

Terbit online pada laman web jurnal: <http://jurnal.iaii.or.id>

JURNAL RESTI

(Rekayasa Sistem dan Teknologi Informasi)

Vol. 5 No. 1 (2021) 91 - 98

ISSN Media Elektronik: 2580-0760

Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST

Firmansyah¹, Abdul Fadlil², Rusydi Umar³^{1,3}Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan²Program Studi Teknik Elektro, Universitas Ahmad Dahlan¹firmanyas@gmail.com, ²fadlil@mti.uad.ac.id, ³rusydi@mti.uad.ac.id

Abstract

The evolution information technology has led to the growth of virtualization technology. Router OS is the operating system of the Mikrotik Router, which supports virtualization. Router Os virtualization technique which is easy to run is a metarouter. Metarouter provides benefits such as, building virtual servers, virtual machines, network topology and savings cost. As an object of research, Metarouter introduces challenges to digital forensic investigations, both practitioners and academics. Investigators need to use methodology and tools in order to prove the perpetrators of crimes. This study uses the Windump forensic tool as a means of recording network traffic activity. Network Miner and Wireshark as an analytical tool for identifying digital evidence. The use of the National Institute of Standard and Technology (NIST) method which collection, examination, analysis and reporting, can be repeated and maintained with the same data. Based on experiments with virtual router network traffic testing, the system built has succeeded in obtaining digital evidence, either by direct or indirectly. The system scenario that has been planned succeeded recording 220494 packages, but by the Windump, it is automatically divided into 9 (nine) parts of the package which are Buktidigital0 to Buktidigital8. The inspection stage produces evidence that has been verified by Wireshark and Network Miner. The analysis stage proves that there were attacks carried out by addresses 192.168.10.10 and 192.168.234.10. Based on the results of forensic testing, the use of the NIST method on a forensic system that has been built with a virtual router object can be used by investigators to identify evidence of cyber-attacks.

Keywords: Virtualization, Forensics, Evidence, Traffic, NIST

Abstrak

Evolusi dalam bidang teknologi informasi menyebabkan lahirnya pertumbuhan teknologi virtualisasi. Router OS adalah sistem operasi dari Router Mikrotik, yang telah mendukung penerapan virtualisasi. Teknik virtualisasi Router OS yang mudah untuk menjalankan topologi jaringan virtual adalah metarouter. Metarouter memberikan manfaat seperti, membangun server virtual, mesin virtual, topologi jaringan dan penghematan biaya. Sebagai objek penelitian, Metarouter memperkenalkan tantangan bagi investigasi forensik digital, baik praktisi maupun akademisi. Penyelidik perlu menggunakan metodologi dan alat forensik agar dapat membuktikan pelaku kejahatan. Penelitian ini menggunakan alat forensik Windump sebagai alat rekam aktifitas lalu lintas jaringan. Network Miner dan Wireshark sebagai alat analisis dari identifikasi bukti digital. Pemanfaatan metode *National Institute of Standard and Technology* (NIST) yang meliputi, koleksi, pemeriksaan, analisis dan pelaporan, dapat diulang dan dipertahankan dengan data yang sama. Berdasarkan dari percobaan dengan pengujian lalu lintas jaringan virtual router, sistem yang dibangun berhasil mendapatkan bukti-bukti digital, baik dengan cara pengamatan secara langsung maupun tidak. Skenario sistem yang telah dirancang berhasil merekam 220494 paket, namun oleh alat Windump, secara otomatis terbagi menjadi 9(sembilan) bagian paket yang diberi nama Buktidigital0 sampai dengan Buktidigital8. Tahapan pemeriksaan menghasilkan bukti yang telah diverifikasi oleh alat Wireshark dan Network Miner. Tahapan analisis membuktikan adanya penyerangan yang dilakukan oleh alamat 192.168.10.10 dan 192.168.234.10. Berdasarkan hasil dari pengujian forensik, penggunaan metode NIST pada sistem forensik yang telah dibangun dengan objek virtual router, dapat digunakan investigator sebagai identifikasi bukti serangan siber.

