



## Analisis Forensik Metarouter pada Lalu Lintas Jaringan Klien

Firmansyah✉, Abdul Fadlil, Rusydi Umar

Program Studi Magister Teknik Informasi, Universitas Ahmad Dahlan Yogyakarta, Indonesia

### Info Artikel

Sejarah Artikel:

Diterima: November 2019

Direvisi: Desember 2019

Disetujui: Desember 2019

Keywords:

Metarouter, Klien, Forensik, Lalu Lintas Jaringan

### Abstrak

Seorang pengusaha atau penyedia jasa di dunia jaringan internet, tentu akan menemukan klien dengan karakter yang berbeda. Klien yang tidak buta teknologi yang khususnya router, terkadang menginginkan akses penuh ke router, atau beberapa dari klien yang meminta untuk menambahkan router untuk dapat secara langsung mengakses router secara penuh. Sebagai pengusaha layanan internet bisa saja memberikan router tambahan, namun tentu akan menambah biaya sesuai harga router. Beberapa kasus lain, misalnya seorang klien akan membuat sebuah laboratorium jaringan komputer, maka akan sangat membutuhkan router yang banyak. Router, saat ini semakin canggih, dengan adanya metarouter, akan dapat menghemat biaya yang keluar. Metarouter memungkinkan klien untuk mengolah jaringan sendiri, seolah-olah klien memiliki router. Kasus yang terjadi membuktikan bahwa router sangatlah penting untuk membagi atau mendistribusikan IP address, baik secara statik maupun dinamik. Forensik jaringan berfungsi untuk merekam kejadian atau aktifitas lalu lintas data pada jaringan komputer, dengan melakukan analisa dari hasil investigasi yang didapat, sehingga menemukan sebuah bukti aliran paket yang mencurigakan. Pengungkapan bertujuan untuk dapat menemukan IP address penyusup dari aplikasi wireshark dengan melakukan analisis paket jaringan. Tujuan lain dari penelitian ini adalah menemukan serangan yang terjadi melalui protokol yang diserang oleh penyusup dan Metode yang diusulkan juga menyarankan cara untuk mencegah serangan DOS secara online. Aplikasi Wireshark dapat melihat paket data yang sedang berjalan secara langsung.

### Abstract

*An entrepreneur or a service provider in the internet network world, will certainly find clients with different characters. Clients who are not technology blind, especially routers, sometimes want full access to the router, or some clients who ask to add a router to be able to directly access the router in full. As an internet service entrepreneur, an additional router can be provided, but it will certainly add costs according to the price of the router. Some other cases, for example a client will create a computer network laboratory, it will require a lot of routers. Routers, now increasingly sophisticated, with the presence of metarouter, will be able to save costs out. Metarouter allows clients to process their own network, as if the client has a router. The case that occurred proved that the router is very important to share or distribute IP addresses, both statically and dynamically. Network forensics functions to record events or data traffic events on a computer network, by analyzing the results of investigations obtained, so as to find evidence of a suspicious packet flow. Disclosure aims to be able to find the intruder IP address of the wireshark application by conducting network packet analysis. Another goal of this research is to find attacks that occur through protocols attacked by intruders and the proposed method also suggests ways to prevent online DOS attacks. Wireshark applications can view currently running data packets directly.*

## PENDAHULUAN

Seorang pengusaha atau penyedia jasa di dunia jaringan internet, tentu akan menemukan klien dengan karakter yang berbeda. Klien yang tidak buta teknologi yang khususnya router, terkadang menginginkan akses penuh ke router, atau beberapa dari klien yang meminta untuk menambahkan router untuk dapat secara langsung mengakses router secara penuh. Sebagai pengusaha layanan internet bisa saja memberikan router tambahan, namun tentu akan menambah biaya sesuai harga router. Beberapa kasus lain, misalnya seseorang klien akan membuat sebuah laboratorium jaringan komputer, maka akan sangat membutuhkan router yang banyak. Router, saat ini semakin canggih, dengan adanya metarouter, akan dapat menghemat biaya yang keluar. Metarouter memungkinkan klien untuk mengolah jaringan sendiri, seolah-olah klien memiliki router. Kasus yang terjadi membuktikan bahwa router sangatlah penting untuk membagi atau mendistribusikan IP address, baik secara statik maupun dinamik. Forensik jaringan berfungsi untuk merekam kejadian atau aktifitas lalu lintas data pada jaringan komputer, dengan melakukan analisa dari hasil investigasi yang didapat, sehingga menemukan sebuah bukti aliran paket yang mencurigakan.

