Edu Komputika 10 (2) (2023)

Edu Komputika Journal

http://journal.unnes.ac.id/sju/index.php/edukom

Evaluasi Optimalisasi Alat Forensik Keamanan Jaringan pada Lalu Lintas Virtual Router

Firmansyah[1)]✉, Abdul Fadlil[2),] dan Rusydi Umar[3)]

[1]Program Studi Ilmu Komputer, Fakultas Teknik, Universitas Islam Al-Azhar, Indonesia
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Indonesia
[3]Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan, Indonesia

Info Artikel

Sejarah Artikel:
Diterima: 2 Agustus 2023
Direvisi: 19 Juli 2024
Disetujui: 29 Juli 2024

Keywords:
Analysis Tools, Forensics, Metarouter, Network Traffic, Recording, Tools

Abstrak

Penelitian ini bertujuan untuk mengevaluasi optimalisasi alat forensik keamanan jaringan pada lalu lintas virtual router (VR). Metodologi yang digunakan meliputi pemilihan beberapa alat forensik pada sistem operasi *Windows* seperti *Wireshark*, *Windump*, dan *Network Miner*, dengan pengujian dalam lingkungan jaringan virtual. Pengujian, mencakup simulasi berbagai skenario serangan untuk menilai efektivitas deteksi ancaman, kinerja alat forensik, dan dampak terhadap kinerja jaringan. Hasil utama menunjukkan bahwa alat-alat tersebut memiliki kemampuan deteksi yang beragam dengan variasi penggunaan sumber daya dan dampak pada latensi jaringan. Lalu lintas jaringan telah berhasil di rekam menggunakan alat *Win-dump* pada metode static forensik, alat *Wireshark* dan *Network Miner* pada metode *live forensics*. Hasil evaluasi alat rekam forensik jaringan meta-router merekomendasikan *Win-dump* sebagai alat rekam yang tidak membebani sistem operasi *windows* dengan penggunaan *Memory* adalah 1696 kb sedangkan aplikasi *Wireshark* dan *Network Miner* tercatat lebih dari 20MB. Berdasarkan penelitian ini metode *static forensic* yang telah dibangun dengan objek meta-router dapat digunakan investigator untuk mendeteksi serangan siber. Pemilihan dan konfigurasi yang tepat dari alat forensik sangat penting untuk mencapai keseimbangan antara keamanan dan kinerja jaringan, serta penyesuaian spesifik terhadap kebutuhan jaringan dapat meningkatkan efektivitas deteksi dan mitigasi ancaman.

Abstract

This research aims to evaluate the optimization of network security forensic tools on virtual router (VR) traffic. The methodology used includes the selection of several forensic tools on the Windows operating system such as Wireshark, Windump, and Network Miner, with testing in a virtual network environment. Testing, includes simulating various attack scenarios to assess the effectiveness of threat detection, performance of forensic tools, and impact on network performance. The main results show that the tools have varying detection capabilities with variations in resource usage and impact on network latency. Network traffic has been successfully recorded using the Win-dump tool in the static-forensics method, the Wireshark tool and Network Miner in the live-forensics method. The evaluation results of the meta-router network forensic recording tool recommend Win-dump as a recording tool that does not burden the Windows operating system with memory usage of 1696 kb while the Wireshark and Network Miner applications are recorded at more than 20MB. Based on this research, the static forensic method which have been built with meta-router objects can be used by investigators to detect cyber attacks. Proper selection and configuration of forensic tools is critical to achieving a balance between security and network performance, and specific adjustments to network requirements can increase the effectiveness of threat detection and mitigation.

✉ Alamat korespondensi:
Gedung Lantai 2, Fakultas Teknik, Universitas Islam Al-Azhar
Sandubaya, Kota Mataram, Nusa Tenggara Barat. 83232
E-mail: firmanyasin@gmail.com

ISSN 2252-6811
E-ISSN 2599-297X

PENDAHULUAN

Kemajuan teknologi virtualisasi jaringan telah membawa manfaat signifikan bagi infrastruktur TI, memungkinkan pengelolaan yang lebih fleksibel dan efisien. Namun, di sisi lain, kompleksitas yang meningkat juga menciptakan tantangan baru dalam hal keamanan jaringan. Salah satu aspek kritis adalah perlindungan terhadap ancaman siber yang terus berkembang dan semakin canggih. Untuk menghadapi tantangan ini, penggunaan alat forensik keamanan jaringan menjadi sangat penting dalam mendeteksi, menganalisis, dan merespons ancaman pada lalu lintas virtual router (VR). Fenomena takut untuk mengeluarkan biaya operasional bagi penyedia jasa keamanan dan forensik jaringan adalah hal yang lumrah, namun di saat sudah terjadi pencurian data, tidak takut untuk mengeluarkan biaya yang bahkan akan lebih besar (Phillips, 2016).

Meskipun berbagai alat forensik telah dikembangkan dan digunakan secara luas, efektivitas dan optimalisasi dalam lingkungan jaringan virtual masih belum dipahami sepenuhnya. Banyak organisasi yang menghadapi kesulitan dalam memilih dan mengonfigurasi alat forensik yang paling sesuai untuk kebutuhan spesifik, terutama dalam lingkungan virtual yang kompleks. Selain itu, penggunaan alat forensik dapat menambah beban pada kinerja jaringan, yang dapat mempengaruhi pengalaman pengguna dan operasi bisnis. Penelitian ini berfokus pada evaluasi optimalisasi alat forensik keamanan jaringan pada lalu lintas virtual router, dengan tujuan untuk mengidentifikasi alat yang paling efektif dan metode optimisasi yang dapat diterapkan untuk meningkatkan keamanan tanpa mengorbankan kinerja jaringan.

Peraturan Menteri (Permen) No 20 Tahun 2016 tentang Perlindungan Data Pribadi (PDP) yang ditetapkan 7 November 2016, diundangkan dan berlaku sejak 1 Desember 2016 (Menteri, 2016). Dalam proses amandemen UU ini, anggota DPR mengusulkan agar Indonesia juga mengadopsi konsep *right to be forgotten*. Usulan ini kemudian diakomodasi dalam Pasal 26 ayat (3) UU No. 19/2016 tentang Perubahan UU No. 11/2008 tentang ITE, yang menyatakan: dalam artikelnya Lanskap, Urgensi, dan Kebutuhan Pembaruan. "Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/ atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendali nya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan" (Djafar, 2019)

(Aji dkk., 2017), pada artikel Analisis Forensik Jaringan. Ilmu pengetahuan tentang keamanan komputer yang terkait dengan penyelidikan untuk menentukan sumber serangan jaringan berdasarkan data log bukti, identifikasi, analisis, dan rekonstruksi kejadian adalah Forensik Jaringan yang merupakan cabang dari Forensik Digital.

