

METODE *LIVE FORENSICS* UNTUK ANALISIS SERANGAN *DENIAL OF SERVICE* (DoS) PADA ROUTER

MUHAMMAD ALIM ZULKIFLI

13917122

Tesis Diajukan Sebagai Syarat untuk Meraih Gelar Magister Komputer

Konsentrasi Forensik Digital

Program Studi Magister Teknik Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2018

METODE *LIVE FORENSICS* UNTUK ANALISIS SERANGAN *DENIAL OF SERVICE* (DoS) PADA ROUTER

MUHAMMAD ALIM ZULKIFLI

13917122

Tesis Diajukan Sebagai Syarat untuk Meraih Gelar Magister Komputer

Konsentrasi Forensik Digital

Program Studi Magister Teknik Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2018

LEMBAR PENGESAHAN PEMBIMBING

METODE *LIVE FORENSICS* UNTUK ANALISIS SERANGAN *DENIAL OF SERVICE* (DoS) PADA ROUTER

MUHAMMAD ALIM ZULKIFLI

13917122

Yogyakarta, 8 April 2018

Pembimbing Utama

Dr. Imam Riadi, M.Kom

LEMBAR PENGESAHAN PENGUJI

METODE *LIVE FORENSICS* UNTUK ANALISIS SERANGAN *DENIAL OF SERVICE* (DoS) PADA ROUTER

MUHAMMAD ALIM ZULKIFLI

13917122

Yogyakarta, 8 April 2018

Tim Penguji,

Dr. Imam Riadi, M.Kom
Ketua

Yudi Prayudi, S.Si, M.Kom
Anggota I

Dr. Bambang Sugiantoro, M.T.
Anggota II

Mengetahui,
Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST., M.Sc

ABSTRAK

Masalah serangan Daniel of Service (DoS) pada suatu jaringan terus berkembangan dilingkungan masyarakat. Khususnya serangan yang DoS dilakukan oleh oknum tertentu dan ditujukkan pada jaringan Router orang lain untuk memperoleh hak akses dan tidak jarang serangan yang dilakukan menyebabkan jaringan Router yang ditargetkan menjadi *down* (lumpuh) karena tidak mampu melayani permintaan *user* yang memiliki hak akses secara sah, sehingga diperlukannya analisis serangan DoS pada Router dan mengali informasi, serta menarik data forensik sebagai bukti digital adanya serangan DoS pada Router dengan metode *live forensics*.

Serangan Denial of Service (DoS) adalah serangan jaringan terstruktur yang berasal dari berbagai sumber dan berkumpul untuk membentuk arus paket besar. Serangan DoS bertujuan untuk mengganggu layanan yang tersedia pada jaringan target dengan membanjiri *bandwidth* atau sistem kapasitas pemrosesan yang membuat jaringan *server* target menjadi kelebihan beban. Wireshark adalah alat yang dapat digunakan untuk mendeteksi serangan DoS pada jaringan Router dan melakukan analisis lalu lintas jaringan yang memiliki fungsi dan berguna untuk para profesional jaringan, administrator jaringan, peneliti, dan pengembangan perangkat lunak jaringan, yang membutuhkan deteksi serangan DoS pada Router dan mengali informasi serta menarik data forensik sebagai bukti digital serangan DoS pada Router melalui metode live forensics.

Outout yang dihasilkan penelitian ini berhasil menarik data informasi serangan DoS terkait data log aktivitas dan alamat IP penyerang.

Kata Kunci: Serangan DoS (Denial of Service), Router, Live Forensics.

ABSTRACT

The problem of attack Daniel of Service (DoS) on a network continues to develop in the community. Specifically, DoS attacks are carried out by a particular person and assigned to another person's Router network to obtain permissions and not infrequently the attacks caused the targeted Router network to be down (paralyzed) for not being able to serve requests of users who have legitimate access rights, analysis of DoS attacks on the Router and multiplying information, as well as attracting forensic data as digital evidence of a DoS attack on the Router with live forensics method.

Denial of Service (DoS) attacks are structured network attacks that originate from multiple sources and converge to form large packet currents. The DoS attack aims to disrupt the services available on the target network by flooding the bandwidth or system processing capacity that makes the target server network overloaded. Wireshark is a tool that can be used to detect DoS attacks on a Router network and perform network traffic analysis that has functions and is useful for network professionals, network administrators, researchers, and network software development, requiring the detection of DoS attacks on the Router and multiplying information as well as attracting forensic data as a digital evidence of DoS attacks on the Router through live forensics methods

Output generated by this research managed to pull the data of DoS attack information related to activity log data and attacker IP address.

***Keywords**: Denial of Service (Denial of Service), Router, Live Forensics.*

PERNYATAAN KEASLIAN PENELITIAN

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli saya, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain, kecuali referensi atas material tersebut dan disebutkan dalam daftar pustaka tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, 8 April 2018



Muhammad Alim Zulkifli

PUBLIKASI SELAMA MASA STUDI

Zulkifli, A. M. I., Riadi, I., & Sugiantoro, Y., (2018). Live Forensics Method For Analysis Denial of Service (DoS) Attack on Routerboard, vol.**180** no.**35**

Publikasi yang menjadi bagian dari tesis

Kontributor	Jenis Kontribusi
Muhammad Alim Zulkifli	Mendesain eksperimen (70%) Menulis *paper* (70%)
Imam Riadi	Mendesain eksperimen (20%) Menulis dan Mengedit *paper* (20%)
Yudi Prayudi	Mendesain eksperimen (10%) Mengedit *paper* (10%)

KONTRIBUSI YANG DIBERIKAN OLEH PIHAK LAIN DALAM TESIS INI

Tidak ada kontribusi dari pihak lain

HALAMAN PERSEMBAHAN

Bismillahirrahmanirrahim…

Kupersembahkan karyaku ini kepada orang-orang yang telah mengajariku belajar memaknai kehidupan.

1. Terimakasihku yang sangat besar untuk Ibuku Tercinta, Ibuku Tersayang, Ibuku Terkasih yang selalu mendoakan dalam setiap proses yang saya kerjakan dan tak henti memberikan semangat dan motivasi agar aku tidak menyerah
2. Bapakku yang juga memberikan dukungan dan selalu mengingatkanku untuk selalu mendekatkan diri kepada Allah SWT dalam menjalani segala proses ini.
3. Adik adik ku Agsa dan Gadis yang menjadi motivasiku untuk menjadi orang yang hebat agar kelak aku bisa menjadi contoh yang layak untuk kalian ikuti dan bahkan bisa lebih dariku.
4. Terima kasih kepada Bapak Yudi Prayudi dan Bapak Imam Riadi selaku dosen dan pembimbing yang telah dengan sabar membimbing saya sampai terselesaikannya tesis ini.
5. Terimaksih yang spesial buat Susan Susanti yang selalu menyemangati dan menemani di dalam pembuatan tesis ini
6. Untuk teman teman seperjuangan yang selalu saling support dan mau berbagi ilmu.

Dengan segala ketulusan hati,

Muhammad Alim Zulkifli

KATA PENGANTAR

Assalamualaikum, Wr, Wb

Alhamdulillah, puji syukur kehadirat Allah SWT atas segala nikmat, karunianya sehingga tesis yang berjudul "Metode Live Forensics untuk Analisis Serangan Denial of Service (DoS) pada Router" dapat diselesaikan.

Tesis ini disusun sebagai salah satu syarat untuk meraih gelar Magister Komputer pada program studi Magister Teknik informatika, Program Pascasarjana Fakultas Teknologi Industri, Universitas Islam Indonesia, disusun sebagai sarana untuk menerapkan ilmu yang telah didapatkan selama masa perkuliahan dengan konsentrasi Forensik Digital.

Dalam penyusunan laporan ini tidak lepas dari dukungan pihak terkait, oleh karena itu pada kesempatan ini penulis dengan kerendahan hati ingin menyampaikan rasa terima kasihnya kepada:

1. Allah SWT, tiada tuhan selain Allah, Muhammad utusan-Nya.
2. Bapak Dr. Imam Riadi, M.Kom. selaku Dosen Pembimbing I.
3. Bapak Yudi Prayudi, S.Si., M.Kom. selaku Dosen Pembiming II.
4. Ketua Program Pascasarjana FTI UII & seluruh formasinya.
5. Dosen Magister Teknik Informatika khususnya untuk konsentrasi forensik digital.
6. Teman-teman Forensik Digital angkatan 8.
7. Pihak-pihak anonim yang langsung maupun tidak langsung memberikan dukungan.
8. Akhir kata semoga laporan ini dapat berguna bagi kemajuan ilmu pengetahuan terutama pada bidang forensika digital. Aamiin.

Wassalamualaikum, Wr. Wb

Yogyakarta, 8 April 2018

Muhammad Alim Zulkifli

DAFTAR ISI

Halaman

HALAMAN JUDUL i

HALAMAN PENGESAHAN PEMBIMBING ii

HALAMAN PENGESAHAN PENGUJI iii

ABSTRAK iv

ABSTRAC v

PERNYATAAN KEASLIAN PENELITIAN vi

PUBLIKASI SELAMA PENELITIAN vii

KONTRIBUSI PIHAK LAIN viii

HALAMAN PERSEMBAHAN ix

KATA PENGANTAR x

DAFTAR ISI xi

DAFTAR TABEL xiii

DAFTAR GAMBAR xiv

DAFTAR TAKARIR DAN SINGKATAN xv

BAB 1 PENDAHULUAN 1

1.1 Latar Belakang 4

1.2 Permasalahan 4

1.3 Rumusan Masalah 4

1.4 Batasan Masalah 4

1.5 Tujuan Penelitian 4

1.6 Manfaat Penelitian 5

1.7 Metode Penelitian 6

1.8 Sistematika Penulisan 6

1.9 Literature Review 7

BAB 2 LANDASAN TEORI 15

2.1 Network Protocol Analyzer 15

2.2 Network Attack 16

2.3 Security Attack Models 16

2.4 Process Attactk 16

2.5 Network Forensics 17

2.6 Live Forensics 17

2.7 Topologi Jaringan 18
2.8 MikroTik Router 20
2.9 DNS Flood Master (DNS Flooding) 21
2.10 Jenis Serangan pada Jaringan Router 23
2.11 Denial of Service (DoS) 25
2.12 Wireshark 26
BAB 3 METODE PENELITIAN 27
3.1 Studi Pustaka 27
3.2 Alat dan Persiapan Penelitian 27
3.3 Rancangan Simulasi Serangan DoS pada Router 28
3.4 Alur Analisis Serangan DoS pada Router 28
3.5 Implementasi Simulasi Serangan 29
3.6 Tahap Akuisisi 29
3.7 Analisis Forensik dan Verifikasi Data 30
BAB 4 HASIL DAN PEMBAHASAN 31
4.1 Proses Observasi pada MikroTik Router 31
4.2 Persiapan Skenario Pengujian Serangan DoS 32
4.2.1 Simulasi Serangan pada Router 32
4.2.2 Analisis Serangan DoS pada Router 33
4.2.3 Pengujian Menggunakan Aplikasi 33
4.3 Akuisis Data 37
4.3.1 Log Activity 39
4.3.2 IP Address List 41
4.4 Hasil Pengujian Analisis Serangan DoS pada Router 41
BAB 5 KESIMPULAN DAN SARAN 43
5.1 Kesimpulan 43
5.2 Saran 43
DAFTAR PUSTAKA 45
LAMPIRAN 47

DAFTAR TABEL

Tabel 2.1 Literature Review 10
Tabel 2.2 Penelitian yang Relevan 14
Tabel 4.1 Komponen-Komponen WinBox MikroTik Router 32
Tabel 4.2 Hasil Analisis Serangan DoS pada Router 42

DAFTAR GAMBAR

Gambar 2.1 Cara Kerja DNS 10
Gambar 2.2 DoS Attack..... 25
Gambar 3.1 Alur Penelitian 27
Gambar 3.2 Desain Analisis Serangan DoS pada Router..... 28
Gambar 3.3 Alur Analisis Serangan DoS pada Router 28
Gambar 3.4 Rancangan Simulasi Serangan DoS dan Akuisisi Data dengan Metode Live Forensics 29
Gambar 4.1 Konsep Simulasi Serangan DoS 32
Gambar 4.2 Tampilan Tourch sebelum ada Serangan DoS..... 33
Gambar 4.3 Serangan Scanning Port DNS Flooding 34
Gambar 4.4 Keadaan Lalu Lintas Ping..... 34
Gambar 4.5 Wireshark Mendeteksi Serangan DoS pada Protocol DNS..... 35
Gambar 4.6 Kondisi CPU dan Memory sebelum ada Serangan DoS pada Router 36
Gambar 4.7 Traffict Monitor System Setelah Terjadi Serangan DoS 36
Gambar 4.8 Mekanisme Akuisisi Data Menggunakan Metode Live Forensik 38
Gambar 4.9 Data Log Activity Serangan pada Router..... 40
Gambar 4.10 Tampilan IP Address List Penyerang 41

DAFTAR TAKARIR DAN SINGKATAN

API	: Application Programming Interface
IP Address	: Internet Protocol Address
Mac Address	: Media Access Control Address
DNS	: Dynamic Name Server
ARP	: Address Resolution Protocol
DHCP	: Dynamic Host Configuration Protocol

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi komputer berbasis jaringan telah banyak memberikan kemudahan kepada para penggunanya untuk melakukan aktivitas secara online dengan tujuan mengirim data atau hanya sekedar mengakses media online. Namun dibalik kecangihan teknologi jaringan komputer, telah banyak juga memunculkan permasalahan Forenksi Jaringan.

Penyebab utama dari masalah forensik jaringan adalah tindak penyalahgunaan teknologi oleh orang-orang yang tidak bertanggung jawab dengan tujuan memanfaatkan fasilitas jaringan pihak lain untuk kepentingan pribadi maupun kelompok, (Sitompul Josua, 2012). Diantara banyaknya serangan yang sering terjadi di Internet adalah serangan DoS (*Denial of Service*) merupakan jenis serangan jaringan komputer yang dapat mengakibatkan server tidak mampu melayani permintaan User, hingga menyebabkan jaringan komputer menjadi down, (E, Wit. and Van K, 2014).

Router merupakan sistem operasi Linux Base yang diperuntukkan sebagai *Network* Router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasi dan pengaturannya bisa dilakukan melalui menu WinBox. Selain itu instalasi dapat dilakukan pada standar komputer PC (*Personal Computer*). PC yang akan dijadikan Router pun tidak memerlukan *resource* yang cukup besar untuk penggunaan standar, misalnya hanya sebagai *Gateway*. Sedangkan untuk keperluan beban yang besar (*network* yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan *resource* PC yang memadai, (Mancill, 2002).

Forensik jaringan merupakan ilmu pengetahuan mengenai keamanan jaringan Komputer yang berkaitan dengan penyelidikan untuk menentukan sumber serangan jaringan berdasarkan Bukti Data Login, Identifikasi, Analisis, dan Rekonstruksi Kejadian. Penempatan Router pada sebuah Topologi yang dijadikan sebagai *Gateway* pada suatu jaringan berfungsi untuk mendistribusikan data keluar masuknya dari dan ke Komputer lainnya, sehingga seluruh Komputer dapat mengakses data bersama-sama seperti Internet *sharing*, (Mancill, 2002).

Hak akses administrator pada perangkat Router memberikan pengendalian penuh terhadap Router yang berarti pengendalian penuh terhadap jaringan. Sedangkan fungsi utama dari sistem operasi Router meliputi Firewall dan NAT, Bandwidth Limiter, Routing, Hospot, Akses Point to Point Tunneling Protocol, DSN Server, Hospot dan lain sebagainya. Hal tersebut membuat banyak *hacker*/penyerang menjadikan Router sebagai target serangan utama karena Router merupakan perangkat penting dalam sebuah jaringan.

Sistem operasi Router dirancang sebagai Router dan terhubung dalam sebuah jaringan, hal inilah yang menyebabkan sebuah jaringan Komputer yang tersambung pada Router rawan dari tindakan serangan jaringan oleh orang-orang yang tidak bertanggung jawab.

Serangan pada Router dilakukan dalam bentuk penyusupan dengan menggunakan berbagai macam jenis serangan jaringan Komputer melalui *Tools* yang dibuat secara mandiri ataupun *Tools* yang di dapat dari pasar, (Abdul Fadlil, Imam Riadi, 2017). Dari uraian tersebut dapat dipahami bahwa pentingnya melakukan analisis serangan pada Router karena keamanan data menjadi hal penting dalam komunikasi data pada suatu sistem jaringan komputer.

Salah satu cara yang bisa digunakan untuk melakukan analisis serangan pada Router, yaitu memanfaatkan aplikasi *Wireshark* yang memiliki fungsi-fungsi bagi jaringan dan administrator jaringan karena *Tools* ini mampu menangkap paket-paket data/informasi dalam berbagai format Protocol yang berjalan dalam jaringan, sehingga data atau informasi tersebut bisa ditarik untuk keperluan pemeriksaan Forensik jaringan, (Dimaio, 2001).

Forensik jaringan merupakan proses mendeteksi, menangkap, mencatat dan menganalisa aktivitas jaringan guna menemukan bukti digital dari suatu serangan atau kejahatan yang dilakukan melalui jaringan Komputer sehingga pelaku kejahatan dapat dituntut sesuai hukum yang berlaku, (Mukkamala, et al, 2003). Bukti digital dapat diidentifikasi dari pola serangan yang dikenali melalui metode Live Forensics.

Live Forensics merupakan keadaan atau proses analisis Forensik yang dilakukan ketika sistem jaringan Komputer sedang beroperasi, (Artformatics, 2013). Hal ini dikarenakan informasi bukti digital hanya bisa didapatkan pada saat sistem berjalan dan informasi tersebut bisa hilang jika sistem jaringan dalam keadaan mati.

Umumnya penarikan data dari Router memanfaatkan CLI (*Command Line Interface*) untuk mengirimkan *syntax* atau perintah untuk mengambil informasi. Namun perintah pengambilan informasi sulit untuk diakukan karena banyaknya *syntax* CLI yang perlu dikirimkan agar mendapatkan informasi yang mencukupi dalam investigasi, sehingga diperlukan solusi yang dapat membantu dan mempermudah proses penarikan data tanpa harus menuliskan banyak perintah, dan salah satu cara yang dapat dilakukan adalah melakukan analisis serangan pada Router melalui aplikasi *Wireshark*.

Wireshark merupakan salah satu dari banyak *Tools Networking* administrator untuk menganalisa lalu-lintas jaringan, termasuk Protocol didalamnya, karena *Wireshark* mampu menangkap paket-paket data atau informasi dalam berbagai format Protocol secara mudah untuk dianalisis, (Sarsono, 2012). Sedangkan untuk keperluan pemeriksaan Forensik jaringan terkait serangan pada Router, maka dalam penelitian ini dilakukan juga simulasi serangan pada Router menggunakan aplikasi DNS Flood Master, (DNS Flooding). DNS atau *Domain Name System* merupakan sistem berbentuk data base terdistribusi yang akan memetakan/mengkonversikan nama host/mesin/domain ke alamat IP (Internet Protocol) dan sebaliknya dari alamat IP ke hostname yang disebut dengan *reverse-mapping*, (Ali. A and Hudaid, 2014).

Jenis serangan yang diterapkan dalam penelitian ini adalah serangan DoS (*Denial of Service*). Umumnya serangan DoS dilakukan secara individual menggunakan mesin komputer. Serangan ini dijalankan komputer penyerang yang lebih kuat dari targetnya sehingga penyerang mampu membanjiri targetnya dengan paket-paket yang dikirim pada target, (Casey, 2010). Tipe serangan DoS yang diterapkan dalam penelitian ini adalah *Flooding,* yang merupakan tipe serangan menggunakan Protocol TPC, UDP atau ICMP untuk membanjiri target dengan paket-paket *request* yang dikirim. Misalnya TPC Flood.

Penelitian terdahulu yang dilakukan (M. Junaidi Syahputra, Ilham Faisal, 2012) terkait analisis deteksi serangan pada jaringan komputer dengan *Wireshark* menggunakan metode anomally-bases IDS, menyimpulkan bahwa dari semua penyerangan yang dilakukan memiliki karakteristik berbeda-beda sehingga dapat dibedakan paket data yang normal dan paket data yang tidak normal. Hasil penelitiannya juga menjelaskan bahwa *Wireshark* dapat digunakan dengan baik untuk mendeteksi serangan pada jaringan Komputer. Begitu juga dengan hasil

penelitian yang dilakukan oleh (I. Riadi & Umar, Rusydi, 2012) terkait analisis forensik serangan SQL *injection* menggunakan metode *Statis* Forensik. Hasil penelitian ini menyimpulkan bahwa dari hasil pengamatan yang dilakukan dengan metode Statis Forensik penyerang hanya melihat isi data belum mengubah data base yang ada di website.

Berdasarkan paparan hasil dari kedua peneliti di atas terkait serangan yang terjadi pada jaringan, dapat diketahui bahwa masih ada celah kelemahan pada kedua penelitian tersebut karena kedua peneliti hanya fokus pada pengamatan serangan yang masuk pada jaringan tanpa melakukan pemetaan dan penarikan data terkait dari mana serangan jaringan tersebut dilakukan. Sehingga penulis berasumsi bahwa untuk proses analisis deteksi jenis serangan DoS pada Router perlu dilakukan akuisisi data pada Router untuk menentukan karakteristik bukti digital melalui metode *Live Forensics*.

1.2 Permasalahan

Berdasarkan paparan latar belakang di atas, dapat dipahami bahwa masalah serangan terhadap suatu jaringan terus berkembangan dilingkungan masyarakat. Khususnya serangan yang dilakukan oleh oknum tertentu dan ditujukkan pada jaringan Router orang lain untuk memperoleh hak akses dan tidak jarang serangan yang dilakukan tersebut menyebabkan jaringan Router yang ditargetkan menjadi *Down* (lumpuh) karena tidak mampu melayani permintaan *User* yang memiliki hak akses sah, sehingga diperlukannya analisis serangan pada Router dan mengali informasi, serta menarik data forensik sebagai bukti digital serangan DoS pada Router melalui metode *Live Forensics*.