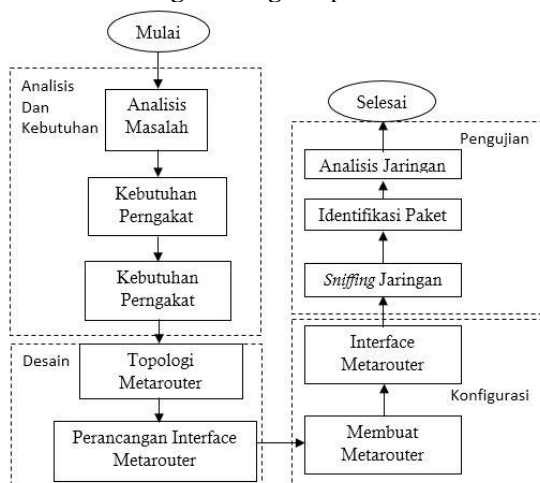
Internet Forensik sangat tidak melanggar hukum, namun memiliki beberapa ketentuan hukum yang telah diatur dalam peraturan menteri. Sebagai bangsa indonesia yang baik, dari seorang pengusaha kecil, menengah dan besar, tugas terpenting dalam membangun jaringan komputer adalah memastikan sistem yang dibuat sudah pada tingkat kelayakan, meliputi adanya alat yang dapat mendeteksi sebuah serangan yang dilakukan oleh penyusup. Tujuan tersebut dapat membangun kepercayaan masyarakat sebagai pengguna karena keamanan data sudah terjaga oleh alat pendeteksi, namun akan tetap merasa tidak nyaman. Prinsip kerja keamanan jaringan tidak terlepas dari sebuah kenyamanan pengguna, semakin nyaman pengguna aplikasi maka akan mengesampingkan keamanan, sebaliknya setiap pengguna merasa tidak nyaman, maka sistem tersebut bisa dikatakan aman. Forensik jaringan memiliki kemampuan untuk merekonstruksi kejadian dengan menggunakan sistem yang menyimpan semua aktifitas lalu lintas data pada jaringan, sehingga investigasi dapat dilakukan dengan melihat kembali kejadian-kejadian yang telah terjadi dan melakukan analisa kejadian yang terjadi di masa lalu. Forensik jaringan memungkinkan dilakukannya proses analisa dan