(Albert & Juni, 2015), pada penelitian pengaman data jaringan mengemukakan, banyak sekali perusahaan yang memiliki cabang dengan menggunakan jasa teknologi internet yang ditawarkan provider internet dengan berbagai jenis dan harga bervariasi guna memenuhi kebutuhan layanan komunikasi perusahaan. Namun, banyak yang memanfaatkan dial-up private dari cabang ke pusat. Sistem ini akan mengeluarkan biaya besar setiap koneksi nya.

(Alim dkk., 2018) menggunakan metode *live forensics* untuk menarik data forensik sebagai bukti digital serangan di jaringan Router.

(Chaudhary dkk., 2017) Virtualisasi dan *cloud computing* sudah menjadi tren teknologi informasi khususnya dan bermanfaat bagi perusahaan skala enterprise.

(Contoli, 2017) pada *Virtualized Network Infrastructures*, memberikan pedoman untuk memutuskan nilai keterlambatan jaringan maksimum yang dapat ditoleransi ketika kondisi kenaikan biaya jaringan yang diizinkan diberikan. Menyajikan wawasan tentang beberapa aspek virtualisasi jaringan, yang membahas analisis, desain, dan implementasi, namun tidak membahas mengenai *virtual network forensics*.

(Dewi dkk., 2017) *Tools Forensik* Jaringan yang bisa dimanfaatkan untuk Forensik Jaringan adalah Snort, log yang tersimpan di database berfungsi sebagai alat bukti pelaporan, namun tidak mengevaluasi alat tersebut.

(F. F. A. Firmansyah & Umar, 2019) pada artikel analisis forensik lalu lintas meta-router, berguna dengan tujuan memecah jaringan. Jika router yang dimiliki hanya 1 (satu) unit maka dapat memiliki router beberapa router virtual dengan fungsi yang sama dengan router fisik sehingga berguna sesuai dengan keinginan klien walau hanya sebuah virtual router.

(Faiz dkk., 2016) Menjelaskan bahwa analisis digital dengan metode live forensik dapat dibagi menjadi dua, yaitu tradisional dan modern. Analisis forensik adalah analisis data sementara yang disimpan pada perangkat atau dikirimkan secara online. Artikel ini membahas tentang analisis forensik sistem operasi terbaru yaitu Windows 10.

Penelitian terpenting tentang virtualisasi dilakukan oleh (Galang dkk., 2017), yang menerapkan teknik router menggunakan Meta-Router. Skenario sering terjadi di kalangan pengguna setiap hari untuk mengakses jaringan

internet dari router. Pada analisis hasil, berbagai jenis data Internet Protocol yang mengakses, apa yang diakses, kapan pengguna mengakses, dan di mana pengguna mengakses.

Kemudian perbandingan aliran data router sebelum dan sesudah jaringan terputus (Hildayanti, 2019), menyebutkan bahwa setiap aliran paket data yang masuk ataupun yang keluar sangat dapat untuk diidentifikasi.

Evaluasi efek dari keterlambatan jaringan maksimum yang dapat ditoleransi pada pedoman untuk alokasi fungsi virtual router, yang meminimalkan total biaya jaringan. Poin-poin dari evaluasi kuantitatif. adalah semakin pendek penundaan jaringan maksimum yang dapat ditoleransi, semakin besar jumlah area di mana fungsi routing harus di alokasikan (Kuribayashi, 2018).

Parameter SMB melalui TCP Port: 445 dengan nama NetBIOS digantikan oleh DNS. Lapisan ini yang mendasarinya menangani keandalan koneksi (Satran, 2018), penelitian ini berfokus pada pergantian protokol pada jaringan.

Penelitian terhadap bukti tindak kriminal, telah dilakukan oleh (Mandowen, 2016) (Sunaringtyas & Prayoga, 2021), yang menganalisis dan melaporkan konten file yang diambil pada jaringan (nitroba.pcap.zip), merupakan arsip yang berisi kegiatan berbasis jaringan yang dipantau dan dicatat dalam jaringan Universitas Nitroba menggunakan alat forensik jaringan yang disebut Wireshark.

Virtualisasi jaringan telah muncul sebagai solusi yang menjanjikan yang dapat memanfaatkan dan mengelola sumber daya jaringan secara sederhana, fleksibel, dan efektif. Dalam virtualisasi jaringan, beberapa jaringan virtual dengan topologi spesifik dan persyaratan sumber daya dapat dibangun melalui jaringan fisik (Nassar & Tachibana, 2018).

Pemrograman JAVA digunakan untuk interface pengiriman tanda bahaya pada IDS yang akan dikirimkan melalui telepon genggam melewati pesan, sehingga membantu pengelola jaringan untuk tetap siaga walaupun tidak pada lokasi server (Akremi dkk., 2018).

Meta-Router Memungkinkan untuk melakukan perlindungan data dan pemulihan data pada satu kartu router meskipun ada banyak klien. Mengatasi kerusakan akibat serangan yang tidak diinginkan, mencegah serangan atau memblokir akses informasi pribadi adalah salah satunya. (Riadi, 2018).

Penelitian selanjutnya dilakukan oleh (Mubaraq, 2019), yang menganalisis proses untuk menentukan alur lalu lintas yang melewati proses penyaringan menggunakan firewall, desain untuk mendapatkan cara yang paling efektif dan efisien mengimplementasikan router, serta pengujian yang dilakukan dengan metode stress test. Paket yang tidak dikenali dapat meningkatkan jumlah akses pengguna sehingga dapat terjadi sebuah serangan dari pihak lain terhadap jaringan tersebut (Riadi dkk., 2019).

Bukti analisis forensik digital pada media penyimpanan utama yaitu SSD pada kondisi sistem komputer yang terinstal software pembeku memori dilakukan dengan metode pengambilan data secara statis serta analisa forensik dengan metode National Institute of Standars and Technology (NIST) untuk memperoleh bukti digital (Riadi dkk., 2017).

Bagi peretas, rover berperan penting dalam melancarkan serangan untuk mendapatkan akses ke sistem host atau pusat data tempat melakukan kejahatan. Kontrol penuh atas router berarti jaringan lain yang terhubung ke router juga dapat dikontrol (Ridho dkk., 2016).

Skenario static routing dapat menggunakan dua unit meta-router dalam satu router-board. Setiap interface pada router virtual dibuat secara manual sesuai dengan kebutuhan dan pengujian antar virtual router, dapat menggunakan masing-masing terminal (Towidjojo & Herman, 2016). Penelitian ini difokuskan dalam tahapan pemeriksaan. Pemeriksaan selanjutnya dijabarkan dalam beberapa tahap (Umar, Riadi, & Muthohirin, 2018) identifikasi yang dibuat untuk menemukan data atau informasi yang akan diambil dan mungkin menghasilkan bukti untuk membantu proses penyelidikan (Sholikhatin dkk., 2023).

