturan terhadap *interface* masing-masing Virtual router, artinya pada tahap ini akan ada 3(tiga) pengaturan, yaitu pada router Skalapeta, Meta1 dan Meta2. Berikut cara *setting network* IP pada mikrotik router Skalapeta, dapat dilihat pada Gambar 10.



Gambar 10. *Ip Address Interface*

IP *address* yang diberikan kepada router Skalapeta adalah 192.168.1.11/24 dengan *interface* yang digunakan adalah ether1. Jika IP sudah tertanam, maka router akan memberikan notifikasi. *Interface* bridgeMeta akan diberikan alamat 10.1.1.254/24, yang akan dijadikan sebagai gerbang utama menuju internet pada masing-masing virtual router yang akan menangani alamat 192.168.123.254/24 pada VM Meta1 dan 192.168.234.254/24 pada VM Meta2. Pengaturan selanjutnya yaitu pengaturan gerbang utama internet yang akan diberika pada router Skalapeta yaitu 192.168.1.1 dan setelahnya pengaturan DNS Server, dapat menggunakan DNS *Google* yaitu 8.8.8.8 dan 8.8.4.4. Sampai pada tahapan ini, pengaturan belum selesai, dikarenakan belum ada internet yang mengaliri lalu lintas, maka selanjutnya diberikan pengaturan IP *masquerade* pada router Skalapeta. Pengaturan *masquerade* dapat ditinjau pada Gambar 11.



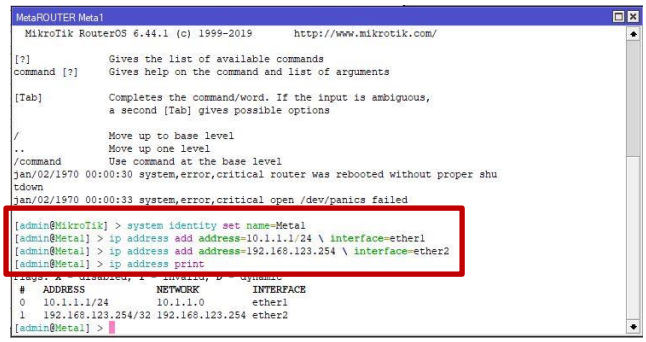
Gambar 11. IP *Firewall*

Firewall akan bekerja menurut kriteria seperti, alamat IP dari komputer sumber, Port TCP/UDP sumber dari sumber, alamat IP dari komputre tujuan, Port TCP/UDP tujuan pada komputer tujuan, dan informasi dari header.

3.1.4 Pengaturan Alamat IP *Virtual router*

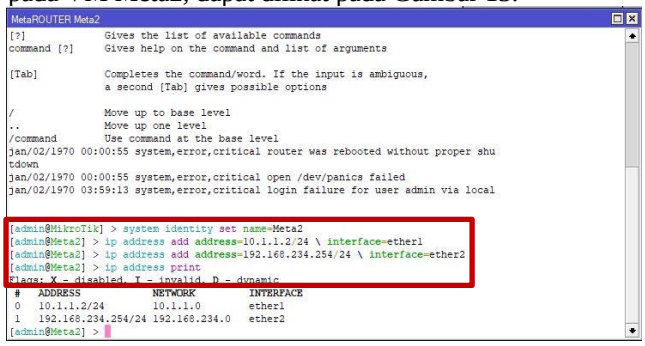
Pada saat berbisnis di dunia internet, tentu kita akan banyak menemui pelanggan yang bermacam kriteria. Beberapa user yang cukup mengenal MikroTik terkadang menginginkan akses full ke router, atau paling tidak membutuhkan router untuk bisa management jaringan secara penuh. Sebagai penyedia jasa bisa saja memberikan lagi router, namun tentu akan membutuhkan biaya yang lebih besar. Kasus lain misalnya hendak membuat laboratorium jaringan yang membutuhkan lebih dari satu router. Solusi hemat adalah dengan memanfaatkan fitur Virtual router menggunakan virtual router. Virtual router merupakan fitur MikroTik yang memungkinkan untuk menjalankan operating system baru secara virtual. Hampir sama seperti aplikasi VMware atau VirtualPC pada Windows. Virtual router bisa di gunakan untuk menjalankan *Operating System* (OS) di dalam OS yang sedang berjalan. Bagian ini menjelaskan bagaimana melakukan pengaturan alamat masing-masing virtual router, berikut perintah pengaturan alamat IP Meta1, dapat dilihat pada Gambar 12.