investigasi data yang telah disimpan sebelumnya. Ada beberapa sumber bukti potensial yang dapat digunakan untuk forensik pada komputer dan 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 (A, Fadlil, dkk, 2019). Virtualisasi dan cloud computing telah menjadi tren teknologi informasi khususnya untuk perusahaan skala enterprise. MetaRouter merupakan implementasi virtualisasi pada RouterOS v3.21 keatas yang berjalan pada RouterBoard dengan platform MIPS-BE. Penelitian sebelumnya telah membuktikan bahwa antar virtual router tidak saling berhubungan dan memiliki fungsi yang berbeda (Asmunin, dkk, 2016). Pengendalian penuh pada router menyebabkan jaringan lain yang terhubung pada router juga dapat dikendalikan. Penelitian sebelumnya memanfaatkan Intrusion Detection System sebagai sistem monitoring untuk mendeteksi serangan distributed denial of service (DDoS) secara real time (Faizin, dkk, 2016). Penelitian mengenai Virtualisasi sebelumnya dilakukan oleh (Galang, dkk, 2019) yang mengimplementasikan teknik virtualisasi router menggunakan MetaRouter. Virtualisasi router dibangun menggunakan metode Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) Network Lifecycle. Penelitian selanjutnya dilakukan oleh (I. Riadi. 2011), yang menganalisis proses untuk menentukan alur lalu lintas yang melewati proses pemfilteran menggunakan firewall, implementasi serta pengujian yang dilakukan dengan metode stress test. Berdasarkan penelitian yang telah dilakukan aplikasi router menggunakan MikroTik yang di hasilkan dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran aplikasi sesuai dengan kebutuhan pengguna. Menanggulangi terjadinya kerusakan data dan serangan yang tidak diinginkan maka melakukan proteksi terhadap serangan atau alur data yang tidak wajar salah satunya dengan melakukan pembatasan akses (Kristono, dkk, 2018). Penelitian terhadap bukti tindak kriminal, telah dilakukan oleh (Mandowen, dkk, 2016), yang menganalisis dan melaporkan konten file yang diambil pada jaringan (nitroba.pcap.zip), yang merupakan arsip yang berisi kegiatan berbasis jaringan yang dipantau dan dicatat dalam jaringan Universitas Nitroba menggunakan alat forensik jaringan yang disebut Wireshark. File tangkapan jaringan yang diunduh berisi aktivitas yang dapat melanggar

hukum cyber. Badai ARP adalah situasi serangan yang sengaja dibuat oleh penyerang dari dalam jaringan lokal. Penelitian tentang ARP Storm telah dilakukan oleh (S. Vidya and R. Bhaskaran, 2011). Paket badai ARP melakukan penyerangan terus-menerus yang menghasilkan siaran paket, dengan alamat IP dalam rentang subnet atau bahkan ke alamat IP yang tidak ada di subnet lokal. Tujuan dari serangan ini adalah penyerang ingin mengurangi bandwidth dengan lalu lintas yang tidak diinginkan atau kumpulan rincian alamat IP / MAC yang membanjiri server, dari semua mesin untuk serangan selanjutnya. Bahkan alat penyerang terkenal suka menggunakan cara ini sebagai *default* untuk membangun host daftar dengan melakukan badai ARP, di mana penyerang mesin mengirimkan permintaan ARP atau ping setiap alamat IP dalam mask net saat ini.

## METODE PENELITIAN

Tujuan penelitian secara garis besar adalah mendapatkan bukti telah terjadinya serangan pada jaringan komputer menggunakan aplikasi wireshark melalui analisis forensik metarouter pada lalu lintas jaringan klien. Terdapat beberapa tahapan dalam mengungkapkan bukti tindak kriminal pada jaringan komputer yang akan dibangun. Tahapan dalam penelitian ini, dijabarkan berdasarkan langkah-langkah pada Gambar 1.



Gambar 1. Langkah-langkah penelitian

### 1. Analisis dan Kebutuhan

Langkah ini dilakukan untuk menganalisis masalah-masalah yang belum diungkapkan oleh penelitian sebelumnya, yaitu teknik tapping. Teknik tapping adalah proses penangkapan banyak atau sedikitnya paket data yang dilalui perangkat jaringan seperti HUB, Switch dan Router. Kebutuhan perangkat

pendukung analisis forensik metarouter pada lalu lintas jaringan klien disajikan pada Tabel 1.

Tabel 1. Kebutuhan Perangkat

No	Perangkat	Kebutuhan
1	Laptop	4 Buah
2	Router RB 951Ui2hnd	1 Buah v6+
3	Modem Adsl (Internet)	1 Buah
4	Modem Adsl (Switch)	1 Buah
5	Smartphone	1 Buah

Kebutuhan perangkat lunak pendukung analisis forensik metarouter pada lalu lintas jaringan klien disajikan pada Tabel 2.