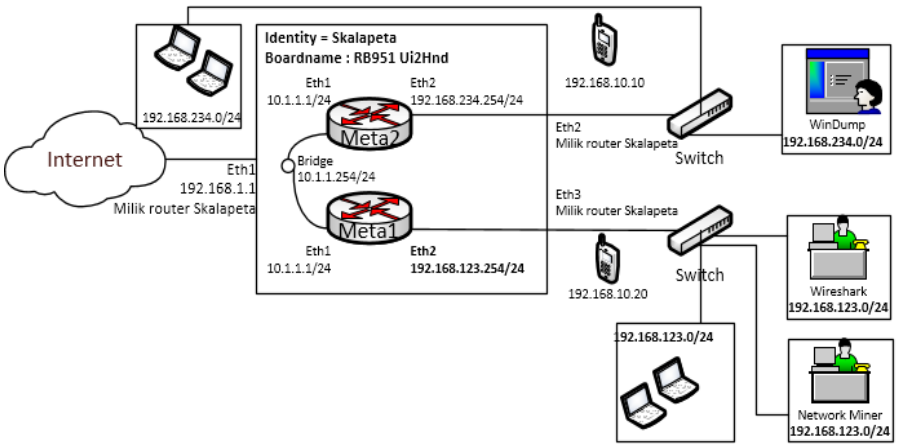
Penelitian terbaru tentang evaluasi selanjutnya, bereksperimen menggunakan alat forensik dengan metode forensik NIST untuk mengekstraksi artefak WhatsApp terbaru, dengan mengevaluasi alat Mobile Forensics (Umar, Riadi, & Zamroni, 2018), namun bukan pada alat forensik lalu lintas jaringan. Badai ARP adalah situasi serangan yang sengaja dibuat oleh penyerang dari dalam jaringan lokal. Penelitian tentang ARP Strom telah dilakukan oleh (F. Firmansyah dkk., 2021).

Hasil analisis kinerja alat forensik dan bukti digital di Facebook Messenger dalam proses akuisisi adalah menggunakan metode National Institute of Standards and Technology (NIST) (Yudhana dkk., 2018). Hasil kejahatan umumnya disembunyikan di media penyimpanan untuk dipergunakan dalam pencurian, pengintaian, bullying, terorisme, dan penipuan (Yuwono dkk., 2019), penelitian yang membandingkan software file carving. Penelitian mengenai evaluasi juga dilakukan oleh (Du dkk., 2017), namun yang dievaluasi adalah kerangka kerja forensik digital, bukan alat forensik digital.

Berdasarkan uraian di atas, tujuan penelitian ini adalah membangun arsitektur forensik jaringan virtual router dengan mengevaluasi alat rekaman paket dan kinerja 3 (tiga) alat forensik jaringan berbasis sistem operasi windows yaitu Wireshark, Network Miner, dan Win-dump dengan kerangka kerja NIST yang berjalan pada perangkat keras secara gratis. National Institute of Standards and Technology (NIST) adalah Departemen Perdagangan Amerika Serikat yang mempunyai keahlian dan kemampuan unik, seperti mengeluarkan pedoman kerja dalam kebijakan dan standar untuk memastikan setiap pemeriksa mengikuti alur kerja yang sama sehingga pekerjaan mereka didokumentasikan dan hasilnya dapat diulang dan dipertahankan.

METODE PENELITIAN

Proses penelitian utama yaitu penggunaan Virtual Router sebagai alat untuk menghemat pembelian alat fisik atau alat sesungguhnya jika harus membeli. Virtual Router akan di tempatkan pada router utama dari sebuah jaringan atau titik tengah pada sebuah kantor, sedangkan pelanggan atau klien akan ditempatkan pada masing-masing meta-router dengan bantuan perangkat switch. Topologi yang digunakan pada skenario ini dapat di lihat pada Gambar 1.



Gambar 1. Topologi yang digunakan

Penerapan meta-router pada skenario nyata maupun untuk simulasi, sebaiknya menentukan topologi jaringan meta-router dan rancangan interface agar meta-router siap untuk menerima konfigurasi sesuai dengan skenario yang diinginkan. Meta-router yang dibuat pada aplikasi winbox, belum mempunyai interface, sehingga langkah ini sangat penting untuk diingat. Meta-router yang akan dibuat sebanyak 2 (dua) unit virtual router, masing-masing akan diberi nama Meta1 dan Meta2, sedangkan router asli diberi nama Skala-peta. Konfigurasi dapat dilakukan dengan cara menggunakan Command Line Interpreter (CLI) atau sering disebut console yang terdapat pada aplikasi winbox. Mengakses meta-router menggunakan CLI akan terlihat lebih rumit untuk pemula jika di bandingkan dengan mengakses menggunakan Graphical User Interface (GUI). Router Utama dengan nama Skalapeta, menjalankan 2 (dua) buah router virtual dengan akses internet melalui interface eth1, yang kemudian disalurkan kepada masing-masing virtual router yaitu Meta1 dan Meta2. Kedua router virtual tersebut saling terhubung dengan menggunakan teknik static bridge pada masing-masing interface eth1 virtual router dan juga dapat menjalin komunikasi dengan perangkat di luar menggunakan switch pada setiap interface yang dibangun. Percobaan akan dilakukan dengan menanam aplikasi rekam paket Windump pada salah satu router virtual, misalnya Meta 2 dengan bantuan perangkat switch, namun tidak menutup kemungkinan, akan menghasilkan data yang sama, jika aplikasi rekam paket ditanam pada router virtual Meta 1, begitupun juga berlaku pada alat analisis paket Wireshark dan Network Miner. Perangkat smartphone sebagai penyerang, akan menggunakan alamat yang diberikan dari router fisik yaitu 192.168.10.0/24. 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 investigasi materi yang ditemukan pada perangkat digital. Model proses evaluasi forensik yang digunakan oleh peneliti ditunjukkan pada Gambar 2.

Gambar 2. Alur penelitian

Analisis dan kebutuhan penelitian, memahami jenis ancaman yang umum terjadi pada jaringan virtual dengan tujuan menentukan alat forensik yang mampu mendeteksi, identifikasi ancaman utama, merespons ancaman-ancaman dan menetapkan tujuan deteksi dan respon alat forensik. Alur pengaturan meta-router akan merancang topologi jaringan virtual yang mencakup meta-router untuk mengatur hubungan antara router virtual, server, dan alat forensik. Alur pengujian yaitu menyiapkan lingkungan pengujian dengan beberapa virtual router dan alat forensik untuk melakukan simulasi skenario serangan dan mengevaluasi hasil pengujian. Selanjutnya pada alur alat forensik jaringan berfungsi untuk memastikan alat forensik dapat menangkap dan menganalisis lalu lintas jaringan. Untuk mengevaluasi alat forensik, sangat penting untuk menyusun laporan kinerja dan memberikan rekomendasi untuk peningkatan lebih lanjut. Pengalokasian IP address dapat dilihat pada Tabel 1.