1.3 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka rumusan masalah penelitian ini adalah:

a. Bagaimana melakukan analisis serangan DoS (*Denial of Service*) pada Router?
b. Bagaimana melakukan akuisisi data pada Router menggunakan metode *Live Forensics*?
c. Bagaimana karakteristik bukti digital pada Router?

1.4 Batasan Masalah

Berdasarkan latar belakang masalah dan rumusan masalah di atas, maka batasan masalah dalam penelitian ini sebagai berikut:

a. Penelitian ini hanya berlingkup pada perangkat jaringan Router.
b. Penelitian ini menggunakan Router RB951Ui Versi 6.
c. Kegiatan akuisisi data penelitian ini bersifat *Live Forensics* (dilakukan pada saat sistem operasi jaringan sedang beroperasi).
d. Skenario simulasi serangan pada Router menggunakan aplikasi DNS Flood Master (DNS Flooding) pada saat proses jaringan Router sedang beroperasi.
e. Skenario untuk analisis serangan pada Router menggunakan aplikasi *Wireshark*.
f. Penelitian ini dibatasi pada proses analisis serangan DoS (*Denial of Service*) pada Router. Artinya tidak ada proses pengembangan proteksi kemananan lalu-lintas pada jaringan Router.

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diajukan, maka tujuan diadakannya penelitian ini sebagai berikut:

a. Melakukan analisis serangan pada Router menggunakan aplikasi *Wireshark*.
b. Mencari informasi lalu-lintas serangan pada jaringan Router yang bisa digunakan sebagai bukti digital melalui metode *Live Forensics.*
c. Melakukan simulasi serangan menggunakan Aplikasi DNS Flooding pada Router.
d. Mengetahui jenis konten serangan DoS pada Router.
e. Melakukan akuisisi data dan analisis serangan pada perangkat Router.
f. Mengetahui karakteristik bukti digital pada perangkat Router untuk keperluan forensik.

1.6 Manfaat Penelitian

Berdasarkan paparan uraian latar belakang masalah, rumusan masalah, batasan masalah dan tujuan penelitian di atas, maka manfaat yang ingin dicapai dalam penelitian ini, yaitu:

a. Bagi Pengembangan Ilmu pengetahuan.
    1) Memberikan panduan dalam proses investigasi Forensik pada jaringan Router.
    2) Sebagai pendalaman materi dalam bidang *Network Forensics* terutama pada sub bidang Router melalui metode *Live Forensics*.
b. Bagi Peneliti lain.

    Sebagai referensi bagi peneliti lain yang meneliti tentang Router menggunakan metode *Live Forensics.*

c. Bagi Penulis

Penelitian ini diharapkan dapat menambah wawasan, kualitas keilmuan baik dalam hal teori maupun praktek.

1.7 Metode Penelitian

Adapun langkah-langkah yang ditempuh selama melakukan penelitian ini, sebagai berikut:

a. Studi Literatur

Penelitian ini dilandaskan pada studi kepustakaan dengan mengumpulkan teori atau referensi yang relevan untuk menunjang tujuan penelitian ini melalui buku-buku, jurnal ilmiah, artikel, paper, makalah, dan akses beberapa situs website yang membahas tentang Router, serangan pada Router, dan metode *Live Forensics*.

b. Pengambilan Data Router

Pada tahap pengambilan data Router peneliti menggunakan aplikasi *Wireshark*.

c. Simulasi Serangan dan Pengujian

Simulasi serangan dalam penelitian ini menggunakan *Tools* DNS Flooding untuk menyerang Router. Tahap implementasi yang dimaksud dalam simulasi dan pengujian ini bertujuan untuk mengetahui keberhasilan dalam penarikan data dan informasi dari Router serta menguji informasi yang telah berhasil ditarik oleh aplikasi *Wireshark*.

d. Analisis

Tahapan analisis ini dilakukan untuk memperoleh informasi dari Router sebagai bukti digital yang dapat difungsikan untuk keperluan Forensik

e. Kesimpulan dan Saran

Tahapan laporan adalah tahapan akhir untuk menyampaikan kesimpulan atas hasil yang diperoleh dari penelitian ini.

1.8 Sistematika Penulisan

Sistematika penulisan ini bertujuan memberikan gambaran secara umum terkait penulisan untuk memberikan penjelasan secara ringkas terhadap kerangka penulisan penelitian, sebagai berikut:

BAB I PENDAHULUAN

Pendahuluan terdiri dari latar belakang, permasalahan, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Landasan teori terdiri dari teori *Network Protocol Analyzer*, *Network Attack*, *Security Attack Models*, *Process Attack*, *Network Forensics*, *Live Forensics*, Topologi Jaringan, MikroTik Router, DNS Flood Master, Jenis Serangan pada Router, DoS (*Denial of Service*), dan Aplikasi *Wireshark*.

BAB III ANALISA DAN PERANCANGAN

Bab ini membahas tentang kerangka konsep penelitian dan gambaran umum mengenai langkah penyelesaian yang dilakukan. Bagan proses investigasi dibuat berdasarkan referensi yang di dapat kemudian digunakan untuk menyelesaikan penelitian dengan pembuatan perancangan simulasi pembuktian bagan proses investigasi yang dikembangkan.

BAB IV IMPLEMENTASI

Bab ini, berisikan simulasi yang telah dirancang pada Bab III kemudian diimplementasikan pada sistem yang sebenarnya. Hasil yang di dapat pada tahap simulasi dianalisis kembali dan dilakukan pembahasan penelitian.

BAB V: KESIMPULAN DAN SARAN

Tahapan ini adalah tahapan terakhir yang dilakukuan dalam penelitian ini dan memuat tentang kesimpulan dari keseluruhan uraian dari bab-bab sebelumnya, serta memberikan saran terkait dengan kekurangan yang diperoleh dalam penelitian untuk pengembangan Ilmu Pengetahuan dikemudian hari.

DAFTAR PUSTAKA DAN LAMPIRAN

Daftar pustaka berisi referensi terkait penelitian, baik melalui buku, artikel, paper, jurnal, makalah, situs yang terkait yang dapat menunjang kegiatan penelitian. Lampiran berisi gambar-gambar ataupun tabel terkait penelitian dan pendukungnya (jika ada).

1.9 *Literature Review*

Pada bagian ini akan dibahas ulasan tentang penelitian sebelumnya yang relevan dan berkaitan dengan Router dan forensik jaringan.

Penelitian terbaru yang dilakukan oleh (Mazdadi, 2017) terkait forensik pada RouterOS menggunakan metode Live Forensics menjelaskan bahwa pada perangkat Router berbasis RouterOS, terdapat suatu media API *(Application Proggraming Interface) service* yang dapat dimanfaatkan untuk menggali informasi dari perangkat Router. informasi yang tersimpan pada RouterOS dapat diakuisisi dengan mengembangkan suatu aplikasi yang bisa berkomunikasi secara *remote* dengan memanfaatkan *port* 8726. Aplikasi yang dibangun dapat menjadi solusi untuk mempermudah proses akuisi dalam aktivitas forensik jaringan terhadap perangkat Router berbasis RouterOS. *Output* yang dihasilkan berupa informasi terkait Log Activity, IP Address List, ARP, DHCP Leases, DNS Cache, dan Router Board *Info* yang dapat digunakan untuk analisis untuk pengungkapan suatu aktivitas serangan yang terjadi pada Router. Peberdaan penelitian ini, dengan penelitian yang akan dilakukan oleh penulis, yaitu penelitian ini menggunakan aplikasi API sebagai media dalam menjelaskan identifikasi pada Router, sedangkan dalam penelitian penulis menggunakan software Wireshark untuk mendeteksi serangan pada Router dan menganalisisnya menggunakan metode Live Forensics.

Penelitian yang dilakukan oleh (Abdul Fadlil, Imam Riadi, 2017) terkait pengembangan sistem pengamanan jaringan komputer berdasarkan analisis forensik jaringan, menjelaskan bahwa deteksi serangan menggunakan WinBox RouterOS v3,6 dimana software tersebut menunjukan *resources*, data penyerang IP Address, Jumlah Paket Data, dan Kapan Terjadi Serangan. Simulasi serangan menggunakan *software* LOIC untuk mengetahui kinerja sistem pengaman jaringan komputer, sedangkan sistem pengamanan jaringan komputer berupa antisipasi terhadap bentuk serangan DDoS. Penelitian yang dilakukan (I. Riadi & Umar, Rusydi, 2012), menjelaskan bahwa SQL *Injection* merupakan sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan *string* yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Dengan menggunakan SQL *Injection* ini, maka akan dapat mengetahui apakah *website* tersebut pernah atau sedang ada penyerang yang memanipulasi data. Berdasarkan hasil penelitian terdapat beberapa ip *address* yang masuk melalui celah keamanan *website* kemahasiswaan. Penyerang menggunakan *tools* SQL *Injection*.

Perbedaan penelitian ini dengan penelitian yang dilakukan oleh penulis, yaitu penelitian ini menggunakan metode statis forensik untuk mendeteksi serangan pada jaringan, sedangkan penelitian ini menggunakan metode *live forensics* dengan media winbox untuk mendeteksi serangan terhadap Router.

Penelitian yang dilakukan oleh (Resi Utami Putri, 2012), terkait forensik jaringan studi kasus serangan SQL *Injection* pada *server* UGM, metode yang digunakan adalah model proses forensik (*The Forensic Process Model*) sebuah model proses investigasi forensik digital, yang terdiri dari tahap pengkoleksian, pemeriksaan, analisis dan pelaporan. Penelitian dilakukan selama lima bulan dengan mengambil data dari *Intrusion Detection System* (IDS) *Snort*. Beberapa *file log* digabungkan menjadi satu *file log*, lalu data dibersihkan agar sesuai untuk penelitian. Terdapat 68 IP *address* yang melakukan tindakan illegal SQL *Injection* pada server www.ugm.ac.id. Kebanyakan penyerang menggunakan *tools* SQL *Injection* yaitu Havij dan SQLMap sebagai *tools* otomatis untuk memanfaatkan celah keamanan pada suatu website. Selain itu, ada yang menggunakan skrip *Python*, yaitu berasal dari benua Eropa yaitu di Romania. Perbedaan penelitian ini dengan penelitian yang akan dilakukan adalah media yang digunakan dalam mendeteksi serangan jaringan berbeda.

Penelitian yang dilakukan (Pidei Wiyanto, Amir Hamzah, 2014) terkait aplikasi monitoring keamanan jaringan dengan menggunakan IDS dan Router mikrotik, menjelaskan bahwa aplikasi keamanan jaringan komputer dengan menggunakan metode dari *Snort Intrusion Detection System* dan mikrotik. Penggabungan metode IDS dan IP Tables mikroti merupakan sistem pencegahan penyusup. Selain itu juga menggunakan web untuk mempermudah admin untuk *monitoring*. Aplikasi ini bertujuan untuk menciptakan sistem keamanan jaringan *computer* yang ringan, berbasiskan web dan mudah dianalisa serta diatur oleh *administrator*. Sistem ini dirancang akan memberikan *blocking* pada alamat IP yang diketahui mengirimkan paket penyusup. Perbedaan kedua penelitian ini terlihat pada metode dan media yang digunakan untuk mendeteksi serangan pada jaringan mikrotik *router* yang dilakukan oleh penyusup pada sistem. Penelitian (Setia, 2010) terkait mikrotik *Personal Computer Router* pada jaringan *local* menjelaskan bahwa untuk mendukung komunikasi data antar karyawan dan dengan pihak *client* maka dibutuhkan koneksi internet yang handal. Koneksi internet ini dilengkapi dengan

system operasi *linux base* atau yang dikenal dengan mikrotik RouterOS™. Jenis mikrotik yang digunakan adalah mikrotik router versi 2.9.27. Prosedur penganalisaan jaringan komputer dimulai dengan menganalisa instalasi LAN, dilanjutkan dengan menganalisa konfigurasi PC Router (IP Address, Konfigurasi Gateway, Konfigurasi *domain name server*, NAT), kemudian menganalisa DHCP *server*, menganalisa *transparent proxy server* dan diakhiri dengan penganalisaan *bandwidth management*. Berdasarkan hasil analisa jaringan menunjukan bahwa kegunaan mikrotik sangat mendukung koneksi internet. Hal ini dapat di lihat dari hasil pengukuran *bandwidth local* dan *internasional*. Perbedaan penelitian, penelitian ini menggunakan media Router untuk mengukur analisis pada pembagian *bandwidth* sedangkan penelitiann yang akan dilakukan penulis lebih difokuskan pada mendeteksi serangan jaringan pada Router dengan menggunakan winbox dan melalui metode *live forensics*.

(Fiebig, 2013) melakukan penelitian terkait DHCP pada Router. Dalam penelitian ini dilakukan penggalian informasi serta mengobservasi cara untuk melakukan extrak informasi dari Router kelas kecil atau yang biasa disebut Home RouterOS. Dengan memanfaatkan JTAG Tobias dapat mengambil informasi *mac address* dan *hostname* terhadap *computer client* yang terhubung pada jaringan tersebut dari image memory router. Pada tahun yang sama Taveras mengimplementasikan *live forensics* untuk mengumpulkan bukti digital pada SCADA (*Supervisory Control and Data Acquisition System)*. Pengumpulan bukti digital didasarkan pada aktivitas perubahan pembacaan sensor yang abnormal, dan trafik komunikasi yang abnormal. Penelitian yang dilakukan (Desti dan Riadi, 2017) terkait *network forensics for detecting flooding attack on web server*, menjelaskan bahwa ancaman serius keamanan jaringan pada *server web* yang mengakibatkan hilangnya *bandwidth* dan kelebihan beban bagi pengguna dan *server web* penyedia layanan. Hasil analisis skenario penelitian ini diperoleh 15 IP *address* yang tercatat melakukan tindakan ilegal pada *web server*. Penelitian ini telah berhasil mendeteksi adanya serangan pada jaringan dengan metode *live forensics* pada *server web*. Penelitian yang dilakukan (Nguyen, K, Tran, D, Ma, W, and Sharma, 2014) tentang pendekatan dalam mendeteksi serangan pada jaringan. Meskipun solusi berdasarkan BFD, SVM, dan *entropy* telah diaplikasikan untuk mengidentifikasi *executable data fragments* namun masih tidak ada solusi untuk *clustered* data *fragments* kedalam *group* yang berbeda berdasarkan *entropy* sebelum deteksi *fragments* dari *group*

tersebut, maka dalam penelitian ini mereka berhasil melakukan pendekatan yang dapat mengclusterkan *fragments* data menjadi 3 *group* berdasarkan nilai *entropy* dan membuat 3 model yang berbeda menggunakan SVM untuk mendeteksi *executable contents* berdasarkan *entropy* dari data *fragment*.

(Hariyadi, D, dan Supriyono, 2017) melakukan penelitian dengan membangun kerangka investigasi forensik *file-sharing* samba pada mesin peladen berdasarkan Standar Nasional Indonesia (SNI) ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital (Badan Standarisasi Nasional 2014). Hasil yang diperoleh pada penelitian ini bahwa 1). Penanganan investigasi forensik pada sistem kritis harus hati-hati karena memiliki karakteristik sistem yang tidak diperkenankan *shutdown*. Mesin peladen file-sharing berbasis Samba merupakan bagian sistem yang kritis. Dalam penelitian ini diusulkan model investigasi forensik khusus mesin peladen file-sharing berbasis Samba, yaitu akuisisi secara langsung pada mesin peladen file-sharing dan akuisisi secara langsung melalui jaringan klien. Kedua model ini berdasarkan dari Standar Nasional Indonesia tentang Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital (SNI ISO/IEC 27037:2014). 2). Kerangka invenstigasi forensik pada penelitian ini belum mencakup pada perangkat elektronik dengan fungsi sebagai peladen *file-sharing* yang sifatnya portabel dan tidak kritis seperti perangkat *Access Point* terbaru. *Access Point* saat ini tidak hanya berfungsi sebagai transmisi dan penerima sinyal secara nirkabel namun telah dilengkapi dengan fitur layanan *file-sharing*. Cukup menambahkan media penyimpanan eksternal seperti SD Card maka *Access Point* tersebut dapat berfungsi sebagai mesin peladen *file-sharing*.

(Dwi et al., 2017) melakukan penelitian terkait analisis forensik digital aplikasi *Instant Messenger* yang terinstal pada sistem operasi Windows 10, peneliti menyimpulkan bahwa dalam menerapkan dan pengimplementasian teknik Live Forensics untuk mendapatkan bukti digital dari aktivitas penggunaan aplikasi *Instant Messenger* membutuhkan Tools dan teknik yang berbeda untuk mendapatkan analisa yang sesuai dengan yang diinginkan. Teknik dan tools untuk Live Forensics sendiri juga tidak dapat digunakan pada waktuyang lama, dikarenakan apabila RAM mati maka tidak dapat dilakukan dumping dan analisabarang bukti. Maka dari itu untuk pelaksanaan Live Forensic dibutuhkan metode baku agar dapat menjamin validitas dan integritas serta kelengkapan data yang dibutuhkan.

Paparan singkat penelitian di atas, selengkapnya diuraikan dalam Tabel 2.1 di bawah ini:

Tabel 2.1 *Literature Review*

No	Nama	Judul	Uraian Singkat	Hasil
1	(Mazdadi, 2017)	Analisis Forensik Pada RouterOS Menggunakan Metode Live Forensics	Penelitian ini menggunakan perangkat Router berbasis RouterOS, melalui media API (*Application Proggraming Interface*) *services* yang dimanfaatkan untuk menggali informasi dari perangkat *Router*.	Informasi yang tersimpan pada RouterOS dapat diakuisisi dengan mengembangkan suatu Aplikasi yang bisa berkomunikasi secara remote dengan memanfaatkan port 8726. Aplikasi yang dibangun dapat menjadi solusi untuk mempermudah proses akuisi dalam aktivitas forensik jaringan terhadap perangkat Router berbasis RouterOS. Output yang dihasilkan berupa informasi terkait Log Activity, IP Address List, ARP, DHCP Leases, DNS Cache, dan RouterBoard Info yang dapat digunakan untuk analisis untuk pengungkapan suatu aktivitas serangan yang terjadi pada Router.
2	(Abdul Fadlil, Imam Riadi, 2017)	Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan	Penelitian ini menggunakan *software* LOIC Untuk keperluan simulasi serangan pada jaringan yang diteliti, sedangkan untuk mendeteksi serangan yang masuk menggunakan *software* winbox	Pengujian dan analisis sistem pengaman jaringan komputer dapat dirancang menggunakan bukti forensik jaringan komputer, dan setelah dibuat sistem pengaman jaringan komputer, penyerang tidak akan mampu melakukan serangan pada waktu yang akan datang menggunakan metode yang sama.
3	(I. Riadi & Umar, Rusydi, 2012)	Analisis Forensik Serangan SQL *Injection* Menggunakan Metode Statis Forensik	Penelitian ini menggunakan metode Statis Forensik untuk menganalisis serangan yang masuk pada jaringan website	Hasil analisis penyerang menggunakan SQL *Injection* untuk masuk ke celah keamanan. Dari hasil pengamatan yang dilakukan dengan metode Statis *Forensics* penyerang hanya melihat isi data belum mengubah *database* yang ada di website.

Lanjutan Tabel 2.1 *Literature Review*

No	Nama	Judul	Uraian Singkat	Hasil
4	(Resi Utami Putri, 2012)	Analisis Forensik Jaringan Srudi Kasus Serangan *SQL Injection* pada *Server* UGM	Dalam penelitian ini menggunakan sistem forensik jaringan yang dirancang merupakan sebuah alat untuk menganalisis bukti dari *file log*. Sistem forensik jaringan diletakkan pada *server* forensik jaringan yang terhubung dengan *core switch* PPTIK dan memiliki IP statik 10.13.253.36. Sistem tersebut terdiri dari skrip *parsing pcap*, skrip *port scanning* dan skrip untuk merubah *file log* ke *database*.	Dari hasil analisis data *log* serangan *SQL Injection* yang menuju ke *server* Universitas Gadjah Mada (www.ugm.ac.id), serangan dilakukan kebanyakan menggunakan *tools* seperti *Havij* dan *SQLMap*. Selain itu, ada yang menggunakan skrip Python yaitu berasal dari benua Eropa, tepatnya di Romania. *Tools* yang dibuat adalah *parsing* PCAP yang dapat memecah *file log* dalam bentuk PCAP berdasarkan tanggal, IP address, *mac address* dan nomor *port*, sedangkan *tools* kedua, yaitu *port scanning* yang dapat mengetahui *port* yang terbuka maupun yang tertutup pada suatu *host* atau *server*, dan yang terakhir adalah *tools* untuk mengubah *file log* PCAP ke bentuk database sehingga data *log* bisa dianalisis secara lebih mendalam.
5	(Pidei Wiyanto, Amir Hamzah, 2014)	Aplikasi *Monitoring* Keamanan Jaringan Dengan Menggunakan IDS Dan *Router* Mikrotik	Pada proses pengujian yang dilakukan mampu mengenali segala aktivitas yang dilakukan *intruder* dalam usaha untuk menyusup ke dalam *system* dengan menggunakan SSH *brute force*, FTP *brute force*, *Port scanner*, kemudian diproses *blocking* terhadap IP *address* yang dianggap sebagai *intruder*.	Kategori serangan yang paling tinggi didalam sistem adalah serangan SSH, bila *intruder* dapat mengetahui *username* dan *password* sebuah *system* maka *intruder* dapat melakukan apa saja terhadap *system* tersebut. Untuk serangan FTP dapat dikategorikan kedalam tingkat menengah, karena tidak mendapat hak akses secara penuh kedalam *server*. Sedangkan *port scanner* dikategorikan serangan paling rendah karena *intruder* hanya mengetahui *port* yang terbuka.