Tabel 2. Kebutuhan Perangkat Lunak

No	Perangkat Lunak	Kebutuhan
1	Winbox	v3.19
2	Wireshark	v3.0.5
3	Termux	Android
4	Sistem Operasi	Windows
		10

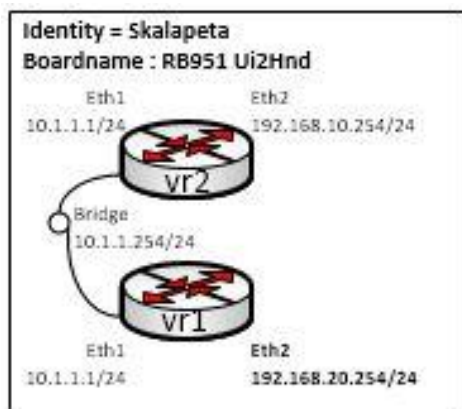
### 2. Desain

Sebelum menerapkan metarouter pada skenario nyata maupun untuk simulasi, sebaiknya tentukan topologi jaringan dan rancangan *interface* agar metarouter siap untuk menerima konfigurasi sesuai dengan skenario yang diinginkan. Metarouter yang akan dibuat sebanyak 2 (dua) unit router, masing-masing akan diberi nama vr1 dan vr2, sedangkan router asli diberi nama skalapeta. Perhatikan Gambar 2 ilustrasi topologi yang akan dibangun dalam tahapan desain metarouter.



Gambar 2. Topologi metarouter

Interface diperlukan untuk menghubungkan router dengan jaringan internet, baik melalui switch maupun perangkat jaringan lainnya. Rancangan interface dapat dilihat pada Gambar 3.



Gambar 3. Rancangan interface metarouter

Perhatikan Gambar 3 di atas, setiap metarouter mempunyai masing-masing 2 (dua) interface yaitu Eth1 digunakan untuk menghubungkan antara vr1 dan vr2 dengan bantuan *bridge* dan Eth2 digunakan untuk menghubungkan metarouter dengan router asli.

### 3. Konfigurasi

Tahapan konfigurasi dapat dilakukan dengan cara menggunakan *Command Line Interpreter (CLI)* atau console yang terdapat pada aplikasi winbox. Mengakses metarouter menggunakan CLI akan terlihat lebih rumit untuk pemula jika di dibandingkan dengan mengakses menggunakan Graphical User Interface (GUI). Pengalokasian IP address pada tahap konfigurasi dapat dilihat pada Tabel 3.

Tabel 3. Pengalokasian IP Address

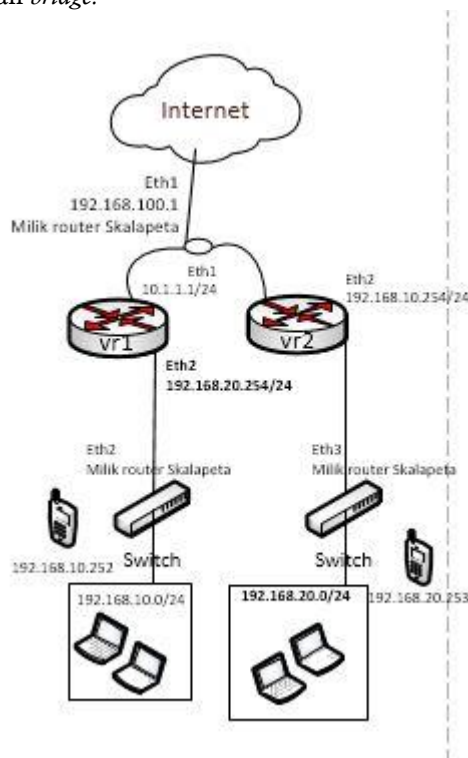
No	Perangkat	IP Address
1	vr1	192.168.20.254
2	vr2	192.168.10.254
3	Laptop1 vr1	192.168.20.5
4	Laptop2 vr2	192.168.10.5
5	Smartphone1	192.168.10.252
6	Smartphone2	192.168.20.253

### 4. Pengujian

Tahapan pengujian merupakan tahapan akhir untuk menguji sitem yang dibuat. Langkah ini akan mengungkapkan adanya serangan yang terjadi pada sistem yang dibuat, melalui *sniffing* jaringan, identifikasi dan analisis jaringan. Pengungkapan bertujuan untuk dapat menemukan IP address penyusup dari aplikasi wireshark dengan melakukan analisis paket jaringan. Tujuan lain dari penelitian ini adalah menemukan serangan yang terjadi melalui protokol yang diserang oleh penyusup dan Metode yang diusulkan juga menyarankan cara untuk mencegah serangan DDOS secara *online*.