Kata kunci: Virtualisasi, Forensik, Bukti, Lalu Lintas, NIST

1. Pendahuluan

Dalam beberapa dekade terakhir, telah terjadi evolusi yang luar biasa dalam lalu lintas di Internet, jaringan perusahaan dan lingkungan pendidikan. Jaringan membantu kelahiran banyak aplikasi. Di sisi lain, ledakan jaringan seluler, dengan permintaan perangkat terus meningkat. Tren ini dapat mengakibatkan kerumitan jaringan, yang mengarah pada manajemen yang sulit dan biaya menjadi tinggi. Pada saat yang sama, evolusi dalam bidang teknologi informasi menyebabkan lahirnya pertumbuhan teknologi virtualisasi. Peluang baru tidak hanya untuk perusahaan tetapi juga untuk pendidikan dan perorangan. Teknologi virtualisasi dapat mengurangi biaya yang dikeluarkan oleh perusahaan maupun perangkat pendidikan khususnya pada bagian IT. Teknologi virtualisasi merupakan pengembangan ilmu pengetahuan berdasarkan kebutuhan. Kebutuhan akan perangkat jaringan komputer sangatlah tinggi dengan harga yang bervariasi sesuai dengan spesifikasi perangkat. Dunia pendidikan dapat menerapkan teknik virtualisasi dari perangkat fisik untuk membuat sebuah laboratorium jaringan komputer sehingga dapat meminimalisir pengeluaran pembayaran listrik dan pembelian perangkat fisik. Jika perusahaan memiliki beberapa server, maka dapat menggunakan teknologi virtualisasi server untuk mengurangi jumlah server fisik, sehingga biaya pemeliharaan dan keamanan akan berkurang. Router Mikrotik dimanfaatkan untuk menerapkan virtualisasi MetaRouter yang berdampak pada penghematan biaya pembelian *hardware* router, penggunaan listrik, dan tempat penyimpanan[1]. Penelitian Virtualisasi router tersebut hanya terbatas pada pemanfaatan teknologi virtualisasi, namun tidak meneliti bagian forensik lalu lintas metarouter. Virtual router dapat saling berkomunikasi maupun tidak, sesuai dengan kebutuhan atau sesuai dengan skenario pengujian yang akan di bangun. Setiap virtual tidak dapat saling berkomunikasi sehingga keamanan dan privasi tetap terjaga [2]. [3]Makalah tersebut memberikan pedoman untuk memutuskan nilai keterlambatan jaringan yang dapat ditoleransi ketika kondisi kenaikan biaya jaringan. Virtualisasi jaringan telah muncul sebagai solusi yang menjanjikan, dapat dimanfaatkan dan dikelola secara sederhana, fleksibel, dan efektif. Dalam virtualisasi jaringan, beberapa jaringan virtual dengan topologi spesifik dan persyaratan sumber daya dapat dibangun melalui jaringan fisik[4].

Deteksi peningkatan jumlah akses pengguna, dapat meminimalisir terjadinya serangan dari pihak lain terhadap jaringan[5]. Analisis tangkapan jaringan dengan file nitroba.pcap, menghasilkan pemulihan sejumlah bukti forensik dengan temuan kunci utama dan bukti pendukung dari analisis[6]. Penelitian tersebut menggunakan aplikasi network miner dan wireshark sebagai analisis paket secara *offline*, namun hanya pada 1(satu) barang bukti berupa hasil rekaman paket.

Software analisis paket secara *offline*, mendeteksi semua kemungkinan IP jahat yang bertanggung jawab atas serangan di antara paket yang tertangkap secara *real-time* menggunakan Wireshark[7]. Penelitian tersebut menjelaskan alat yang dapat medeteksi, mencegah ataupun mengurangi tusukan serangan yang muncul sesuai dengan kebutuhan lingkungan jaringan. Kerangka kerja analisis forensik, disajikan mempertimbangkan data yang dicatat terkait dengan aktivitas di lapisan aplikasi serta lapisan yang lebih rendah[8], namun menunjukkan bahwa, alat analisis forensik untuk mengotomatisasi korelasi bukti dari klien dan penyedia layanan *cloud* untuk merekonstruksi skenario serangan dalam penyelidikan forensik. Serangan DoS di jaringan Router terus berkembang di lingkungan masyarakat, khususnya dilakukan oleh individu tertentu dan ditujukan ke jaringan Router untuk mendapatkan hak akses. Skenario serangan dibutuhkan pada analisis Router untuk menggali informasi, serta menarik data forensik sebagai bukti digital dengan metode pengamatan secara langsung[9]. Aplikasi wireshark dapat digunakan sebagai alat penyadapan secara langsung pada router fisik. Pada analisis hasil, berbagai jenis data *Internet Protocol* yang mengakses jaringan, apa yang diakses?, kapan pengguna mengakses?, dan di mana pengguna mengakses?, kemudian perbandingan aliran data router sebelum dan sesudah jaringan terputus[10]. Meyebutkan, setiap aliran paket data yang masuk ataupun yang keluar, dapat diidentifikasi. Penelitian tersebut menggunakan aplikasi netcut sebagai alat penyerang dan wireshark sebagai alat analisis jaringan.

Skenario *static routing* dapat menggunakan dua unit metarouter dalam satu Routerboard. Setiap *interface* pada router virtual dibuat secara manual dan pengujian antar virtual router menggunakan masing-masing terminal[13]. Buku ini menjelaskan tentang pengaturan penggunaan metarouter untuk keperluan simulasi maupun berlatih memahami teknik jaringan komputer. Acuan penelitian terdahulu yang dikutip pada penelitian ini memiliki beberapa kesamaan diantaranya pada objek penelitian, metode dan *tools* yang digunakan seperti pada Tabel 1.

