


# Metode Live Forensics Acquisition File Sharing Samba untuk Eksplorasi Bukti Digital pada Smart Router

Abdul Rohman Supriyono

13917133

*Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer*

*Konsentrasi Forensika Digital*

*Program Studi Magister Teknik Informatika*

*Program Pascasarjana Fakultas Teknologi Industri*

*Universitas Islam Indonesia*

2018

**Lembar Pengesahan Pembimbing**

**Metode Live Forensics Acquisition File Sharing Samba**
**Untuk Eksplorasi Bukti Digital Pada Smart Router**

Abdul Rohman Supriyono
13917133

Yogyakarta, Bulan Februari, Tahun 2018

| Pembimbing I | Pembimbing II |
| --- | --- |
| Dr. Bambang Sugiantoro, S.Si., M.T. | Yudi Prayudi, S.Si., M.Kom. |

**Lembar Pengesahan Penguji**

**Metode Live Forensics Acquisition File Sharing Samba**
**Untuk Eksplorasi Bukti Digital Pada Smart Router**

Abdul Rohman Supriyono
13917133

Yogyakarta, Bulan Februari, Tahun 2018

Tim Penguji,

Dr. Bambang Sugiantoro, S.Si., M.T.
Ketua

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

Dr. Imam Riadi, S.Pd., M.Kom.
Anggota II

Mengetahui,
Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. Raden Teduh Dirgahayu, S.T., M.Sc.

## Abstrak

### Metode Live Forensics Acquisition File Sharing Samba untuk Eksplorasi Bukti Digital pada Smart Router

Perkembangan perangkat keras jaringan saat ini telah mengarah ke-fleksibilitas penggunaannya, dimana penggunaan media kabel mulai berkurang dengan munculnya berbagai perangkat keras jaringan nirkabel, seperti *wireless router*. *Smart router* sering disebut dengan *smart wifi routers*, yaitu perangkat *wireless router* yang sudah dilengkapi dengan perangkat lunak yang memungkinkan kita mengatur dan memantau jaringan dengan mudah, serta memiliki layanan yang lebih dibandingkan dengan router biasa pada umumnya, router jenis ini selain dapat berfungsi sebagai *router, access point, switch, firewall*, juga dapat dijadikan sebagai *file server* untuk berbagi data (*file sharing*). Secara umum *file sharing* memiliki manfaat diantaranya: Kenyamanan; Mengurangi Biaya; Menghemat Waktu; Mengurangi Ruang Penyimpanan; Peningkatan Integritas Data; Aksebiltas yang lebih baik; File dapat diakses dari mana saja. Tetapi dengan adanya fasilitas seperti ini tidak menutup kemungkinan dalam proses perpindahan pada jaringan terjadi perpindahan konten–konten ilegal ataupun konten yang dapat menimbulkan suatu tindak kejahatan atau pelanggaran hukum dalam hak cipta. Tindak kejahatan tersebut antara lain: meningkatnya ketidakamanan seperti akses yang tidak sah, *worm*, virus, *phising*, dan tindakan lain yang serupa; plagiarisme atau pelanggaran hukum hak cipta seperti mengambil gagasan orang lain dan menjadikannya milik sendiri; kehilangan privasi karena memungkinkan informasi sensitif dapat dengan mudah diakses oleh pihak lain yang tidak sah.

Dengan ke-fleksibilitas yang ada pada *smart router*, maka *smart router*-pun banyak diterapkan di kalangan perumahan dan kantor kecil, namun *smart router* ini paling mudah diretas sehingga terlalu rentan menjadi obyek dari sebuah tindak kejahatan di dunia maya. Hal seperti ini menjadikan tantangan untuk bidang forensik digital dalam menggali lebih dalam tentang mekanisme forensik pada router seiring semakin beragamnya jenis router yang berpotensi sebagai obyek atau barang bukti elektronik. Dalam bidang forensika digital terdapat beberapa tahapan sebelum barang bukti dilaporkan atau disajikan dalam persidangan, seperti mengumpulkan barang bukti, pemeriksaan barang bukti, dan menganalisa barang bukti. Pada tahap pengumpulan barang bukti terdapat dua metode yang sering digunakan yaitu metode *dead forensics* dan metode *live forensics*, dimana dari dua metode tersebut memiliki perbedaan dalam penanganan barang bukti. Metode *dead forensics* atau bisa disebut dengan *traditional forensics* adalah metode yang digunakan pada bukti elektronik yang telah dimatikan, dan merupakan metode yang sederhana. Lain halnya dengan metode *live forensics*, dimana metode ini digunakan untuk mengumpulkan data pada bukti elektronik yang masih dalam kondisi/keadaan menyala. *Smart router* merupakan salah satu jenis perangkat router yang memiliki fitur *file sharing* dan termasuk salah satu perangkat jaringan yang membutuhkan sistem dalam keadaan menyala (*running*) pada saat dilakukan proses investigasi dan bisa disebut sebagai sistem kritis karena memiliki karakteristik sistem yang tidak diperkenankan mati (*shutdown*). Untuk mendapatkan objek–objek digital diperlukan proses investigasi dan uji forensik yang tepat. Oleh karena itu, bagaimana proses investigasi yang efektif untuk kasus–kasus kejahatan *file sharing* pada perangkat *smart router*, bagaimana mekanisme untuk mendapatkan bukti digital dari aktivitas ilegal *file sharing*, serta bukti digital apa saja yang dapat diperoleh dari aktivitas *file sharing* pada *smart router*.

Pada penelitian mekanisme atau metode *live forensics acquisition* yang digunakan untuk mendapatkan bukti digital, dan ada 4 (empat) proses investigasi yang efektif seperti preservasi, akuisisi, analisis, dan laporan. Untuk pengujian yang dilakukan pada kedua perangkat *smart router* menghasilkan bukti digital berupa *log system* yang beragam. Untuk membuktikan adanya tindakan ilegal dalam berbagi data, maka perlu adanya pencocokan list dan direktori yang dihasilkan dari proses imaging pada masing–masing media penyimpanan baik yang ada pada *server* maupun klien yang disesuaikan dengan *timestamp* pada *log system*.

**Kata kunci**

Forensika Digital, Forensik *Live*, Akuisisi *Live*, Berbagi *File*, Samba, *Smart* Router, Bukti Digital, RouterOS, OpenWrt, Konten Ilegal, SNI ISO/IEC 27037:2014.

## Abstract

### Live Forensics Acquisition Method for File Sharing Samba Digital Evidence for Exploration on Smart Router

The development of recent network hardware has led the use of flexibility, in which the use of cable is beginning to reduce by the rise of various wireless network hardware, e.g., wireless router. Smart router is often called smart wifi routers, i.e., hardware of wireless router which has been completed with software that we possible arrange and observe network easily, and also it has the service which generally compares to the usual router, this type of router can function as router, access point, switch, firewall and also file server for file sharing. Generally, file sharing has benefits, such as comfort, reducing the cost, time-saving, reducing storage room, the increase of data integrity, better accessibility, available to access. By the available facilities, it possible happens the movement of illegal content or other contents in the movement process on the network which causes crimes or law in infringement of the copyright. Some of those crimes are the increase of unsafe condition, such as illegal access, worm, virus, phishing, and others; plagiarism or infringement of the copyright, e.g., adopt people's ideas and bring them into being ourselves; loss of privacy because possible sensitive information can be accessed by illegal users. With the available flexibility on the smart router, then it is used in homes and small offices, however, it is often opened, until it has been susceptible being the object of cybercrime on the internet. This creates a challenge for digital forensic in further exploring mechanism of forensic on router along with more variety of router types as object or electronic evidence. In digital forensics, there are some steps before the evidence is reported or provided in court, e.g., collect, investigate, and analyze evidence. In the process of collecting evidence, there are two methods which often used, i.e., dead forensic and live forensic, in which on those two methods have a difference in handling evidence. Dead forensic method or it can be called traditional forensics, i.e., a method which used on the turned out electronic evidence, and it is a simple method. On the other hand, a live forensic method is used to collect data on the electronic evidence which is running. The smart router is one of a set of equipment of router which has file sharing and includes one of network hardware which needs a system in running condition when being conducted investigation process and it is called as a critical system because of having system characteristics which not allowed to shut down. It is needed investigation process and exact forensic test to obtain digital objects. Therefore, how effective is investigation process for some crime cases of file sharing on the smart router, how is the mechanism to obtain digital evidence from illegal file sharing, and also what digital evidence can it be obtained from file sharing on the smart router. In this research, the mechanism or live forensic method which used to obtain digital evidence, and there are 4 (four) effective investigation processes, e.g., preservation, acquisition, analysis, and report. The test which conducted on the second hardware of smart router creates digital evidence in the form of various log system. To verify whether an illegal action for sharing data, then it needs to do reconciliation list and directory which provided from imaging process on each storage media both on server and client which conformed to the timestamp on the log system.



**Keywords**

Digital Forensics, Live Forensics, Live Acquisition, File Sharing, Samba, Smart Router, Digital Evidence, RouterOS, OpenWRT, Illegal Content, SNI ISO/IEC 27037:2014.

## Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam 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 analisis 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. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Februari 2018




Abdul Rohman Supriyono, S.T

## Daftar Publikasi

**Publikasi selama masa studi**

Hariyadi, D., & Supriyono, A. R. (2017). Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI ISO/IEC 27037:2014. *TELEMATIKA, 14*(1), 62–67.