e-ISSN 3046-773X



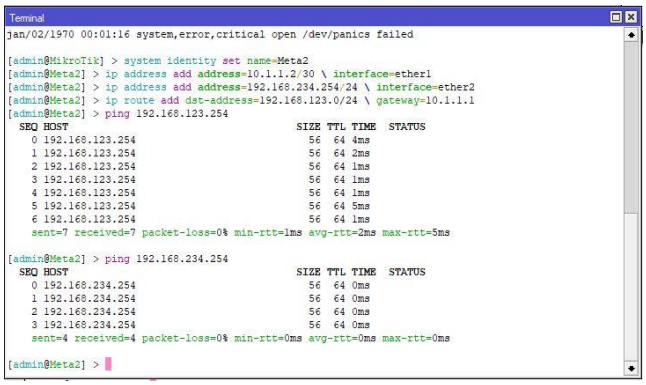
Gambar 12. Pengaturan Alamat IP Meta1

Pada Gambar 12 menjelaskan tentang bagaimana mengatur alamat IP virtual router pada VM Meta1. Pemberian identitas setiap virtual router sangat dianjurkan untuk mengurangi kekeliruan akses. Identitas virtual router pada VM Meta1 yaitu diberikan nama Meta1 dengan alamat IP 10.1.1.1/24 pada *interface* ether1, sedangkan kluaran untuk alamat tersebut adalah diberikan alamat IP 192.168.123.254/24 sebagai gerbang awal dengan jumlah pengguna /24 yaitu 255 alamat yang akan ditangani. Selanjutnya pengaturan alamat IP pada VM Meta2, dapat dilihat pada Gambar 13.



Gambar 13. Pengaturan Alamat IP Meta2

Pengaturan selanjutnya melalui tahapan yang hampir sama dengan sebelumnya, letak perbedaan terdapat pada identitas dan alamat pada setiap *interface*. Meta2 dengan identitas yang diberikan nama Meta2 dengan alamat 10.1.1.2/24 pada *interface* ether1 dan alamat keluaran diberikan pada ether2 192.168.234.254/24 yang akan difungsikan sebagai gerbang awal perangkat luar. Mengingatkan kembali bahwa untuk setiap keluaran masing-masing virtual router dapat diakses melalui router skalapeta menggunakan ether2 pada Meta1 dan ether3 pada Meta2. Setelah pengaturan alamat IP virtual router, selanjutnya pengaturan gerbang utama dan pengaturan alamat DNS. Gerbang utama dan DNS yang akan diberikan memiliki alamat yang sama pada masing-masing virtual router yaitu 10.1.1.254. Sampai pada tahap ini seharusnya setiap virtual router sudah dapat saling berkomunikasi dengan baik dan telah mengakses internet melalui gerbang 192.168.1.1. Untuk memastikan komunikasi berjalan dengan baik, dapat ditinjau pada Gambar 14.

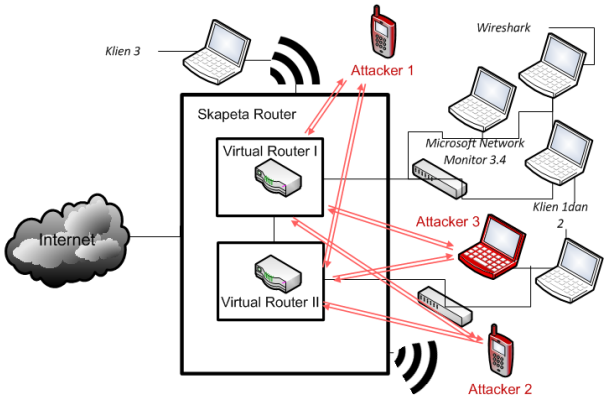


Gambar 14 Uji Komunikasi Melalui PING

Pengujian dapat dilakukan dengan memanfaatkan konsole atau terminal pada router Skalapeta maupun masing-masing virtual router, namun pada gambar di atas dilakukan menggunakan terminal pada VM Meta2, peneliti meyakini jika uji ping berjalan pada router, maka akan berjalan pada router lain.