Lanjutan Tabel 2.1 *Literature Review*

No	Nama	Judul	Uraian Singkat	Hasil
6	(Fiebig, 2013)	Forensic DHCP Information Extraction from Home Routers	Dalam penelitian ini dilakukan penggalian informasi serta mengobservasi cara untuk melakukan extrak informasi dari *Router* kelas kecil atau yang biasa disebut *Home Routers.* Dengan memanfaatkan JTAG.	Dapat mengambil informasi *mac address* dan *hostname* terhadap *computer client* yang terhubung pada jaringan dari *image memory router*. Implementasi metode *live forensics* untuk mengumpulkan bukti digital pada SCADA (*Supervisory Control and Data Acquisition System)*. Pengumpulan bukti digital didasarkan pada aktivitas perubahan pembacaan *sensor* yang abnormal, dan *traffic* komunikasi yang abnormal.
7	(Desi dan Riadi, 2017)	*Network Forensics For Detecting Flooding Attcak On Web Server*	Sistem IDS yang berlaku untuk skenario penelitian ini telah bekerja seperti yang diharapkan, sistem dapat merekam aktivitas jaringan dalam bentuk *file log* dengan ekstensi P.CAP *file* tersebut dapat dianalisis dengan alat *Wireshark*.	Diketahui bahwa 15 *server* web alamat IP *addres* melakukan tindakan ilegal, yang mengakibatkan lalu lintas macet. Dengan menerapkan model proses forensik, sistem IDS pada *server web* dapat digunakan untuk membantu memenuhi kebutuhan forensik, selain itu *administrator* dapat memantau dan mencegah serangan di masa depan.
8	(Nguyen, K, Tran, D, Ma, W, and Sharma, 2014)	*An Approach to Detect Network Attacks Applied for Network Forensics*	Penelitian ini dilakukan untuk mendeteksi serangan pada jaringan berdasarkan *entropy* dan data *fragment*	Meskipun solusi berdasarkan BFD, SVM, dan *entropy* telah diaplikasikan untuk mengidentifikasi *executable data fragments* namun masih tidak ada solusi untuk *clustered* data *fragments* kedalam *group* yang berbeda berdasarkan *entropy* sebelum deteksi *fragments* dari *group* tersebut, maka dalam penelitian ini mereka berhasil melakukan pendekatan yang dapat mengclusterkan *fragments* data menjadi 3 *group* berdasarkan nilai *entropy* dan membuat 3 model yang berbeda menggunakan SVM untuk mendeteksi *executable contents* berdasarkan *entropy* dari data *fragment*.

Lanjutan Tabel 2.1 *Literature Review*

No	Nama	Judul	Uraian Singkat	Hasil
9	(Hariyadi, D, dan Supriyono, 2017)	Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI	Dalam penelitian ini diusulkan model investigasi forensik khusus mesin peladen *file-sharing* berbasis Samba, yaitu akuisisi secara langsung pada mesin peladen *file-sharing* dan akuisisi secara langsung melalui jaringan klien	Penanganan investigasi forensik pada sistem kritis harus hati-hati karena memiliki karakteristik sistem yang tidak diperkenankan *shutdown*. Mesin Peladen *file-sharing* berbasis Samba merupakan bagian sistem yang kritis. Kedua model ini berdasarkan dari Standar Nasional Indonesia tentang Pedoman Identifikasi, Pengumpulan, Akuisisi, dan *Preservasi* Bukti Digital (SNI ISO/IEC 27037:2014). Kerangka invenstigasi forensik pada penelitian ini belum mencakup pada perangkat elektronik dengan fungsi sebagai peladen *file-sharing* yang sifatnya portabel dan tidak kritis seperti perangkat *Access Point* terbaru. *Access Point* saat ini tidak hanya berfungsi sebagai transmisi dan penerima sinyal secara nirkabel namun telah dilengkapi dengan fitur layanan *file-sharing*. Cukup menambahkan media penyimpanan eksternal seperti SD Card maka *Access Point* tersebut dapat berfungsi sebagai mesin peladen *file-sharing*.
10	(Dwi et al., 2017)	Analisis Forensik Digital Aplikasi *Instant Messenger* yang Terinstal Pada Sistem Operasi Windows 10	Dalam penelitian digunakan teknik *live forensics* untuk mendapatkan bukti digital dari aktivitas penggunaan aplikasi *Instant Messenger*	peneliti menyimpulkan bahwa dalam menerapkan dan pengimplementasian teknik *live forensics* untuk mendapatkan bukti digital dari aktivitas penggunaan aplikasi *Instant Messenger* membutuhkan *tools* dan teknik yang berbeda untuk mendapatkan analisa yang sesuai dengan yang diinginkan. Teknik dan tools untuk *live forensics* sendiri juga tidak dapat digunakan pada waktuyang lama, dikarenakan apabila RAM mati maka tidak dapat dilakukan dumping dan analisabarang bukti. Maka dari itu untuk pelaksanaan *live forensic* dibutuhkan metode baku agar dapat menjamin validitas dan integritas serta kelengkapan data yang dibutuhkan.

Berbeda dengan penelitian terdahulu, dalam penelitian ini berada pada kategori metode *live forensics* menggunakan media *software* winbox dengan objek penelitian *Router* Mikrotik. Berikut paparan singkat mengenai uraian singkat penelitian ini, seperti yang tertera pada Tabel 2.2 berikut:

Tabel 2.2 Penelitian yang Diusulkan

Judul	**Uraian Singkat Masalah Penelitian**	**Solusi**	**Hasil yang Diharapkan**
Metode Live Forensics Untuk Mendeteksi Serangan Pada Router	Melakukan explorasi terhadap bukti digital yang bisa didapatkan dari Sistem Operasi Router untuk memperoleh informasi yang dapat digunakan dalam investigasi forensik jaringan, serta memetakan jenis informasi pada Router dan bagaimana proses pengambilan data terkait deteksi serangan pada Router	Melakukan pendeteksian sedini mungkin pada perangkat Router untuk mengetahui jenis serangan pada Router dengan memanfaatkan aplikasi DNS Flood Master (DNS Flooding) sebagai media semulasi serangan, dan untuk keperluan deteksi serangan pada Router menggunakan aplikasi *Wireshark*.	1. Menggali informasi yang bisa digunakan sebagai bukti digital dari perangkat Router menggunakan aplikasi Wireshark 2. Melakukan akuisisi data pada perangkat Router melalui metode Live Forensics untuk mendapatkan data yang memungkinkan untuk digunakan sebagai bukti digital Forensik. 3. Mengetahui karakteristik bukti digital pada perangkat Router untuk keperluan forensik. 4. Mengetahui jenis konten serangan apa saja yang dideteksi melalui perangkat Router.

BAB 2
LANDASAN TEORI

Teori-teori yang digunakan untuk menunjang penelitian ini, terdiri dari teori *Network* Protocol *Analyzer*, *Network Attack*, *Security Attack Models*, *Process Attack*, *Network Forensics*, *Live Forensics*, Topologi Jaringan, MikroTik Router, DNS Flood Master, Jenis Serangan pada Router, DoS (*Denial of Service*), dan Aplikasi *Wireshark*.

2.1 *Network* Protocol *Analyzer*

Jaringan protokol analisis adalah proses untuk sebuah program atau perangkat untuk memecahkan kode *header* protokol jaringan dan trailer untuk memahami data dan informasi di dalam paket di enkapsulasi oleh protokol. Untuk melakukan analisis protokol, paket harus ditangkap pada *real time* untuk analisis jalur kecepatan atau analisis nanti. Program atau perangkat disebut analyzer protocol, (Dimaio, 2001).

Protokol pada satu lapisan harus berkomunikasi dengan protocol pada lapisan yang sama. Fungsi utama dari *network* protocol *analyzer* adalah untuk *decode* protokol di setiap lapisan. Protocol Informasi dari beberapa lapisan dapat digunakan oleh network protocol analyzer untuk mengidentifikasi kemungkinan masalah dalam komunikasi jaringan, yang disebut ahli analisis. Analisa protocol dapat men-*decode* protocol lapisan ganda dan paket untuk kembali membangun paket tingkat yang lebih rendah (seperti tingkat *Link, IP* atau *TCP*) ke tingkat yang lebih tinggi (seperti tingkat aplikasi) pesan untuk pemahaman mendalam tentang lalu lintas jaringan dan aktivitas pengguna. Teknik ini digunakan dalam analisa protocol ketika lalu lintas jaringan pemantauan dan pengawasan pengguna adalah tujuan utama, (Arasteh, 2007).

Network protocol analyzer dapat digunakan baik untuk manajemen jaringan yang sah atau untuk mencuri informasi dari jaringan. Jaringan operasi dan personil pemeliharaan menggunakan *network protocol analyzer* untuk memonitor lalu lintas jaringan, menganalisis paket, menonton pemanfaatan sumber daya jaringan, melakukan analisis forensik dari pelanggaran keamanan jaringan dan memecahkan masalah jaringan. Analisa protocol yang tidak sah bisa sangat berbahaya bagi keamanan jaringan karena mereka hampir mustahil untuk mendeteksi dan dapat dimasukkan hampir di mana saja, (Arasteh, 2007).

2.2 *Network Attack*

Network attacks dikategorikan menurut letak dan dapat dibagi menjadi dua, yaitu *network attacks* yang berasal dari dalam *network* itu sendiri dan *network attacks* yang berasal dari luar *network*. Sedangkan bentuk *network attacks* dapat berasal dari sebuah host dan dapat juga berupa sebuah *device*/perangkat keras yang berhubungan dengan target, sebagai contoh kasus *wiretapping* yang menjadi sasaran atau target dari sebuah *attacks* dapat berupa *host* maupun *network* itu sendiri. Jika diasumsikan bahwa pengamanan terhadap infrastruktur dari sebuah *network* telah dilakukan, maka yang perlu diwaspadai adalah serangan dari luar *network*, dimana hanya proteksi saja yang dapat diandalkan untuk menghindari bahaya dari *network attacks* yang berasal dari luar. Untuk mengetahui bagaimana cara untuk memproteksi sebuah *network* dari *attacks* yang berasal dari luar *network* maka ada baiknya mengetahui apa yang menjadi motivasi adanya sebuah *attacks*, (Casey, 2010).

2.3 *Security Attack Models*

*Interruptio*n adalah perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availabilit*y) dari sistem.Contoh serangan adalah "*Denial of Service attack.*" Jika *interception* yang dari pihak yang tidak berwenang dan berhasil mengakses asset atau informasi jaringan. Contoh dari serangan ini adalah penyadapan *(wiretapping). Modification* merupakan pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari *website* dengan pesan-pesan yang merugikan pemilik *website. Fabrication* merupakan pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer, (L. Volonino and R, 2008).

2.4 *Process Attack*

Menurut (Fiebig, 2013) serangan atau *attacks* pada sebuah *network* biasanya mempunyai proses atau tahap atau fase yang harus dilalui. Misalnya pada fase pertama adalah fase persiapan. Dalam fase persiapan, *attacker* akan mengumpulkan informasi sebanyak mungkin mengenai target yang menjadi sasarannya. Fase kedua adalah fase eksekusi, fase ini merupakan *attack* yang sebenarnya dimana *attacker* melangsungkan *attack* pada sebuah sistem. Antara fase pertama dan fase kedua terkadang ditemui kasus di mana saat fase pertama berlangsung, berlangsung juga

fase kedua. Contoh *scanning* untuk mendapatkan informasi pada sebuah *host* sama dengan *attack* pada *network* yang melingkupinya. Fase ketigan dalah fase akhir yang disebut dengan fase *post-attack*. Fase ketiga merupakan fase akibat dari fase pertama dan fase kedua. Bisa jadi terjadinya kerusakan pada sebuah *network*, atau dikuasainya sebuah sistem *network* yang kemudian digunakan kembali oleh penyerang untuk melakukan serangan pada sistem *network* lainnya. Contoh jenis serangan ini adalah DoS (*Denial of Service*).

2.5 *Network Forensics*

Forensik jaringan merupakan suatu usaha untuk menemukan informasi penyerang, mencari bukti-bukti potensial setelah terjadi serangan atau insiden pada jaringan. Serangan-serangan ini antara lain Probing, DDoS, User to Root (U2R) dan Remote to Local.

Forensik jaringan merupakan proses menangkap, mencatat dan menganalisa aktivitas jaringan guna menemukan bukti digital dari suatu serangan atau kejahatan yang dilakukan menggunakan jaringan Komputer sehingga pelaku kejahatan dapat dituntut sesuai hukum yang berlaku, (Mukkamala, et al, 2003). Bukti digital dapat diidentifikasi dari pola serangan yang dikenali, penyimpangan dari perilaku normal jaringan ataupun penyimpangan dari kebijakan keamanan yang diterapkan pada jaringan. Forensik jaringan memiliki berbagai aktivitas dan teknik analisis. Sebagai contoh analisis dari proses pada *Network Intrusion Detection System* (NIDS), (Dimaio, 2001), analisis dari lalu-lintas jaringan dan analisis dari piranti jaringan dianggap sebagai bagian dari Forensik Jaringan.

2.6 *Live Forensics*

Live Forensics merupakan keadaan atau proses analisa yang dilakukan ketika sistem jaringan sedang berjalan. Metode yang dilakukan dan Filosofi pendekatannya adalah sama dengan proses Forensik tradisional yang ada, namun ketika sistem mati proses terhenti dan dilanjutkan dengan menggunakan proses Forensik tradisional/biasa, (Casey, 2010).

Live Forensics dilakukan untuk mencari informasi dan barang bukti dalam sebuah jaringan lokal, artinya kita menghadapi keadaan di mana Komputer atau alat bukti yang ditemui di tempat kejadian perkara terhubung pada sebuah jaringan Komputer dan dalam keadaan *Power On*, (Casey, 2010). Hal ini memberikan keuntungan dari kekurangan proses Forensik tradisional yang tidak dapat

menganalisa sebuah jaringan Komputer untuk mencari barang bukti serta informasi didalamnya, (Dimaio, 2001).

Menurut (Dimaio, 2001) setiap metode maupun cara yang dilakukan pasti ada kekurangan dan kelebihannya masing-masing, tidak terkecuali pada metode *Live Forensics*, kelemahan pada *Live Forensics*, meliputi:

a. Berbedanya instalasi setiap Komputer, keterbatasan pengetahuan ataupun keahlian yang dimiliki oleh seorang analisis Forensik akan menjadi sebuah hambatan karena *Environment* setiap Komputer berbeda sistem operasinya dan perangkat *Hardwarenya*.
b. Kemungkinan data termodifikasi dan mempengaruhi akuisisi data untuk disajikan pada saat persidangan kasus penyerangan jaringan.
c. Berkaitan dengan File gambar yang akan mengalami kompresi ketika akan diambil atau dipindahkan mempengaruhi kualitas dari gambar tersebut dan akan menjadi sulit untuk diidentifikasi pada saat melakukan analisa ataupun ketika dihadirkan pada saat persidangan.
d. Bukti yang diambil dari jaringan menjadi barang bukti yang tidak terpercaya karena kemungkinan hadirnya teknik Anti Forensik yang dapat mengelabui seorang investigator.
e. Data yang diambil dalam sebuah jaringan menjadi sebuah data yang Korup, sehingga mengurangi akuisisi barang bukti.

Live Forensics memiliki pengaruh positif ketika teknik *Forensics* tradisional tidak mampu mengambil barang bukti berupa data dari jaringan, (Arasteh, 2007).

2.7 Topologi Jaringan

Topologi jaringan Komputer adalah infrastruktur fisik jaringan Komputer yang digunakan untuk mengimplementasikan LAN, (Irawan, 2005).

Berikut adalah jenis Topologi jaringan LAN yang sering digunakan:

a. Topologi Bintang: Topologi bintang adalah topologi jaringan Komputer yang menggunakan *concentrator* (hub/*switch*) sebagai pengatur paket data. Topologi bintang memiliki kontrol yang terpusat. Semua Link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau *client* yang dipilihnya. Simpul pusat dinamakan stasiun primer atau *server* dan lainnya dinamakan stasiun sekunder atau *client server*. Setelah hubungan jaringan dimulai oleh *server*

maka setiap *client server* sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari *server*.

1) Kelebihan:
   a) Kerusakan pada satu saluran hanya akan mempengaruhi jaringan pada saluran tersebut dan *station* yang terpaut.
   b) Tingkat keamanan termasuk tinggi.
   c) Tahan terhadap lalu lintas jaringan yang sibuk.
   d) Kemudahan deteksi dan isolasi kesalahan/kerusakan pengelolaan jaringan.
2) Kelemahan
   a) HUB jadi elemen kritis karena kontrol terpusat.
   b) Jaringan tergantung pada terminal pusat.
   c) Biaya jaringan lebih mahal.

b. Topologi Bus: Topologi Bus adalah topologi jaringan komputer yang menggunakan sebuah kabel utama (*backbone*) sebagai tulang punggung jaringan.
   1) Keunggulan
      a) Hemat kabel sehingga biaya instalasi relatif lebih murah.
      b) Penambahan dan pengurangan terminal dapat dilakukan tanpa menganggu operasi yang berjalan.
      c) *Layout* kabel sederhana sehingga instalasi relatif lebih mudah.
   2) Kelemahan
      a) Kepadatan pada jalur lalu lintas.
      b) Bila terdapat gangguan di sepanjang kabel pusat, maka keseluruhan jaringan akan mengalami gangguan.
c. Topologi Token Ring: Topologi Ring adalah topologi jaringan yang berupa lingkaran tertutup yang berisi node-node. Semua komputer yang saling tersambung membentuk lingkaran (seperti Bus, tetapi ujung-ujungnya disambung). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai loop. Data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan.

1) Keunggulan

a) Dapat melayani aliran lalulintas data yang padat.
b) Aliran data mengalir lebih cepat karena dapat melayani data dari kiri atau kanan dari *server*.
c) Trasmisi data yang relatif sederhana seperti perjalanan paket data dalam satu arah saja.

2) Kelemahan

a) Kerusakan pada salah satu media pengirim/terminal dapat melumpuhkan kerja seluruh jaringan.
b) Paket data harus melewati setiap komputer antara pengirim dan penerima, sehingga menjadi lebih lambat.
c) Pengembangan jaringan menjadi lebih kaku karena penambahan terminal atau node menjadi lebih sulit bila port sudah habis.

2.8 MikroTik Router

MikroTik Router merupakan sistem operasi Linux Base yang diperuntukkan sebagai Network Router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui WinBox. Selain itu instalasi dapat dilakukan pada standar komputer PC (*Personal Computer*). PC yang akan dijadikan Router pun tidak memerlukan *resource* yang cukup besar untuk penggunaan standar, misalnya hanya sebagai *Gateway*. Untuk keperluan beban yang besar (*network* yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan *resource* PC yang memadai.

Router memiliki kemampuan melewatkan paket IP Address dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router yang saling terhubung dalam jaringan internet turut serta dalam sebuah Algoritma *routing* terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP *address* dari sistem ke sistem lain.

Router memiliki antarmuka konfigurasi *command-line* yang kuat namun mudah dipelajari dengan kemampuan scripting yang terintegrasi.

a. WinBox GUI *over* IP dan MAC.
b. CLI dengan Telnet, SSH, konsol lokal dan konsol serial.
c. API untuk memprogram alat Anda sendiri.
d. Antarmuka web.

Proses routing dilakukan secara *hop by hop*. (Dimaio, 2001). IP address tidak mengetahui jalur keseluruhan menuju tujuan setiap paket. IP *routing* hanya menyediakan IP Address dari Router berikutnya yang menurutnya lebih dekat ke host name tujuan. Fungsi Router antara lain:

a. Membaca alamat logika IP Address *source* dan *destination* untuk menentukan routing dari suatu LAN ke LAN lainnya.
b. Menyimpan routing *table* untuk menentukan *rute* terbaik antara LAN ke WAN.
c. Perangkat di layer 3 OSI Layer. d. Bisa berupa box atau sebuah OS yang menjalankan sebuah *deamon* routing.
d. Interfaces Ethernet, Serial, ISDN BRI.

2.9 DNS Flood Master (DNS Flooding)

Menurut (Ardiantoro, 2003) DNS atau *Domain Name System* merupakan sistem berbentuk data base terdistribusi yang akan memetakan/mengkonversikan nama host/mesin/domain ke alamat IP (Internet Protocol) dan sebaliknya dari alamat IP ke host name yang disebut dengan *reverse-mapping*. Sebagai contoh, www untuk penggunaan di Internet, lalu diketikan nama domain, misalnya: ilkom.uii.ac.id maka akan dipetakan ke sebuah IP, yaitu 222.124.194.11.

DNS biasa digunakan pada aplikasi yang terhubung ke Internet atau jaringan yang menggunakan TCP/IP (Transmission Control Protocol/Internet Protocol) seperti *web browser*, *email (electronic-mail), browsing, ssh/telnet, ftp,* maupun aplikasi yang lain yang ada kaitannya dengan internet. Dimana setiap komputer di jaringan Internet memiliki nama komputer (*host name*) dan alamat Internet Protocol IP Address. Secara umum, setiap client yang akan mengkoneksikan Komputer satu ke Komputer lain akan menggunakan hostname. Lalu Komputer anda akan menghubungi DNS Server untuk mengecek hostname yang anda minta tersebut berapa IP Address-nya. IP Address ini yang digunakan untuk mengkoneksikan komputer anda dengan Komputer lainnya atau dengan kata lain DNS digunakan untuk pencarian nama Komputer (*name resolution*).