**Publikasi yang menjadi bagian dari tesis**

*Sitasi publikasi 1*

| **Kontributor** | **Jenis Kontribusi** |
|---|---|
| Dedi Hariyadi | Mendesain eksperimen (60%)<br>Menulis *paper* (70%) |
| Abdul Rohman Supriyono | Mendesain eksperimen (40%)<br>Pengujian (100%)<br>Menulis dan mengedit *paper* (30%) |

## Halaman Kontribusi

**Tidak ada kontribusi dari pihak lain**

## Halaman Persembahan

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

Sembah sujud serta syukur kepada Allah SWT. Taburan cinta dan kasih sayang-Mu telah memberikanku kekuatan, membekaliku dengan ilmu serta memperkenalkanku dengan cinta. Lantunan shalawat beriring salam menjadi persembahan penuh kerinduan pada revolusioner Islam, pembangun peradaban manusia yang beradab habibana wanabiyana Muhammad SAW.

Tetes peluh yang membasahi asa, ketakutan yang memberatkan langkah, tangis keputus asaan yang sulit dibendung, dan kekecewaan yang pernah menghiasi hari – hari, kini menjadi tangisan penuh kesyukuran dan kebahagiaan yang tumpah dalam sujud panjang. Alhamdulillah maha besar Allah, atas seizin-Mu kuberhasil melewati satu rintangan untuk sebuah keberhasilan, namun kutahu keberhasilan bukanlah akhir dari perjuanganku, tapi awal dari sebuah harapan dan cita – cita. Jalan didepanku masih panjang, masih jauh perjalananku untuk menggapai masa depan yang cerah tuk bisa membahagiakan orang-orang yang kucintai.

Dengan hanya mengharap ridho-Mu semata, kupersembahkan karya sederhana ini kepada orang yang sangat kusayangi.

**Mama dan Bapa**

Sebagai tanda bakti, hormat, dan rasa terimakasih yang tiada terhingga kupersembahkan karya kecil ini kepada Mama dan Bapa yang telah memberikan kasih sayang, segala dukungan, dan cinta kasih yang tiada terhingga, yang tiada mungkin dapat kubalas hanya dengan selembar kertas yang bertuliskan kata cinta dan persembahan. Semoga ini menjadi langkah awal untuk membuat Mama dan Bapa bahagia, karena kusadar selama ini belum bisa berbuat yang lebih. Untuk Mama dan Bapa yang selalu membuatku termotivasi dan selalu menyirami kasih sayang, selalu mendo'akanku, selalu menasehatiku menjadi lebih baik. Terimakasih Mama....Terimakasih Bapa....

Maaf Bapa kalau anakmu ini belum sempat membuat Bapa bangga sampai akhir hayatmu... hanya do'a yang tulus semoga Bapa selalu dilapangkan dan selalu diterangi makamnya, semoga Allah SWT menerima segala amal ibadah Bapa dan mengampuni segala kekhilafan yang pernah dilakukan, dan semoga kelak kita dipertemukan di Surga-Nya... Aamiin ya Rabbal 'alamin....

**Istriku**

Sebagai tanda cinta kasihku, aku persembahkan karya kecil ini buatmu. Terimakasih atas kasih sayang, perhatian, dan kesabaranmu yang telah memberikanku semangat dan inspirasi dalam menyelesaikan tesis ini, semoga engkau pilihan yang terbaik buatku dan masa depanku. Terimakasih "ay"...

**Aanak – anakku**

Untuk anak – anakku, tiada yang paling mengharukan saat kumpul bersama kalian, kalian adalah warna – warni kehidupan yang tak akan bisa tergantikan, terimakasih buat waktu bersama dengan kalian yang terbuang hanya untuk sebuah karya kecil ini. Maaf belum bisa menjadi pemimpin yang baik buat kalian, tapi bapak akan selalu berusaha menjadi yang terbaik buat kalian semua....

**Abah dan Umi**

Buat Abah dan Umi, terimakasih atas apa yang sudah Abah dan Umi berikan, dukungan baik moril dan materil. Maaf kalau belum bisa menjadi menantu yang baik, yang masih suka bikin Abah dan Umi repot harus mengurus anak – anak kami. Semoga amal ibadah Abah dan Umi bisa menjadi amalan untuk bekal kelak di akhirat.

**Saudara dan Keluarga Besar**

Buat mbakku satu – satunya, terimakasih atas motivasi yang telah mba berikan, atas do'amu yang selalu mengiringiku. Terucap kata maaf untukmu karena selalu mengabaikan nasehatmu. Selalu terdiam dan pergi dengan keluhan bila kata – kata lembut yang penuh pengetahuan kau lemparkan padaku. Tapi yakinlah, tak ku jadikan sebagai dendam melainkan motivasi yang ku kemas dalam harapan. Berharap apa yang kau katakan akan ku wujudkan. Ku berdo'a agar suatu saat nanti kita jadi partner saudara yang akur, kompak dan dapat membahagiakan orang tua kita. Aamiin ya Rabbal 'alamin...

Buat keluarga besar Bani Nasucha dan Bani Sholeh Hasan yang tidak mungkin aku sebutkan satu persatu, terimakasih buat motivasi yang selalu kalian berikan, maaf kalau hanya sekedar ucapan terimakasih, semoga segala kebaikan kalian semua menjadikan amalah di hadapan Allah SWT. Aamiin ya Rabbal 'alamin

**Komunitas Ngapak "Pandansari"**

Ade karo Wili Suwun ya...wis gelem ditunuti, go numpang ngaso... tanpa kowe kowe pada ndeane aku turu nang SPBU. PokokE matur suwun banget lah.....Hehehehe

ٱلْحَمْدُ لِلَّهِ رَبِّ ٱلْعَٰلَمِينَ

## Kata Pengantar

Assalamu'alaikum Wr.Wb.

Alhamdulillah segala puji syukur penulis panjatkan kehadirat Allah SWT atas segala nikmat, rahmat, taufik, dan hidayah-Nya, sehingga tesis yang berjudul "*Metode Live Forensics Acquisition File Sharing Samba untuk Eksplorasi Bukti Digital pada Smart Router*", dapat terselesaikan. Tidak lupa shalawat serta salam penulis haturkan kepada junjungan Nabi Besar Muhammad SAW, Keluarga Beliau dan para Sahabat Beliau yang telah membimbing umat manusia kejalan yang lurus.

Tesis ini disusun sebagai salah satu syarat memperoleh gelar Magister Komputer pada program studi Magister Teknik Informatika, Program Pascasarjana Fakultas Teknologi Industri, Universitas Islam Indonesia, serta sebagai sarana untuk menerapkan ilmu yang telah didapatkan selama masa perkuliahan dengan konsentrasi Forensika Digital. Dalam penyusunan tesis ini tidak lepas dari dukungan pihak terkait yang telah banyak membantu dalam menyelesaikan laporan ini. Oleh karena itu, pada kesempatan ini penulis dengan kerendahan hati ingin menyampaikan rasa terimakasih kepada:

1. Allah SWT, tidak ada Tuhan yang patut disembah selain Engkau, dan Muhammad SAW, Rasulullah penutup dari para nabi.
2. Bapak Dr. Raden Teduh Dirgahayu, ST., M.Sc sebagai Ketua Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta.
3. Bapak Yudi Prayudi, S.Si., M.Kom selaku Ketua PUSFID Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta sekaligus Pembimbing II yang telah meluangkan banyak waktunya dalam membimbing dan mebantu penulis selama penulisan Tesis ini.
4. Bapak Dr. Bambang Sugiantoro, MT selaku Pembimbing I yang telah memberikan arahan-arahan dalam membimbing dan membantu penulis selama penulisan Tesis ini.
5. Bapak Dr. Imam Riadi, M.Kom selaku Penguji yang telah memberikan masukan, saran dan kritikannya kepada penulis dalam tahap perbaikan-perbaikan penyusunan laporan tesis ini.
6. Segenap Dosen dan Staf Universitas Islam Indonesia Yogyakarta, khususnya Fakutas Teknologi Industri, Terima kasih atas semuanya.

7. Teman-teman semuanya dari Magister Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta dan juga khususnya Konsentrasi Forensika Digital Angkatan 8, Terima kasih banyak sudah saling mengingatkan.

Penulis menyadari sepenuhnya bahwa penyusunan laporan Tesis ini masih jauh dari kata sempurna sehingga masih diperlukan penyempurnaan lebih lanjut. Untuk itu saran, kritik dan tambahan yang sifatnya membangun penulis harapkan dari pembaca untuk selanjutnya. Harapan penulis, semoga Laporan Tesis ini dapat bermanfaat bagi penulis pribadi pada khususnya dan untuk kita semua pada umumnya, serta dapat berguna bagi kemajuan bidang ilmu Forensik Digital. Aamiin.