3.2 Perancangan Serangan

Perancangan serangan dibuat agar dapat dipastikan bahwa lalu lintas paket jaringan terhambat, adapun rencana penyerangan jaringan virtual router dapat di lihat pada Gambar 15.



Gambar 15. Rencana Serangan

Serangan akan dilakukan oleh 3(tiga) perangkat dengan tujuan agar virtual router terbebani terhadap serangan yang dilancarkan. Serangan pada *smartphone* akan memanfaatkan aplikasi *termux* dengan melakukan penyerangan badai ARP dan DOS, sedangkan serangan pada *Notebook* dapat dimanfaatkan PING melalui *Command Prompt* (CMD) dengan membanjiri server virtual. Alamat setiap perangkat jaringan, lebih jelas dapat di lihat pada Tabel 2.

Tabel 2. Alamat Perangkat

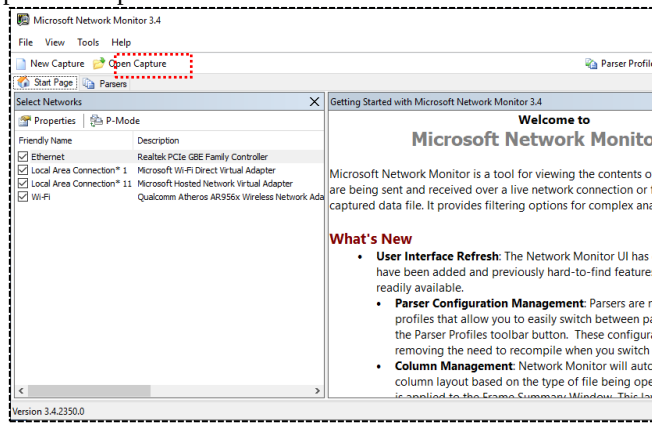
No	Perangkat	*IP Address*
1	*Virtual Router I*	192.168.10.254/24
2	*Virtual Router II*	192.168.20.254/24
3	*Microsoft Network Monitor 3.4*	192.168.10.100
4	*Attacker* 1	192.168.10.252
5	*Attacker* 2	192.168.20.253
6	*Attacker 3*	192.168.20.123
7	*Wireshark*	192.168.10.200

e-ISSN 3046-773X

8	*Client* 1	192.168.10.5
9	*Client* 2	192.168.20.5
10	*Internet*	192.168.100.1
11	*Client 3*	192.168.100.132

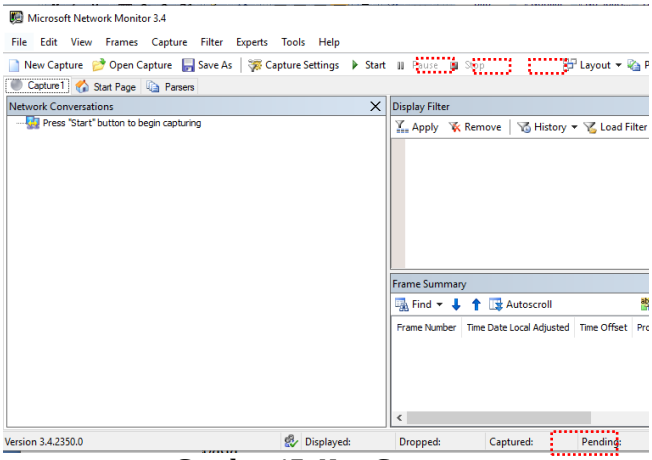
3.3 Pengujian Forensik Jaringan

Pada kasus ini, perekaman dan analisis kejadian-kejadian lalu lintas Virtual router merupakan tugas dari alat forensik jaringan, namun sebelumnya akan dilengkapi dengan pengaturan rancangan jaringan forensik Virtual router, maka tahapan pengaturan alat forensik atau instalasi dapat dilakukan pertama kali pada perangkat *Notebook* dengan penanaman alat forensik *Microsoft Network Monitor* 3.4, dapat dilihat pada Gambar 16.