Tabel 1. Acuan Penelitian Terdahulu

Penulis (thn)	Judul Penelitian	Hasil Penelitian
Firmansyah, Abdul Fadlil, Rusydi Umar (2019)	Analisis Forensik Metarouter Pada Lalu Lintas Jaringan Klien [14]	Membuktikan adanya serangan dengan cara pengamatan secara langsung
Imam Riadi, Abdul Fadlil, & Muhammad Immawan Aulia. (2020)	Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST) [13]	Disimpulkan dari 10 file asli dengan mengakuisisi data menggunakan <i>tools</i> FTK Imager dan Autopsy
Anton Yudhana, Abdul Fadlil,	Analisis Recovery Bukti Digital Skype berbasis	Bukti digital <i>Skype</i> berbasis <i>Smartphone</i> Android pada

& Setyawan, M. R. (2020)	Smartphone Android Menggunakan Framework NIST [14]	Framework NIST berhasil mengembalikan bukti digital dari <i>smartphone</i> Samsung J2
Sunardi, Imam Riadi, & Muh. Hajar Akbar. (2020)	Application of Static Forensics Method for Extracting Steganographic Files on Digital Evidence Using the DFRWS Framework [15]	Bukti digital dalam penggunaan metode <i>static forensics</i> dengan penerapan <i>framework Digital Forensics Research Workshop (DFRWS)</i>
Putu Adhika Dharmesta, I Made Agus Dwi Suarjaya, & I Made Sunia Raharja. (2020)	Effectiveness of Sniffer Using Natural Language in Learning Computer Network Traffic [16]	<i>Natural language</i> lebih efektif pada proses <i>sniffer</i> untuk meningkatkan pemahaman jaringan komputer.

Hasil rangkuman diatas merupakan acuan yang digunakan dalam penelitian ini. Tujuan penelitian ini adalah melakukan identifikasi bukti forensik jaringan virtual router dengan pemanfaatan *static forensics* menggunakan alat WinDump, Wireshark dan Network Miner pada metode NIST.

2. Metode Penelitian

Panduan integrasi teknik forensik pada NIST SP800-86[17] merekomendasikan proses forensik untuk menemukan bukti, seperti juga[18]. Tahapan penelitian identifikasi bukti forensik lalu lintas metarouter dengan NIST melakukan skenario penyadapan jaringan metarouter dan analisis paket jaringan, dapat dilihat pada Gambar 1.

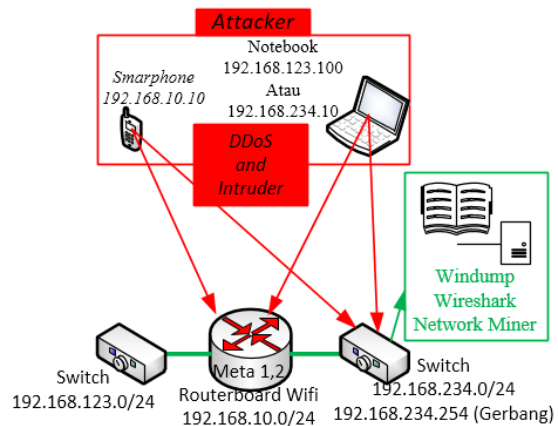


Gambar 1. Tahapan Metode NIST

- Collection:** Tahapan ini, akan mengumpulkan data-data yang diperoleh dari rekaman paket data dan pengamatan lalu lintas secara langsung maupun tidak langsung pada jaringan metarouter.
- Examination:** Pada langkah selanjutnya, akan ada proses identifikasi data yang dapat digunakan sebagai bukti. Setelah ditentukan, data akan diambil, proses pengambilan data akan diuji secara forensik.
- Analysis:** Data yang telah diambil akan dianalisis untuk mencari hal-hal yang dapat digunakan sebagai bukti, terkhusus jaringan komputer, hal yang akan menjadi bukti adalah *Internet Protocol Address*.
- Reporting:** Tahap akhir dari langkah forensik lalu lintas metarouter adalah pelaporan hasil analisis forensik dari awal hingga akhir dalam bentuk laporan tertulis sehingga dapat memberikan rekomendasi untuk perbaikan kebijakan, pedoman, prosedur, alat, dan aspek lain dari proses forensik [17].

2.1. Skenario Kasus

Skenario metarouter yang digunakan adalah virtual router dapat saling berkomunikasi dengan tujuan terciptanya skenario penyerangan dan penyusupan yang baik, sehingga analisis paket yang bergerak menjadi lebih banyak, ketika semakin banyak protokol lalu lintas yang tertangkap, maka akan semakin banyak yang akan diamati pada tahapan analisis paket jaringan. Rancangan skenario penyerangan dan penyusupan, dapat dilihat pada Gambar 2.



Gambar 2. Skenario Penyerangan dan Penyadapan

Penyerangan oleh *smartphone* menggunakan aplikasi termux pada alamat 192.168.10.10 dengan target perangkat pada alamat 192.168.234.0/24 dan 192.168.10.0/24. Penyusupan dan penyerangan oleh *Notebook* dengan alamat 192.168.123.100 dan alamat 192.168.234.10. Perangkat Windump merekam aktifitas lalu lintas pada setiap perangkat, sedangkan alat Wireshark dan Network Miner sebagai alat analisis paket lalu lintas jaringan.