Wassalamu'alaikum, Wr. Wb

Yogyakarta, Februari 2018

Abdul Rohman Supriyono

## Daftar Isi


Lembar Pengesahan Pembimbing ..... i

Lembar Pengesahan Penguji ..... ii

Abstrak ..... iii

Abstract ..... v

Pernyataan Keaslian Tulisan ..... vi

Daftar Publikasi ..... vii

Halaman Kontribusi ..... viii

Halaman Persembahan ..... ix

Kata Pengantar ..... xi

Daftar Isi ..... xiii

Daftar Tabel ..... xvi

Daftar Gambar ..... xvii

Glosarium ..... xix

BAB 1 Pendahuluan ..... 1

1.1 Latar Belakang ..... 1

1.2 Permasalahan ..... 7

1.3 Rumusan Masalah ..... 8

1.4 Batasan Masalah ..... 8

1.5 Tujuan Penelitian ..... 8

1.6 Manfaat Penelitian ..... 9

1.7 *Review* Penelitian ..... 9

1.8 Metodologi Penelitian ..... 19

1.9 Sistematika Penulisan ..... 20

BAB 2 Tinjauan Pustaka ..... 22

2.1 *Forensics Science* ..... 22

2.2 *Digital Forensics* ..... 22
2.3 *Network Forensics* ..... 23
2.4 *Router, Smart Router* ..... 25
2.5 Referensi Model OSI (*Open System Interconnection*) ..... 26
2.6 Klasifikasi Barang Bukti Digital ..... 28
2.7 Proses Investigasi ..... 29
2.8 *Live Forensics* ..... 36
2.9 *File Log* ..... 38
2.10 Samba ..... 39
2.11 Hak Cipta ..... 40
BAB 3 Metodologi Penelitian ..... 41
3.1 Studi Pustaka ..... 41
3.2 Persiapan Alat dan Bahan Penelitian ..... 41
3.3 Persiapan Skenario ..... 42
3.3.1 Skenario 1 (satu) ..... 44
3.3.2 Skenario 2 (dua) ..... 44
3.4 Simulasi Kasus ..... 45
3.5 Investigasi dan Olah TKP ..... 45
3.5.1 Identifikasi ..... 45
3.5.2 Pengumpulan ..... 45
3.5.3 Akuisisi ..... 46
3.5.4 Preservasi ..... 49
3.6 Analisis Forensik ..... 49
3.7 Laporan ..... 51
BAB 4 Hasil dan Pembahasan ..... 52
4.1 Hasil Rancangan / Desain ..... 52
4.2 Data ..... 53

4.3 Skenario ..... 53
4.4 Simulasi Kasus ..... 54
4.5 Investigasi dan Olah TKP ..... 54
4.5.1 Pengamanan Barang Bukti ..... 54
4.5.2 Akuisisi Barang Bukti ..... 55
4.6 Pengujian ..... 62
4.6.1 MikroTik RB951Ui-2HnD ..... 63
4.6.2 GL-inet AR300 ..... 67
4.7 Analisis Hasil dari Pengujian ..... 70
4.7.1 Analisis pada *smart router* MikroTik RB951Ui-2HnD ..... 70
4.7.2 Analisis pada *smart router* GL-inet AR300 ..... 73
4.8 Analisis Hasil Penelitian ..... 76
4.8.1 Bukti digital yang diperoleh dari aktifitas *file sharing* pada *Smart Router* ... 76
4.8.2 Mekanisme untuk mendapatkan Bukti Digital dari aktivitas *file sharing*. ..... 77
4.8.3 Proses investigasi untuk kasus kejahatan *file sharing* pada *smart router* ..... 78
BAB 5 Kesimpulan dan Saran ..... 84
5.1 Kesimpulan ..... 84
5.2 Saran ..... 85
Daftar Pustaka ..... 86

# Daftar Tabel

Tabel 1.1 Literature *Review* Terhadap Penelitian Sebelumnya ..... 16
Tabel 3.1 Persiapan Alat dan Bahan Penelitian..... 41
Tabel 4.1 Detail Akuisisi *USB Thumbdrive* MikroTik RB951Ui-2HnD ..... 61
Tabel 4.2 Detail Akuisisi *USB Thumbdrive* GL-inet AR300 ..... 62
Tabel 4.3 Akuisisi *USB Thumbdrive* MikroTik RB951Ui-2HnD [skenario2]..... 65
Tabel 4.4 Akuisisi Media Penyimpanan Klien(Tersangka) MikroTik [skenario2]..... 66
Tabel 4.5 Akuisisi *USB Thumbdrive* GL-inet AR300 [skenario2]..... 68
Tabel 4.6 Akuisisi Media Penyimpanan Klien(Tersangka) GL-inet [skenario2]..... 69
Tabel 4.7 Detail Informasi Kasus pada Perangkat MikroTik..... 70
Tabel 4.8 Detail Informasi Kasus pada Perangkat GL-inet..... 73
Tabel 4.9 Analisis Forensik untuk *Smart Router* ..... 79

## Daftar Gambar


Gambar 1.1 Pertumbuhan Pemakaian Internet ..... 1
Gambar 1.2 Penggunaan Layanan Berbagi Konten *peer-to-peer* ..... 3
Gambar 1.3 Alur Metodologi Penelitian ..... 19
Gambar 2.1 Akuisisi Bukti Elektronik dalam Kondisi Menyala ..... 35
Gambar 3.1 Topologi Jaringan ..... 43
Gambar 3.2 Alur Skenario 1 (satu) ..... 44
Gambar 3.3 Alur Skenario 2 (dua) ..... 44
Gambar 3.4 Mekanisme Investigasi *Live Acquisition* ..... 46
Gambar 3.5 Akuisisi Perangkat Router Melalui Jaringan ..... 47
Gambar 3.6 Akuisisi pada *Storage* (*USB Thumb Drive*) ..... 48
Gambar 3.7 Alur kerja Forensik ..... 50
Gambar 3.8 Alur Proses Investigasi Forensik ..... 51
Gambar 4.1 Rancangan Topologi Jaringan dengan Packet Tracer ..... 52
Gambar 4.2 Perangkat *Smart Router* (kiri GL-inet AR300, kanan MikroTik RB951Ui-2HnD) 53
Gambar 4.3 Barang Bukti Elektonik ..... 55
Gambar 4.4 Perangkat Komputer Akuisisi Barang Bukti ..... 56
Gambar 4.5 Tampilan Proses pada MikroTik ..... 57
Gambar 4.6 Tampilan Proses pada GL-inet ..... 58
Gambar 4.7 Akses File *Log* Menggunakan FTP ..... 59
Gambar 4.8 Akses File *Log* Menggunakan SSH ..... 60
Gambar 4.9 *USB Write Blocker* ..... 60
Gambar 4.10 Proses *Imaging* media penyimpanan *USB Thumbdrive* pada MikroTik ..... 61
Gambar 4.11 Proses *Imaging* media penyimpanan *USB Thumbdrive* pada GL-inet ..... 62
Gambar 4.12 Koneksi *client* ke *server* ..... 63
Gambar 4.13 Aktivitas Klien ..... 64
Gambar 4.14 Aktivitas *client* pada *File Sharing* ..... 64
Gambar 4.15 Aktivitas *Log* pada *smart router* MikroTik RB951Ui-2HnD_skenario2 ..... 65
Gambar 4.16 a. Aktivitas *Log* pada *smart router* GL-inet AR300_skenario1 ..... 67
Gambar 4.17 b. Aktivitas *Log* pada *smart router* GL-inet AR300_skenario1 ..... 67
Gambar 4.18 Aktivitas *Log* pada *smart router* GL-inet AR300_skenario2 ..... 68
Gambar 4.19 Aktivitas Klien ..... 71

Gambar 4.20 Aktivitas Klien mengakses *File Sharing* ..... 71
Gambar 4.21 Bukti perubahan isi dari *file sharing* pada *USB Thumbdrive* MikroTik..... 72
Gambar 4.22 *List* Direktori *Root* pada Media Penyimpanan Klien MikroTik ..... 72
Gambar 4.23 Proses Koneksi Klien ke *Server* ..... 74
Gambar 4.24 Klien Melihat Isi Direktori *Server* ..... 74
Gambar 4.25 Aktivitas Klien terkait tindakan ilegal *file sharing*..... 74
Gambar 4.26 *List* Direktori *Root* pada Media Penyimpanan *Server* GL-inet ..... 75
Gambar 4.27 *List* Direktori *Root* pada Media Penyimpanan Klien..... 75
Gambar 4.28 Direktori File Samba pada *smart router* GL-inet AR300..... 77

## Glosarium

| | |
|---|---|
| CIFS | - Common Internet File System, merupakan protokol berbagi-file asli pada Windows 2000, versi yang disempurnakan dari protokol Server Message Block oleh Open Microsoft. |
| Client | - Merupakan komputer atau end device yang diperbolehkan untuk masuk kedalam jaringan dan mengambil/menggunakan segala sumber daya yang tersedia di dalam jaringan. |
| DHCP | - Dynamic Host Control Protokol, merupakan protokol yang berbasis arsitektur client/server yang dipakai untuk memudahkan pengalokasian alamat IP pada host klien dalam satu jaringan secara otomatis, perangkat yang memberikan nomor IP disebut sebagai DHCP server, sedangkan perangkat yang meminta nomor IP disebut sebagai DHCP Client. |
| File Sharing | - Merupakan sebuah cara untuk menyediakan layanan penyimpanan digital pada sebuah server. |
| Forensika | - Merupakan aplikasi ilmu pengetahuan dan teknologi untuk menyelidiki dan menetapkan fakta dalam kaitannya dengan hukum. |
| IEC | - International Electrotechnical Commission, merupakan organisasi non profit internasional yang didirikan pada tahun 1906 dan bekerja untuk penyusunan dan penerbitan Standar Internasional di bidang "electrotechnology ", yaitu semua teknologi listrik, elektronik, dan yang terkait dengannya. |
| Image | - File yang mengandung seluruh konten dan merepresentasikan struktur dari sebuah media penyimpanan. |
| IP | - Internet Protocol, merupakan salah satu protokol komunikasi yang dikembangkan oleh Internet Engineering Task Force (IETF) dalam memberikan alamat terhadap sebuah end device, yang digunakan untuk menyampaikan datagram (paket) di sebuah internetwork menggunakan Internet Protocol Suite. |
| ISO | - International Organization for Standardization, merupakan badan penetap standar internasional yang terdiri dari wakil-wakil dari badan standardisasi nasional setiap negara, dan bekerjasama dengan International |