Tabel 1. Konfigurasi Alamat Perangkat

No	Perangkat	IP Address
1	Meta1	192.168.123.254/24
2	Meta2	192.168.234.254/24
3	Laptop1 Meta1	192.168.123.100
4	Laptop2 Meta2	192.168.234.100
5	Smartphone1	192.168.10.10
6	Smartphone2	192.168.10.20

Tahapan pengujian dan analisis merupakan tahapan akhir untuk menguji sistem yang dibuat. Langkah ini akan mengungkapkan adanya serangan yang terjadi pada sistem yang dibuat, melalui proses *Sniffing, Collection, Examination, Analysis dan Report* dapat di tinjau pada Gambar 3.

Gambar 3. Alur pengujian dan analisis

Alur pengujian di atas merupakan bagian dari *framework National Institute of Standards and Technology* (NIST) (Sachowski, 2018), yang peneliti modifikasi dengan menambahkan proses *sniffing* agar tercipta alur yang dapat dimengerti. Tahapan *sniffing* ini merupakan proses rekam semua paket yang melewati jaringan pada alamat yang telah ditentukan dengan menggunakan alat forensik windump. *Collection* adalah tahapan pertama dari proses digital forensik dengan metode NIST, yang melibatkan identifikasi, analisis, dan memperoleh data dari sumber yang relevan, sementara mengikuti pedoman dan prosedur untuk menjaga integritas data. Tahapan ini, akan mengumpulkan data-data yang diperoleh dari rekaman paket data dan pengamatan lalu lintas secara langsung pada jaringan meta-router. *Examination* adalah proses yang melibatkan penilaian data yang diperoleh dari tahap pengumpulan dan penggalian data yang relevan. Pada langkah ini, paket yang dikumpulkan akan di sortir sehingga dapat digunakan sebagai bukti. Setelah ditentukan, paket akan diambil dan proses pengambilan data akan diuji secara forensik yang artinya paket akan dianalisis guna pencarian bukti yang valid. Tahapan *Analysis* adalah data yang telah diambil akan dianalisis untuk mencari hal-hal yang dapat digunakan sebagai bukti, terkhusus jaringan komputer sehingga akan menjadi bukti yang valid. Bukti pada analisis jaringan pada umumnya adalah *Internet Protocol* (IP) *Address*. *Reporting* adalah tahap akhir sebelum proses evaluasi dari langkah forensik lalu lintas meta-router yang melaporkan aktivitas forensik dari awal hingga akhir bersama dengan hasil analisis ke dalam bentuk laporan tertulis. Akhir dari alur penelitian ini selanjutnya melakukan evaluasi alat forensik jaringan yaitu setiap alat forensik akan dianalisis penggunaannya dalam setiap pengoprasian forensik dengan menggunakan alat Task Manager pada windows, dengan membandingkan penggunaan memori pada setiap alat forensik jaringan.

A. Objek Penelitian

Objek penelitian berkaitan tentang Network Forensic Meta-router untuk antisipasi tindak kriminal pada lalu lintas jaringan di dunia maya seperti *cyber crime*, dengan menggunakan perspektif alat forensik jaringan untuk mengkaji bagaimana sifat, kinerja dan waktu untuk membantu memilih akuisisi data yang tepat. Penyidik forensik digital harus mengikuti hukum dan peraturan di negara tempat mereka bekerja. Uji coba untuk alat forensik jaringan dapat dikategorikan menjadi 2(dua), yaitu kategori alat rekam dan kategori alat analisis. Setiap objek yang berjalan pada OS akan dipantau melalui *task manager* pada sistem windows untuk mengetahui penggunaan CPU, Memory dan Disk pada OS yang berjalan, dapat dilihat pada Tabel 2.

Tabel 2. Kategori Alat Rekam Forensik

No	Alat Rekam Forensik	Proses		
1	Windump	CPU	Memory	Disk
2	Wireshark	CPU	Memory	Disk
3	Network Miner	CPU	Memory	Disk

Setiap alat rekam forensik akan dijalankan sampai pada proses rekaman, setelah itu akan dipantau melalui aplikasi task manager pada windows sehingga akan tampak proses CPU, Memory dan Disk yang diperlukan untuk setiap alat rekam forensik. Penelitian ini juga akan melakukan percobaan pada host, protocol, Time Display Format dan statistic dari masing-masing alat analisis forensik jaringan, dapat dilihat pada Tabel 3.

Tabel 3. Kategori Alat Analisis Forensik

Alat Forensik	Host	Protocol	Time Display Format	Statistik	
				I/O	Length
Wireshark	Deteksi	Jumlah	Format zona?	Grafik	Paket
Network Miner	Deteksi	Jumlah	Format zona?	Grafik	Paket

Analisis pada *host* adalah bagian penting untuk menemukan perangkat lain yang terhubung pada jaringan komputer, masing-masing host akan melewati tahapan evaluasi deteksi *host*, jika alat forensik tidak mendeteksi *host* maka dapat disebut sebagai kekurangan dari alat tersebut. *Protocol* merupakan sistem peraturan yang memungkinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua komputer atau lebih, sehingga perlu untuk di analisis jumlah masing-masing alat forensik. Aturan ini harus dipenuhi oleh pengirim dan penerima agar komunikasi dapat berlangsung dengan baik. *Time Display Format* merupakan tipe data tanggal dan waktu yang memiliki beragam format untuk membantu memenuhi keadaan unik di setiap kejadian menurut zona waktu yang diinginkan. Statistic adalah kumpulan data dalam bentuk angka maupun bukan angka yang disusun dalam bentuk paket (daftar) dan atau grafik yang menggambarkan atau berkaitan dengan suatu masalah, hal ini sangat penting untuk diamati dan di evaluasi pada masing-masing alat forensik.