2.2. Alat dan Bahan

Alat dan bahan yang diperlukan untuk menunjang penelitian ini dapat dilihat pada Tabel 2.

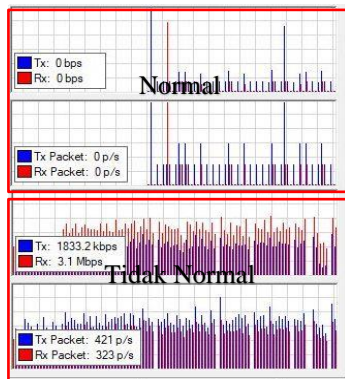
Tabel 2. Alat dan Bahan

No.	Alat dan Bahan	Spesifikasi	Keterangan
1	Mikrotik RB951Ui-2HnD	Versi 6	Hardware
2	Modem ADSL	ZTE f609 dan Huawei hg8045h	Hardware
3	Notebook	Prosesor Intel Core i5	Hardware
4	Netbook	Prosesor intel Centrino	Hardware
5	Smartphone	Sony Z5	Hardware
6	Winbox	v3.19	Software
7	Termux	v0.98	Software
8	Microsoft Windows 10	Windows 10 Pro File sistem NTFS	Software

9	Microsoft Windows 7	Windows 7 Ultimate File sistem NTFS	Software
10	Windump	Windows 95, 98, ME, NT, 2000, XP, 2003, Vista dan 2007	Alat Rekam Paket
11	Network Miner	v2.5	Alat Analisis Paket
12	Wireshark	Win64 v3.0.5	Alat Analisis Paket

3. Hasil dan Pembahasan

Skenario yang akan dibangun adalah percobaan alat analisis perangkat jaringan forensik melalui serangan DDos, pada sistem kantor terpusat yang diciptakan menggunakan metarouter dari perangkat Routerboard RB951Ui-2HnD. Tujuan serangan maupun penyusupan terletak pada alamat IP 192.168.234.0/24 yang dimiliki oleh modem ADSL, alamat IP 10.1.1.254 yang berfungsi sebagai jembatan terletak pada router. Terlihat perbedaan yang signifikan pada Gambar 3.



Gambar 3. Lalu Lintas Normal dan Tidak Normal

Perbedaan sangat terlihat jelas pada lalu lintas normal dan tidak normal di atas, pada mikrotik melalui aplikasi winbox, namun ini belum cukup untuk membuktikan bahwa adanya serangan ataupun tidak. Aktifitas juga bergerak jika virtual mesin melakukan perjalanan menuju situs-situs yang diinginkan, tidak hanya itu, unggah dan unduh data juga dapat menaikkan traffic lalu lintas[2]. Penelitian ini mendapatkan bukti alamat IP penyerang yang mengirimkan banyak paket sehingga membuat server virtual mesin Meta2 tidak dapat terkoneksi internet, Gambar 4 adalah bukti alamat penyerang.

Alamat penyerang yaitu 192.168.123.100, melakukan transfer rate sebesar 163.8 kbps pada alamat 192.168.234.254, yang merupakan alamat gerbang internet, bukti tersebut dilihat melalui mikrotik torch. Bukti paket lalu lintas yang berhasil terekam oleh alat windump dapat dilihat pada Gambar 5.

Terdapat 220494 paket data yang berhasil terekam oleh windump dari 220495 paket yang terkirim dan tidak

terdapat paket yang terlewat. Bukti paket dapat ditemukan pada folder c:\perflog\Buktidigital0, Buktidigital1, Buktidigital2, hingga Buktidigital8, yang akan di validasi menggunakan aplikasi Wireshark dan Network Miner, dengan jumlah rekaman paket yang sama, jika jumlah paket yang diterima tidak sama, maka dipastikan bukti tidak valid.

Total RX Meta2.JPG - Picasa Photo Viewer			
Eth. Protocol:	800 (ip)	Src.:	192.168.234.254
Dst.:	192.168.10.253	Tx Rate:	24.7 kbps
Rx Rate:	63.5 kbps	Tx Packet Rate:	33
Rx Packet Rate:	10		
Eth. Protocol:	800 (ip)	Src.:	192.168.234.254
Dst.:	192.168.123.100	Tx Rate:	163.8 kbps
Rx Rate:	163.8 kbps	Tx Packet Rate:	14
Rx Packet Rate:	14		
Eth. Protocol:	800 (ip)	Src.:	10.1.1.2
Dst.:	10.1.1.254	Tx Rate:	0 bps
Rx Rate:	0 bps	Tx Packet Rate:	0
Rx Packet Rate:	0		
Eth. Protocol:	800 (ip)	Src.:	192.168.234.200
Dst.:	152.199.43.37	Tx Rate:	0 bps
Rx Rate:	0 bps	Tx Packet Rate:	0
Rx Packet Rate:	0		
Eth. Protocol:	800 (ip)	Src.:	192.168.234.254
Dst.:	10.1.1.254	Tx Rate:	1841.0 kbps
Rx Rate:	1841.0 kbps	Tx Packet Rate:	152
Rx Packet Rate:	152		
Eth. Protocol:	800 (ip)	Src.:	192.168.234.200
Dst.:	195.244.31.10	Tx Rate:	0 bps
Rx Rate:	0 bps	Tx Packet Rate:	0
Rx Packet Rate:	0		
6 Items		Total Tx: 2.0 Mbps	Total Rx: 2.0 Mbps
		Total Tx Packet: 199	