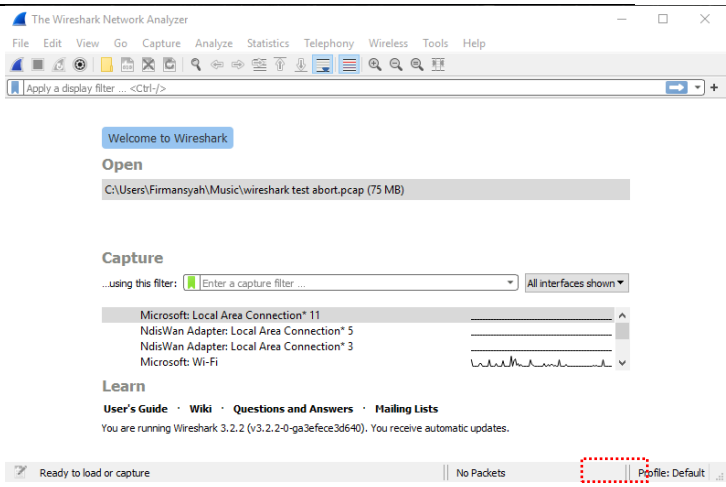
Gambar 16. Microsoft Network Monitor

Jika instalasi berhasil selanjutnya akan melakukan proses penangkapan lalu lintas jaringan dengan menekan tombol *New Capture.* Selanjutnya akan muncul jendela baru seperti pada Gambar 17.



Gambar 17. *New Capture*

Tombol *start* berfungsi untuk memulai proses perekaman paket lalu lintas yang berjalan, tombol *pause* untuk menghentikan sementara dan tombol *stop* akan menghentikan proses perekaman pertama. Pada barisan bawah terdapat sebuah informasi, penelitian ini fokus pada nilai *Captured*, karena sangat dibutuhkan untuk memvalidasi paket. Instalasi aplikasi Wireshark, jika berhasil dapat dilihat seperti pada Gambar 18.

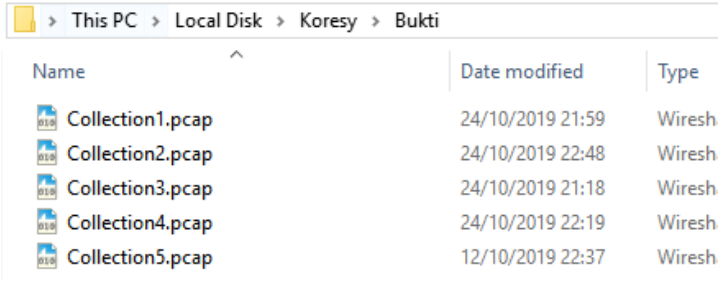


Gambar 18. Tampilan Aplikasi Wireshark

Alat forensik wireshark dapat digunakan sebagai alat rekam maupun alat analisis. Cara menjalankan Wireshark setelah proses instalasi selesai adalah dengan mengklik kanan aplikasi lalu kemudian pilih pada tombol Run Administrator, karena wireshark membutuhkan akses penuh pada jaringan. Terlihat pada gambar awal pada wireshark, tidak terdapat paket atau *no packets*, informasi ini sangat berguna untuk memvalidasi paket. Tahapan ini selanjutnya akan diteruskan dengan pemanfaatan kerangka kerja NIST.

3.3.1 Collection

Tahapan pengkoleksian paket merupakan proses awal dari kerangka kerja nist, yaitu dengan mengumpulkan paket-paket lalu lintas untuk kemudian diidentifikasi. Proses dimulainya pengkoleksian pada penelitian ini dilakukan saat ada penyerangan. Peneliti telah melakukan pengujian dan mendapatkan rekaman paket lalu lintas, dapat ditinjau pada gambar 19.