Tabel 4. Alat dan Bahan Penelitian

No	Alat dan Bahan	Deskripsi	Keterangan
1	Mikrotik RB951Ui-2HnD	RouterOS versi 6	Router Fisik
2	Modem ADSL	ZTE dan Huawei	Switch
3	Notebook	Prosesor Intel Core i5	Perangkat keras analisis/investigator
4	Netbook	Prosesor intel Centrino	Perangkat keras rekam paket
5	Smartphone	Sony Z5 dan Sony C3	Perangkat Penyerang
6	Winbox	v3.19	Antar muka router
7	Termux	Android	Alat penyerang
8	Microsoft Windows 10	Windows 10 Pro File sistem NTFS	Perangkat lunak sistem operasi
9	Microsoft Windows 7	Windows 7 Ultimate File sistem NTFS	Perankat lunak sistem operasi
10	*Task Managar*	Microsoft Windows	Terdapat pada Sistem Operasi Microsoft Windows
11	Windum	Berjalan pada Windows 95, 98, ME, NT, 2000, XP, 2003, Vista dan 2007	Alat rekam yang akan diinstal pada Microsoft Windows 7
12	Network Miner	*Live sniffing* dan *Static Forensic*	Alat akan diinstal pada Microsoft Windows 10
13	Wireshark	*Live sniffing* dan *Static Forensic*	Alat analisis paket akan diinstal pada Microsoft Windows 10

B. Persiapan Alat dan Bahan

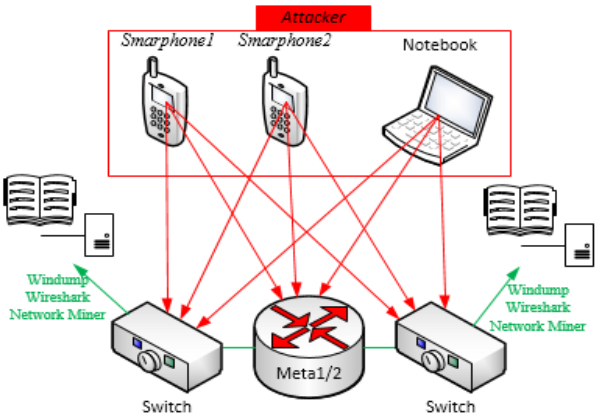
Alat dan bahan yang diperlukan untuk menunjang penelitian ini dapat dilihat seperti pada Tabel 4.

HASIL DAN PEMBAHASAN

Bagian ini menjelaskan hasil penelitian berdasarkan desain dan tujuan penelitian, seperti membangun jaringan meta-router jaringan dan situs forensik yang dibuat dengan alat router, menganalisis sumber daya, dan mengevaluasi hasil alat analisis jaringan pada tahap laporan pengujian forensik.

A. Analisis dan Kebutuhan

Persyaratan dasar analisis yang dilakukan pada penelitian ini adalah penggunaan Sistem Operasi Router sebagai perangkat keras yang akan dikloning dan alat analisis paket yang berjalan pada router virtual. Perkembangan teknologi jaringan telah bergerak naik secara signifikan terkhusus memanfaatkan teknologi virtual, sehingga forensik pada virtual router sangat dibutuhkan. Pada penelitian ini digunakan software manajemen Mikrotik RouterOs, software Wireshark, software Winbox seperti Network Miner dan Windump digunakan sebagai alat forensik, dan software Task Manager digunakan sebagai alat diagnostik untuk masing-masing alat forensik. Buat router meta di RouterBoard di mana beberapa router diinstal dan sistem operasi berjalan pada satu RouterBoard. Selain itu kinerja penelitian ini juga digunakan untuk traffic forensik sebanyak paket pada manajemen router yang terdiri dari banyak paket. router memberikan sinyal paket yang baik, ekonomis dan mudah ditemukan dalam *network forensics*. Faktor penyerangan dan penyadapan dapat dilihat pada Gambar 4.



Gambar 4. Faktor serangan dan penyadapan

Terdapat 1(satu) server meta yang dianggap memiliki fungsi yang sama dengan server meta lainnya sebagai virtual router. Perangkat switch akan memberikan alamat untuk aplikasi windump sebagai alamat penyadapan bukti lalu lintas paket. *Notebook* dan *Smartphone* berfungsi sebagai penyerang, yang akan menyerang perangkat virtual router maupun perangkat switch. Paket-paket akan datang melalui switch dan akan direkam oleh *detection engine* yang sudah terinstall *Windump*. Paket tersebut akan diperiksa dan ditangkap oleh aplikasi windump selama itu di aktifkan. Ketika paket tersebut mengandung konten serangan maka akan tersimpan di rekaman paket Windump dengan kata lain proses ini menggunakan metode *static forensic*.

B. Pengaturan Meta-router

Alamat IP meta-router untuk masing-masing akan digunakan sebagai alamat rekam paket lalu lintas jaringan pada *real scenario* sampai pada tahap akhir yaitu terciptanya rancangan forensik jaringan virtual router menggunakan meta-router dengan memanfaatkan 3 (tiga) alat forensik paket data yang bergerak pada jaringan.

C. Pengujian Alat Rekam Paket Lalu Lintas

Setelah tahapan instalasi berhasil dilakukan, maka selanjutnya menguji kinerja dari masing -masing alat forensik. Perbandingan akan meliputi waktu dan hasil rekam paket. Waktu yang akan digunakan pada masing-masing alat rekam adalah maksimal 1(satu) jam. Hasil rekam paket dapat meliputi protokol maupun kelengkapan penunjang dari masing-masing alat forensik. WinDump mencetak nilai paket dari

hasil *sniffing* pada jaringan sesuai dengan ekspresi yang diinginkan dengan beberapa pengaturan. WinDump dapat dijalankan dengan parameter -w, yang menyimpan paket ke file untuk selanjutnya di analisis, dan parameter -r, yang akan membaca paket yang disimpan dari hasil rekam paket yang berhasil di *sniffing* pada jaringan. Tahapan untuk menghentikan paket yang berjalan yaitu hanya dengan menekan tombol kontrol C. Pengujian selanjutnya pada alat rekam Wireshark dengan menggunakan skenario serangan yang sama. Wireshark mempunyai keunikan sebagai alat forensik jaringan, karena memiliki fungsi sebagai alat rekam dan analisis paket lalu lintas. Hasil rekam paket lalu lintas yang berhasil di *sniff*, selanjutnya dikoleksi. Fokus pengujian bahwa bukti telah diidentifikasi sesuai dengan data awal.

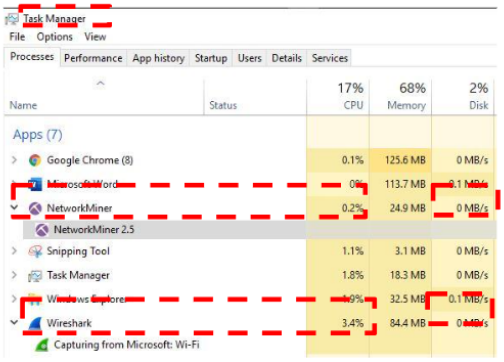
D. Analisis Alat Forensik Jaringan

Terdapat alamat host yang berhasil direkam oleh Network Miner serta identitas-identitas pemilik alamat. Alamat-alamat tersebut dapat dianalisis kembali, apakah benar dan sesuai dengan tangkapan dari aplikasi *wireshark*, agar dapat melakukan verifikasi kembali terhadap bukti yang di temukan. Program aktivitas jaringan dapat menyimpan informasi penting sekaligus mengungkap ancaman atau serangan terhadap jaringan komputer. Sebagai alat perekam, hasil Wireshark kemudian dianalisis untuk mencari lalu lintas yang tidak biasa. Protokol ICMP menunjukkan bahwa serangan tersebut sangat merusak hingga ke titik akhir dan terdapat kolom informasi bahwa *Destination Unreachable*.