| | |
|---|---|
| | Electrotechnical Commission (IEC) yang bertanggung jawab terhadap standardisasi peralatan elektronik. |
| LAN | - Local Area Network, merupakan jaringan komputer yang jaringannya hanya mencakup wilayah kecil; seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil. |
| MAC | - Media Access Control, merupakan sebuah metode untuk mentransmisikan sinyal yang dimiliki oleh node-node yang terhubung ke jaringan tanpa terjadi konflik. |
| NAS | - Network Attached Storage, merupakan jenis perangkat penyimpanan file khusus yang dikhususkan melayani kebutuhan berkas data dan dapat diakses langsung melalui jaringan area lokal. |
| NFS | - Network File System, merupakan protokol sistem berkas terdistribusi yang awalnya dikembangkan oleh Sun Microsystems. |
| NIC | - Network Interface Card, merupakan perangkat keras jaringan berupa sebuah kartu yang berfungsi sebagai jembatan untuk menghubungkan dari komputer ke sebuah jaringan komputer. |
| ONC RPC | - Open Network Computing Remote Procedure Call, merupakan sistem panggilan prosedur jarak jauh yang dikembangkan oleh Sun Microsystems pada tahun 1980an sebagai bagian dari proyek Network File System. |
| OpenWrt | - Merupakan sistem operasi distribusi GNU/Linux untuk perangkat keras, biasanya digunakan pada perangkat embedded dari untuk lalu lintas jaringan rute seperti perangkat wireless router. |
| P2P | - Peer to Peer, merupakan sebuah topologi jaringan dimana terdapat 2 node yang saling berkomunikasi secara langsung |
| PC | - Personal Computer, merupakan seperangkat komputer yang digunakan oleh satu orang saja / pribadi, dan biasanya berada di lingkungan rumah, kantor, toko, dan dimana saja, yang berfungsi untuk mengolah data input dan menghasilkan output berupa data/informasi sesuai dengan keinginan user (pengguna). |
| RAM | - Random Access Memory, merupakan sebuah tipe penyimpanan komputer yang isinya dapat diakses dalam waktu yang tetap tidak memperdulikan letak data tersebut dalam memori yang sifatnya hanya sementara yaitu saat computer sedang diaktifkan yang dijalankan secara acak. |

RFC - Request For Comments, merupakan salah satu dari seri dokumen infomasi dan standar Internet bernomor yang diikuti secara luas oleh perangkat lunak untuk digunakan dalam jaringan, Internet dan beberapa sistem operasi jaringan, mulai dari Unix, Windows, dan Novell NetWare.

RouterOS - Merupakan sistem operasi yang dikembangkan oleh perusahaan network MikroTik yang diperuntukkan sebagai network router, mencakup berbagai fitur seperti Firewall & Nat, Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server, Hotspot, yang dibuat untuk ip network dan jaringan wireless.

Server - Merupakan sebuah sistem komputer yang menyediakan jenis layanan (service) tertentu dalam sebuah jaringan komputer.

Smart Router - Merupakan perangkat router yang memiliki layanan dan fungsi lebih yang sudah ter-*install* sebelumnya dibandingkan dengan perangkat router pada umumnya, hanya dengan menambah beberapa perangkat tambahan (eksternal).

SMB - Server Message Block, merupakan protokol dalam teknologi informasi yang mengacu kepada protokol client/server yang ditujukan sebagai layanan untuk berbagi berkas (file sharing) di dalam sebuah jaringan.

SNI - Standar Nasional Indonesia, merupakan satu-satunya standar yang ditetapkan oleh Badan Standardisasi Nasional dan berlaku secara nasional di Indonesia.

SOP - Standar Operasional Prosedur, merupakan dokumen yang berkaitan dengan prosedur dalam mengatur tahapan suatu proses kerja atau prosedur kerja tertentu yang dilakukan secara kronologis dan berstandar untuk menyelesaikan suatu pekerjaan yang bertujuan untuk memperoleh hasil kerja yang paling efektif.

TKP - Tempat Kejadian Perkara, merupakan tempat di mana suatu tindak pidana dilakukan atau terjadi dan tempat-tempat lain di mana tersangka dan/atau korban dan/atau barang-barang bukti yang berhubungan dengan tindak pidana tersebut dapat ditemukan.

USB - Universal Serial Bus, merupakan teknologi standar bus serial yang memungkinkan kita untuk menghubungkan alat eksternal (peripheral) seperti scanner, printer, mouse, papan ketik (keyboard), alat penyimpan

data (zip drive), flash disk, kamera digital atau perangkat lainnya ke komputer kita.

UTP - Unshielded Twisted Pair, merupakan salah satu media transmisi berupa sepasang kabel yang ditwist/dipilin satu sama lain dengan tujuan untuk mengurangi interferensi listrik yang dapat terdiri dari dua, empat atau lebih pasangan kabel, yang digunakan untuk menghubungkan sebuah jaringan yang berbasis lokal atau Local Area Network (LAN).

WiFi - Wireless Fidelity, merupakan sebuah teknologi yang memanfaatkan peralatan elektronik untuk bertukar data secara nirkabel (menggunakan gelombang radio) melalui sebuah jaringan komputer, termasuk koneksi Internet berkecepatan tinggi.

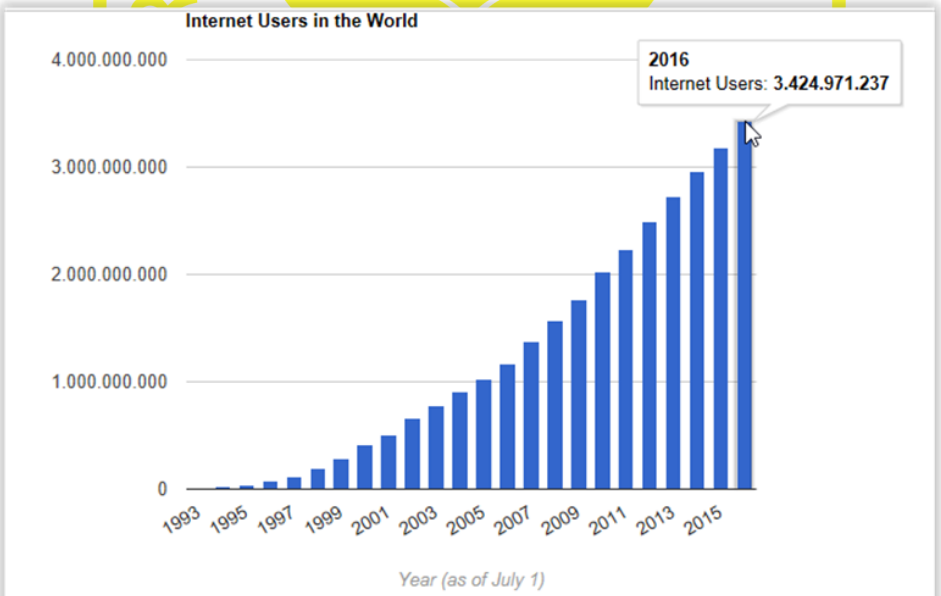
WLAN - Wireless Local Area Network, merupakan teknologi komunikasi data dengan tidak menggunakan kabel untuk menghubungkan antara klien dan server.

# BAB 1

# Pendahuluan

## 1.1 Latar Belakang

Teknologi *internet* dikalangan masyarakat indonesia semakin meningkat dari tahun ke tahun, seperti yang dikutip dari hasil survei yang dilakukan oleh *Internet Live Stats*, bahwa secara global sekitar 46% dari populasi di dunia sebagai pengguna *internet* aktif, saat ini hampir 3.4 milyar orang terkoneksi dengan *internet*, ini merupakan pertumbuhan yang cukup pesat. Meningkatnya jumlah perangkat yang terkoneksi dan terintegrasi dengan *internet* di masa kini telah mengubah perilaku pengguna dan cara mereka mengakses dan mengintegrasikan teknologi ke dalam seluruh aspek kehidupan, baik untuk kepentingan personal maupun bisnis. Untuk gambaran hasil survei yang dilakukan oleh *Internet Live Stats* mengenai pertumbuhan pemakaian teknologi *internet* dapat dilihat pada Gambar 1.1.(Internet Live Stats, 2016).




| Year | Internet Users** | Penetration (% of Pop) | World Population | Non-Users (Internetless) | 1Y User Change | 1Y User Change | World Pop. Change |
|---|---|---|---|---|---|---|---|
| 2016* | **3,424,971,237** | 46.1 % | 7,432,663,275 | 4,007,692,038 | 7.5 % | 238,975,082 | 1.13 % |
| 2015* | **3,185,996,155** | 43.4 % | 7,349,472,099 | 4,163,475,944 | 7.8 % | 229,610,586 | 1.15 % |
| 2014 | **2,956,385,569** | 40.7 % | 7,265,785,946 | 4,309,400,377 | 8.4 % | 227,957,462 | 1.17 % |
| 2013 | **2,728,428,107** | 38 % | 7,181,715,139 | 4,453,287,032 | 9.4 % | 233,691,859 | 1.19 % |