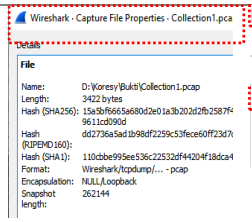
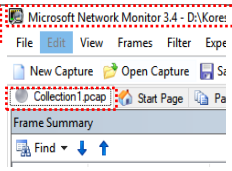
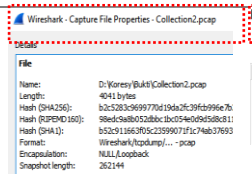
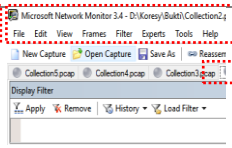
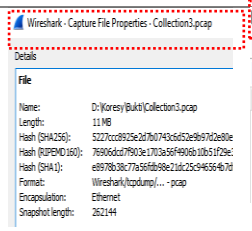
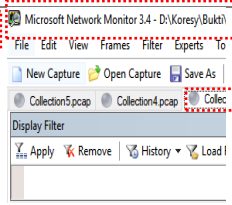
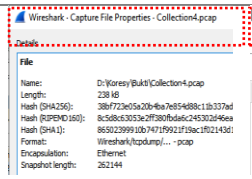
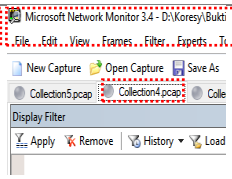
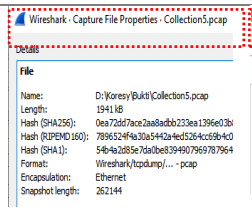
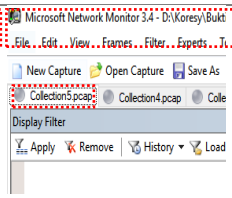


Gambar 19. Rekaman Paket

Bukti-bukti disimpan langsung pada memori laptop, kemudian untuk menjaga integritas bukti, saran dari NIST SP800-86, agar dilakukan pengkloningan, sehingga bukti dapat terjaga dengan aman. Pengkloningan tidak akan merubah nilai-nilai pada paket yang telah terekam. Memprioritaskan pengumpulan data jenis data yang banyak, maka dapat dikumpulkan dengan toolkit bergantung pada kebutuhan spesifik, jika diduga terjadi gangguan jaringan, mungkin akan berguna jika mengumpulkan informasi konfigurasi jaringan, koneksi jaringan, sesi login, dan proses yang berjalan untuk menentukan bagaimana seseorang

e-ISSN 3046-773X

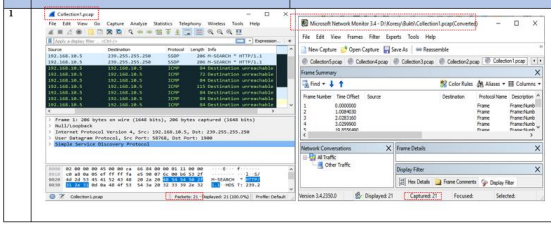
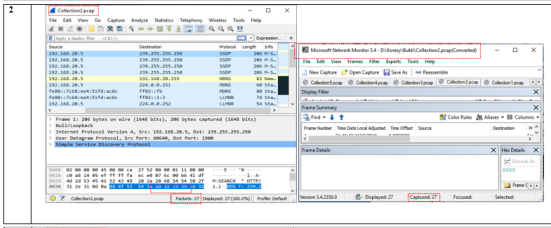
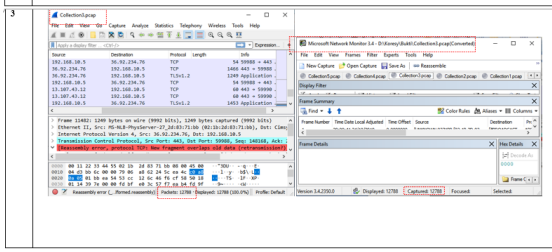
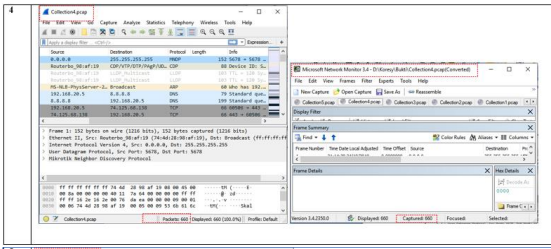
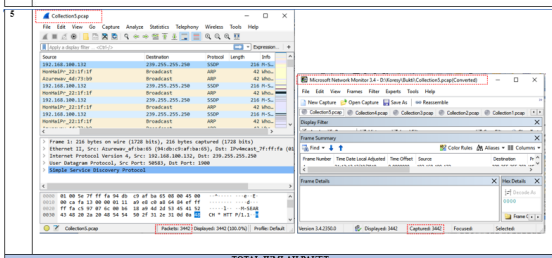
memperoleh akses ke sistem. Artinya akan kembali pada tujuan penelitian yang akan dicapai yaitu dapat merekonstruksi kejadian penyerangan, sesuai dengan perancangan serangan. Pemberian nama setiap rekaman sangat penting untuk memudahkan proses identifikasi selanjutnya dan sangat tidak mempengaruhi isi paket. Lebih jelas jika dilihat pada Tabel 3.