Jika transmisi ulang terdeteksi dalam koneksi TCP, logis untuk mengasumsikan bahwa *packet loss* telah terjadi pada jaringan antara klien dan server. Tahap pengumpulan, pengambilan data dan analisis dilakukan sesuai metode, tahap terakhir adalah pembuatan bukti forensik di meta-router pada lalu lintas jaringan, namun hal ini tidak dijelaskan dalam dokumen ini karena hanya akan menampilkan hasil evaluasi materi alat forensik.

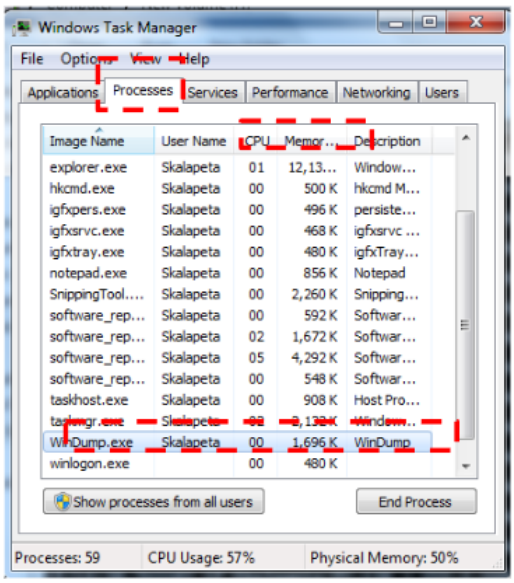
E. Evaluasi Alat Forensik Jaringan

Perbedaan penggunaan aplikasi dapat terlihat pada proses monitor yang berjalan pada Task Manager dengan cara menekan CTRL+SHIFTH+ESCAPE atau dapat menggunakan cara klik kanan pada task bar lalu pilih *task manager*, tunggu sementara aplikasi akan terbuka. dapat dilihat pada Gambar 5.



Gambar 5. Task Manager Windows 10

Task Manager pada fitur Windows memberikan detail tentang program dan proses yang berjalan di komputer. Aplikasi ini juga menampilkan ukuran kinerja yang paling umum digunakan untuk proses. Menggunakan *Task Manager* dapat memberi detail tentang program penggunaan saat ini, dan melihat program mana yang berhenti merespons. Terlihat pada menu proses, aplikasi yang berjalan pada Windows 10 dengan keterangan penggunaan CPU, *Memory* dan *Disk*, berbeda dengan Windows 7, menu proses yang ditampilkan tidak dikategorikan setiap aplikasi yang berjalan, seperti pada Gambar 6.



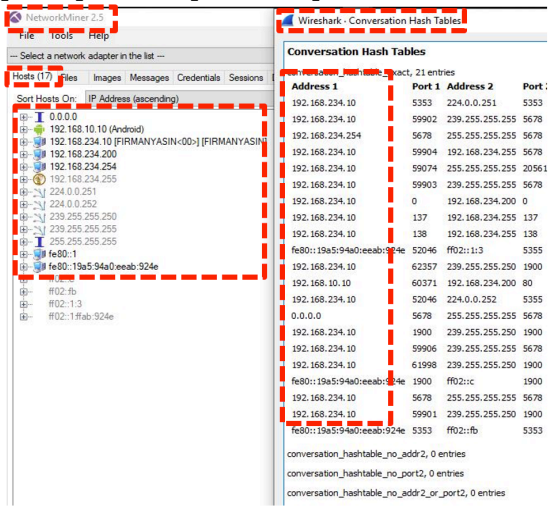
Gambar 6. Task Manager Windows 7

Menu proses menunjukkan daftar proses yang berjalan pada sistem operasi untuk melihat persentase atau nilai yang tepat untuk memori, disk, dan CPU, dengan kata lain, dapat memilih apakah ingin melihat jumlah memori yang tepat dalam MB atau persentase yang digunakan aplikasi memori sistem, lebih jelas pada Tabel 5.

Tabel 5. Evaluasi Alat Rekam Forensik Jaringan

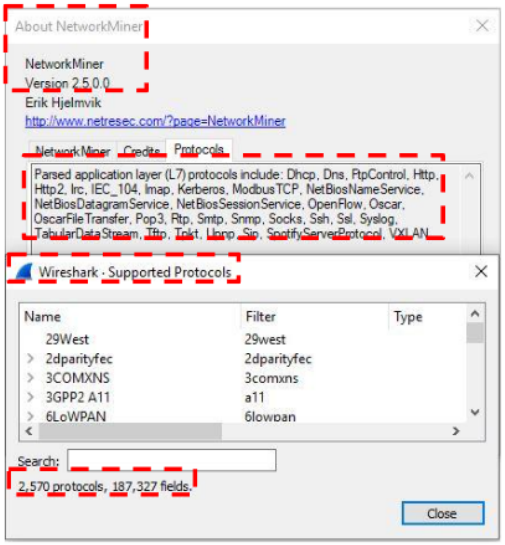
Alat Forensik	CPU	*Memory*	*Disk*
Windump	0 %	1696 Kb	0 Mb/s
Network Miner	0.2 %	24.9 Mb	0 Mb/s
Wireshark	3.4 %	84.4 Mb	0 Mb/s

Hasil dari tabel 5 adalah menjelaskan penggunaan CPU, *Memory* dan *Disk* pada setiap alat forensik windump, network miner dan wireshark. Evaluasi alat rekam forensik jaringan menggunakan meta-router, merekomendasikan Windump sebagai alat rekam yang tidak membebani sistem operasi windows dengan rincian penggunaan CPU, *Memory* dan *Disk* berturut-turut adalah 0%, 1696 kb dan 0 MB/s sedangkan aplikasi Wireshark dan Network Miner tercatat >20MB menggunakan memory. Evaluasi bagi kemajuan setiap disiplin rekayasa dan pengujian perangkat lunak selalu menjadi fundamental (Kävrestad, 2018), mendefinisikan tujuh metrik untuk mengevaluasi alat forensik yaitu Kecepatan absolut, Kecepatan relatif, Akurasi, Kelengkapan, Keandalan, Kemampuan audit, Kemampuan pengulangan, namun tidak memberikan definisi detail atau contoh tabel yang benar. Temuan ini menyoroti pentingnya memilih alat forensik yang tepat berdasarkan kebutuhan spesifik jaringan. Melihat dari hasil-hasil bukti yang ditemukan serta dianalisis, maka diperoleh perbedaan dan persamaan atau kekurangan maupun kelebihan yang terdapat pada aplikasi, dapat dilihat pada Gambar 7.