Gambar 4. IP Address Penyerang

```
windump: listening on \Device\NPF_{F6191BE8-EFE1-46AE-BCF0-75D613B5A005}
220494 packets captured
220495 packets received by filter
0 packets dropped by kernel
```

Gambar 5. Hasil Rekam Alat Windump

3.1. Collection

Proses koleksi, sebagaimana telah dijelaskan sebelumnya, memiliki beberapa tahapan, dapat dilihat pada Gambar 6.



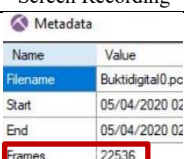
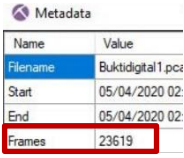
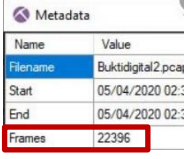
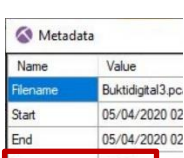
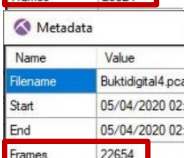
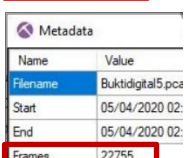
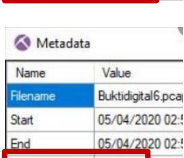
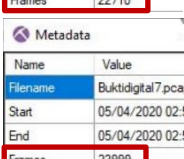
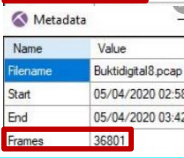
Gambar 6. Proses Tahapan Koleksi

Proses tahapan di atas merupakan pengumpulan data yang akan dijadikan barang bukti digital pada lalu lintas jaringan virtual router, terdapat sejumlah data dengan beragam nilai dan kapasitas yang berbeda agar dapat mempermudah pada tahapan pemeriksaan. Pemeriksaan awal bukti digital yang berhasil terekam dapat dilihat pada Tabel 3 dengan menggunakan alat Network Miner.

Pengumpulan hasil rekam paket pada Tabel di atas merupakan total nilai rekaman 220494 paket pada perangkat windump yang sekaligus sebagai pemeriksaan

awal.

Tabel 3. Pemeriksaan Melalui Network Miner

No	Evidence	Screen Recording	Record
1	Packet recording bukti0.pcap		22536 Packet
2	Packet recording bukti1.pcap		23619 Packet
3	Packet recording bukti2.pcap		22396 Packet
4	Packet recording bukti3.pcap		23024 Packet
5	Packet recording bukti4.pcap		22654 Packet
6	Packet recording bukti5.pcap		22755 Packet
7	Packet recording bukti6.pcap		22710 Packet
8	Packet recording bukti7.pcap		23999 Packet
9	Packet recording bukti8.pcap		36801 Packet
Total Value 220494 Packet			

3.2. Examination

Tahapan pemeriksaan dilakukan agar dapat mengetahui bahwa nilai paket pada bukti digital yang berhasil direkam sama antara 2(dua) alat forensik yaitu

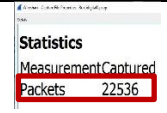
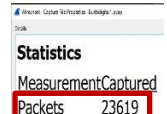




Wireshark dan Network Miner. Alur proses dapat dilihat pada Gambar 7.

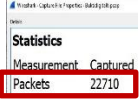
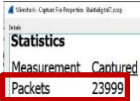
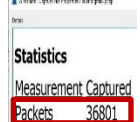


Gambar 7. Proses Tahapan Pemeriksaan

Pemeriksaan bukti pada tahap ini akan menggunakan paket yang terekam dengan pemanfaatan alat analisis jaringan yaitu wireshark dan network miner. Proses verifikasi selanjutnya menggunakan alat wireshark, dapat dilihat pada Tabel 4, jika data sesuai dengan hasil pemeriksaan awal, akan dilanjutkan pada tahapan analisis sistem.