Menurut (Ardiantoro, 2003) selain digunakan di Internet, DNS juga dapat di implementasikan ke *Private Network* atau intranet dimana DNS memiliki keunggulan seperti:

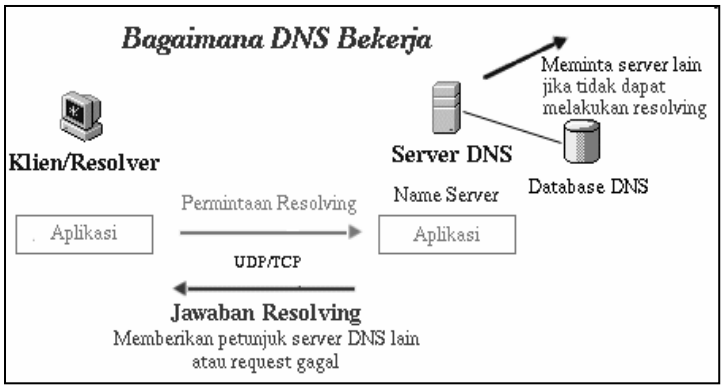
a. Mudah, DNS sangat mudah karena *User* hanya perlu mengingat hostname saja dan tidak lagi direpotkan untuk mengingat IP Address sebuah Komputer. Manusia lebih mudah untuk mengingat nama daripada alamat IP dengan panjang 32 bit itu.
b. Konsisten, karena IP Address sebuah Komputer bisa berubah tapi host name tidak berubah.
c. *Simple*, karena *User* hanya menggunakan satu nama domain untuk mencari baik di Internet maupun di Intranet.

Domain ditentukan berdasarkan tingkatan kemapuan yang ada di struktur hirarki yang disebut dengan level.

a. *Level* paling atas di hirarki disebut dengan Root-*Level* domain yang dilambangkan ".".
b. Beberapa contoh Top-*Level* Domain: info, edu, com, org, net, mil, xx (dua huruf untuk kode negara seperti id: Indonesia, sg:Singpura, tw:Taiwan, dll).
   Top-*Level* Domain dapat berisi Secondary-*Level* Domain dan Sub-*Level* Domain serta host.
c. Domain *name* yang digunakan dengan host name akan menciptakan fully qualified domain *name* (FQDN) untuk setiap komputer. Contohnya, jika terdapat www.yahoo.com, www adalah host name dan yahoo.com adalah domain name.

Cara kerja DNS, ketika akan melakukan *query* (bisa berupa *ping*, *ssh*, *dig*, *host*, *nslookup*, *email*, dan lain sebagainya) ke sebuah *host* misalnya *www.training.microsoft.com* maka *name server* akan memeriksa terlebih dahulu apakah ada *record host* tersebut di *cache name server* lokal, (Ali. A and Hudaid, 2014).

Jika tidak ada, *name server* lokal akan melakukan *query* kepada *root server* dan mereferensikan *name server* untuk *TLD.com*, *name server* lokal kembali melakukan *query* kepada *name server.com* dengan jenis *query* yang sama dan mereferensikan *microsoft.com. Name server* lokal kembali melakukan *query* ke *name server microsoft.com* dan mereferensikan *query* selanjutnya ke *name server* lokal yaitu *training.microsoft.com.* Kemudian *name server* lokal melakukan *query* kepada *name server* lokal yaitu *training.microsoft.com* dan akhirnya mendapatkan jawaban *address* yang diminta, berikut adalah Gambar tampilan cara kerja DNS.



Gambar 2.1 Cara Kerja DNS

Server nama dan zona, merupakan program server yang menyimpan informasi tentang *domain name*/*host* tertentu disebut server nama (*name server*). Server nama mempunyai informasi yang lengkap mengenai bagian-bagian dari domain name space yang disebut zona (*zone*), yang biasanya diambil dari file atau dari Server nama lainnya. Server nama mempunyai otoritas (*authority*) untuk zona tersebut, dan Server nama juga dapat mempunyai otoritas untuk banyak zona. Sebagai contoh domain id bisa dibagi menjadi beberapa zone yaitu ac.id, net.id dan dari zone tersebut bisa dibagi lagi menjadi zone-zone yang lebih kecil misal uii.ac.id. Disini yang bertanggung jawab ialah organisasi/lembaga yang memiliki domain tersebut.

DNS berfungsi untuk menerjemahkan *hostname* menjadi alamat IP Address atau menerjemahkan alamat IP Address menjadi hostname. Sebagai contohnya tadi host name google.com dengan alamat IP address 172.217.21.206. Orang lebih suka mengetik google.com daripada IP addressnya pada bar *search* baik itu di mozila maupun chrome. Hal ini karena nama google.com lebih mudah diingat daripada angka IP Address. DNS digunakan untuk mengetahui informasi secara lengkap mengenai sebuah *hostname* yang ada di internet baik itu alamat IP Address, alamat lokasi *server* atau *host name*, dan waktu yang digunakan saat *online*, (Irawan, 2005).

Jika kita menggunakan RouterOS atau Modem untuk akses ke jaringan internet, maka kita bisa membuat DNS *server* sendiri. *Setting* pengaturan DNS *server* ini bisa dilakukan pada *internet protocol version 4 (TCP/IPv4) properties*. Biasanya sebelum melakukan pengaturan perlu menemukan IP Address dari LAN yang digunakan dan *subnet mask*.

2.10 Jenis Serangan Pada Jaringan Router

Keamanan telah menjadi permasalahan setiap orang. Terkadang bukan mesin atau sistem yang menjadi penyebab masalah, melainkan penyebabnya adalah manusia

sendiri. Di masa berkembang sekarang ini, peralatan teknologi tinggi yang juga dapat menghalangi orang-orang yang ingin merugikan kita, sama seperti kita mengunci pintu kita dari penyusup. Permasalahan keamanan harus dipertimbangkan baik-baik sebagai pokok yang paling mendasar dalam setiap topik diskusi tentang keamanan, (Artformatics, 2013).

Banyak yang dapat dilakukan oleh penyusup untuk menghancurkan informasi, program dan sistem operasi yang dimiliki. Selain menghancurkan, penyusup juga dapat mencuri informasi, *hardware*, dan *software*. Pencurian ini termasuk pengambilan yang seharusnya bukan milik mereka, baik dilakukan secara langsung maupun tidak. Meliputi juga penggunaan sistem yang tidak sah. Penyusup juga dapat memperlihatkan informasi kepada pihak yang sebenarnya tidak memiliki akses terhadap informasi tersebut.

a. ***Denial of Service*** **(Dos/DDos)** adalah sebuah serangan yang disengaja yang bertujuan untuk menghalangi akses user yang legal. Dilakukan dengan cara meminta pelayanan terhadap server secara terus-menerus dan dalam skala yang besar sehingga menyebabkan *server down*. *Server* tidak dapat memberikan layanan karena alamat IP sumber terus menerus melakukan *flood* ke *server*.

b. **SQL** ***Injection*** adalah sebuah perusahaan misalnya, pasti memiliki *database* untuk menyimpan data-data digital perusahaan. Untuk itu diperlukan SQL *server*, penyerang memanfaaatkan kelemahan dari SQL *server* ini untuk mengacaukan sistem kita.

c. ***Trojan Horse*** adalah instruksi tersembunyi yang memiliki kemampuan merusak yang dikemas dalam bentuk program. Biasanya istilah *Trojan horse* digunakan ketika instruksi yang mencurigakan diinstal pada saat program ditulis. Tidak jarang program yang terlihat oleh user menunjukkan kegiatan yang berguna, padahal dibaliknya program secara diam-diam sedang menghapus *file user*.

d. ***Virus*** adalah sekumpulan instruksi yang ketika dieksekusi akan menginfeksi program lain dengan melakukan modifikasi pada program yang diinfeksi oleh *virus* tersebut, kemudian hasil modifikasinya akan tersebar ke program lainnya. Pada umumnya, *virus* bekerja pada sistem operasi tertentu dan untuk beberapa kasus bekerja pada *platform hardware* tertentu sehingga *virus* didesain untuk mengambil keuntungan dari kelemahan sistem tersebut.

e. ***Bacterium*** adalah sebuah program tunggal yang menggandakan dirinya, sangat merugikan dengan mengkonsumsi sumber daya yang ada.

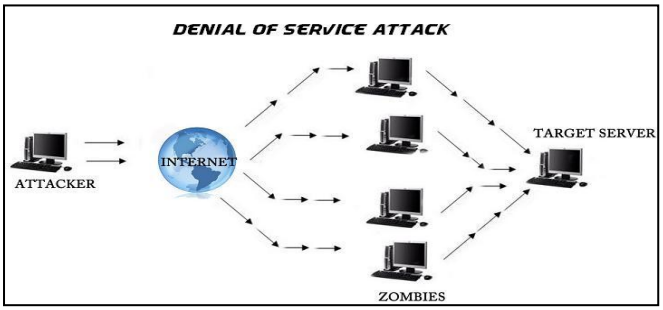
f. ***Worm*** adalah sebuah program yang menggandakan dirinya sendiri dengan menginstal duplikat dirinya ke dalam mesin lain melalui jaringan. Hampir sama seperti *bacterium*, hanya saja *worm* berkembang melalui jaringan sedangkan *bacterium* hanya berkembang di dalam satu mesin saja.

g. ***Trap Door*** adalah Titik masuk tak terdokumentasi rahasia di satu program untuk memberikan akses tanpa metode-metode otentifikasi normal.

h. ***Logic Bomb*** adalah Logika yang ditempelkan pada program komputer agar memeriksa suatu kumpulan kondisi di sistem. Ketika kondisi yang dimaksud ditemui, logika mengeksekusi suatu fungsi yang menghasilkan kegiatan yang tidak diotorisasi.

2.11 *Denial of Service* (DoS)

Serangan DoS dapat dilakukan dengan tingkat keterampilan rendah dan tanpa harus memiliki akses pada sistem (Ali. A and Hudaid, 2014), Ilustrasi serangan DoS ditunjukkan pada Gambar 2.2 berikut.



Gambar 2.2 *Denial of Service Attack*

Gambar 2.2 di atas menunjukkan bahwa posisi serangan yang berakibat pada data maupun informasi tidak tersedia, jenis serangan DoS pada umumnya ditujukan untuk: 1) membebani jaringan; 2) menghabiskan CPU; 3) mengurangi kapasitas pemroses; 4) manipulasi waktu; 5) DNS Poisoning; 6) Application Level of Denial of Service; dan 7) Permanent Denial of Service (Phlashing) (Rao, 2011), cara kerja TCP SYN Flooding ditunjukan gambar 2.2.

Penyerang akan mengirimkan data secara terus menerus atau memanfaatkan kelemahan sistem dengan memaksa kapasitas pemroses yang berakibat sistem tidak lagi dapat bekerja normal (Ardiantoro, 2003), TCP SYN Flood adalah serangan yang paling mudah dan paling umum ditemukan di internet, cara kerja TCP SYN Flood

adalah dengan memanfaatkan sejumlah sumberdaya yang disediakan oleh sistem untuk melakukan operasi Three-Way Handshake, penyerang berusaha untuk membebani (flooding) sistem dengan banyak permintaan hubungan hingga tidak dapat lagi menangani permintaan yang berasal dari pengguna sah. Hal ini pernah dibuktikan (Sarsono, 2012) menyatakan serangan *Denial of Service* merupakan ancaman yang nyata bagi organisasi.

2.12 *Wireshark*

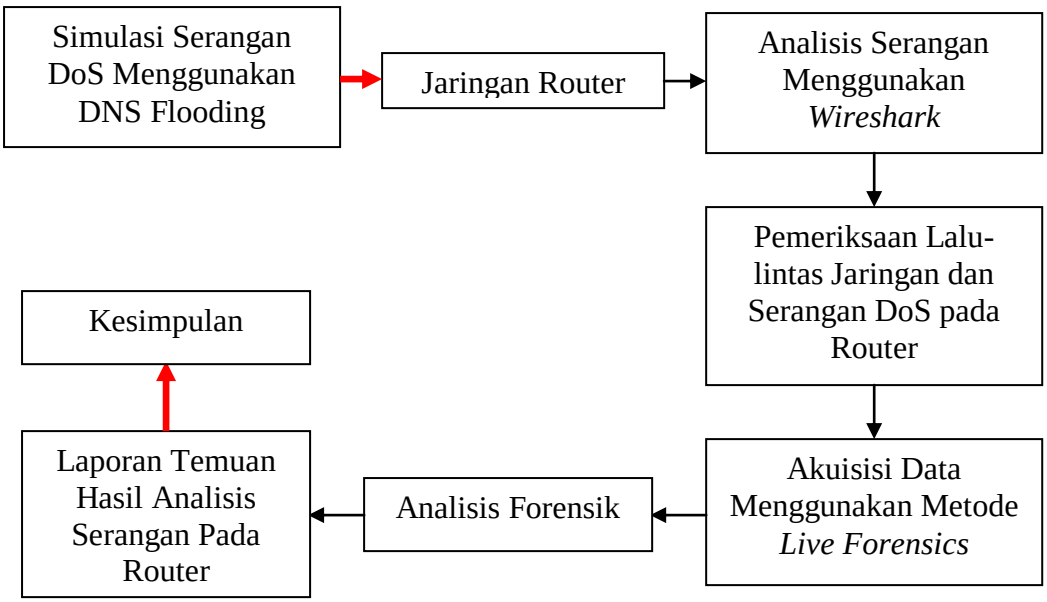
Wireshark merupakan salah satu dari sekian banyak *tools network analyzer* yang banyak digunakan oleh network administrator untuk menganalisa kinerja jaringannya termasuk protokol didalamnya. *Wireshark* banyak disukai karena interface-nya yang menggunakan *Graphical User Interface* (GUI) atau tampilan grafis. *Wireshark* mampu menangkap paket-paket data atau informasi yang melewati jaringan.semua jenis paket informasi dalam berbagai format protocol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang *tools* ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting seperti *password* email atau *account* lain) dengan menangkap paketpaket yang melewati jaringan dan menganalisanya, (Sarsono, 2012).

BAB 3
METODE PENELITIAN

3.1 Studi Pustaka

Studi pustaka merupakan kegiatan untuk mempelajari, mengkaji berbagai sumber literatur-literatur dan teori yang mendukung dalam melakukan penelitian ini. Studi literatur melalui paper, jurnal, artikel, buku, website yang terkait teori *Network Protocol Analyzer*, *Network Attack*, *Security Attack Models*, *Process Attack*, *Network Forensics*, *Live Forensics*, Topologi Jaringan, MikroTik Router, DNS Flood Master, Jenis Serangan pada Router, DoS (*Denial of Service*), dan Aplikasi *Wireshark*.

Berikut adalah tahapan pelaksanaan penelitian ini.



Bagan 3.1 Alur Penelitian

3.2 Alat dan Persiapan Penelitian

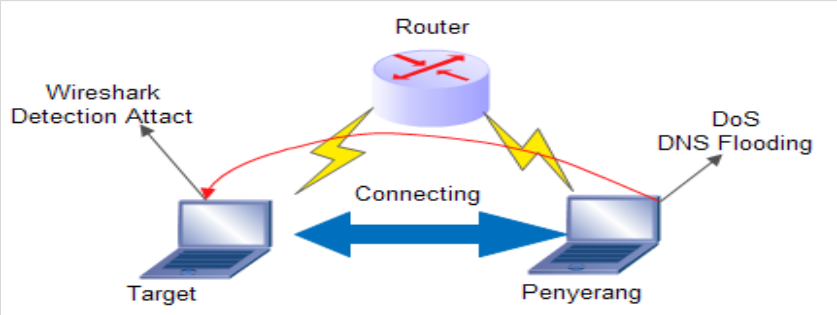
Pelaksanaan penelitian ini memerlukan perangkat keras dan perangkat lunak sebagai alat penelitian:

a. ***Hardware*** terdiri dari:
   1) Router RB951Ui Versi 6.
   2) Laptop Core i3, RAM 4GB untuk melakukan penarikan data dan analisis.
   3) Laptop sebagai *client* jaringan.

b. ***Software*** terdiri dari: WinBox, Linux Ubuntu, dan Tools DNS Flood Master, dan *Wireshark*.

3.3 Rancangan Simulasi Serangan DoS pada Router

Rancangan simulasi serangan DoS pada Router menggunakan DNS Flooding, dan analisis serangan pada Router menggunakan aplikasi *Wireshark*.



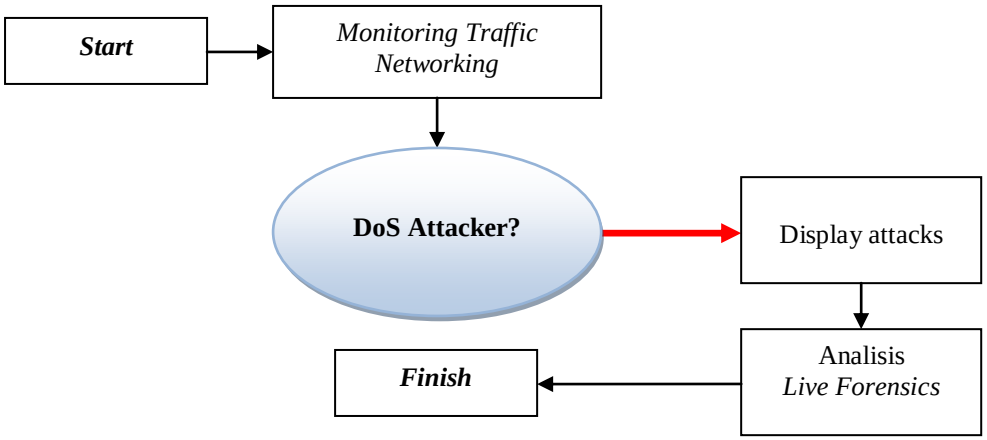
Gambar 3.2 Desain Analisis Serangan DoS pada Router

Berikut penjelasan Gambar perancangan desain analisis serangan DoS pada Router yang diterapkan dalam penelitian ini.

a. Internet, digunakan untuk menangkap jaringan internet melalui *SignalBolt*.
b. Router, kegunaannya untuk membagi jaringan internet ke komputer penyerang dan target.
c. Server, digunakan sebagai tempat pendeteksian dan analisis serangan DoS pada Router.
d. Penyerang, digunakan untuk keperluan simulasi serangan DoS pada Router.

3.4 Alur Analisis Serangan DoS pada Router

Tahapan simulasi serangan di atas bertujuan untuk menguji apakah aplikasi *Wireshark* mampu menampilkan beberapa aktivitas dari usaha serangan DoS pada Router. Berikut skema alur analisis serangan DoS pada Router berdasarkan metode *Live Forensics*.



Bagan 3.3 Alur Analisis Serangan DoS pada Router

Berikut penjelasan alur analisis serangan DoS pada Router yang diterapkan dalam penelitian ini.

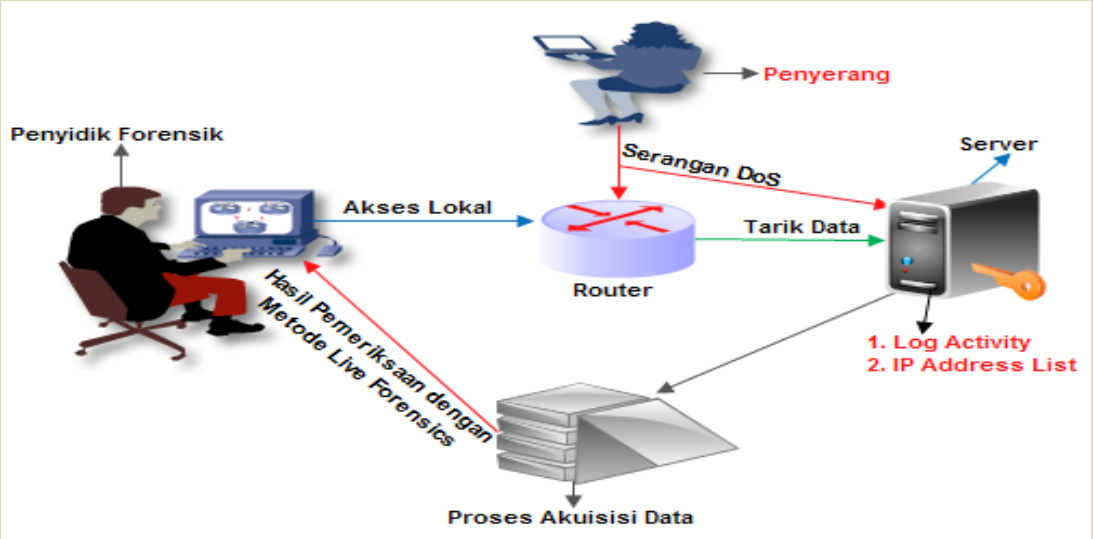
a. Proses awal adalah sistem akan menangkap serta mencatat setiap komunikasi data yang keluar maupun masuk dari setiap jaringan.
b. Setiap informasi yang diperoleh akan terlihat pada daftar yang ada diaplikasi mengenai apakah telah terjadi serangan DoS atau tidak.
c. Jika "ada serangan DoS" maka dilakukan analisis deteksi menggunakan *Wireshark* dan melakukan periksaan dengan metode *Live Forensics* hingga selesai. Jika "tidak ada serangan DoS pada Router" maka tidak diperlukan analisis serangan DoS pada Router.

3.5. Implementasi Simulasi Serangan

Proses simulasi serangan DoS pada Router dalam penelitian ini menggunakan aplikasi DNS Flooding. DNS Flooding, ditujukan untuk menyerang *name server* dengan cara membanjiri jaringan dari berbagai arah sehingga permintaan *client* untuk menerjemahkan alamat yang dituju menjadi terhambat dan ditolak oleh *server*.

3.6 Tahap Akuisisi

Tahapan akuisisi data dalam penelitian ini sebagai berikut.



Gambar 3.4 Rancangan Simulasi Serangan DoS dan Akuisisi Data dengan Metode *Live Forensics*

Kondisi utama yang harus dipenuhi dalam metode *Live Forensics* adalah kondisi di mana sistem sedang dalam keadaan beroperasi/*running* dikarenakan beberapa informasi serangan pada jaringan Router akan hilang jika sistem dimatikan ataupun

dilakukan *reboot*, sehingga untuk pengambilan data pada Router Komputer *investigator* perlu untuk bergabung dengan jaringan sebagai *client*, (Casey, 2010).