No	Alat Forensik		Keterangan
	Wireshark	Microsoft Network Monitor	
1			Collection1.Pcap Belum Valid
2			Collection2.Pcap Belum Valid
3			Collection3.Pcap Belum Valid
4			Collection4.Pcap Belum Valid
5			Collection5.Pcap Belum Valid

Tabel di atas menunjukan akan ada proses validasi setelah tahap koleksi berakhir. Sebelumnya telah dijelaskan bahwa informasi setiap alat foreksik akan ditemukan di bagian *captured* pada aplikasi *microsoft network monitor* dan bagian informasi *packet* pada *wireshark.* Tahap pada *table collection* di atas merupakan penunjukan paket yang berhasil direkam dan diberi nama *collection*1-5. Sampai pada tahap ini, proses dapat dilanjutkan.

3.3.2 Examination

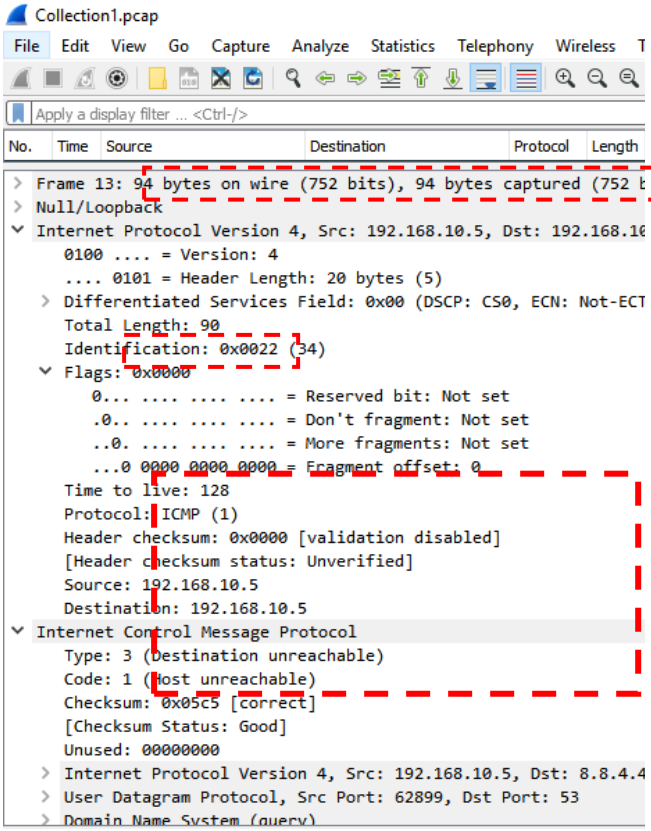
Tahap ini akan digunakan paket-paket yang telah dikoleksi. Pemeriksaan paket lalu lintas akan menghasilkan paket-paket yang valid, artinya dibutuhkan nilai-nilai setiap paket yang terkoleksi. Nilai paket berupa informasi jumlah paket yang berhasil ditangkap. Alat forensik akan berfungsi mencari nilai-nilai tersebut pada paket yang sama, misalnya pada paket *Colection*1, jika nilai informasi yang didapat tidak sama, dapat dipastikan paket tersebut tidak valid dan proses tidak dapat dilanjutkan, lebih jelas dapat dilihat pada Tabel 4.