## HASIL DAN PEMBAHASAN

Dari pembahasan metode di atas, maka dapat dibuat sebuah scenario jaringan dengan membuat 2 (dua) unit router virtual yang akan terkoneksi dengan internet dan router asli. Topologi yang akan dibuat, dapat dilihat pada Gambar 4. Gambar 4 menjelaskan ISP dengan IP 192.168.100.1, yang akan menjadi DNS server bagi router asli/fisik. Router fisik di beri nama Skalapeta yang terdapat 2(dua) router virtual di dalamnya, dengan masing-masing dihubungkan dengan *bridge*.



Gambar 4. Topologi jaringan

Router fisik dan virtual, masing-masing dapat saling berkomunikasi, dapat dilihat pada Gambar 5 dan Gambar 6.

```
Pinging 192.168.10.254 with 32 bytes of data:
Reply from 192.168.10.254: bytes=32 time=2ms TTL=62
Reply from 192.168.10.254: bytes=32 time=2ms TTL=62
Reply from 192.168.10.254: bytes=32 time=2ms TTL=62
Reply from 192.168.10.254: bytes=32 time=2ms TTL=62

Ping statistics for 192.168.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Gambar 5. Ping vr2

```
Pinging 192.168.20.254 with 32 bytes of data:
Reply from 192.168.20.254: bytes=32 time=3ms TTL=62
Reply from 192.168.20.254: bytes=32 time=2ms TTL=62
Reply from 192.168.20.254: bytes=32 time=2ms TTL=62
Reply from 192.168.20.254: bytes=32 time=2ms TTL=62

Ping statistics for 192.168.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Gambar 6. Ping vr1



Gambar 5 dan 6 menjelaskan bahwa terjadinya komunikasi yang baik antara router virtual. Perbedaan dari penelitian sebelumnya juga adalah penelitian tentang analisis forensik metarouter pada jaringan klien yang dapat membuktikan adanya serangan pada virtual router, dapat dilihat pada Gambar 7 dan 8.

No.	Time	Source	Destination	Protocol	Length	Info
127	2019-10-24 13:13:42.544113	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:43.127628	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:43.127839	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:44.127839	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:45.135780	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:45.543637	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:46.135780	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:46.543637	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:47.127864	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:47.543637	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:48.135787	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:48.543637	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:49.127723	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:49.543638	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:50.122862	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:51.465836	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:51.128084	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:51.543635	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:52.129757	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:52.543635	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:53.200480	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:54.128769	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:55.122866	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:55.482864	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:56.122478	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:56.543788	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5
127	2019-10-24 13:13:57.123289	SonyHbl_6e:17:eb	Broadcast	ARP	60	who has 192.168.10.254? Tell 192.168.10.252
127	2019-10-24 13:13:57.543814	Clevisy_33:44:55	Broadcast	ARP	42	who has 192.168.10.254? Tell 192.168.10.5