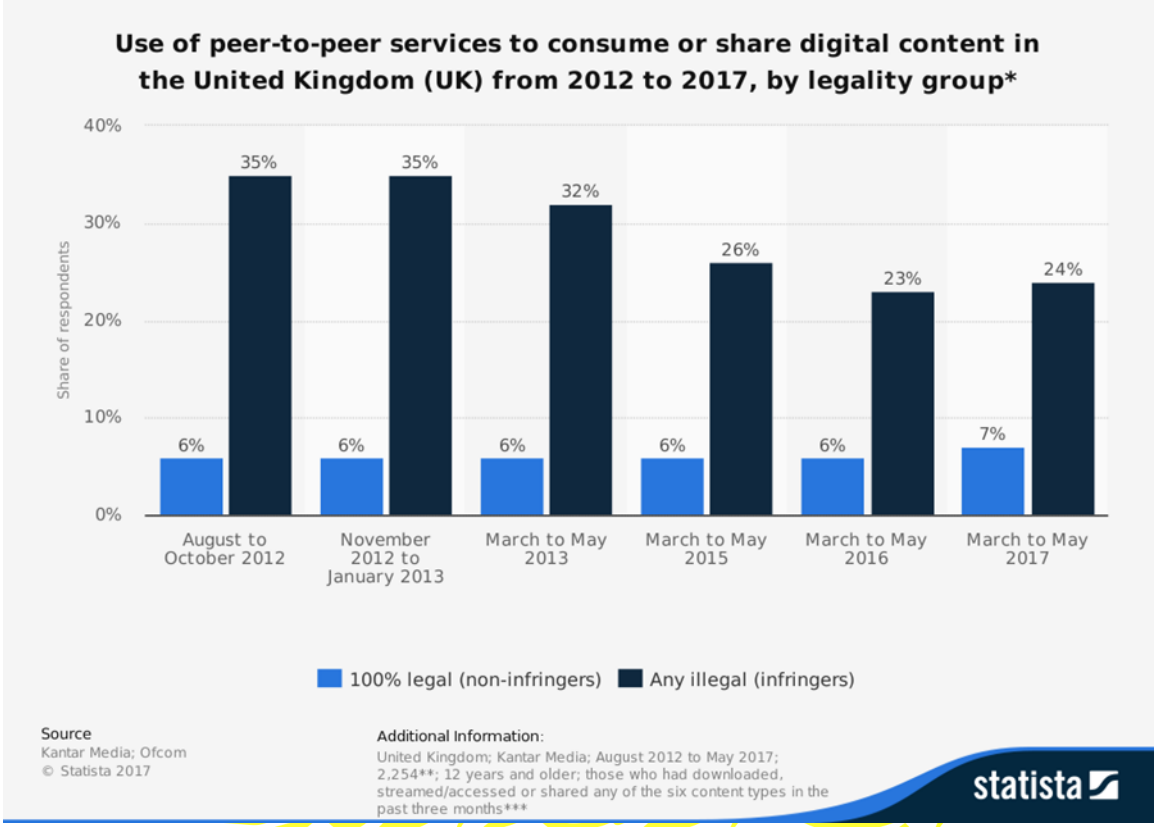
Gambar 1.1 Pertumbuhan Pemakaian Internet

Jaringan komputer merupakan jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data, dengan tujuan setiap bagian dari jaringan komputer dapat meminta dan memeberi layanan (*service*). Pihak yang meminta/menerima layanan disebut dengan klien (*client*) dan yang memberi/mengirim yalanan disebut peladen (*server*). Beberapa perangkat masing – masing memiliki kartu jaringan (*Network Interface Card*) yang saling terhubung satu dengan yang lain melalui kabel maupun tanpa kabel/nirkabel sebagai media transmisi data, dan terdapat perangkat lunak sistem operasi jaringan.

Perkembangan perangkat keras jaringan saat ini telah mengarah ke-fleksibilitas penggunaannya, dimana penggunaan media kabel mulai berkurang dengan munculnya berbagai perangkat keras jaringan menggunakan media nirkabel (Telematika, 2013). Seperti yang dikutip dari laman omnicoreagency dan techradar yang membahas tentang beberapa produk *smart wifi router* yang diimplementasikan di rumah seperti *Securifi Almond, TP-Link Archer C7, NETGEAR AC1750, Google Wifi, Asus RT-AC86U, Netgear Orbi, Linksys WRT32X Gaming Router, Billion BiPac 8900AX-2400, Starry Station, Synology RT2600ac, Linksys WRT 3200 ACM, Zyxel Armor Z2 AC2600, Linksys Velop*(Aslam, 2018; Bastounis, 2018). Salah satu perangkat jaringan yang menggunakan media nirkabel yaitu *wireless router*. *Smart Router* atau sering disebut dengan *Smart Wi-Fi Routers*, yaitu suatu perangkat router yang sudah dilengkapi dengan perangkat lunak *Smart Wi-Fi* yang memungkinkan kita mengatur dan memantau jaringan rumah dengan mudah, serta memiliki fitur atau layanan yang lebih banyak dibandingkan dengan router biasa pada umumnya (Ideaing, 2016). Penggunaan router dengan media nirkabel sekarang banyak beredar, router jenis ini selain dapat berfungsi sebagai *router,* dapat berfungsi sebagai *access point, switch, firewall*, juga dapat dijadikan sebagai *file server* untuk berbagi data (*file sharing*) dan pencetakan (Mag, 2017b)(Mag, 2017a). Ada beberapa kelebihan yang dimiliki oleh router jenis ini (*Smart WiFi Router*), seperti memonitor perangkat jaringan, membatasi akses ke dalam situs tertentu, memantau kamera jaringan secara *live*, dan *streaming* foto atau video (Pcmag, 2018). Pemanfaatan perangkat router jenis ini (*Smart Router*) dalam memenuhi keperluan rumah seperti dijadikannya router sebagai media layanan *file sharing* cukup dengan menambahkan perangkat penyimpanan atau *media storage*, dan dapat dijadikan sebagai *network attached storage* (Cutter, 2017).

*File sharing* atau pertukaran berkas merupakan sebuah metode dalam pendistribusian dan pertukaran file atau menyediakan akses informasi yang tersimpan secara digital, seperti teks, grafik, program komputer, file multimedia (*audio, image, video*) atau buku elektronik

dari satu komputer ke komputer lain melalui jaringan yang memungkinkan pertukaran file secara lokal maupun global secara gratis dan mudah. Hal ini dapat dilakukan dengan beberapa cara diantaranya dengan penggunaan manual yaitu pemanfaatan media yang dapat dilepas, pemakaian *server* terpusat pada jaringan komputer, dokumen *hyperlink* yang dapat diakses melalui situs web, serta dengan metode *peer-to-peer*, seperti aplikasi *P2P sharing* musik *Napster, Gnutella* dan *BitTorrent* (Rouse, 2014). Seperti hasil survey yang dilakukan oleh Kantar Media pada laman statista.com, pada Gambar 1.2 dimana statistik ini menggambarkan penggunaan layanan berbagi konten *peer-to-peer* di Inggris Raya (Inggris) mulai tahun 2012 sampai tahun 2017, yang dilakukan oleh kelompok legalitas. Di antara pelanggar, 24 persen dilaporkan menggunakan layanan *peer-to-peer* pada bulan Mei 2017 (Media, 2017).




Gambar 1.2 Penggunaan Layanan Berbagi Konten *peer-to-peer*

*File-sharing* atau pertukaran berkas untuk pertama kalinya diperkenalkan oleh Ward Christensen pada tahun 1970an dimana merupakan titik awal pertukaran suatu berkas melalui jaringan. Teknologi untuk pertukaran berkas melalui jaringan pada saat itu disebut dengan XMODEM. Dimana XMODEM adalah protokol transfer file sederhana yang dikembangkan oleh Ward Christensen untuk digunakan dalam program terminal MODEM.ASM. Hal ini memungkinkan pengguna mengirimkan file antar komputer mereka

saat kedua belah pihak menggunakan MODEM (Glossbrenner, 1984). *File sharing* atau pertukaran berkas secara umum memiliki manfaat diantaranya: Kenyamanan; Mengurangi Biaya; Menghemat Waktu; Mengurangi Ruang Penyimpanan; Peningkatan Integritas Data; Aksebiltas yang lebih baik; File dapat diakses dari mana saja(Lee, 2017; Multipage, 2015).

Tipe yang digunakan dalam berbagi file seperti: berbagi file secara *peer-to-peer*, dimana *file sharing* didasarkan pada arsitektur aplikasi *peer-to-peer* (P2P) (Schollmeier, 2001). Teknologi yang paling populer untuk *peer-to-peer* (P2P) sharing adalah BitTorrent (Bandara & Jayasumana, 2013; Carmack, 2005). Tipe lain dalam berbagi file yaitu dengan layanan sinkronisasi dan berbagi file berbasis *cloud* yang menerapkan transfer file otomatis dengan memperbarui file dari direktori khusus pada setiap perangkat jaringan pengguna (Geel, 2013). File yang ditempatkan di direktori ini juga biasanya dapat diakses melalui situs web dan aplikasi seluler, dan dapat dengan mudah dibagikan dengan pengguna lain untuk dilihat atau berkolaborasi (Nikiforakis, Balduzzi, Van Acker, Joosen, & Balzarotti, 2011).

Protokol yang sering digunakan dalam pertukaran berkas atau *file sharing* didalam sebuah *NAS* adalah *NFS*, dan *CIFS*. *NAS* sendiri merupakan jenis perangkat penyimpanan file khusus yang dikhususkan melayani kebutuhan berkas data dan dapat diakses langsung melalui jaringan area lokal (Rouse, 2015). *NFS* merupakan protokol sistem berkas terdistribusi yang awalnya dikembangkan oleh Sun Microsystems pada tahun 1984 (Sandberg, Goldberg, Kleiman, Walsh, & Lyon, 1985), yang memungkinkan pengguna di komputer klien mengakses file melalui jaringan komputer seperti penyimpanan lokal yang dapat diakses. Seperti banyak protokol lainnya, NFS dibangun di sistem *Open Network Computing Remote Procedure Call*. NFS adalah standar terbuka yang didefinisikan dalam *Request for Comments*, yang memungkinkan seseorang untuk menerapkan protokol tersebut. Sedangkan *CIFS* merupakan cara standar yang digunakan pengguna komputer untuk berbagi file di *intranet* maupun *Internet*. CIFS merupakan versi yang disempurnakan dari protokol *SMB* oleh *Open Microsoft*, CIFS adalah protokol berbagi-file asli pada Windows 2000, dimana CIFS mendefinisikan serangkaian perintah yang digunakan untuk menyampaikan informasi antara komputer berjejaring (TechNet, 2017).