NO	ALAT FORENSIK		KETERANGAN
	WIRESHARK	MICROSOFT NETWORK MONITOR	
1			JUMLAH PADA COLLECTION 1.PCAP 21 PAKET (VALID)
2			JUMLAH PADA COLLECTION2 .PCAP 27 PAKET (VALID)
3			JUMLAH PADA COLLECTION3 .PCAP 12788 PAKET (VALID)
4			JUMLAH PADA COLLECTION4 .PCAP 660 PAKET (VALID)
5			JUMLAH PADA COLLECTION5 .PCAP 3442 PAKET (VALID)
	TOTAL JUMLAH PAKET		16938 PAKET

3.3.3 Analysis

e-ISSN 3046-773X

Dalam banyak kasus, analisis forensik tidak hanya melibatkan data dari file, tetapi juga data dari sumber lain, seperti status OS, lalu lintas jaringan, atau aplikasi. Rekomendasi dari NIST SP 800-86 sangat banyak untuk mengupayakan analis forensic menjadi handal, salah satunya adalah *log* yang terkait dengan insiden keamanan komputer perlu disimpan untuk jangka waktu yang jauh lebih lama daripada log lainnya, agar dapat dipelajari lagi. Log aktifitas jaringan dapat menyimpan beberapa informasi yang sangat penting dalam mengungkap terjadinya ancaman atau serangan terhadap jaringan komputer. Lalu lintas jaringan dapat mengungkapkan tindakan kriminal dengan cara melihat kembali log, terlihat pada Gambar 19.



Gambar 19. *Wireshark Collection1.pcap*

Ditemukan pada *frame* 13, terdapat 94 *bytes* dalam 1(satu) *frame*, ini dapat diartikan sebagai lalu lintas penyerangan, karena melebihi dari kapasitas normal. Protokol yang diserang adalah *Internet Control Message Protocol (*ICMP) dengan tipe *destination unreachable* dank ode *host unreachable*. Jika dilihat pada alamat pada gambar, merupakan alamat milik dari klien dengan status *header* adalah *unverified*.

3.3.4 Report

Proses penyusunan dan penyajian informasi yang dihasilkan dari tahap analisis menjadi faktor yang memengaruhi pelaporan. Pembahasan penelitian ini mencakup protokol-protokol lalu lintas, dapat di lihat pada Tabel 5.

Tabel 5. *Report*

No	Tipe Informasi	Catatan
1.	Total jumlah paket.	16938 paket
2.	Bukti analisis.	Setiap bukti yang di peroleh akan diperiksa dan dianalisis menggunkan 2(dua) alat untuk perolehan yang valid
3.	Bukti *Collection*1.pcap, Wireshark mendeteksi aliran pada protokol ICMP, namun MNM hanya mendeteksi panjang paket.	Bukti masih dinyatakan belum valid, salah satu alat *forensic* tidak mendukung protokol.
4.	Bukti *Collection*2.pcap, Wireshark mendeteksi aliran pada protokol LLMNR, namun MNM hanya mendeteksi panjang paket.	Protokol ini dapat di non aktifkan, agar pihak penyerang tidak mendapatkan data.
5.	Bukti *Collection*3.pcap, Wireshark dan MNM mendeteksi aliran pada protokol TLS.	Penyerang menggunakan alamat 192.168.10.252 terdeteksi menggunakan perangkat SonyMobile dengan *Mac Address* 58:48:22:6e:17:e0.
6.	Bukti *Collection*4.pcap, Wireshark dan MNM mendeteksi aliran pada protokol ARP.	Penyerangan melakukan *broadcast* pada server vitual dengan menggunakan alamat Ip 192.168.20.253, sehingga terdeteksi sebagai Badai ARP.
7.	Bukti *Collection*5.pcap, Wireshark dan MNM mendeteksi aliran pada protokol TCP	Port 443 yang digunakan oleh klien memberikan kenyaman dalam berselancar internet.

IV. KESIMPULAN

Melihat dari hasil penelitian, Analisis Forensik Jaringan Virtual Router Menggunakan Framework Nist Sp800-86, berdasarkan rumusan masalah, tujuan penelitian dan hipotesis dapat disimpulkan bahwa, perancangan virtual router sangat dapat memberikan router tambahan jika hanya dimilki 1(router) saja yang memiliki fungsi dan manfaat yang sama,

e-ISSN 3046-773X

sehingga jelas memastikan dapat mengurangi biaya pembelian router. Dibutuhkan waktu yang singkat dalam proses analisis serangan DOS forensik jika memanfaatkan rancangan jaringan pada penelitian ini, terbukti dalam setiap protokol mendeteksi lalu lintas yang tidak biasa. Bukti diperoleh menggunakan kerangka kerja NIST SP800-86 dengan pemanfaatan dua(2) alat analisis jaringan dengan proses yang konsisten. Karakteristik bukti pada virtual router dalam penelitian ini, mendapatkan alamat penyerang dan alamat MAC perangkat yang digunakan.