Selanjutnya diperlukan *login* admin agar bisa mendapatkan hak akses admin untuk membaca seluruh informasi serangan DoS pada Router kemudian dilakukan proses penarikan data dan dianalisis untuk memperoleh laporan serangan DoS pada Router sebagai hasil akhir dari investigasi penyidik forensik.

3.7 Analisis Forensik dan Verifikasi Data

Proses analisis Forensik dalam penelitian ini mengambil fokus utama pada analisis serangan DoS pada Router menggunakan aplikasi *Wireshark* untuk keperluan proses penarikan data atau informasi mengenai Log Activity dan IP Address List si penyerang. Setelah memperoleh informasi, langkah selanjutnya adalah melakukan *monitoring system traffic* pada Router terkait serangan DoS pada Router. Untuk hasil pelaporannya adalah menjelaskan kondisi Router sebelum diserang dan sesudah diserang sebagai mekanisme analisis serangan DoS pada Router.

Menurut (Fiebig, 2013) komponen-komponen Router yang berpotensi dan dapat digunakan sebagai bukti digital meliputi Log Akses, Log Aktivitas, Daftar Pengguna, DNS Cache, IP *address*, Hostname, Mac *address*, dan versi Router.

Khusus dalam penelitian ini penarikan data difokuskan pada komponen Log Activity, dan IP Address List. Berikut penjelasan masing-masing komponen.

a. Log Activity berisikan informasi aktivitas apa saja yang tercatat pada Router terkait perubahan konfigurasi.
b. IP Address List berisikan tentang informasi pelaku penyerangan.

Proses *Live Forensics* memiliki konsekuensi atas beberapa aktivitas yang dilakukan, di mana hal tersebut mengakibatkan perubahan data atau penambahan data pada barang bukti. Hal ini terkait proses terhubungnya komputer investigator pada jaringan serta aktivitas permintaan data yang dilakukan melalui *service* WinBox pada Router.

Tahapan terakhir dari proses Forensik adalah pelaporan atau *reporting.* Dalam tahapan ini disajikan segala data dan temuan hasil analisis serangan DoS PADA Router berdasarkan hasil analisis yang telah dilakukan. Data-data temuan akan dilampirkan bersama dengan analisis penelitian.

BAB 4
HASIL DAN PEMBAHASAN

Bab ini berisikan penjelasan yang diperoleh dari proses penelitian yang telah dilakukan berdasarkan rumusan masalah dan tujuan penelitian yang diajukan sebelumnya, yaitu: 1) Analisis serangan DoS pada Router, 2) Proses akuisisi data pada Router menggunakan pendekatan metode *Live Forensics*, 3) Karakteristik bukti digital pada Router yang bisa dijadikan sebagai laporan atau hasil temuan penelitian terkait analisis serangan DoS pada Router.

4.1 Proses Observasi pada MikroTik Router

Sebelum masuk dan melakukan konfigurasi ke sistem, terlebih dahulu digunakan aplikasi WinBox untuk me-remote Router. Penggunaan aplikasi WinBox membutuhkan alamat IP Router, IP *User* berserta Password dari Router yang akan di remote, dan setelah melakukan konfigurasi diketahui IP Router adalah 192.168.1.1.

Banayaknya komponen yang terdapat dalam MikroTik Router sehingga perlu dilakukan observasi lokasi dimana letak informasi yang dapat digunakan sebagai bukti digital. Dalam penelitian ini, tahapan observasi dan pemetaan Router dilakukan melalui CLI (*Command Line Interface*). Menu utama Router pada Terminal CLI.

Setelah melakukan Observasi pada Router diketahui terdapat banyak menu dan submenu dalam jaringan MikroTik Router. Selanjutnya untuk keperluan simulasi serangan pada Router menggunakan Aplikasi DNS Flood Master (DNS Flooding). Berdasarkan studi literatur Michael Gregg tentang Router Forensik dalam buku "*Alternate Data Strorage*" (2007) dinyatakan bahwa komponen Router yang bisa digunakan dan berpotensi dijadikan sebagai barang bukti digital dari Router adalah Log Akses, **Log Activity**, User List, **IP Address List**, Hostname, Mac Address, dan Versi Router.

Menginggat banyak komponen Router yang dapat dijadikan sebagai bukti digital dalam proses akuisisi data untuk keperluan Forensik, maka untuk penarikan data sebagai temuan deteksi serangan pada Router dalam penelitian ini difokuskan pada penarikan data berupa **Log Activity** dan **IP Address List**. Berikut adalah komponen-komponen isi Router pada menu dan submenu WinBox yang bisa digunakan dalam proses penarikan data forensik, dapat dilihat pada tabel di bawah ini.

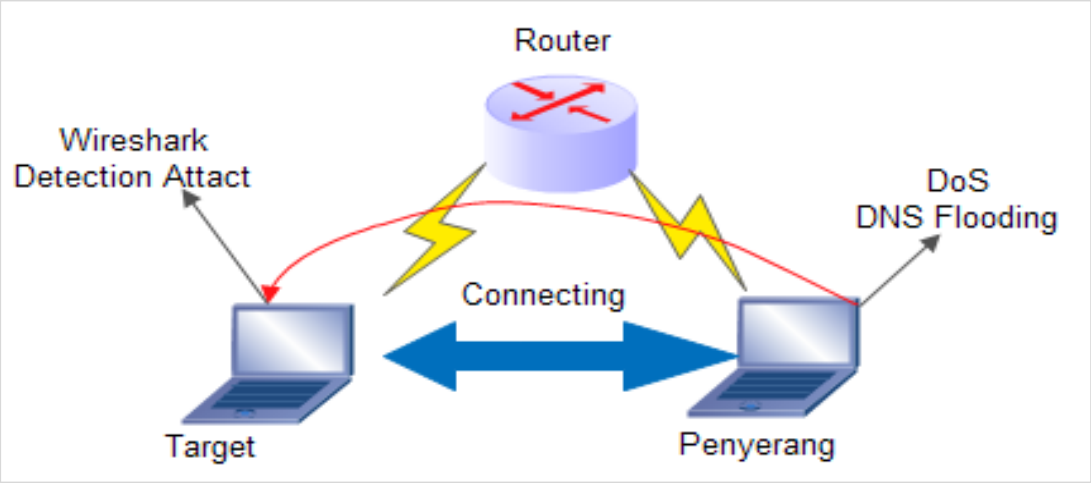
Tabel 4.1 Komponen-Komponen WinBox MikroTik Router

No	Komponen	Lokasi
1	Log Akses	/log
2	**Log Aktivity**	**/log**
3	Pengguna	/User
4	**IP Address List**	**/ip/address**
5	Hostname Client	/ip/dhcp-server/dhcp-leases
6	Mac Address Client	/ip/arp
7	Router Version	/system/resource
8	ARP	/ip/arp
9	Torch	/tools/torch

4.2 Persiapan Skenario Pengujian Serangan DoS (*Denial of Service*)

4.2.1 Simulasi Serangan pada Router

Denial of Service (DoS) merupakan jenis serangan yang disengaja dan bertujuan untuk menghalangi akses *User* yang memiliki hak akses. Proses serangan DoS dilakukan dengan cara meminta pelayanan terhadap Server secara terus-menerus (Flooding) dan dalam skala yang besar sehingga menyebabkan Server *Down*. Server tidak dapat memberikan layanan karena alamat IP sumber terus-menerus melakukan Flood ke Server, (Szewczyk, 2007).



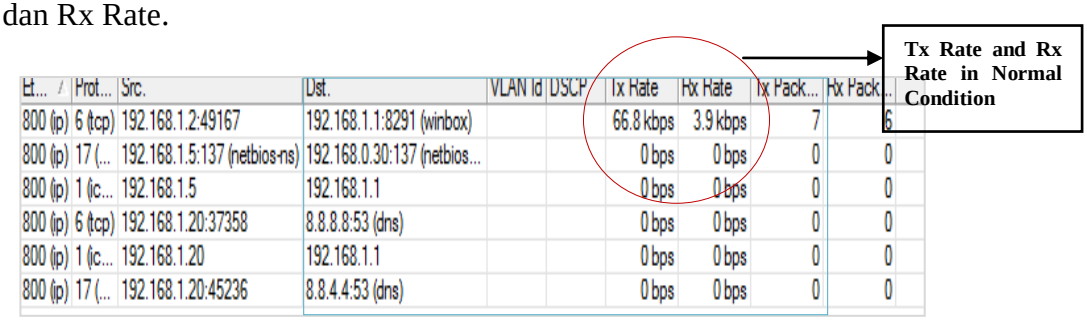
Gambar 4.1 Konsep Simulasi Serangan DoS

Konsep simulasi serangan *Denial of Service* (DoS), yaitu penyerang akan mengirimkan data secara terus-menerus atau memanfaatkan kelemahan sistem dengan memaksa kapasitas pemrosesan yang berakibat sistem tidak lagi beroperasi secara normal (Ardiantoro, 2003).

Tipe serangan DoS yang diterapkan dalam penelitian ini adalah *Flooding*, yang merupakan tipe serangan menggunakan Protocol TPC, UDP atau ICMP untuk membanjiri target dengan paket-paket *request* yang dikirim penyerang ke target jaringan Router.

4.2.2 Analisis Serangan DoS pada Router

Proses awal untuk analisis apakah Router masih dalam keadaan normal atau sudah ada serangan DoS, dapat dilakukan melalui pengecekan pada menu WinBox, yaitu melalui menu *Tourch Running*. Setelah dilakukannya pengecekan diketahui belum ada serangan yang masuk, hal ini dapat dilihat pada lalu-lintas *Destination*, Tx Rate dan Rx Rate.



Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	192.168.1.2:49167	192.168.1.1:8291 (winbox)			66.8 kbps	3.9 kbps	7	6
800 (ip)	17 (...	192.168.1.5:137 (netbios-ns)	192.168.0.30:137 (netbios...			0 bps	0 bps	0	0
800 (ip)	1 (ic...	192.168.1.5	192.168.1.1			0 bps	0 bps	0	0
800 (ip)	6 (tcp)	192.168.1.20:37358	8.8.8.8:53 (dns)			0 bps	0 bps	0	0
800 (ip)	1 (ic...	192.168.1.20	192.168.1.1			0 bps	0 bps	0	0
800 (ip)	17 (...	192.168.1.20:45236	8.8.4.4:53 (dns)			0 bps	0 bps	0	0

Gambar 4.2 Tampilan *Tourch* Sebelum Ada Serangan DoS

Proses awal pengecekan berdasarkan tampilan Gambar di atas, dapat disimpulkan belum ada serangan yang masuk dan menganggu lalu-lintas jaringan pada Router. Hal ini dapat dilihat pada kolom *Source* dan *Destination* terdapat IP dari masing-masing Komputer dalam melakukan komunikasi antara satu dengan lainnya secara normal.

Langkah selanjutnya adalah mulai melakukan simulasi serangan DoS pada Router menggunakan aplikasi DNS Flood Master (DNS *Flooding*) untuk mengetahui apakah serangan DoS yang diluncurkan berhasil menembus jaringan Router. Pada kondisi ini juga dilakukan analisis serangan DoS pada Router menggunakan aplikasi *Wireshark* untuk mengetahui apakah *Wireshark* mampu mendeteksi serangan pada Router sehingga dapat dilakukan analisis serangan untuk menarik data sebagai bukti digital melalui metode *Live Forensics*.

4.2.3 Pengujian Menggunakan Aplikasi

Setelah melakukan pengujian pengecekan awal terhadap lalu-lintas jaringan Router, maka selanjutnya dilakukan pengujian menggunakan aplikasi. Pada proses ini aplikasi DNS Flood Master dijalankan melalui Linux uBuntu untuk melancarkan

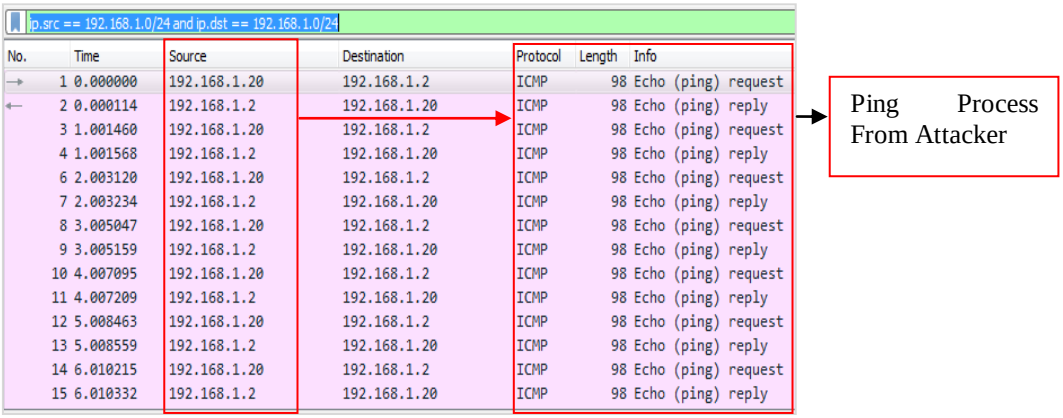
penyerangan DoS menggunakan DNS *Flooding* langsung menuju ke target jaringan Router yang diserang, seperti tampilan pada Gambar berikut.



Gambar 4.3 Serangan Scanning Port DNS *Flooding*

Berdasarkan tampilan Gambar di atas, dapat dijelaskan bahwa aplikasi DNS berhasil dijalankan dan siap melancarkan serangan ke jaringan Router yang menjadi target serangan. Setelah serangan dilancarkan, proses selanjutnya melakukan pengecekan serangan yang masuk pada Router melalui aplikasi *Wireshark*.

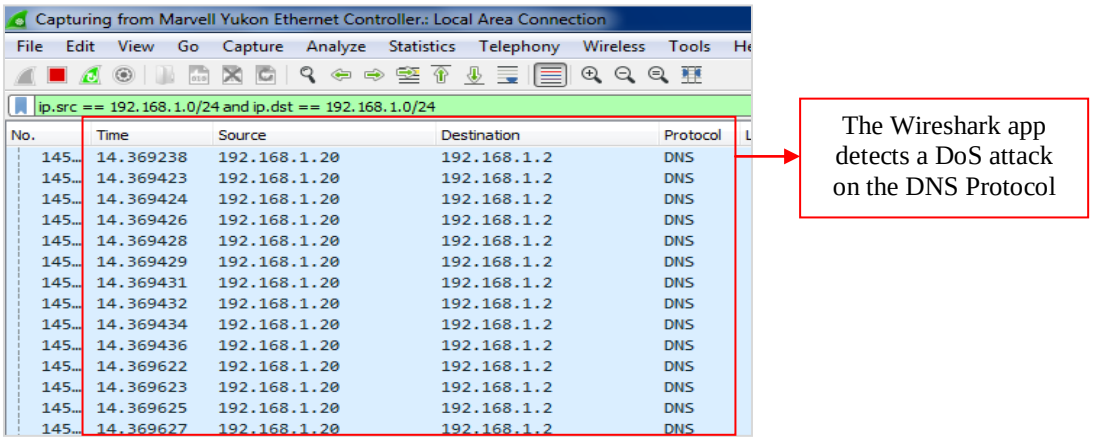
Setelah dicek percobaan simulasi serangan ini sudah berhasil masuk, sehingga dapat dilakukan *Monitoring Flooding Connection* untuk mengirim *Package* ke Protocol UDP menggunakan Port DNS ke IP Address List yang digunakan untuk melakukan serangan pada Router. Pada pengujian ini juga dilakukan *monitoring* menggunakan aplikasi *Wireshark* dengan men-*capture* hasil lalu-lintas jaringan dalam keadaan normal atau hanya menunjukkan kegiatan lalu-lintas yang biasa atau dalam hal ini hanya melakukan Ping diantara kedua komputer. Dapat dilihat pada Gambar di bawah ini.



Gambar 4.4 Keadaan Lalu-Lintas Ping

Tampilan Gambar di atas sudah menunjukkan adanya aktivitas serangan DoS yang dilakukan penyerang melalui proses mengirim Ping ke target jaringan Router. Hal ini dapat dilihat pada kolom *Sourece* di mana IP 192.168.1 terus melakukan *requets* atau mengirim Ping ke target *Destination* dengan IP 192.168.1.20. langkah

selanjutnya adalah mengecek serangan yang masuk pada Router melalui aplikasi *Wireshark*.



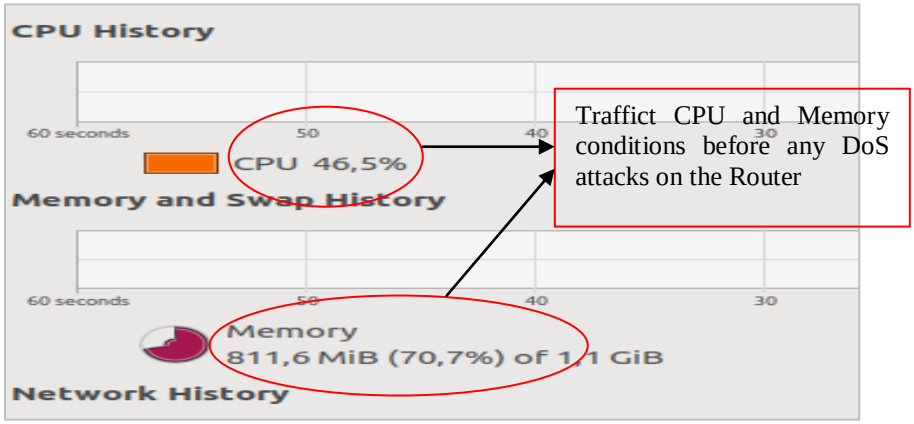
Gambar 4.5 *Wireshark* Mendeteksi Serangan DoS pada Protocol DNS

Gambar di atas dapat dilihat adanya lalu-lintas tidak biasa yang menunjukkan adanya kegiatan penyerangan Port *Scanning*, dari Kolom *Source* terdapat IP dari Komputer penyerang, yaitu 192.168.1.20 yang melakukan penyerangan tersebut, dan pada Kolom *Destination* adalah IP 192.168.1.2 yang merupakan komputer target. Protocol yang digunakan adalah DNS dan pada Kolom Info menyatakan bahwa Port dari penyerang sedang melakukan *Scanning* pada semua Port Komputer target, disitu dapat juga dilihat pada Port Protocol (penyerang) adalah 8291 menuju ke Port 49167 atau Port (53) sebagai (target). Artinya Port 49167 (53) dalam keadaan terbuka dengan mengirim umpan balik ke komputer penyerang dan telah siap menerima koneksi dari luar.

Jika serangan pada jaringan Router dilakukan secara terus-menerus dapat mengakibatkan MikroTik Router melakukan Restart sendiri akibat kelebihan beban. Peneliti juga berhasil melakukan analisis mengenai *Load* (beban) penggunaan CPU dan *memory* pada jaringan Router sebelum dan sesudah terjadi serangan DoS.

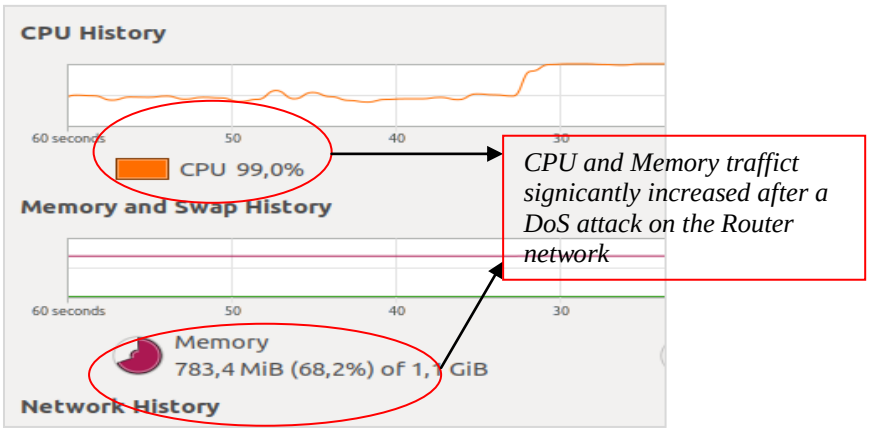
Berdasarkan hasil analisis pada *Traffic Monitor System* Sebelum Terjadi Serangan DoS, diketahui bahwa keadaan *Traffic System* sebelum terjadi serangan menunjukkan *Presentase* CPU (*memory and Swap History*) adalah 47.5 % dan *Memory* 782.6 MiB belum bergerak secara Signifikan karena belum terjadi transaksi serangan DoS yang dapat mempengaruhi kinerja atau *Load* pada jaringan Router. Namun setelah ada serangan DoS, CPU dan *Memory* mengalami kenaikan akses

secara Signifikan dan menyebabkan kinerja atau *Load* dari *Packet* data pada Router menjadi *Down*.



Gambar 4.6 Kondisi CPU dan *Memory* sebelum ada Serangan DoS pada Router

Gambar di atas menunjukkan *traffict* CPU dan *Memory* perangkat jaringan Router target masih dalam keadaan normal. Namun setelah ada serangan DoS yang masuk pada jaringan Router, *Load* CPU dan *Memory* meningkat. Berdasarkan hasil *Traffic Monitor System* setelah terjadi serangan DoS diketahui Traffic *System Monitor Packet* data *Load* CPU meningkat menjadi 99.0 % dan *Memory* 783.4 MiB naik secara Signifikan. Hal ini yang menyebabkan *Down* pada *Network Traffic* akibat ada serangan DoS pada Router. Berikut adalah tampilan *traffict monitoring system* CPU dan *Memory* setelah ada serangan DoS pada jaringan Router.



Gambar 4.7 *Traffic Monitor System* Setelah Terjadi Serangan DoS

Berdasarkan uraian hasil analisis di atas, mulai dari proses awal pencegekan serangan hingga pencegecekan pada *monitoring traffict system* pada jaringan Router yang diserang. Dapat diketahui bahwa *Wireshark* berhasil mendeteksi

adanya serangan DoS yang dilancarkan penyerang menggunakan aplikasi DNS *Flooding* dan telah berhasil tembus ke sistem jaringan Router yang menjadi target.