Terdapatnya fasilitas penyimpanan dalam jaringan dapat membantu pengguna komputer dalam mengatasi kekurangan media penyimpanan serta dengan adanya protokol tersebut dapat memudahkan pertukaran berkas dalam sebuah jaringan, terutama pertukarangan berkas dalam jaringan lokal. Tetapi dengan adanya fasilitas seperti ini tidak menutup kemungkinan dalam proses perpindahan terutama pada jaringan *peer-to-peer* terjadi perpindahan konten – konten ilegal atau pun konten yang dapat menimbulkan suatu

tindak kejahatan atau pelanggaran hukum dalam hak cipta(Desk, 2017; ISU, 2017). Konten – konten tersebut dapat berupa teks, grafik, program komputer, file multimedia (*audio*, *image*, *video*) atau konten sejenis yang dapat disimpan dalam bentuk digital. Adapun resiko dalam berbagi file yang dapat memicu tindak kejahatan tersebut antara lain: meningkatnya ketidakamanan seperti akses yang tidak sah, *worm*, virus, *phising*, dan tindakan lain yang serupa; plagiarisme atau pelanggaran hukum hak cipta seperti mengambil gagasan orang lain dan menjadikannya milik sendiri; kehilangan privasi, berbagi file dapat menyebabkan meningkatnya hilangnya privasi individu atau perusahaan karena memungkinkan informasi sensitif mengenai individu atau perusahaan dapat dengan mudah diakses oleh pihak lain yang tidak sah (Lee, 2017).

Tindakan atau prilaku *cybercrime* yang dapat dilakukan melalui protokol SMB antara lain: a) *Illegal file sharing*, merupakan salah satu tindak kejahatan yang dilakukan dengan melakukan *sharing file* yang bersifat ilegal seperti musik bajakan, *software* bajakan, gambar dan *video*. Dengan melakukan *sharing* data-data ilegal dapat dengan mudah tersebar ke seluruh komputer yang berada dalam 1 jaringan; b) Penyebaran virus, penyebaran virus terjadi akibat fasilitas *sharing* dijalankan sehingga virus dapat dengan mudah menduplikasikan diri ke seluruh media penyimpanan yang ada pada jaringan; c) *Exploit*, SMB ternyata merupakan kelemahan yang dimiliki komputer berbasis sistem operasi Windows. Melalui SMB *exploit/metasploit* yang ada akan dengan mudah melakukan injeksi kedalam sistem Windows. Akibatnya adalah apabila aplikasi *exploit/metasploit* telah dijalankan maka dimungkinkan komputer berbasis windows dapat diambil alih dalam satu hari (*zero day*) (Yudha & Prayudi, 2013).

Menurut laporan hasil survei yang dilakukan oleh statista.com menuntjukan bahwa statistik dan fakta mengenai pembajakan yang dilakukan oleh beberapa *user* dengan memanfaatkan media *file sharing* secara ilegal atau tidak sah untuk mendapatkan beberapa konten yang ada di *internet* seperti *video*, musik, dan beberapa konten yang mengandung hak cipta. Pembajakan media seperti di Indonesia dan Mesir, dimana 16 persen konsumen mengaku melakukan pembajakan konten lebih dari sekali seminggu pada Februari 2017. Beberapa situs populer untuk bahan pembajakan meliputi 4shared.com dan rapidgator.net, dengan hampir 19 juta URL yang melanggar. Lebih dari setengah pengguna *internet* global berusia 16-24 telah mengakses musik melalui pelanggaran hak cipta, dengan melakukan "*ripping*" musik yang disukai untuk diunduh ke semua kelompok usia. Pembajakan lain juga terjadi dengan melakukan pengunduhan *ebook* secara ilegal, perkiraan menunjukkan bahwa ada 16,5 juta pengunduh buku ilegal di Amerika Serikat. Ada beberapa alasan bahwa mereka

dipaksa mengunduh buku elektronik ilegal karena buku pilihan mereka tidak tersedia dari penyedia *online*(Fuller, 2017).

Dengan kemajuan teknologi yang ada pada perangkat *smart router*, maka perangkat *smart router* pun banyak diterapkan di kalangan perumahan dan kantor kecil, namun perangkat jaringan jenis *smart router* nirkabel ini paling mudah diretas sehingga terlalu rentan menjadi obyek dari sebuah tindak kejahatan di dunia maya, seperti laporan yang ditulis oleh *Seth Rosenblatt* pada 17 April 2013 dengan judul "**Top Wi-Fi routers easy to hack, says study**", memaparkan sebuah riset yang dilakukan oleh perusahaan riset *Independent Security Evaluators of Baltimore*, menemukan bahwa setidaknya terdapat 13 dari router nirkabel jenis *smart wifi router* dapat diambil alih dari jaringan lokal oleh peretas melalui jaringan LAN dan WAN. Laporan tersebut mencatat bahwa semua perangkat memiliki kerentanan keamanan kritis yang dapat dieksploitasi oleh peretas dan dapat menyebabkan akses kontrol yang tidak sah (Rosenblatt, 2013). Hal seperti ini yang menjadikan tantangan untuk bidang forensik digital dalam menggali lebih dalam tentang mekanisme forensik pada router seiring semakin beragamnya jenis router yang berpotensi sebagai obyek atau barang bukti elektronik.

Dalam bidang forensika digital terdapat beberapa tahapan sebelum barang bukti dilaporkan atau disajikan dalam persidangan, seperti mengumpulkan barang bukti, pemeriksaan barang bukti, dan menganalisa barang bukti. Pada tahap pengumpulan barang bukti terdapat dua metode yang sering digunakan yaitu metode *dead forensic* dan metode *live forensic*, dimana dari dua metode tersebut memiliki perbedaan dalam penanganan barang bukti. Metode *dead forensic* atau bisa disebut dengan *traditional forensic* adalah metode yang digunakan pada bukti elektronik yang telah dimatikan, dan merupakan metode yang sederhana. Lain halnya dengan metode *live forensic*, dimana metode ini digunakan untuk mengumpulkan data pada bukti elektronik yang masih dalam kondisi/keadaan menyala. Hal ini dikarenakan informasi barang bukti hanya bisa didapatkan pada saat sistem berjalan dan informasi tersebut bisa rusak atau mengalami perubahan bahkan dapat hilang jika sistem dimatikan. *Live forensic* juga dapat dijadikan sebagai metode alternatif pada proses *traditional forensic* (Jones, 2007; Lessing & Solms, 2008).

*Smart Router* merupakan salah satu jenis perangkat router yang memiliki fitur *file sharing* dengan SMB sebagai protokolnya, *smart router* juga termasuk salah satu perangkat jaringan yang membutuhkan sistem dalam keadaan menyala (*running*) pada saat dilakukan proses investigasi dan bisa disebut sebagai sistem kritis. Penanganan investigasi forensik pada sistem kritis harus hati – hati karena memiliki karakteristik sistem yang tidak

diperkenankan mati (*shutdown*). Untuk mendapatkan objek – objek digital pada protokol SMB diperlukan proses investigasi dan uji forensik yang tepat. Proses investigasi forensik secara umum, langkah – langkah yang digunakan pada proses investigasi hanya terbatas untuk melakukan investigasi pada satu jenis barang bukti saja, sedangkan pada investigasi protokol SMB diperlukan beberapa jenis barang bukti yaitu media penyimpanan, *network traffic*, dan *log file* (Yudha, 2013).

Melihat adanya potensi kejahatan yang melibatkan protokol *file sharing* terutama pada protokol SMB, maka perlu dilakukannya proses investigasi forensik yang dapat membantu dalam memecahkan kasus – kasus kejahatan digital terutama dalam proses berbagi data atau *file sharing* untuk mendapatkan barang bukti apa saja yang dapat diperoleh dari *file sharing*. Hasil dari penelitian ini dapat dijadikan sebagai bagian dari upaya untuk mendukung pengungkapan kasus – kasus *cybercrime* berbasiskan pada *file sharing*.

## 1.2 Permasalahan

Berdasarkan latar belakang yang telah dipaparkan terdapat beberapa permasalahan – permasalahan yang terjadi diantaranya: meningkatnya kebutuhan akan media penyimpanan yang dapat diakses secara bersama memungkinkan terjadinya tindak kejahatan dalam berbagi file ilegal, maka diperlukannya suatu tindakan seperti menganalisis atau memforensik kejadian tersebut; belum dilakukannya proses investigasi dengan menggunakan metode *live forensics* dan *live acquisition* untuk protokol SMB pada sistem yang sedang berjalan supaya barang bukti seperti *file log* tidak hilang; semakin banyak beredarnya perangkat *wireless access point portable* yang dapat difungsikan sebagai media *file sharing* tidak menutup kemungkinan tindakan kejahatan dengan memanfaatkan perangkat tersebut, maka perlu adanya suatu kerangka investigasi forensik pada perangkat peladen (*server*) portabel, seperti pada perangkat router cerdas (*Smart Router*). Maka ranah dalam penelitian ini fokus pada metode yang digunakan untuk mengidentifikasi dan mendeteksi serta menggali informasi dan melakukan analisis terhadap bukti digital pada perangkat router cerdas (*Smart Router*) yang dalam hal ini berlaku sebagai mesin peladen (*server*) portabel terkait penggunaan atau pemanfaatan *file sharing*, serta bagaimana cara memperoleh data yang dapat dijadikan sebagai informasi pelengkap pada proses investigasi.