DAFTAR PUSTAKA

[1] Achyani, Y. E. (2016). Keamanan Jaringan Dengan Packet Filtering Firewall (Studi Kasus: Pt. Sukses Berkat Mandiri Jakarta). *Jurnal Khatulistiwa Informatika*, *04*(May), 31–48.

[2] Dewi, E. K., Harini, D., & Miftachurohmah, N. (2017). Snort Ids Sebagai Tools Forensik Jaringan Universitas Nusantara Pgri Kediri. January, 411–418.

[3] Fadlil, A., Riadi, I., Aji, S., & Dahlan, U. A. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. 3(1).

[4] Firmansyah, F., Fadlil, A., & Umar, R. (2019). Analisis Forensik Virtual router pada Lalu Lintas Jaringan Klien. *Edu Komputika Journal*, *6*(2), 54–59. https://doi.org/10.15294/edukomputika.v6i2.35221

[5] Hafizh, M. N., Riadi, I., & Fadlil, A. (2020). Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic. *Jurnal Telekomunikasi Dan Komputer*, *10*(2), 111. https://doi.org/10.22441/incomtech.v10i2.8757

[6] Hariyadi, D., Wijayanto, H., & Sari, I. D. (2019). Analisis Barang Bukti Digital Aplikasi Paziim Pada Ponsel Cerdas Android Dengan Pendekatan Logical Acquisition. *Cybersecurity Dan Forensik Digital*, *2*(2), 1–5.

[7] Helmi, I., Widiyasono, N., & Gunawan, R. (2019). Simulasi Analisis Bukti Digital Pada Layanan Cloud Computing Menggunakan Metode NIST 800-86. *Jurnal Media Informatika Budidarma*, *3*(3), 217. https://doi.org/10.30865/mib.v3i3.1193

[8] Imam Riadi, Anton Yudhana, M. C. F. P. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ). 4, 219–227.

[9] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. *The National Institute of Standards and Technology*.

[10] Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Times*, *5*(2), 35–42. http://stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/viewFile/556/126

[11] Martias, & Djuanda, R. F. (2018). Pembatasan Jumlah Client Menggunakan Security MAC- Address with Cisco. *Transistor EI (Jurnal Elektro Dan Informatika) UNISSULA*, *3*(3). http://lppm-unissula.com/jurnal.unissula.ac.id/index.php/EI/article/view/3481

[12] Mustafa, Riadi, I., & Umar, R. (2018). Rancangan Investigasi Forensik E-mail dengan Metode National Institute of Standards and Technology (NIST). *Snst Ke-9*, *9*, 121–124.

[13] Pemerintah Indonesia. (2010). Peraturan Menteri Komunikasi Dan Informatika Nomor : 16 /Per/M.Kominfo/ 10 /2010. 1–5.

[14] Ridho, F., Yudhana, A., & Riadi, I. (2016). Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time. 2(1), 111–116. http://ars.ilkom.unsri.ac.id

[15] Siddharth Sachin Kulkarni. (2017). Routing Table Size Aware Dynamic Routing for Maximization of Throughput of an SDN. In *Project Submission Sheet – 2016/2017 School of Computing*.

[16] Supardi, W. (2012). *IP Address & Subnetting*. *1*, 1–9.

[17] Wicaksono, G., & Prayudi, Y. (2013). Teknik Forensika Audio Untuk Analisa Suara Pada Barang Bukti Digital. *Semnas Unjani*.

[18] Yogyantoro, F. S. (2015). Instalasi jaringan komputer pada dinas kesehatan puskesmas patihan kota madiun. *Teknik Informatika*, *21*(2), 1–17.

[19] Yudhana, A., Umar, R., & Ahmadi, A. (2019). Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method. *Scientific Journal of Informatics*, *6*(1), 54–63. https://doi.org/10.15294/sji.v6i1.17767