Tabel 4. Pemeriksaan Melalui Wireshark

No	Evidence	Screen Recording	Record
1	Packet recording bukti0.pcap		22536 Packet
2	Packet recording bukti1.pcap		23619 Packet
3	Packet recording bukti2.pcap		22396 Packet
4	Packet recording bukti3.pcap		23024 Packet
5	Packet recording bukti4.pcap		22654 Packet
6	Packet recording bukti5.pcap		22755 Packet

7	Packet recording bukti6.pcap		22710 Packet
8	Packet recording bukti7.pcap		23999 Packet
9	Packet recording bukti8.pcap		36801 Packet
Total Value 220.494 Packet			

Tabel 3 dan 4 diidentifikasi bahwa paket telah diekstrak dengan alat Network Miner dan wireshark dengan penggabungan paket dinyatakan valid, setelah diamati sesuai dengan total paket yaitu sama-sama menghasilkan 220494 paket yang terekam.

3.3. Analysis

Pada tahapan ini bukti digital yang ditemukan pada proses pemeriksaan akan dijadikan sebagai barang bukti yang sah karena telah dilakukan validasi nilai paket yang sama. Bukti digital pada objek virtual router yang digunakan, melakukan verifikasi 2(dua) alat analisis. Tahapan pada proses analisis ini dapat dilihat pada Gambar 8.



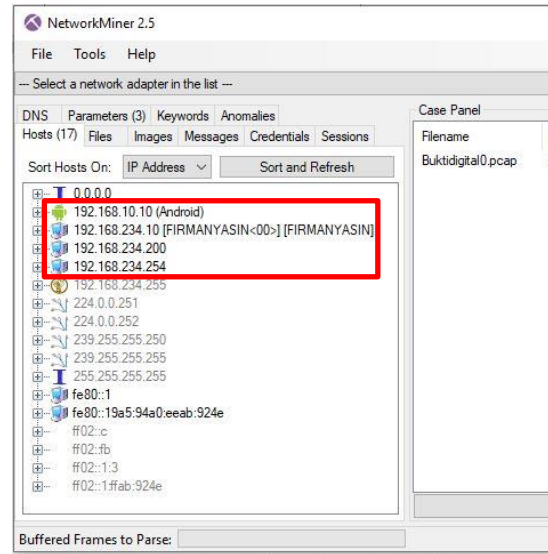
Gambar 8. Proses Tahapan Analisis

Proses tahapan analisis seperti pada Gambar 8 menampilkan diagram alur, dimana proses akuisisi ditemukannya barang bukti digital serta verifikasi bukti menggunakan 2(dua) alat analisis forensik. Network Miner menampilkan *host* aktif pada buktidigital0.pcap, dapat dilihat pada Gambar 9.

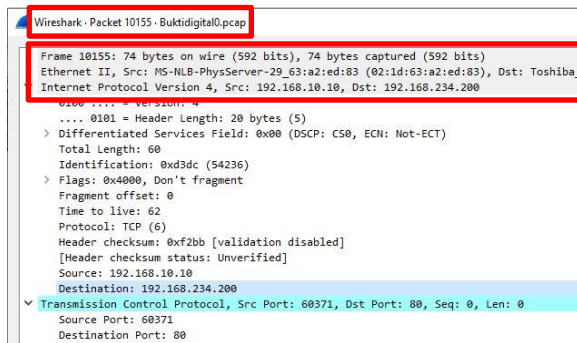
Alamat IP 192.168.10.10 terverifikasi melalui alat forensik Wireshark dengan paket yang sama, lebih jelas pada Gambar 10.

Letak paket terdeteksi oleh wireshark pada *frame* 10155, dengan panjang rata-rata paket yang di kirim 74 bytes atau 592 bits, melalui jaringan *wireless*. *Internet protocol version 4* (IPv4) mencatat tujuan alamat IP 192.168.10.10, menggunakan OS Android, menuju

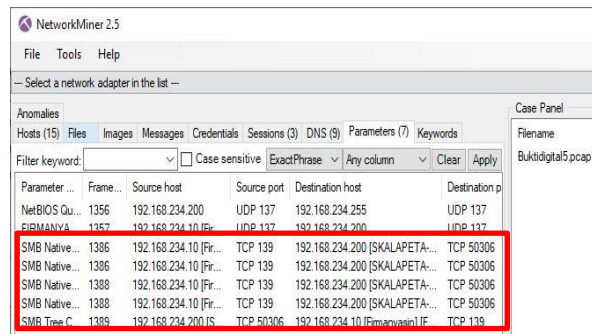
alamat IP 192.168.234.200 yang merupakan alamat dari Toshiba. *Protocol* TCP juga membuktikan bahwa ada serangan melalui *port* 80, terlihat pada Gambar 11.