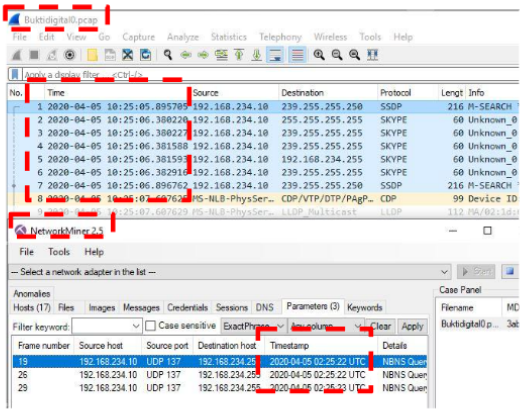
Gambar 7. *Host*

Masing-masing alat analisis memperlihatkan tangkapan yang sama yaitu tangkapan host, sangat bagus pada Network Miner jika ingin mengetahui nama host yang dimiliki oleh alamat IP karena tidak hanya mengandalkan lalu lintas DNS yang diambil untuk melakukan resolusi nama host pasif. Gambar 8 menunjukan jumlah protokol yang di support.



Gambar 8. Protokol

Protokol memiliki banyak fungsi dalam jaringan komputer. Tidak semua protokol mempunyai fungsi yang sama. Beberapa diantaranya berfungsi sama meskipun ada di tingkatan yang berbeda. Sejumlah protokol harus bergabung dengan protokol lainnya untuk membangun sistem komunikasi yang utuh. Terlihat bahwa aplikasi Wireshark telah *support* lebih dari 500 protokol jika di bandingkan dengan Network Miner. Selanjutnya membandingkan waktu yang dapat direkam, dapat dilihat pada Gambar 9.



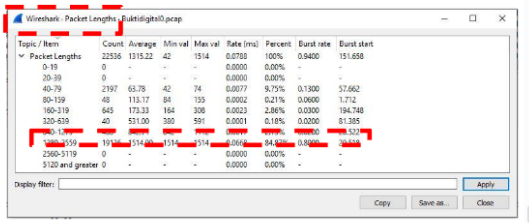
Gambar 9. Time Display Format

Wireshark membuktikan kehandalan dalam pengaturan waktu yang dapat di tentukan sesuai dengan waktu setempat sedangkan Network Miner tidak bisa mengatur waktu setempat. Zona waktu, yang diurutkan menurut pengaturan waktu dari *Coordinated Universal Time* (UTC) seharusnya adalah (UTC+8) untuk waktu

indonesia tengah. Wireshark menyediakan berbagai statistik jaringan, Statistik ini berkisar dari informasi umum tentang file tangkapan yang dimuat hingga statistik tentang protokol tertentu, namun penelitian ini akan menunjukan statistik I/O dan *Length*, dapat ditinjau pada Gambar 10.

Gambar 10. Statistik I/O Wireshark

Jendela Grafik I / O Wireshark tidak membedakan antara nilai yang hilang dan nol. Untuk sebar plot diasumsikan bahwa nilai nol menunjukkan data yang hilang, dan nilai-nilai tersebut dihilangkan. Nilai nol ditampilkan dalam grafik garis, dan diagram batang. Seperti yang ditunjukkan, jendela berisi area gambar bagan bersama dengan daftar grafik yang dapat disesuaikan, dibagi ke dalam interval waktu dan menunjukkan paket terakhir di setiap interval. Jumlah total paket, byte paket, atau bit paket adalah rata-rata di atas 75 Byte/s dengan total waktu TCP *error* lebih dari 150s. Beban user yang sangat tinggi untuk mengakses jaringan akan menyebabkan *bottleneck* jaringan yang mengarah pada kelambatan jaringan dapat dilihat pada Gambar 11.



Gambar 11. *Statistic Packet Length*

Panjang paket antara 1280-2559 dengan jumlah 19126byte dan rata-rata paket yang bergerak saat itu adalah 1514 dengan persentase 84.87% dari 100%, data ini dapat membuktikan adanya serangan setiap 0.668s. Evaluasi alat forensik berdasarkan *host, protocol, time display format dan statistic* dapat dilihat pada Tabel 6.

Tabel 6. Evaluasi Alat Analisis Forensik Jaringan

Alat Forensik	Host	Protokol	Time Display Format	Statistik	
				I/O	Length
Wireshark	√	√	√	√	√
Network Miner	√	√	-	-	-

Tabel 6 menjelaskan hasil dari evaluasi alat analisis forensik berdasarkan *host, protocol, time display format dan statistic* yang menunjukan Wireshark lebih lengkap, namun pada alat network miner tidak terdapat *time display format dan statistic*. Wireshark juga memiliki keunggulan pada akurasi dengan >500 protokol jika mengacu pada Gambar 4.33, juga unggul pada kelengkapan statistik pada I/O dan *Length* paket dan kemampuan audit data pada waktu sesuai zona. Praktik forensik harus mempertimbangkan dampak alat forensik terhadap kinerja jaringan dan Praktik forensik mencakup proses evaluasi dan peningkatan berkelanjutan untuk menjaga efektivitas sistem keamanan.

SIMPULAN

Hasil evaluasi alat forensik jaringan yaitu aplikasi Windump sangat di rekomendasikan sebagai alat forensik pada kategori alat rekam paket lalu lintas karena tidak membebani Sistem Operasi yang hanya membutuhkan < 2000 kb penggunaan memori jika di bandingkan dengan Aplikasi Wireshark membutuhkan > 80 MB dan Network Miner membutuhkan > 20 MB.

Berdasarkan evaluasi dari hasil analisis alat forensik jaringan pada tahap laporan pengujian forensik dapat disimpulkan bahwa, evaluasi alat analisis jaringan berdasarkan *host, protocol, time display format dan statistic*, diperoleh bahwa aplikasi Wireshark merupakan aplikasi analisis lalu lintas terbaik, karena protokol yang lebih banyak, kelengkapan dan penyuguhan statistik yang lengkap jika dibandingkan dengan Aplikasi Network Miner yang hanya memiliki protokol < 100.