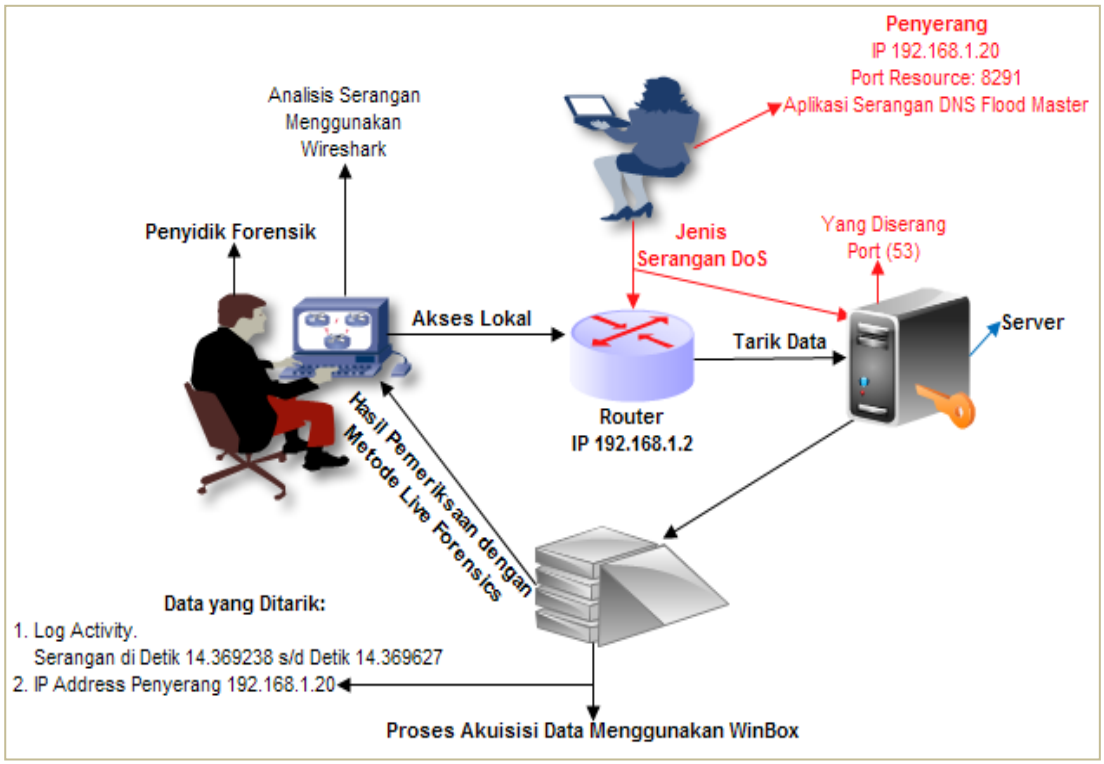
Paparan hasil analisis serangan pada Router di atas, sejalan dengan keseimpulan hasil penelitian yang pernah dilakukan oleh (M. Junaidi Syahputra, Ilham Faisal, 2012) bahwa serangan pada Router yang masuk secara bertubi-tubi dapat berakibat pada menurunnya performa kerja jaringan Router karena *Load* Komputer pada jaringan terus meningkat dan tidak dapat melayani pengguna lainnya. Hasil penelitian tersebut juga menjelaskan bahwa *Wireshark* mampu mendeteksi serangan yang masuk dan mengenali IP penyerang.

Menurut hasil penelitian yang dilakukan (Mazdadi, 2017) bahwa serangan pada Router dapat diketahui melalui beberapa identifikasi. Misalnya mengenai kapan terjadinya serangan, siapa yang melakukan serangan, dan serangan tersebut masuk melalui Port apa, sehingga Informasi yang tersimpan dalam MikroTik Router dapat diakuisisi dengan mengembangkan suatu aplikasi yang bisa berkomunikasi secara Remote dengan memanfaatkan Port-Port pada *system* jaringan Router. Aplikasi yang dibangun dapat menjadi solusi untuk mempermuda proses akuisisi dalam aktivitas Forensik jaringan terhadap perangkat Router berbasis RouterOS.

4.3 Akuisisi Data

Kondisi utama yang harus dipenuhi dalam metode *Live Forensics* adalah kondisi dimana sistem sedang dalam keadaan beroperasi/*running* dikarenakan beberapa informasi jaringan pada Router akan hilang jika sistem dimatikan ataupun dilakukan *reboot*, sehingga untuk pengambilan data pada Router Komputer *investigator* perlu untuk bergabung dengan jaringan sebagai *client*. Selanjutnya diperlukan Login Admin agar bisa mendapatkan hak akses admin untuk membaca seluruh informasi pada Router yang diserang kemudian dilakukan proses penarikan data dan dianalisis untuk memperoleh laporan sebagai hasil akhir dari investigasi Forensik, (Symantec, 2016).

Berikut adalah Gambar alur proses akuisisi data analisis serangan DoS pada Router.



Gambar 4.8 Mekanisme Akuisisi Data Menggunakan Metode *Live Forensics*

Berdasarkan Gambar di atas dapat dijelaskan alur mekanisme penyeledikan analisis serangan DoS pada Router menggunakan metode *Live Forensics*, sebagai berikut:

1. Penyidik Forensik

a) *Wireshark*, digunakan penyidik forensik untuk melakukan analisis serangan DoS pada Router

b) Akses Lokal, penyidik forensik meminta izin kepada admin jaringan untuk mengakses jaringan Router untuk keperluan analisis serangan yang masuk pada Router. Setelah penyidik forensik masuk dan berhasil mengakses jaringan sebagai salah satu *client,* diketahui bahwa Port Protocol DNS beberapa kali diserang dengan proses mengirim Ping secara bertubi-tubi hingga berhasil menyerang jaringan Router.

c) Tarik Data, penyidik forensik mempelajari, mencermati, serta menaganalisis data informasi serangan pada Router. Dari proses ini penyidik forensik sudah mengetahui bahwa proses serangan yang masuk adalah serangan DoS menggunakan aplikasi DNS Flooding dan berhasil menyerang Port (53).

d) Proses Akuisisi Data, pada proses ini penyidik forensik melakukan pemetaan komponen Router yang diserang serta menentukan komponen apa yang akan diambil sebagai bukti digital atas tindak serangan DoS pada Router.
e) Data yang Ditarik, pada proses ini penyidik forensik sudah memperoleh data bukti digital berupa Log Activity penyerang melakukan serangan pada Router di detik 14.369238 sampai dengan detik 14.369627, dengan IP Address List penyerang, yaitu 192.168.1.20. Penyidik forensik juga berhasil menganalisis kondisi CPU dan Memory meningkat setelah ada serangan DoS, yaitu dari kondisi CPU (47,5%) naik menjadi (99,0%), dan kondisi Memory dari (782.6 MiB) naik menjadi (783.4 MiB).
f) Laporan Hasil Akuisisi Data, pada proses ini penyidik forensik sudah memperoleh informasi data serangan DoS berdasarkan komponen Router yang bisa dijadikan sebagai bukti digital forensik, berupa Log Activity dan IP Address List penyerang.

2. Penyerang

a) DNS Flood Master (DNS Flooding), digunakan penyerang untuk meluncurkan serangan DoS pada Router dengan IP 192.168.1.2, dan menggunakan Port protocol 8291 untuk menyerang protocol DNS.
b) Jenis Serangan, yaitu serangan DoS (*Denial of Service*). Pada proses ini penyerang secara bertubi-tubi mengirim Ping *request* pada Router dengan IP 192.168.1.2. Serangan dilakukan pada detik 14.369238 sampai dengan detik 14.369627.
c) Port yang Diserang, pada proses ini penyerang menggunakan Port 8291 dan berhasil menyerang Port (53).

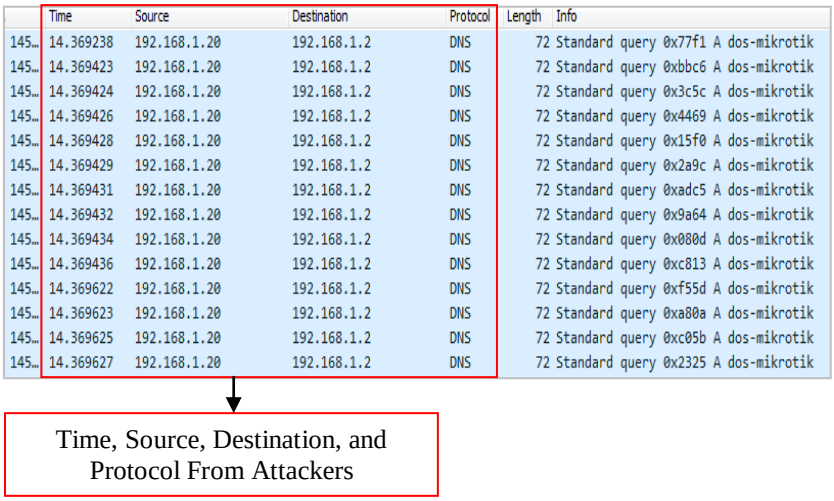
Setelah melakukan proses analisis serangan DoS pada Router, maka tahap selanjutnya adalah melakukan proses akuisisi data untuk menemukan bukti digital sebagai laporan pemeriksaan forensik. Proses pemeriksaan Forensik yang menjadi fokus utama dalam penelitian ini adalah melakukan analisis serangan DoS pada Router melalui pencarian informasi data Log Activity dan IP Address List pelaku penyerangan jaringan pada Router menggunakan metode *Live Forensics*.

4.3.1 Log Activity

Log Activity merupakan bukti digital kunci dalam mencatat setiap kegiatan yang terjadi pada Router. Setiap kegiatan dicatat berdasarkan *Time, Topic, dan Massage*.

Time merupakan waktu dari kejadian dari suatu kegiatan yang merupakan *element* paling penting dalam proses investigasi. Untuk melakukan Verifikasi waktu pada Router. Selain waktu, informasi selanjutnya yang bisa didapatkan pada Log Activity adalah Topic yang merupakan kategori jenis aktivitas. Topic akan mengkategorikan jenis aktivitas menjadi *Error, Info, Critial* dan *Warning* diikuti dengan komponen yang berkaitan dengan informasi tersebut. Pada bagian *message* menjelaskan rincian lebih detail tentang informasi terkait Topic.

Berikut ini adalah Gambaran akuisisi data analisis serangan DoS pada Router yang berhasil peneliti himpun, seperti yang ditampilkan pada Gambar 4.9 di bawah ini.



	Time	Source	Destination	Protocol	Length	Info
145…	14.369238	192.168.1.20	192.168.1.2	DNS	72	Standard query 0x77f1 A dos-mikrotik
145…	14.369423	192.168.1.20	192.168.1.2	DNS	72	Standard query 0xbbc6 A dos-mikrotik
145…	14.369424	192.168.1.20	192.168.1.2	DNS	72	Standard query 0x3c5c A dos-mikrotik
145…	14.369426	192.168.1.20	192.168.1.2	DNS	72	Standard query 0x4469 A dos-mikrotik
145…	14.369428	192.168.1.20	192.168.1.2	DNS	72	Standard query 0x15f0 A dos-mikrotik
145…	14.369429	192.168.1.20	192.168.1.2	DNS	72	Standard query 0x2a9c A dos-mikrotik
145…	14.369431	192.168.1.20	192.168.1.2	DNS	72	Standard query 0xadc5 A dos-mikrotik
145…	14.369432	192.168.1.20	192.168.1.2	DNS	72	Standard query 0x9a64 A dos-mikrotik
145…	14.369434	192.168.1.20	192.168.1.2	DNS	72	Standard query 0x080d A dos-mikrotik
145…	14.369436	192.168.1.20	192.168.1.2	DNS	72	Standard query 0xc813 A dos-mikrotik
145…	14.369622	192.168.1.20	192.168.1.2	DNS	72	Standard query 0xf55d A dos-mikrotik
145…	14.369623	192.168.1.20	192.168.1.2	DNS	72	Standard query 0xa80a A dos-mikrotik
145…	14.369625	192.168.1.20	192.168.1.2	DNS	72	Standard query 0xc05b A dos-mikrotik
145…	14.369627	192.168.1.20	192.168.1.2	DNS	72	Standard query 0x2325 A dos-mikrotik

Gambar 4.9 Data Log Activity Serangan pada Router

Kondisi Log Activity yang ditampilkan di atas menunjukkan sudah ada kegiatan serangan DoS pada MikroTik Router. Hal ini bisa diketahui melalui Time, Topic, dan Massage dari IP Address 192.168.1.20 secara bertubi-tubi menyerang pada Protocol Port Router. Terdapat kegagalan login yang cukup banyak dalam rentang waktu antara **detik 14.369238 sampai dengan detik 14.369627** Aktivitas ini dicurigai sebagai aktivitas yang tidak wajar yang melakukan komunikasi data pada Protocol DNS dengan IP 192.168.1.20 terhadap Router dengan IP 192.168.1.2.

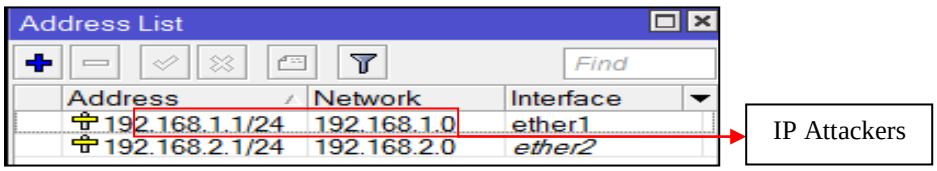
Hal ini pernah juga dibuktikan melalui hasil penelitian yang dilakukan oleh (Mazdadi, 2017) mengenai Analisis Forensik pada RouterOS Menggunakan Metode *Live Forensics*. Hasil penelitiannya menunjukkan bahwa *Output* yang dihasilkan berupa informasi terkait Log Activity, IP Address List, ARP, DHCP Leases, DNS

Cache, dan RouterBoard Info yang dapat digunakan untuk analisis untuk pengungkapan suatu aktivitas serangan yang terjadi pada Router.

4.3.2 IP Address List

IP Address List yang ditampilkan adalah hasil konfigurasi melalui kolom Segmentasi Network tersebut yang biasa diakhiri dengan angka 0. Sedangkan pada kolom Interface dapat dilihat nama Interface atau Ether LAN Port fisik ataupun WLAN Port dari RouterBoard.

IP Address pada suatu Port Router bisa juga dapat berarti *Gateway* pada *Network Segment*. IP *Gateway* biasa dijadikan sebagai target dari suatu aktivitas serangan pada jaringan. Berdasarkan tab informasi IP Address List.



Gambar 4.10 Tampilan IP Address List Penyerang

Pembahasan hasil di atas sejalan dengan pernyataan (Dimaio, 2001) yang menyatakan bahwa paket-paket yang dikirimkan melintasi masing-masing data *Link* dengan cara Enkapsulasi paket kedalam Frame menggunakan pengenal data *Link* agar *Frame* dapat dikirimkan dari sumber ke tujuan di dalam Protocol *Link Network* yang lebih rendah.

4.4 Hasil Pengujian Analisis Serangan DoS pada Router

Berdasarkan hasil pengujian analisis serangan DoS pada Router, maka dapat disajikan hasil penelitian sebagai laporan Forensik Jaringan berdasarkan proses analisis serangan DoS pada Router yang telah peneliti lakukan di atas.

Hasil analisis serangan DoS pada Router lebih lanjut dijelaskan pada Tabel hasil analisis serangan DoS pada Router di bawah ini.

Tabel 4.2 Hasil Analisis Serangan DoS Pada Router

No	Jenis Informasi Analisis	Keterangan
1	Serangan DoS pada Router menggunakan aplikasi DNS Flooding	Berhasil melakukan serangan pada jaringan Router secara bertubi-buti hingga membuat jaringan menjadi *Down*.
2	Aplikasi *Wireshark* berhasil menangkap aktivitas lalu-lintas yang mencurigakan melalui Protocol DNS	Diperoleh informasi adanya serangan DoS pada Router mulai dari proses penyerang mengirim Ping untuk me*request* akses masuk pada Router
3	Protocol Serangan yang berhasil ditembus adalah	Protocol DNS
4	Port Protocol Penyerang	8291
5	Port Destination Target	49167 atau Port (53)
6	Kondisi CPU dan *Memory* perangkat jaringan sebelum diserang	CPU (47.5 %) *MEMORY* (782.6 MiB)
7	Kondisi CPU dan *Memory* perangkat jaringan setelah diserang	CPU naik menjadi (99.0 %) *MEMORY* naik menjadi (783.4 MiB)
8	Log Activity	Terdapat kegagalan login yang cukup banyak dengan rentang waktu antara detik 14.369238 sampai dengan detik 14.369627. Aktivitas ini dicurigai sebagai aktivitas yang tidak wajar yang melakukan komunikasi data pada Protocol DNS dengan IP 192.168.1.20 terhadap Router dengan IP 192.168.1.2.
9	IP Address List Penyerang	192.168.1.20

BAB 5
KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Setelah melakukan simulasi serangan DoS pada Router, analisis serangan DoS pada Router, dan menarik data forensik sebagai bukti digital sebagai hasil penelitian, maka dapat ditarik beberapa temuan penelitian sebagai kesimpulan. Berikut kesimpulan penelitian ini:

a. Analisis serangan pada Router, dari proses penyerangan yang dilakukan dapat peroleh informasi bahwa serangan DoS menggunakan aplikasi DNS Flooding memiliki karakteristik yang dapat melakukan Ping atau mengirim pesan secara bertubi-tubi dan mampu membuat jaringan Router menjadi Down akibat beban yang masuk berlebihan. Hasil penelitian ini membuktikan bahwa penyidik forensik berhasil menggunakan aplikasi *Wireshark* untuk melakukan analisis serangan DoS pada Router.
b. Proses akuisisi data pada Router menggunakan pendekatan metode *Live Forensics*, setelah dilakukan akuisisi data, dapat disimpulkan bahwa aktivitas yang tidak wajar melakukan komunikasi data pada Protocol DNS dengan IP 192.168.1.20 terhadap Router dengan IP 198.168.1.2 dengan rentang waktu antara detik 14.369238 sampai dengan detik 14.369627. Hasil penelitian ini juga berhasil mengidentifikasi IP Address List dari penyerang, yaitu IP 192.168.1.20.
c. Karakteristik bukti digital pada Router yang bisa dijadikan sebagai laporan atau hasil temuan penelitian terkait analisis serangan DoS pada Router, meliputi jenis serangan yang masuk, Port jenis serangan yang masuk, Port Protocol Penyerang, Port *Destination* target jaringan Router yang diserang, dan untuk proses analisis *History* penyerangan diketahui melalui Log Activity dan IP Addrees Lits penyerangan.

5.2 SARAN

a. Melakukan perbandingan terhadap beberapa penelitian terkait Router untuk membangun keamanan data pada jaringan Router yang lebih baik melalui pengaturan Firewall dengan pendekatan metode Forensik Jaringan.

b. Analisis serangan DoS pada Router yang dilakukan masih cukup sederhana, sehingga masih dapat dilakukan pengembangan untuk memperoleh hasil yang lebih akurat untuk keperluan bukti digital atas serangan DoS pada Router.

DAFTAR PUSTAKA

Abdul Fadlil, Imam Riadi, S. A. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Ilmu Elektro Komputer Dan Informatika (Jiteki)*, *3*(June).

Ali. A and Hudaid, Z. (2014). DNS Advanced Attacks and Analysis, *8.1*, 63–74.

Arasteh, M. D. (2007). Analyzing Multiple Logs For Forensics Evidence. *Digital Investigation*, *5*(82), 91.

Ardiantoro, D. (2003). Pengantar DSN (Domain Name System). Retrieved from IlmuKomputer.com

Artformatics. (2013). *Live Forensics*. Retrieved from https://artformatics.wordpress.com/2013/02/16/live-forensic/

Casey, E. (2010). *Handbook of Digital Forensics and Investigation*. London: Elsevier Inc.

Dimaio, V. J. (2001). *Forensics Pathology. 2nd ed.* London: CRC Press.

Dwi, T., Cahyo, B., Informasi, D. S., Teknologi, F., Arief, J., Hakim, R., & Indonesia, S. (2017). Analisis Live Forensics untuk Perbandingan Aplikasi Instant Messenger pada Sistem Operasi Windows 10. *Sesindo*, *6*(November).

E, Wit. and Van K, E. (2014). Forensics Analysis of Consuner Router Previous Research, *1*(2).

Fiebig, T. (2013). *Forensic DHCP Information Extraction from Home Routers*.

Hariyadi, D, dan Supriyono, A. R. (2017). Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI. *Telematika*, *14*(1), 62–67.

Irawan, B. (2005). *Jaringan Komputer*. Yogyakarta: Graha Ilmu.

L. Volonino and R, A. (2008). *Computer Forensics For Dummies*. (Indianapolis, Ed.). Wiley.

M. Junaidi Syahputra, Ilham Faisal, A. B. (2012). Deteksi Serangan Pada Jaringan Komputer Dengan Wireshark Menggunakan Metode Anomaly-Based IDS. *Jurnal Teknik Elektro Terapan*, *1 (2)*.

Mancill, T. (2002). *Linux Routers : A Primer for Network Administrator, 2 ed*. Retrieved from https://www.amazon.com/Linux-Routers-Primer-Network-Administrators/dp/0130090263

Mazdadi, M. I. (2017). *Analisis Forensik pada RouterOS Menggunakan Metode Live Forensics*. Universitas Islam Indonesia.

Mukkamala, Srinivas dan Andrew, H. S. (2003). *Feature Selection For Instrusion Detection Using Neural Network and Support Vector Machines*. *Departemen Of Computer Science*. USA.