Gambar 7. Serangan ARP vr2

Time	Source	Destination	Proto	Length	Info
424	2019-10-24 14:16:57.832422	Clevisy_33:44:55	HS-RS-PhysLs	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
430	2019-10-24 14:16:58.832377	Clevisy_33:44:55	HS-RS-PhysLs	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
440	2019-10-24 14:17:02.238674	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
453	2019-10-24 14:17:03.831959	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
458	2019-10-24 14:17:04.832018	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
461	2019-10-24 14:17:05.238762	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
464	2019-10-24 14:17:06.831966	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
465	2019-10-24 14:17:07.831939	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
466	2019-10-24 14:17:09.653914	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
467	2019-10-24 14:17:10.548055	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
468	2019-10-24 14:17:11.548062	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
469	2019-10-24 14:17:15.167541	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
470	2019-10-24 14:17:16.842338	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
472	2019-10-24 14:17:17.842294	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
473	2019-10-24 14:17:18.842343	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
473	2019-10-24 14:17:21.639970	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
474	2019-10-24 14:17:22.445091	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
475	2019-10-24 14:17:23.643902	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
476	2019-10-24 14:17:24.645383	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
477	2019-10-24 14:17:24.776641	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
478	2019-10-24 14:17:25.542048	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
479	2019-10-24 14:17:25.645193	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
480	2019-10-24 14:17:26.541995	Clevisy_33:44:55	Broadcast	ARP	42 who has 192.168.20.254? Tell 192.168.20.5
481	2019-10-24 14:17:26.633982	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
486	2019-10-24 14:17:27.644930	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
487	2019-10-24 14:17:28.445023	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
488	2019-10-24 14:17:29.653864	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
489	2019-10-24 14:17:30.644729	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
490	2019-10-24 14:17:31.645362	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
491	2019-10-24 14:17:32.646168	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
492	2019-10-24 14:17:32.646170	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253
494	2019-10-24 14:17:33.645375	SonyHbl_6e:17:eb	Broadcast	ARP	60 who has 192.168.20.254? Tell 192.168.20.253

Gambar 8. Serangan ARP vr1

Serangan badai ARP pada masing-masing virtual router dilakukan oleh perangkat smartphone dengan inisial sonymobile, melalui IP 192.168.10.252 dan 192.168.20.253. Tercatat Mac Address dari perangkat sonimobile adalah 58:48:22:6e:17:e0. Perangkat tersebut membanjiri protokol ARP agar permintaan terhadap server tidak dapat terpenuhi. Protokol ICMP dapat membuktikan bahwa serangan tersebut sangat menghambat permintaan tujuan selanjutnya, dapat dilihat pada Gambar 9 dan 10.

Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 13:53:20.185649	192.168.10.5	SSDP	206	M-SEARCH * HTTP/1.1
2	2019-10-24 13:53:21.194052	192.168.10.5	SSDP	206	M-SEARCH * HTTP/1.1
3	2019-10-24 13:53:22.213965	192.168.10.5	SSDP	206	M-SEARCH * HTTP/1.1
4	2019-10-24 13:53:23.215639	192.168.10.5	SSDP	206	M-SEARCH * HTTP/1.1
5	2019-10-24 13:53:40.041109	192.168.10.5	ICMP	74	Destination unreachable
6	2019-10-24 13:53:43.043699	192.168.10.5	ICMP	72	Destination unreachable
7	2019-10-24 13:53:47.540223	192.168.10.5	ICMP	84	Destination unreachable
8	2019-10-24 13:53:52.045402	192.168.10.5	ICMP	115	Destination unreachable
9	2019-10-24 13:54:01.055271	192.168.10.5	ICMP	84	Destination unreachable
10	2019-10-24 13:54:04.541802	192.168.10.5	ICMP	84	Destination unreachable
11	2019-10-24 13:54:09.053620	192.168.10.5	ICMP	84	Destination unreachable
12	2019-10-24 13:55:02.053283	192.168.10.5	ICMP	84	Destination unreachable
13	2019-10-24 13:55:06.044663	192.168.10.5	ICMP	94	Destination unreachable
14	2019-10-24 13:55:08.045414	192.168.10.5	ICMP	84	Destination unreachable
15	2019-10-24 13:55:12.543317	192.168.10.5	ICMP	84	Destination unreachable
16	2019-10-24 13:55:20.188556	192.168.10.5	SSDP	206	M-SEARCH * HTTP/1.1
17	2019-10-24 13:55:21.188974	192.168.10.5	SSDP	206	M-SEARCH * HTTP/1.1
18	2019-10-24 13:55:22.208013	192.168.10.5	SSDP	206	M-SEARCH * HTTP/1.1
19	2019-10-24 13:55:23.213297	192.168.10.5	SSDP	206	M-SEARCH * HTTP/1.1