Gambar 9. Buktidigital0.pcap Network Miner

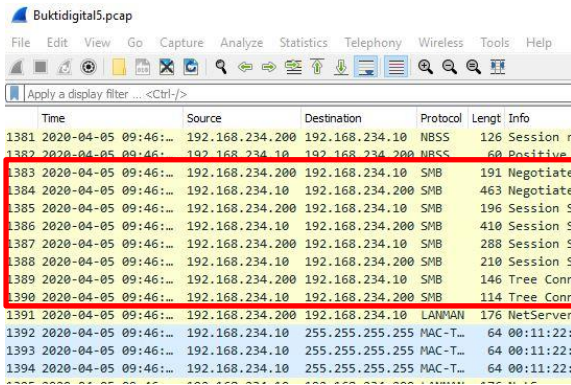


Gambar 10. Buktidigital0.pcap Wireshark



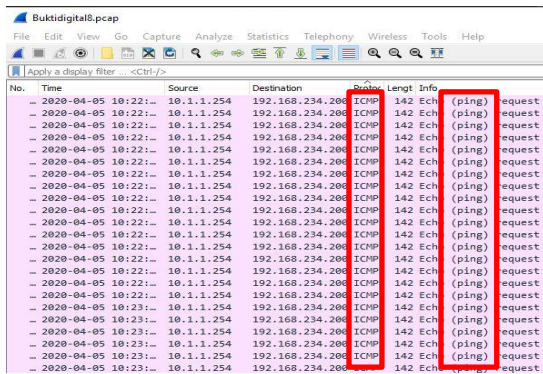
Gambar 11. Buktidigital5.pcap Network Miner.

Parameter SMB melalui TCP Port: 445 dengan nama NetBIOS digantikan oleh DNS. Lapisan ini mendasari adanya kendala koneksi [19] sehingga alamat IP 192.168.234.200 dengan nama SKALAPETA-PC mengalami gangguan yang disebabkan oleh alamat IP 192.168.234.10 yang diberi nama firmansyah, simak Gambar 12.



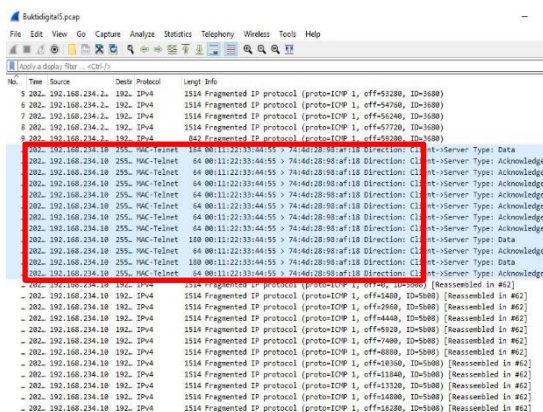
Gambar 12. Buktidigital5.pcap Wireshark.

Terbukti pada alat wireshark, bahwa adanya kendala koneksi benar terjadi. Serangan melalui protokol sangat efektif jika pintu protokol dalam keadaan terbuka. Protokol ICMP juga dapat membuktikan adanya serangan, lebih jelas dapat lihat Gambar 13.



Gambar 13. Buktidigital8.pcap Wireshark

Bukti serangan pada protokol ICMP benar terjadi dan terlihat pada alat analisis Wireshark, dengan alamat korban 192.168.234.200, namun tidak terdeteksi oleh alat Network Miner, ini juga terjadi pada Gambar 14. Bukti semakin kuat jika dilakukan proses pengujian kembali menggunakan lebih dari 1(satu) alat forensik.



Gambar 14. Buktidigital5.pcap Wireshark.

Sangat jelas bahwa alamat ip 192.168.234.10 berusaha dan berhasil masuk server melalui telnet, namun rekaman kejadian ini tidak terlihat oleh aplikasi Network Miner.

3.4. Reporting

Tahapan pengumpulan, pengambilan dan analisis telah berjalan sesuai dengan metode, tahapan terakhir adalah membuat laporan bukti-bukti forensik lalu lintas metarouter. Penelitian ini berusaha dengan baik dan sungguh untuk membuat laporan bukti, namun akan coba dipaparkan melalui Tabel 5 agar pembaca dapat memahami laporan ini.

Tabel 5. Laporan Bukti

No	Bukti	Wireshark	Network Miner	Ket.
1	Gambar 3	-	-	Mikrotik
2	Gambar 4	-	-	Mikrotik
3	Gambar 5	ok	ok	220494 bit
4	Gambar 9	-	ok	Alamat IP
5	Gambar 10	ok	-	
6	Gambar 11	-	ok	Protokol SMB
7	Gambar 12	ok	-	Protokol ICMP
8	Gambar 13	ok	-	Protokol Telnet
9	Gambar 14	ok	-	

Bukti-bukti setiap paket memiliki kekurangan dan kelebihan, misalnya pada Gambar 5 adalah hasil dari rekam aplikasi windump, yang telah di verifikasi oleh alat Wireshark dan Network Miner dengan nilai yang sama yaitu 220494 paket. Beberapa paket tidak dapat diverifikasi karena tidak terdeteksi oleh alat lainnya, sebagai contoh Gambar 13 dan 14, tidak adanya aliran paket dengan protokol ICMP dan Telnet. Selanjutnya akan disederhanakan pada Tabel 6.

Tabel 6. Bukti Terverifikasi

Wirehark	Network Miner	Gambar
√	√	Gambar 5
√	√	Gambar 9
√	√	Gambar 10
√	√	Gambar 11
√	√	Gambar 12

Tabel di atas adalah laporan akhir verifikasi bukti yaitu gambar 5 dan gambar 9-12, menyatakan bahwa sistem yang dibuat berhasil membuktikan adanya penyerangan karena telah melewati proses-proses *examination*.