## 1.3 Rumusan Masalah

Berdasarkan permasalahan yang telah dipaparkan sebelumnya maka rumusan masalah pada penelitian ini yaitu:

1. Bukti digital apa saja yang dapat diperoleh dari *file sharing* pada *Smart Router*?
2. Bagaimana mekanisme *live forensics aquisition* untuk mendapatkan Bukti Digital dari aktivitas ilegal *file sharing*?
3. Bagaimana proses investigasi yang efektif untuk kasus – kasus kejahatan *file sharing* pada perangkat *Smart Router*?

## 1.4 Batasan Masalah

Untuk lebih fokus dan terarahnya penelitian yang dilakukan dan berdasarkan rumusan masalah yang telah dipaparkan sebelumnya maka diberikan batasan dalam penelitian ini yaitu:

1. Penelitian hanya berlingkup pada perangkat router yang memiliki layanan *file sharing*, perangkat yang digunakan adalah *Smart Router* GL-inet AR300 dengan Sistem Operasi OpenWrt dan *Smart Router* MikroTik RB951Ui-2HnD dengan Sistem Operasi RouterOS.
2. Kegiatan akuisisi data bersifat *live forensics aquisition* (dilakukan pada saat perangkat dalam kondisi menyala) berdasarkan SNI ISO/IEC 27037:2014.
3. Penelitian berlingkup pada jaringan yang menggunakan *Smart Router* (*Router Home*) yang sering dipakai di perumahan (kalangan rumah tangga).
4. Area penelitian akan terbatas pada penyelidikan keberadaan perangkat tertentu dalam jaringan lokal atau LAN yang dikendalikan oleh satu router cerdas (*Smart Router*).

## 1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diajukan, maka dapat ditujukan tujuan dari penelitian ini.

Adapun tujuan yang ingin dicapai pada penelitian ini yaitu:

1. Menggali informasi yang bisa digunakan sebagai bukti digital pada perangkat *Smart Router* menggunakan *live forensics.*
2. Melakukan akuisisi data pada perangkat *Smart Router* menggunakan *live acquisition* untuk mendapatkan data yang memungkinkan untuk digunakan sebagai barang bukti digital.

3. Mensimulasikan proses investigasi yang efektif yang dapat dipergunakan dalam proses investigasi *file sharing* pada perangkat *Smart Router* untuk keperluan forensik.

## 1.6 Manfaat Penelitian

Berdasarkan latar belakang, rumusan masalah, batasan masalah dan tujuan dari penelitian yang telah disampaikan pada bagian sebelumnya, adapun manfaat yang ingin dicapai dalam penelitian ini yaitu:

1. Untuk Pengembangan Ilmu pengetahuan.
   - Memberikan panduan dalam proses investigasi forensik pada jaringan yang menggunakan perangkat *Smart Router*.
   - Sebagai pendalaman materi dalam bidang Komputer Forensik terutama pada sub bidang Router Forensik.
2. Untuk Peneliti lain.

   Sebagai referensi bagi peneliti lain yang mengambil kajian terkait dengan bidang Router Forensik, atau dapat digunakan untuk memperkaya wawasan dalam pengembangan penelitian selanjutnya.
3. Untuk Penulis

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

## 1.7 *Review* Penelitian

Pada bagian ini akan dibahas ulasan tentang penelitian yang telah dilakukan sebelumnya yang relevan dan berkaitan dengan penelitian yang akan dilakukan.

Jurnal penelitian yang berjudul Rancang Bangun Sistem *Hotspot Portable* dengan OpenWrt. Jurnal ini disusun oleh L. Budi Handoko dan Oki Setiono, yang dipublikasikan pada Jurnal Ilmiah SISFOTENIKA. Dalam penelitian ini mengungkapkan bahwa perangkat router yang ada masih memiliki kekurangan dan belum optimal dikarenakan antara router belum memiliki keseragaman fasilitas dan tidak standar. Oleh karena itu, perlu dibangun sistem baru yang memiliki fitur dan dapat mengoptimalkan fungsi router yang beredar sehingga dapat diterapkan pada router lain secara *portable*. Dengan memasang sistem operasi OpenWrt pada perangkat router *wireless* dan ditambahkannya beberapa alat tambahan untuk mendukung fungsionalitasnya seperti *flashdrive*, modem *gsm*, *usb soundcard* dan *speaker*. Sehingga sistem yang dihasilkan memiliki fitur dan layanan yang sama antara router satu

dengan yang lain, diantaranya dapat memberikan layanan *captive portal*, sistem juga mampu memberikan fasilitas *chatting*, *audio* dan *video player*, sebagai penyimpanan lokal, mesin *download* dan *voucher* akses internet untuk *login captive portal*, dimana sistem ini dapat diterapkan pada perangkat lain dan digunakan secara *portable*. Berangkat dari hal tersebut dapat disimpulkan bahwa pemakaian sistem operasi OpenWrt dapat diterapkan pada beberapa perangkat router yang memiliki perbedaan standar, serta dapat mengoptimalkan router yang beredar di pasaran dan dapat dimanfaatkan sebagai *hotspot portable*. Dengan membangun suatu sistem *hotspot* berbasis OpenWrt dengan alasan bahwa jaringan komputer sangat berperan penting untuk memenuhi kebutuhan masyarakat, terbukti dapat mempermudah pemakai untuk saling berkomunikasi dan memperoleh informasi yang dibutuhkan seperti saling berkirim pesan, mengirim dan mengambil *file*, dan salah satu perangkat jaringan komputer tersebut adalah router(Handoko & Setiono, 2016).

Jurnal penelitian yang berjudul Penerapan *Network Attached Storage* Menggunakan OpenWrt Studi Kasus: Bagian Kemahasiswaan STIKOM Bali. Jurnal ini disusun oleh I Komang Dharmendra dan Luh Putu Ayu Desiani, yang dipublikasikan pada Konferensi Nasional Sistem & Informatika 2015. Dalam penelitian mengungkapkan bahwa penerapan NAS dalam berbagi *file* pada jaringan dengan menggunakan perangkat *access point router* yang ter-*install* sistem operasi OpenWrt dan aplikasi Samba dapat dijadikan sebagai *file server* dengan penyimpanan data yang terpusat. Dengan sistem operari OpenWrt dan aplikasi Samba dapat memudahkan dalam menyimpan data dan lebih mudah diakses(Dharmendra, Putu, & Desiani, 2015). Penelitian sejenis tentang manfaat dari NAS dilakukan oleh Nathwani Namrata pada publikasi *International Journal of Computer Engineering and Technology* (IJCET) dengan judul *Network Attached Storage Different From Traditional File Servers & Implementation Of Windows Based NAS*. Dengan melakukan pengujian pembandingan NAS dengan *Traditional File Server* yang diimplementasikan pada Windows. Pendekatan ini (NAS) memungkinkan dalam sebuah rumah atau perusahaan dapat menyimpan dan mengambil serta berbagi data dalam jumlah yang besar yang lebih terjangkau. Dengan menggunakan NAS dapat mempermudah pengelolaan penyimpanan dan meningkatkan keandalan, kinerja dan efisien jaringan (Namrata, 2013).

Jurnal penelitian yang berjudul Teknik Eksplorasi Bukti Digital Pada *File Sharing* Protokol SMB Untuk Mendukung Forensika Digital Pada Jaringan Komputer. Jurnal ini disusun oleh Fietyata Yudha dan Yudi Prayudi, yang dipublikasikan pada Konferensi Nasional Informatika. Dalam penelitian ini bahwa protokol SMB merupakan protokol *file*

*sharing* yang digunakan dalam berbagi file pada sebuah jaringan komputer, dan pada kenyataannya banyak tindak kejahatan yang melibatkan protokol *file sharing* terutama pada protokol SMB, maka dari itu diperlukan suatu proses investigasi yang sesuai untuk protokol SMB, supaya dapat diidentifikasi karakteristik objek-objek digital pada *file sharing* serta pengujian terhadap metode yang digunakan untuk mendapatkan barang bukti digital pada *file sharing*. Penelitian yang dilakukan terbatas pada *platform* sistem operasi Windows dan Linux, barang bukti digital yang diambil merupakan barang bukti digital yang berasal dari hasil *capture* jaringan yang menjalankan fasilitas *file sharing* dengan protokol SMB, *log file server*, dan *hardisk server*. Keterbatasan pada penelitian ini bahwa proses investigasi hanya dilakukan pada perangkat dalam kondisi mati (*off*) sehingga perlu dilakukannya penelitian lanjut bagaimana proses investigasi pada perangkat dalam keadaan masih hidup (*on*) (Yudha & Prayudi, 2013).

Jurnal penelitian yang berjudul *Live Forensics on RouterOS using API Services to Investigate Network Attacks*. Jurnal ini disusun oleh Muhammad Itqan Mazdadi, Imam Riadi, dan Ahmad Luthfi, yang dipublikasikan pada *International Journal of Computer Science and Information Security* (IJCSIS). Dalam penelitian mengungkapkan bahwa perangkat router sangat vital terhadap ancaman serangan karena menjadi pondasi utama dalam mengatur lalu lintas komunikasi pada suatu jaringan. Oleh karena itu, dalam bidang forensik hal ini menjadi perhatian khusus dibidang forensik jaringan terkait dengan analisa dari *log* lalu lintas ketika terjadi aktivitas serangan pada perangkat router. Pada perangkat Router berbasis RouterOS, terdapat suatu media *Application Proggraming Interface* (API) *services* yang dapat dimanfaatkan untuk menggali informasi dari perangkat Router. Berangkat dari hal tersebut, maka untuk mendapatkan bukti digital yang terdapat pada mikrotik RouterOS dapat memanfaatkan API (*Aplication Programing Interface*) sebagai media akuisisi dalam implementasi forensik jaringan dengan menggunakan metode *live forensics*. Hasil yang didapat pada penelitian ini bahwa bukti digital pada RouterOS memiliki karakteristik yaitu bersifat *volatile* atau mudah hilang jika router mengalami *reboot* ataupun dimatikan. Informasi terkait *log activity* tersimpan sementara pada *memory* sehingga mengharuskan proses akuisis data pada RouterOS dilakukan dengan metode *Live Forensics*(Mazdadi, Riyadi, & Luthfi, 2017).