Nguyen, K, Tran, D, Ma, W, and Sharma, D. (2014). An Approach to Detect Network Attacks Applied for Network Forensics. In *International Conference on Fuzzy System and Knowledge Discovery* (pp. 1–57). Retrieved from https://doi.org/10.1109/FSKD.2014.6980912

Pidei Wiyanto, Amir Hamzah, M. S. (2014). Aplikasi Monitoring Keamanan Jaringan Dengan Menggunakan IDS Dan Router Mikrotik. *Jurnal Jarkom*, *2*(1), 89–98.

Resi Utami Putri, J. E. I. (2012). Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *IJCCS*, *6*(2), 101–112.

Riadi, D. M. dan I. (2017). Network Forensics For Detecting Flooding Attack On Web Server. *(IJCSIS) International Journal of Computer Science and Information Security*, *15*(2), 326–331.

Riadi, I., & Umar, Rusydi, W. (2012). Analisis Forensik Serangan SQL Injection Menggunakan Metode Statis Forensik. *Prosiding Interdisiplinary Postgraduate Studen Conference*, *ISBN: 978-*, 102–103.

Sarsono, W. (2012). Pemantauan Jaringan Komputer dengan DNS Server Berbasis Routing Statis Menggunakan Wireshark.

Setia, I. B. (2010). *Analisis Mikrotik PC Router Pada Jaringan Local Di PT.Dang Desaindo Internusa*.

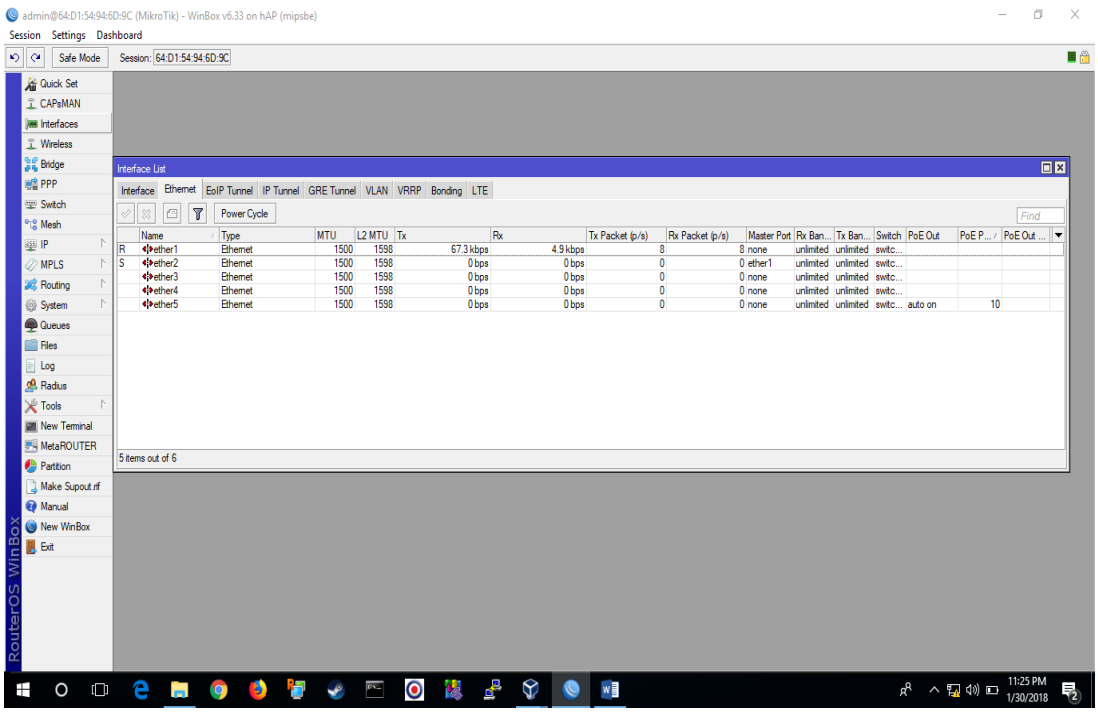
Sitompul Josua. (2012). *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa. Retrieved from http://www.tatanusa.co.id/index.php/produk-buku/buku-referensi/160-cyberspace-cybercrimes-cyberlaw.html

Symantec, T. (2016). Internet Security Threat Report, *21*(April). Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

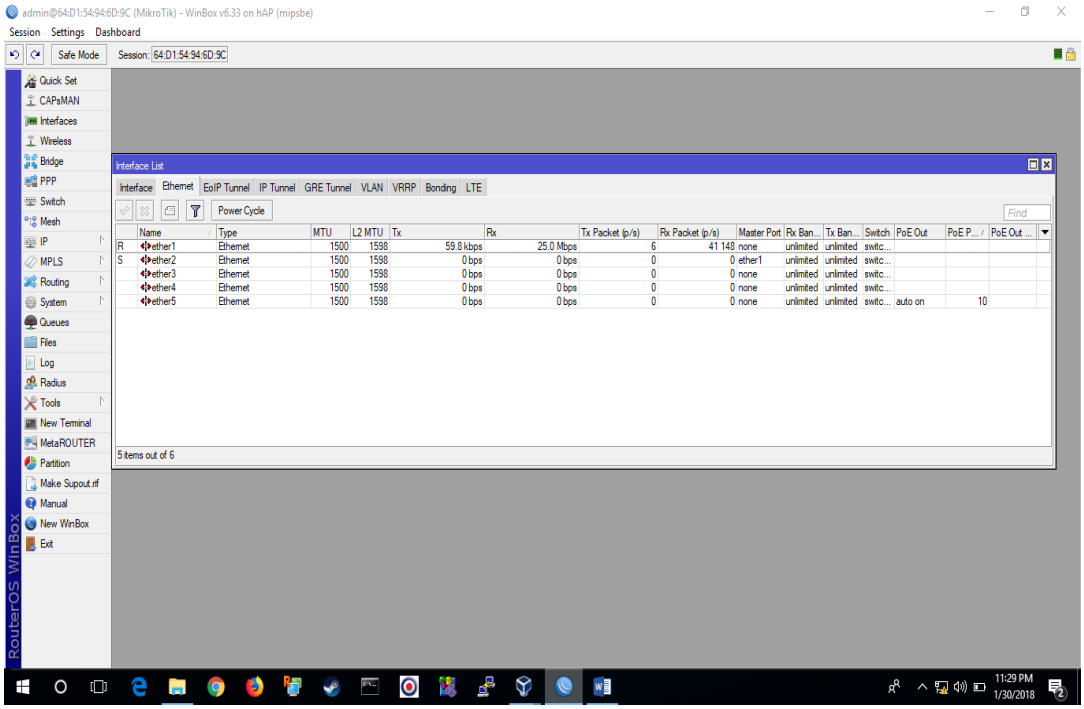
Szewczyk, P. (2007). *ADSL Router Forensics Part 1 : An Introduction to a New Source of Electronic Evidence.* (Edition Cowan University).

LAMPIRAN

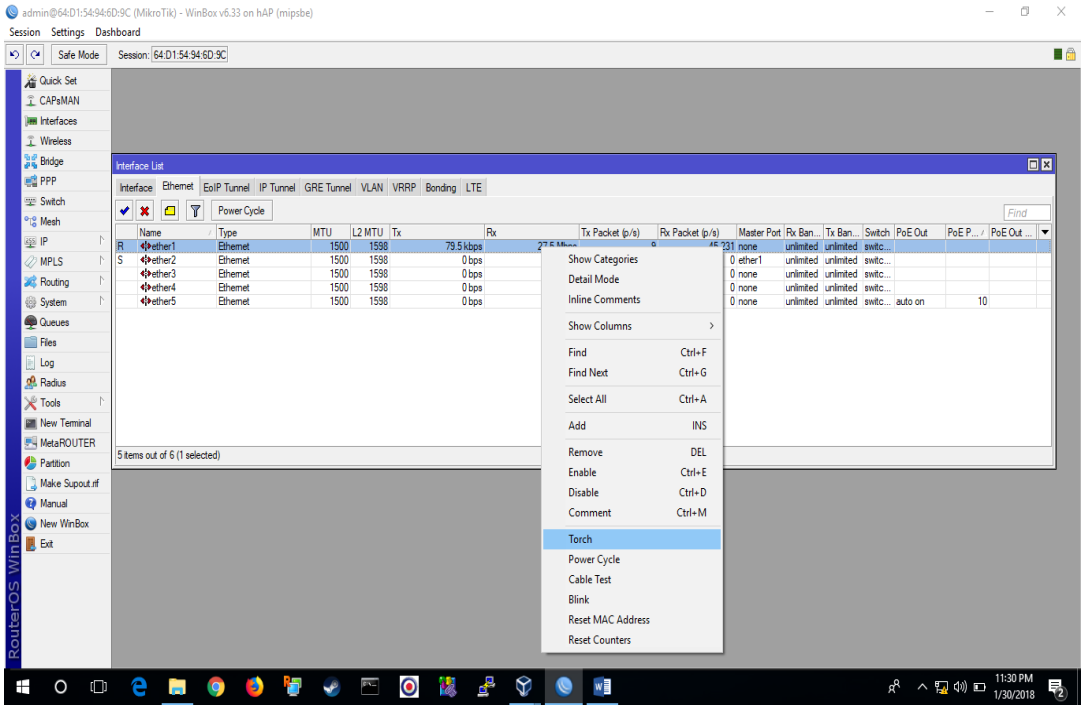
Sebelom diserang



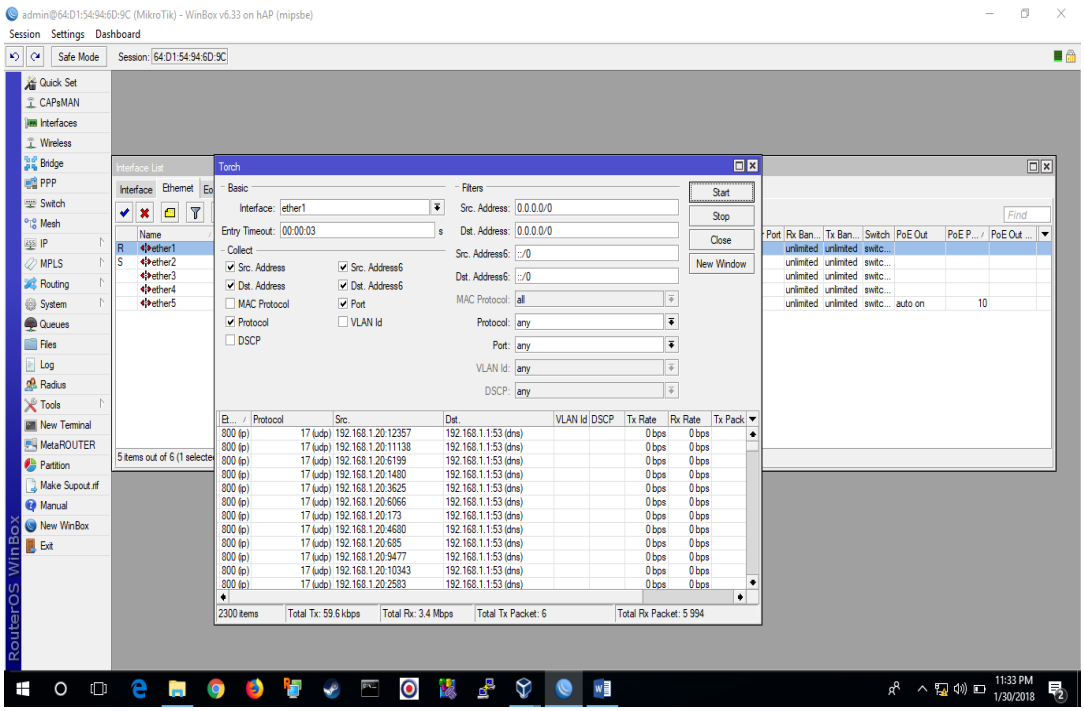
Setelah diserang



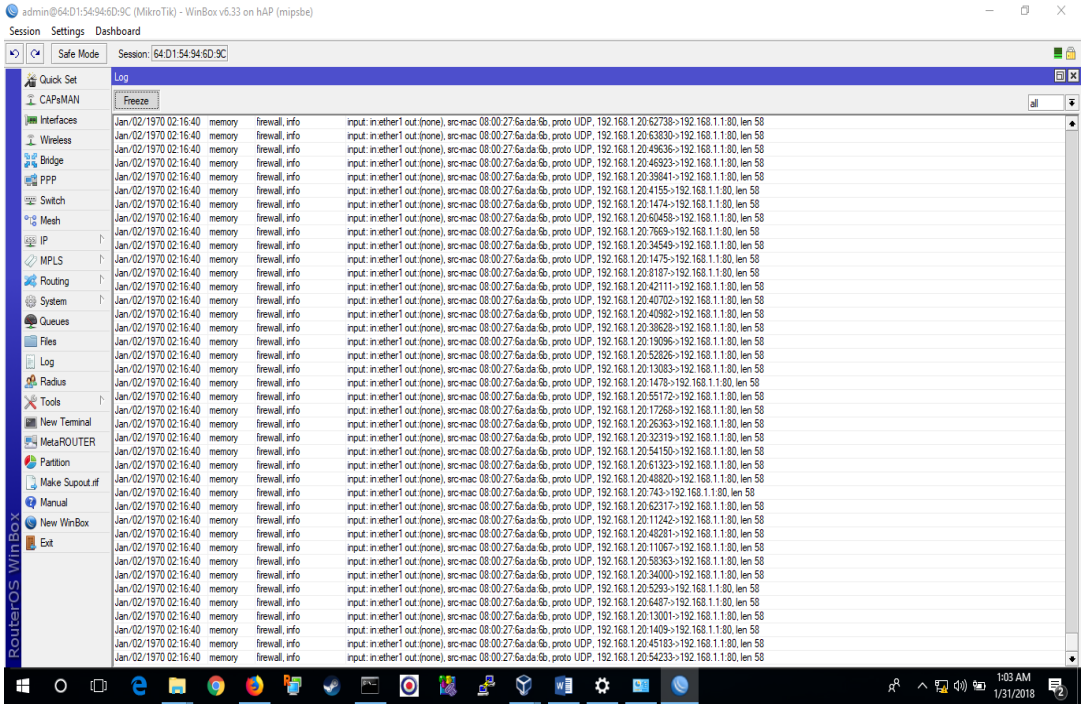
Untuk mengetahui IP yang masuk



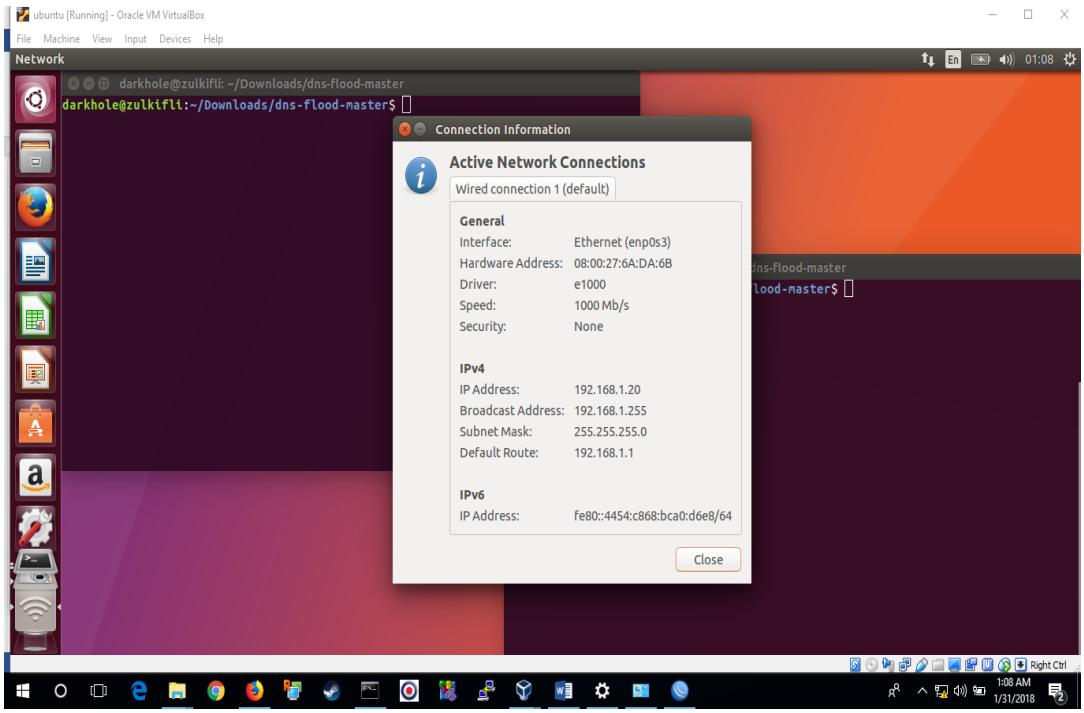
IP addres yang menyerang port 20 dan yang diserang port 53