4. Kesimpulan

Pemanfaatan metode NIST yang meliputi, koleksi, pemeriksaan, analisis dan pelaporan, dapat diulang dan dipertahankan. Berdasarkan dari percobaan dengan pengujian lalu lintas jaringan virtual router, sistem yang dibangun berhasil mendapatkan bukti-bukti digital, baik dengan cara pengamatan secara langsung maupun tidak. Bukti pengamat secara langsung dapat ditinjau pada Gambar 3 dan 4. Skenario sistem yang telah dirancanag berhasil merekam 220494 paket, namun oleh alat Windump, secara otomatis terbagi menjadi 9(sembilan) bagian paket yang diberi nama Buktidigital0 sampai dengan Buktidigital8. Tahapan pemeriksaan menghasilkan bukti yang telah diverifikasi oleh alat Wireshark dan Network Miner. Tahapan analisis

membuktikan adanya penyerangan yang dilakukan oleh alamat 192.168.10.10 dan 192.168.234.10. Berdasarkan hasil dari pengujian forensik, penggunaan metode NIST pada sistem yang telah dibangun dengan objek virtual router, dapat digunakan investigator sebagai identifikasi bukti serangan siber. Saran selanjutnya yaitu melakukan penelitian analisis paket secara *offline* dengan menggunakan aplikasi selain wireshark dan network miner, seperti Microsoft Network Monitor dan NetIntercept.

Daftar Rujukan

- [1] C. M. Galang, S. Eko, and A. Imam, "Teknik Virtualisasi Router Menggunakan Metarouter Mikrotik (Studi Kasus: Laboratorium Jaringan Komputer Politeknik Negeri Lampung)," 2017.
- [2] A. Asmunin and A. Hermawan, "Penerapan dan Analisis Virtualisasi Router Menggunakan RouterOS," *Multinetics*, 2 (1), pp. 31–34, 2016.
- [3] S. I. Kuribayashi, "Virtual routing function deployment in NFV-based networks under network delay constraints," *Int. J. Comput. Networks Commun.*, 10 (1), pp. 35–44, 2018.
- [4] B. O. Nassar and T. Tachibana, "Path splitting for virtual network embedding in elastic optical networks," *Int. J. Comput. Networks Commun.*, 10 (2), pp. 1–13, 2018.
- [5] I. Riadi, R. Umar, and F. D. Aini, "Analisis Perbandingan Deteksi Traffic Anomaly Dengan Metode Naive Bayes Dan Support Vector Machine (Svm)," *Ilk. J. Ilm.*, 11 (1), pp. 17–24, 2019.
- [6] S. A. Mandowen, "Analisis forensik komputer pada lalu lintas jaringan," *J. Sains*, 16 (1), pp. 14–20, 2016.
- [7] S. Vidyia and R. Bhaskaran, "ARP Storm Detection and Prevention Measures," *Int. J. Comput. Sci. Issues*, 8 (2), pp. 456–460, 2011.
- [8] A. S. and D. W. Changwei Liu, "IDENTIFYING EVIDENCE FOR CLOUD FORENSIC ANALYSIS," 2017.
- [9] M. Alim, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *Int. J. Comput. Appl.*, 180 (35), pp. 23–30, 2018.
- [10] N. Hildayanti, "Forensics Analysis of Router On Computer Networks Using Live Forensics Method," *Int. J. Cyber-Security Digit. Forensics*, 8 (1), pp. 74–81, 2019.
- [11] R. Towidjojo and Herman, *Mikrotik MetaROUTER*. Jasakom, 2016.
- [12] A. F. Fadlil and R. Umar, "Analisis Forensik Metarouter pada Lalu Lintas Jaringan Klien," *Edu Komputika*, 6 (2), pp. 54–59, 2019.
- [13] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, 4 (5), pp. 820–828, 2020.
- [14] M. R. Anton Yudhana, Abdul Fadlil, Setyawan, "Analisis Recovery Bukti Digital Skype berbasis Smartphone Android Menggunakan Framework NIST," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, 4 (4), pp. 682–690, 2020.
- [15] M. H. A. Sunardi, Imam Riadi, "Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, 4 (3), pp. 576–583, 2020.
- [16] & I. M. S. R. Putu Adhika Dharmesta, I Made Agus Dwi Suarjaya, "Efektivitas Sniffer Menggunakan Natural Language dalam Pembelajaran," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, 4 (3), pp. 392–403, 2020.
- [17] A. K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *NIST SP800-86*, August, pp. 1–20, 2006.
- [18] D. T. Yuwono, A. Fadlil, and S. Sunardi, "Performance Comparison of Forensic Software for Carving Files using NIST Method," *J. Teknol. dan Sist. Komput.*, 7 (3), p. 89, 2019.
- [19] R. Leutert and L. Netservices, "Microsoft SMB Troubleshooting," 2013.