Gambar 9. Komputer klien vr2

Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 14:45:42.260641	192.168.20.5	SSDP	206	M-SEARCH * HTTP/1.1
2	2019-10-24 14:45:43.261859	192.168.20.5	SSDP	206	M-SEARCH * HTTP/1.1
3	2019-10-24 14:45:44.263244	192.168.20.5	SSDP	206	M-SEARCH * HTTP/1.1
4	2019-10-24 14:45:45.264207	192.168.20.5	SSDP	206	M-SEARCH * HTTP/1.1
5	2019-10-24 14:45:54.684934	192.168.20.5	NBNS	82	Name query NB vP4000 A
6	2019-10-24 14:45:54.686668	192.168.20.5	NBNS	60	Standard query NB vP4000 A
7	2019-10-24 14:45:54.686727	fe80::7c68:ee4::ff02::1b	NBNS	80	Standard query NB vP4000 A
8	2019-10-24 14:45:54.688138	fe80::7c68:ee4::ff02::1b	LLMNR	74	Standard query NB vP4000 A
9	2019-10-24 14:45:54.688516	192.168.20.5	LLMNR	54	Standard query NB vP4000 A
10	2019-10-24 14:45:55.089624	fe80::7c68:ee4::ff02::1b	LLMNR	74	Standard query NB vP4000 A
11	2019-10-24 14:45:55.099805	192.168.20.5	LLMNR	54	Standard query NB vP4000 A
12	2019-10-24 14:45:55.434624	192.168.20.5	NBNS	82	Name query NB vP4000 A
13	2019-10-24 14:45:55.680520	192.168.20.5	NBNS	60	Standard query NB vP4000 A
14	2019-10-24 14:45:55.687943	fe80::7c68:ee4::ff02::1b	NBNS	80	Standard query NB vP4000 A
15	2019-10-24 14:45:56.186595	192.168.20.5	NBNS	82	Name query NB vP4000 A
16	2019-10-24 14:46:02.543712	192.168.20.5	ICMP	580	Destination unreachable
17	2019-10-24 14:46:32.543364	192.168.20.5	ICMP	110	Destination unreachable
18	2019-10-24 14:46:36.043360	192.168.20.5	ICMP	84	Destination unreachable
19	2019-10-24 14:46:39.043072	192.168.20.5	ICMP	84	Destination unreachable
20	2019-10-24 14:46:42.043656	192.168.20.5	ICMP	84	Destination unreachable
21	2019-10-24 14:46:45.043458	192.168.20.5	ICMP	84	Destination unreachable
22	2019-10-24 14:46:48.043517	192.168.20.5	ICMP	73	Destination unreachable
23	2019-10-24 14:46:52.043900	192.168.20.5	ICMP	72	Destination unreachable
24	2019-10-24 14:47:42.261708	192.168.20.5	SSDP	206	M-SEARCH * HTTP/1.1
25	2019-10-24 14:47:43.262594	192.168.20.5	SSDP	206	M-SEARCH * HTTP/1.1
26	2019-10-24 14:47:44.262941	192.168.20.5	SSDP	206	M-SEARCH * HTTP/1.1
27	2019-10-24 14:47:45.263843	192.168.20.5	SSDP	206	M-SEARCH * HTTP/1.1

Gambar 10. Komputer klien vr1

## SIMPULAN

Melihat dari hasil penelitian, analisis forensik metarouter pada lalu lintas jaringan klien, dapat disimpulkan bahwa: Metarouter sangat berguna untuk tujuan memecah jaringan jika router yang dimiliki hanya 1 (satu) unit. Terlihat bahwa klien dapat memiliki router dan mempunyai fungsi yang sama dengan router fisik sehingga dapat digunakan sesuai dengan keinginan klien walau hanya sebuah virtual router. Aplikasi Wireshark dapat 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.