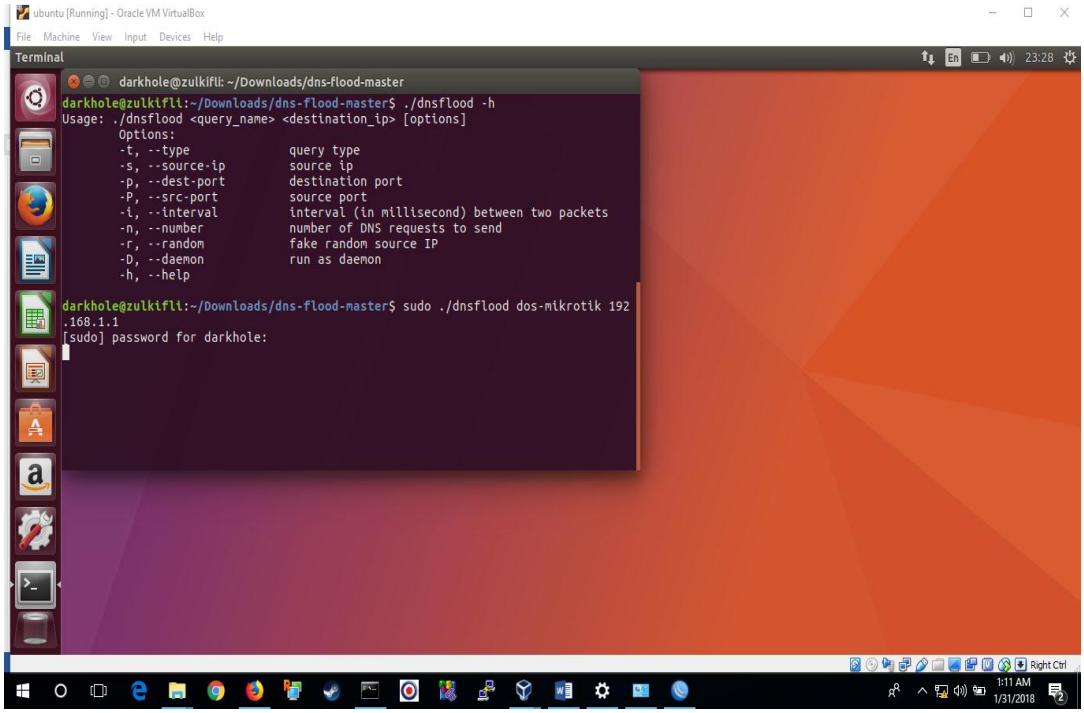
Log port 80



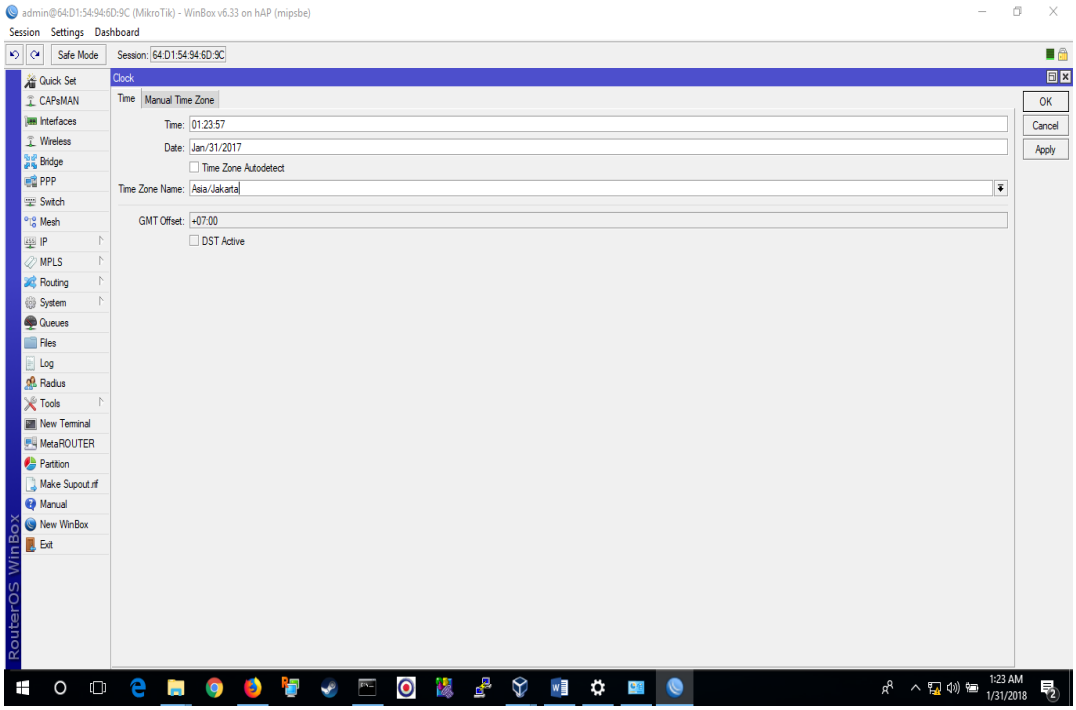
IP penyerang



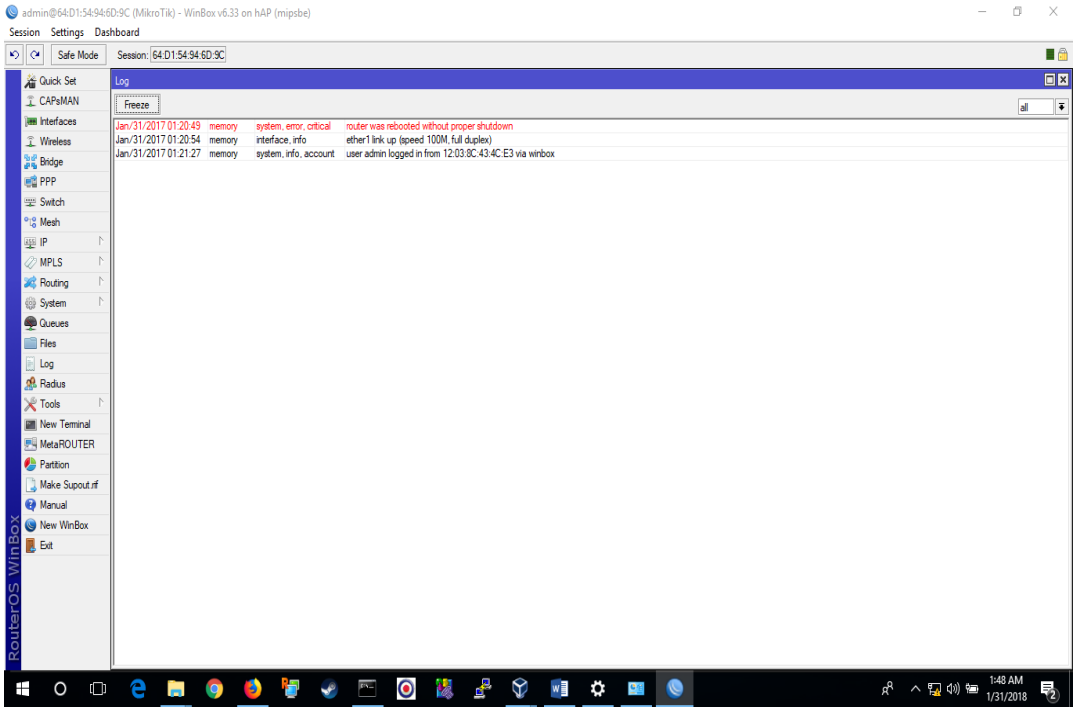
Perintah menyerang



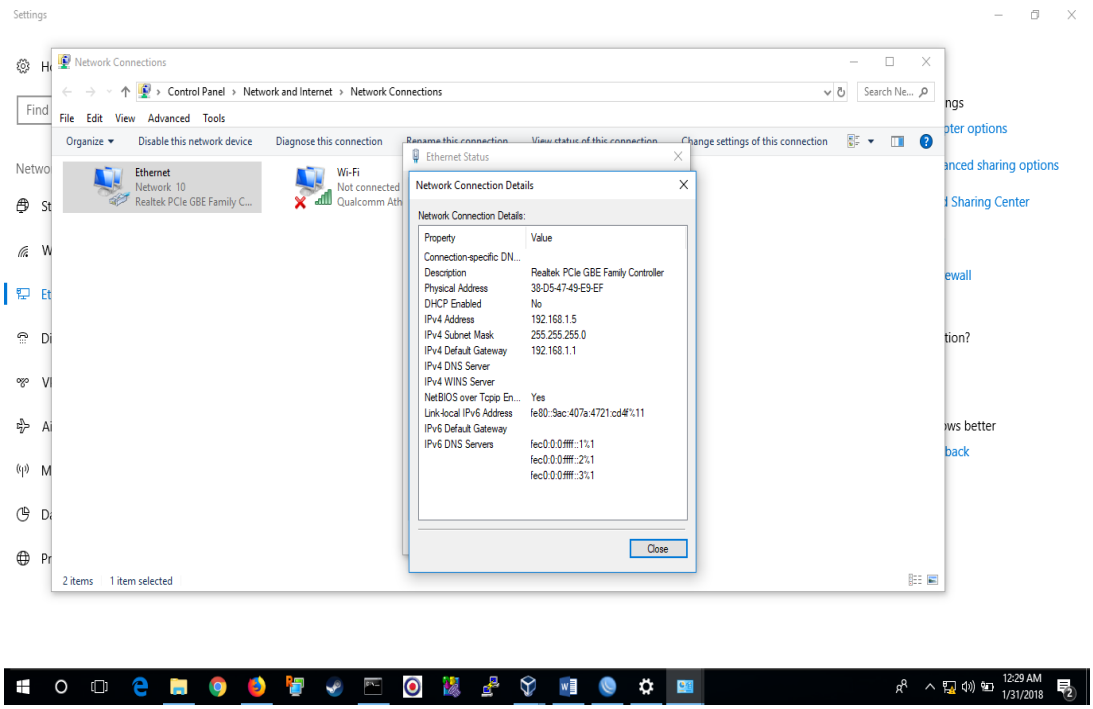
Verifikasi waktu router



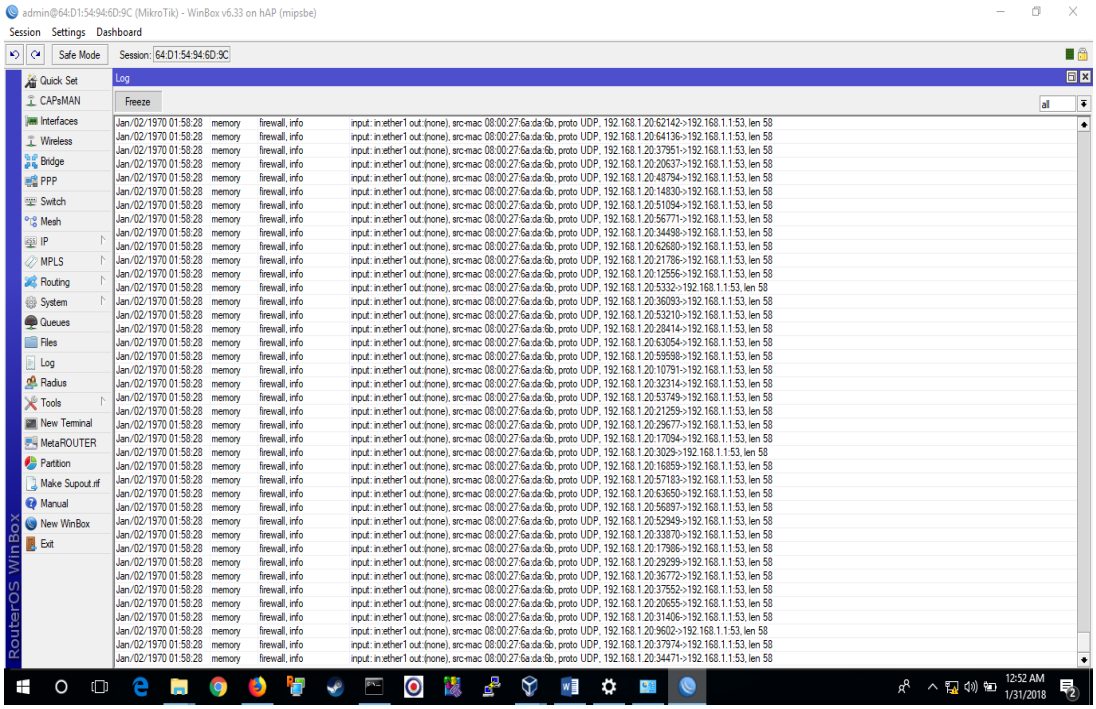
Tampilan awal untuk tabel perbandingan



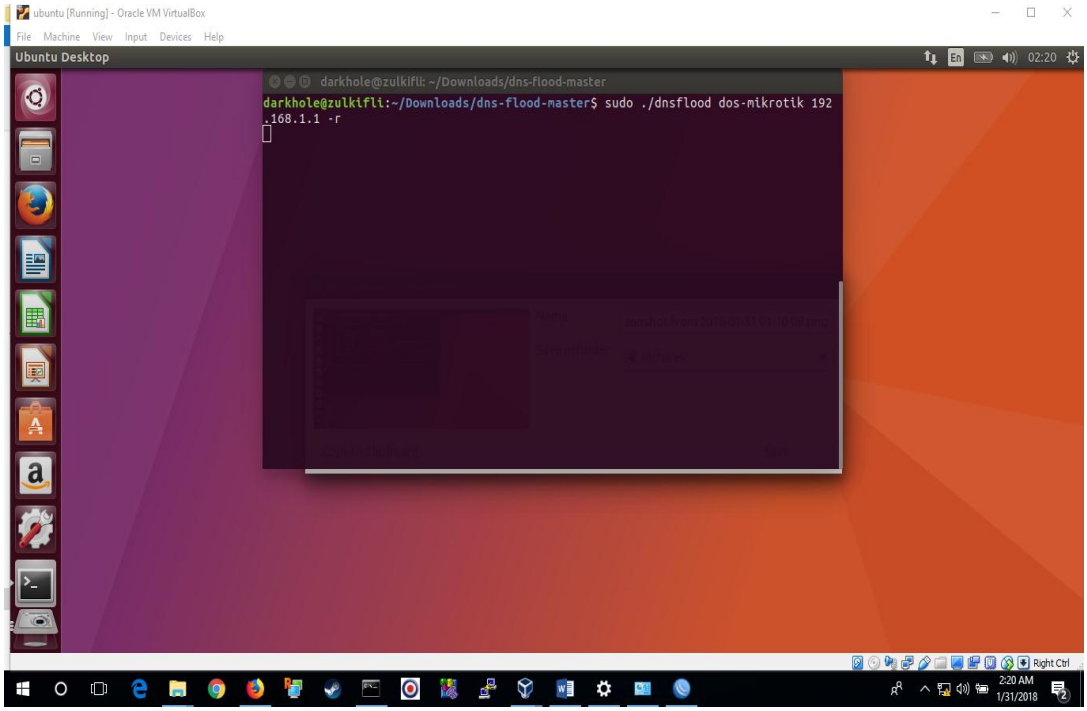
Penerapan uji coba serangan



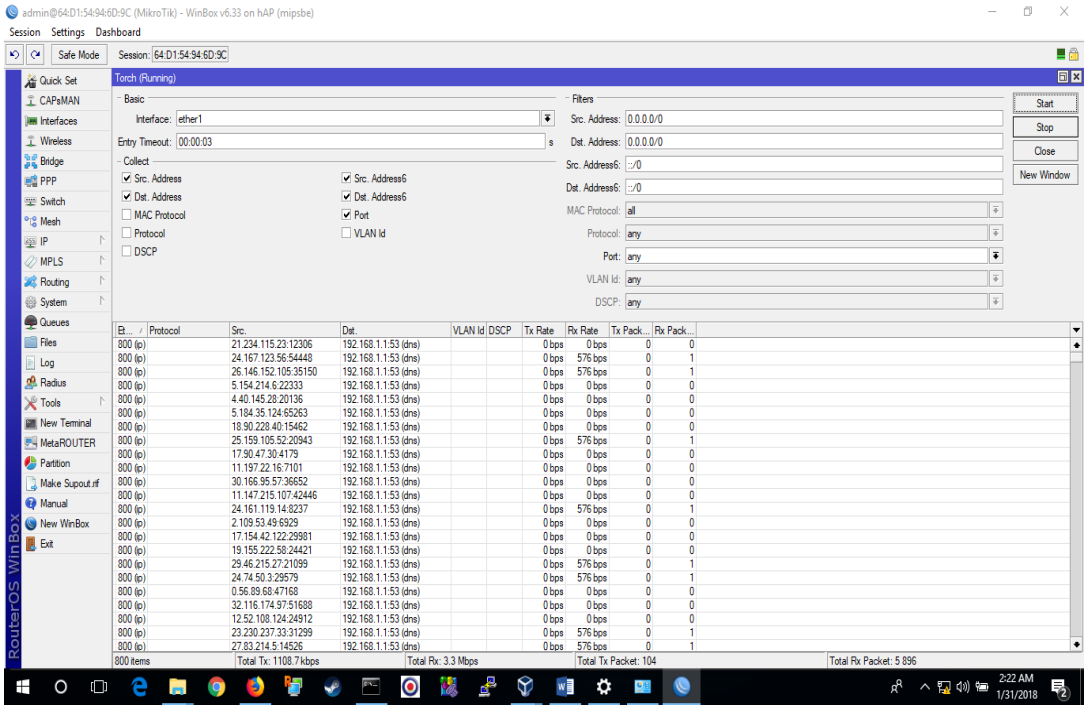
Log serangan pada port 53



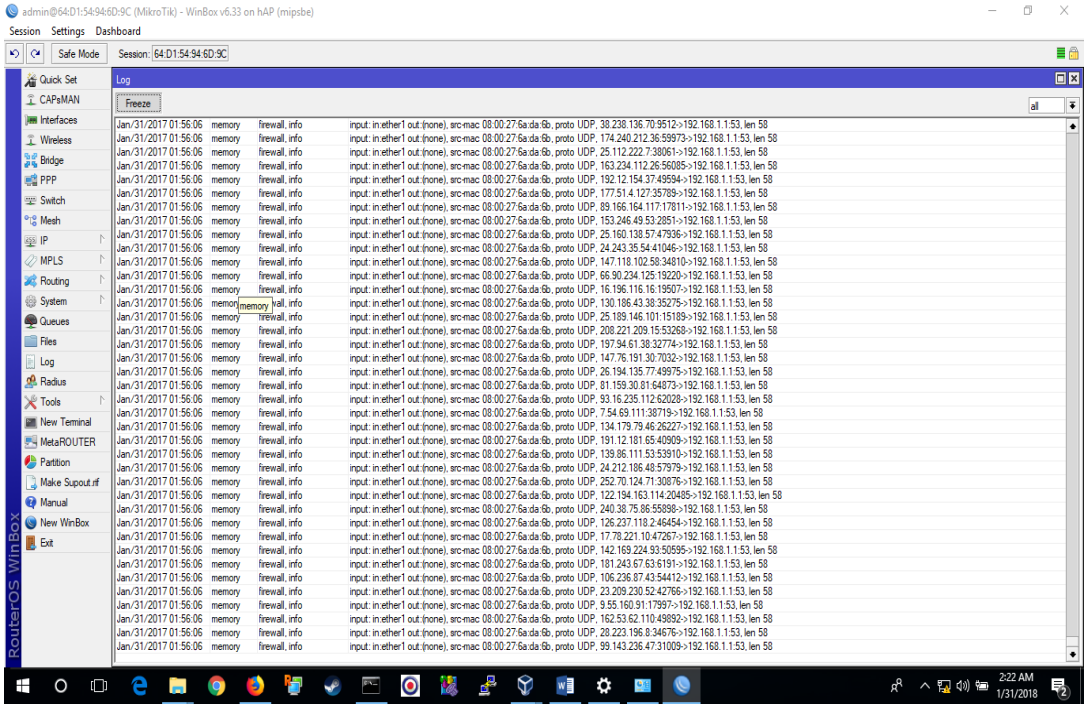
Random port 53



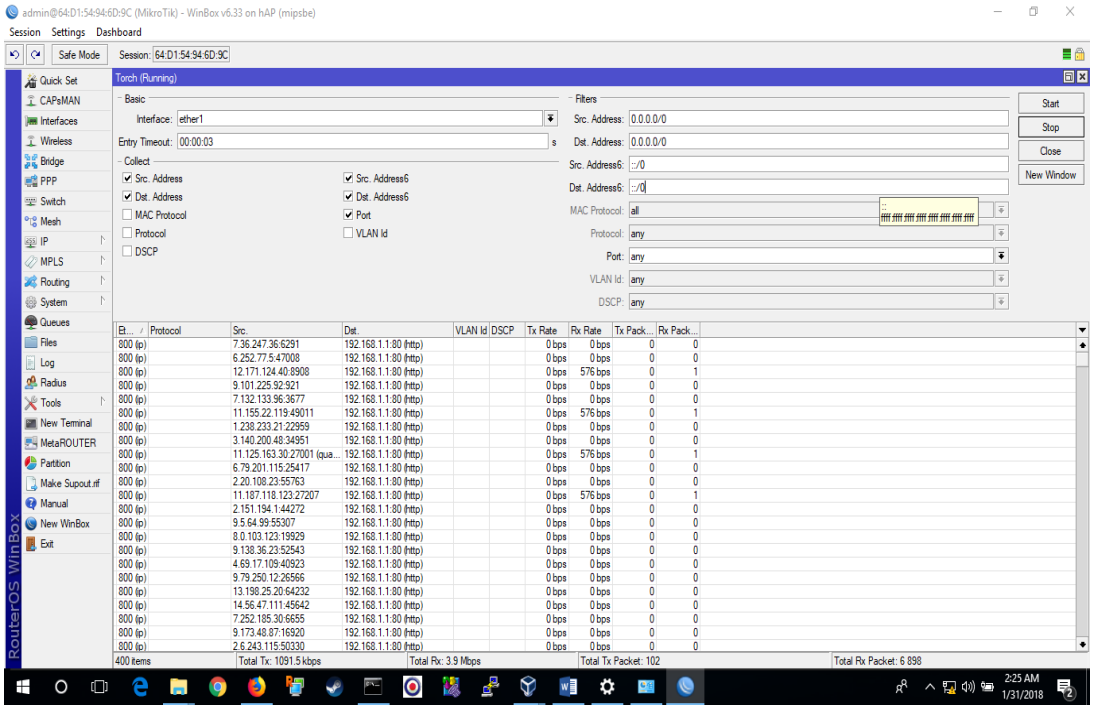
Torce random port 53



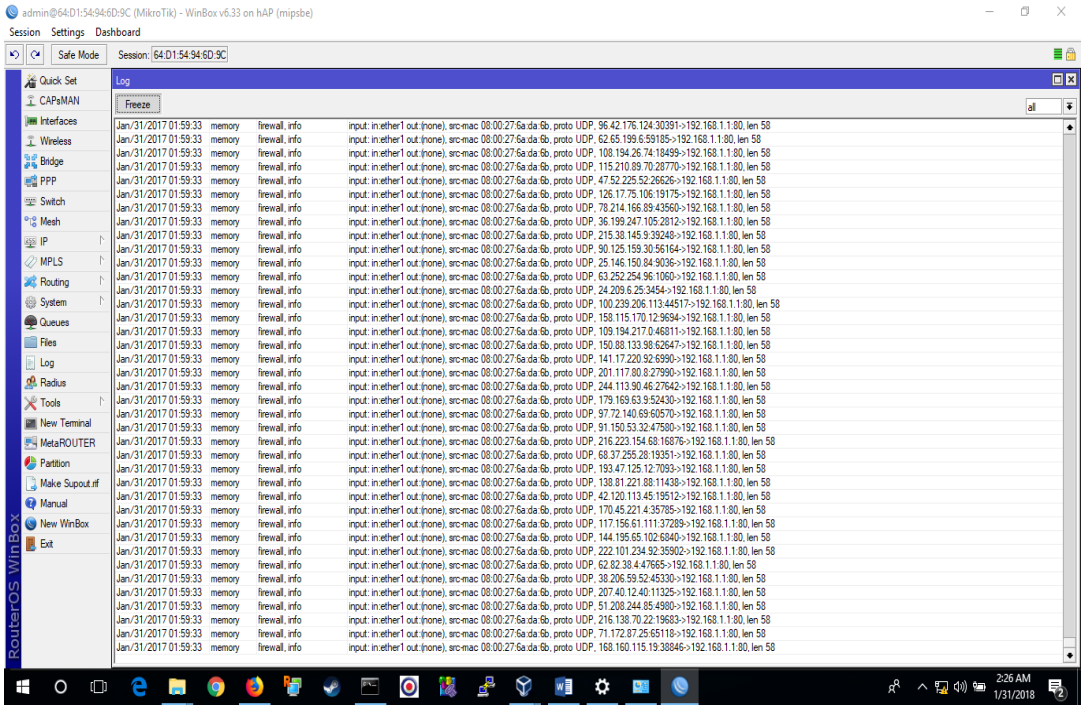
Log random 53



Torce random port 80



Log random port 80



Script untuk deteksi serangan DoS dan Script bloking

DDoS Detection and Blocking

This is the way to prevent (D)DoS Attack from your users to attacked resources, and drop (D)DoS directed to your clients.

First, we catch all new connections and send them to dedicated firewall chain:

```
/ip firewall filter
add chain=forward connection-state=new action=jump jump-target=detect-ddos
```

Note: In RouterOS, any single UDP packet is considered to be new connection by Connection Tracking in any Firewall section (except NAT) until the packet in opposite direction is sent. It's good behaviour, because legitimate traffic (like uTorrent's or Skype's UDP stream) is bidirectional, so it triggers 'connection-state=new' only once per stream; on the other side, any unidirectional flooding (the only exception I can imagine is NetFlow traffic) generates 'connection-state=new' per each packet even if all packets have the same Src and Dst Addresses and Ports, so it can be easily detected as DoS Attack.

Then, for each "SrcIP:DstIP" pair we allow some number of new connections. One may want also add some exceptions (like DNS servers - it won't be good if they will be blocked):

```
/ip firewall filter
add chain=detect-ddos dst-limit=32,32,src-and-dst-addresses/10s action=return
add chain=detect-ddos src-address=192.168.0.1 action=return
```

Now, we have only packets which exceed our limits - and we add their source to 'ddoser' and the target to 'ddosed' address lists:

```
/ip firewall filter
add chain=detect-ddos action=add-dst-to-address-list address-list=ddosed address-list-timeout=10m
add chain=detect-ddos action=add-src-to-address-list address-list=ddoser address-list-timeout=10m
```

Then packet processing returns to 'forward' chain, where we block any packets from ddosers to ddosed resources:

```
/ip firewall filter
add chain=forward connection-state=new src-address-list=ddoser dst-address-list=ddosed action=drop
```

Discussion on the Forum: http://forum.mikrotik.com/viewtopic.php?f=2&t=54607