Untuk penelitian masa depan tentang alat forensik, alat tambahan seperti Zeek, ELK Stack (Elasticsearch, Logstash, Kibana), dan XDR (Extended Detection and Response) bisa dievaluasi. Alat-alat tersebut menawarkan fitur dan pendekatan yang berbeda untuk deteksi dan

analisis ancaman. Integrasi dengan teknologi baru dengan melakukan evaluasi alat forensik dalam integrasi dengan teknologi baru seperti 5G, IoT (Internet of Things), dan SD-WAN (Software-Defined Wide Area Network). Dengan menerapkan rekomendasi untuk penelitian masa depan, organisasi dapat meningkatkan kemampuan deteksi dan respons terhadap ancaman, serta memastikan bahwa infrastruktur jaringan tetap aman dan efisien.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Program Studi Magister Teknik Informatika Universitas Ahmad Dahlan yang telah mengizinkan untuk menggunakan fasilitas sebagai penunjang dalam penelitian ini.

DAFTAR PUSTAKA

Aji, S., Fadlil, A., & Riadi, I. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik *Jaringan. Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, 3*(1), 11. https://doi.org/10.26555/jiteki.v3i1.5665

Akremi, A., Sallay, H., & Rouached, M. (2018). Intrusion detection systems alerts reduction: New approach for forensics readiness. Dalam *Security and Privacy Management, Techniques, and Protocols*. https://doi.org/10.4018/978-1-5225-5583-4.ch010

Albert, S., & Juni, E. (2015). Analisa Sistem Pengaman Data Jaringan Berbasis VPN. *Stmik Ikmi*, 10(18), 220. www.ikmi.ac.id

Alim, M., Riadi, I., & Prayudi, Y. (2018). Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard. *International Journal of Computer Applications, 180* (35), 23–30. https://doi.org/10.5120/ijca2018916879

Chaudhary, S., Somani, G., & Buyya, R. (2017). Research Advances in Cloud Computing. Dalam *Research Advances in Cloud Computing.* https://doi.org/10.1007/978-981-10-5026-8

CONTOLI, C. (2017). *Virtualized Network Infrastructures: Performance Analysis, Design and Implementation*. 1–121.

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

Djafar, W. (2019). Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan. *Jurnal Becoss*, *1*(1), 147–154.

Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. *European Conference on Information Warfare and Security, ECCWS*, 573–581.

Faiz, M. N., Umar, R., & Yudhana, A. (2016). Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary. *ILKOM Jurnal Ilmiah, 8*(3), 242. https://doi.org/10.33096/ilkom.v8i3.79.242-247

Firmansyah, F. F. A., & Umar, R. (2019). Analisis Forensik Metarouter pada Lalu Lintas Jaringan Klien. *Edu Komputika, 6*(2), 54–59.

Firmansyah, F., Fadlil, A., & Umar, R. (2021). Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 5*(1), 91–98. https://doi.org/10.29207/resti.v5i1.2784

Galang, C. M., Eko, S., & Imam, A. (2017). Teknik Virtualisasi Router Menggunakan Metarouter Mikrotik (Studi Kasus: Laboratorium Jaringan Komputer Politeknik Negeri Lampung). *Politeknik Negeri Lampung.*

Hildayanti, N. (2019). Forensics Analysis of Router On Computer Networks Using Live Forensics Method. *International Journal of Cyber-Security and Digital Forensics, 8*(1), 74–81. https://doi.org/10.17781/P002559

Kävrestad, J. (2018). Fundamentals of digital forensics: Theory, methods, and real-life applications. Dalam *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*. https://doi.org/10.1007/978-3-319-96319-8

Kuribayashi, S. I. (2018). Virtual routing function deployment in NFV-based networks under network delay constraints. International *Journal of Computer Networks and Communications, 10*(1), 35–44. https://doi.org/10.5121/IJCNC.2018.10103

Mandowen, S. A. (2016). Analisis forensik komputer pada lalu lintas jaringan. *Jurnal Sains, 16* (1), 14–20.

Menteri, P. (2016). Perlindungan Data Pribadi Dalam Sistem Elektronik. *BERITA NEGARA REPUBLIK INDONESIA, 1829,* 1–24.

Mubaraq, M. H. (2019). Notifikasi Jaringan pada Router Mikrotik Berbasis BOT Telegram. Dalam *Eprints Mercubuana Yogya.*

Nassar, B. O., & Tachibana, T. (2018). Path splitting for virtual network embedding in elastic optical networks. *International Journal of Computer Networks and Communications, 10*(2), 1–13. https://doi.org/10.5121/ijcnc.2018.10201

Phillips, T. (2016). Protect your network . *Ridgeback Interac ve Defense Pla orm EXECUTIVE.* 1–19.

Riadi, I. (2018). *SIMULATION FOR DATA SECURITY IMPROVEMENT IN EXPLOITED*. June.

Riadi, I., Umar, R., & Aini, F. D. (2019). Analisis Perbandingan Detection Traffic Anomaly Dengan Metode Naive Bayes Dan Support Vector Machine (Svm). *ILKOM Jurnal Ilmiah, 11*(1), 17–24. https://doi.org/10.33096/ilkom.v11i1.361.17-24

Riadi, I., Umar, R., & Nasrulloh, I. M. (2017). Analisis Forensik Bukti Digital pada Frozen Solid State Drive dengan Metode National Institute of Standards and Technology (NIST). *Jurnal Insand Comtech, 2*(2), 33–40.

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

Sachowski, J. (2018). Digital Forensics and Investigations. Dalam *Digital Forensics and Investigations*. https://doi.org/10.4324/9781315194820

Satran, M. (2018). *Microsoft SMB Protocol and CIFS Protocol Overview*. Msdn.microsoft.com.

Sholikhatin, S. A., Kuncoro, A. P., Munawaroh, A. L., & Setiawan, G. A. (2023). Comparative Study of RSA Asymmetric Algorithm and AES Algorithm for Data Security. *Edu Komputika Journal, 9*(1). https://doi.org/10.15294/edukomputika.v9i1.57389

Sunaringtyas, S. U., & Prayoga, D. S. (2021). Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On. *Edu Komputika Journal, 8*(1). https://doi.org/10.15294/edukomputika.v8i1.47179

Towidjojo, R., & Herman. (2016). *Mikrotik MetaROUTER.* Jasakom. http://www.jasakom.com

Umar, R., Riadi, I., & Muthohirin, B. F. (2018). Acquisition of Email Service Based Android Using NIST. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 3*(3), 263–270. https://doi.org/10.22219/kinetik.v3i4.637

Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. *International Journal on Advanced Science, Engineering and Information Technology*. https://doi.org/10.18517/ijaseit.8.3.3591

Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *It Journal Research and Development, 3*(1), 13–21. https://doi.org/10.25299/itjrd.2018.vol3(1).1658

Yuwono, D. T., Fadlil, A., & Sunardi, S. (2019). Performance Comparison of Forensic Software for Carving Files using NIST Method. *Jurnal Teknologi dan Sistem Komputer, 7*(3), 89. https://doi.org/10.14710/jtsiskom.7.3.2019.89-92