## SARAN

1. Penelitian selanjutnya akan lebih baik apabila tidak hanya terbatas pada penggunaan aplikasi Wireshark saja sebagai alat analisis paket, namun menggunakan aplikasi lainnya seperti tcpdump ataupun network miner.
2. Melakukan penelitian secara *offline*, agar dapat membandingkan dengan lalu lintas *online*, sehingga dapat menemukan periode waktu rata-rata, khususnya pada serangan badai ARP.
3. Uji coba serangan menggunakan koneksi jaringan *Ethernet*, lakukan analisis dan perbandingan dengan serangan menggunakan Wireless, khususnya pada lalu lintas paket data yang akan dikirim oleh penyusup sehingga dapat menemukan hasil yang lebih efisien berdasarkan jenjang waktu tangkapan.

## UCAPAN TERIMA KASIH

Ucapan terima kasih ditujukan kepada Dr. Abdul Fadlil, M.T, Rusydi Umar, S.T., M.T., Ph.D, Sunardi, S.T., M.T., Ph.D, Dr. Imam Riadi, M.Kom, Anton Yudhana, S.T., M.T., Ph.D. Seluruh dosen Program Studi Magister Teknik Informasi Universitas Ahmad Dahlan Yogyakarta. Serta teman-teman HM2TIF angkatan 2019.

## DAFTAR PUSTAKA

- A, Fadlil., I, Riadi., & S, Aji. (2017). Pengembangan Sistem Pengamanan Jaringan Komputer Berdasarkan Analisis Forensik Jaringan.
- A, Fadlil., I, Riadi., & S, Aji. (2017). Pengaman Jaringan Menggunakan Sistem Berbasis Mikrokontroler Berdasarkan Analisis Forensik Jaringan, Palembang.
- Albert, S., & Juni, E. (2015). Analisa Sistem Pengaman Data Jaringan Berbasis VPN.
- Asmunin, Aditya Hermawan (2016). Penerapan dan Analisis Virtualisasi Router Menggunakan RouterOS.
- Faizin Ridho, Anton Yudhana, Imam Riadi. (2016). Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Denial of Service (DDoS) Secara Real Time, Yogyakarta.
- Galang, C. M., Eko, S., & Imam, A. (2017). Teknik Virtualisasi Router Menggunakan Metarouter Mikrotik (Studi Kasus: Laboratorium Jaringan Komputer Politeknik Negeri Lampung).
- I, Riadi. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik.
- I, Riadi, R. Umar, F. Aini (2019). Analisis Perbandingan Detection Traffic Anomaly Dengan Metode Naive Bayes Dan Support Vector Machine (Svm).
- Kristono & Riadi, I. 2018. Simulation for Data Security Improvement In Exploited Metarouter. International Journal of Computer Science and Information Security.
- Kurniawan, Agus (2012). *Network Forensics* – Panduan analisis dan investigasi paket data jaringan menggunakan wireshark.
- Mandowen, S.A., (2016). Wireshark dan NetworkMiner dalam investigasi mengekstrak dan menganalisa paket file yang direkam pada jaringan dan mendapatkan bukti. Universitas Cenderawasih, Jayapura.
- R Umar, A Yudhana, MN Faiz. (2016). Analisis Live Forensics Untuk Perbandingan Keamanan Email Pada Sistem Operasi Proprietary. ILKOM, Universitas Ahmad Dahlan Yogyakarta.
- T, Rendra., Herman. (2016). Mikrotik Metarouter 100% *illusion*. Jasakom.
- Vidya.S, R. Bhaskaran (2011). ARP Storm Detection and Prevention Measures. IJCSI International Journal of Computer Science. Department of Computer Science, Fatima College, India.
- Y. Prayudi, D. Afrianto (2007). Antisipasi Cybercrime Menggunakan Teknik Komputer Forensik. Seminar Nasional Aplikasi Teknologi Informasi 2007 (SNATI 2007) Yogyakarta, 16 Juni 2007