Jurnal penelitian yang berjudul Analisis *Live Forensics* untuk Perbandingan Aplikasi *Instant Messenger* Pada Sistem Operasi Windows 10. Jurnal ini disusun oleh Tayomi Dwi Larasati dan Bekti Cahyo Hidayanto, yang dipublikasikan pada Seminar Nasional Sistem Informasi Indonesia (SESINDO), 6 November 2017. Bahwa metode *live forensics* juga

digunakan untuk menganalisis aplikasi *Instant Messenger* yang ter-*instal* 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 waktu yang lama, dikarenakan apabila RAM mati maka tidak dapat dilakukan *dumping* dan analisa barang bukti. Maka dari itu untuk pelaksanaan *live forensics* dibutuhkan metode baku agar dapat menjamin validitas dan integritas serta kelengkapan data yang dibutuhkan (Larasati & Hidayanto, 2017). Penelitian sejenis dalam menggunakan teknik akuisisi secara langsung juga dilakukan oleh Soni, Yudi Prayudi, dan Bambang Sugiantoro pada publikasi Teknomatika dengan judul Teknik Akuisisi *Virtualisasi Server* menggunakan Metode *Live Forensic*. Dalam penelitian dibahas mengenai *virtualisasi server* yang dapat mengundang celah kejahatan, sehingga memunculkan tantangan untuk menemukan petunjuk dan bukti digital dalam mengungkap kasus kejahatan yang terjadi. Dikarenakan hal ini akan menyulitkan para penyidik untuk melakukan akuisisi terhadap salah satu sistem operasi yang ter-*install* di dalam *server* tersebut tanpa mengganggu dan tanpa mematikan komputer mengingat betapa pentingnya *server* tersebut. Selama ini teknik akuisisi umumnya digunakan secara tunggal dimana hanya memuat satu sistem operasi. Oleh karena itu, diperlukan teknik untuk mengakuisisi virtualisasi *server* dengan menggunakan metode *live forensics* tanpa mengganggu atau mematikan sistem operasi lainnya yang sedang berjalan.Teknik Akuisisi yang dilakukan dengan mengakuisisi salah satu sistem operasi melalui *server* proxmox, untuk mendapatkan bukti digital pada *server* proxmox(Soni, Prayudi, & Sugiantoro, 2017).

Jurnal penelitian yang berjudul Investigasi *Live* Forensik dari Sisi Pengguna untuk Menganalisa Serangan *Man In The Middle Attack* berbasis *Evil Twin*. Jurnal ini disusun oleh Muhammad Sabri Ahmad, Imam Riadi, dan Yudi Prayudi, yang dipublikasikan pada ILKOM Jurnal Ilmiah Volume 9 Nomor 1 April 2017. Bahwa MITM *based Evil Twin* menjadi suatu ancaman yang berbahaya bagi para pengguna jaringan WiFi, karena penyerangan ini memanfaatkan *Access Point* (AP) palsu dengan konfigurasi *gateway* yang berbeda dengan *legitimate* AP, sehingga jenis serangan ini menjadi cukup sulit untuk dideteksi. Oleh karena itu, perlu dilakukan teknik forensik menggunakan metode *live forensics* dengan pendekatan dari sisi user untuk mendeteksi aktivitas ilegal yang terjadi di dalam jaringan WiFi mengenai kasus *MITM Based Evil Twin Attack* yang dapat membantu dalam menemukan beberapa petunjuk ataupun temuan – temuan yang dapat dijadikan

informasi yaitu berupa *IP address*, *MAC address* pelaku dan beberapa file yang mencurigakan seperti *file* html, css, jpg dan png, dengan empat tahapan, yaitu *collection*, *examination*, *analysis* dan *reporting*. Peneliti juga menyimpulkan bahwa barang bukti digital dari serangan *Evil Twin AP* dapat diketahui dengan cara menganalisa atribut-atribut dari *Acess Point* tersebut, ada beberapa informasi yang dapat dijadikan sebagai perbandingan yaitu *SSID*, *Mac Kode Vendor*, kekuatan Sinyal, *Authentication*, *Frequency* dan *Channel*. Proses dalam tahapan analisa dan pengumpulan barang bukti dilakukan dengan menerapkan metode *Live Forensics*, hal ini dikarenakan pengumpulan barang bukti dilakukan dalam sistem yang sedang berjalan, selain itu pendekatan *user side* cukup efektif dalam proses pengidentifikasian aktivitas serangan *Evil Twin Based MITM* (Ahmad, Riadi, & Prayudi, 2017). Penggunaan teknik *live forensics* juga dilakukan oleh Aan Kurniawan dan Yudi Prayudi pada publikasi *Hacking And Digital Forensics Expose* (H@DFEX 2014) dengan judul Teknik *Live Forensics* pada Aktivitas *Zeus Malware* untuk mendukung Investigasi *Malware Forensics*. Penggunaan teknik *Live Forensics* pada aktivitas *Zeus Malware* untuk mendukung investigasi *malware forensics*, penelitian yang dilakukan bertujuan untuk mengidentifikasikan karakteristik dan bukti digital dari sebuah aktivitas *zeus malware* dengan menggunakan teknik *live forensics*, hal ini terkait dengan analisa bahwa *zeus malware* melakukan serangan melalui jaringan komputer dan aktivitasnya berjalan ketika sistem dalam keadaaan menyala, maka teknik *live forensics* diperlukan sebagai solusi untuk medapatkan bukti digital dari sebuah aktivitas *zeus malware* yang berupa *image memory* dari sebuah sistem, yang menghasilkan data artefak berupa karakteristik dari aktivitas *zeus malware* (Aan Kurniawan & Prayudi, 2014).

Jurnal penelitian yang berjudul Instrumen Evaluasi *Framework* Investigasi Forensika Digital Menggunakan SNI 27037:2014. Jurnal ini disusun oleh Didik Sudyana, Bambang Sugiantoro, dan Ahmad Luthfi, yang dipublikasikan pada JISKa, Vol. 1, No. 2, September, 2016, Pp. 75 – 83. Bahwa hal penting yang harus diperhatikan oleh setiap petugas investigator forensika digital dalam menjalankan aktivitas forensika digital adalah diikutinya setiap tahapan dan prosedur dalam forensika digital. Tahapan tersebut dikenal dengan istilah *frameworks* ataupun SOP investigasi. Tahapan dalam proses forensika digital harus sesuai dengan aturan hukum dan juga mekanisme yang tepat, berdasarkan hasil identifikasi terhadap dokumen SNI ISO/IEC 27037:2014, didapatkan bahwa terdapat 38 proses penting yang diatur oleh SNI ISO/IEC 27037:2014 dalam melakukan investigasi forensika digital. Dari hasil identifikasi tersebut maka dapat dihasilkan sebuah instrument yang dapat berguna bagi penyidik ataupun praktisi forensika digital untuk melakukan penyesuaian atau

pengecekkan terhadap SOP/*framework* investigasinya sehingga proses investigasi yang dilakukan telah mengikuti standar yang berlaku (Sudyana, Sugiantoro, & Luthfi, 2016). Penelitian sejenis terkait pemakaian SNI ISO/IEC 27037:2014 juga dilakukan oleh Dedy Hariyadi, Wing Wahyu Winarno, dan Ahmad Luthfi, pada publikasi TEKNOMATIKA Vol. 9, No. 1, Juli 2016 dengan judul Analisis Konten Dugaan Tindak Kejahatan Dengan Barang Bukti Digital Blackberry Messenger. Dalam penelitian ini menggunakan SOP SNI ISO/IEC 27037:2014 yang mengatur prosedur akuisisi barang bukti elektronik dan barang bukti digital khusus untuk perangkat dalam kondisi menyala, dimana pada SNI ISO/IEC 27037:2014 telah mengaturnya pada bagian 7.1.2.1.1. Peneliti merancang aplikasi *logical forensics* berlisensi MIT yang dikembangkan menggunakan IGN- SDK dengan fungsi utama untuk melakukan analisis percakapan Blackberry Messenger yang berjalan di ponsel bersistem operasi Android yang diberi nama BBMPork, aplikasi tersebut dirancang menyesuaikan dengan SNI ISO/IEC 27037:2014 (Hariyadi, Winarno, & Luthfi, 2016).

Jurnal penelitian yang berjudul Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI ISO/IEC 27037:2014. Jurnal ini disusun oleh Dedy Hariyadi dan Abdul Rohman Supriyono, yang dipublikasikan pada TELEMATIKA, Vol. 14, No. 01, BULAN, TAHUN, Pp. 62 – 67. Penelitian ini membahas tentang membangun kerangka investigasi forensik *file-sharing* samba pada mesin peladen berdasarkan SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital. 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 SNI 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 *portable* 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* (Hariyadi & Supriyono, 2017).

Rangkuman dari *literature review* terhadap penelitian – penelitian yang telah dipaparkan secara singkat dapat dilihat pada Tabel 1.1 dimana akan menunjukkan perbandingan dari beberapa penelitian sebelumnya.

Tabel 1.1 Literature *Review* Terhadap Penelitian Sebelumnya

| **Paper Utama** | **Perangkat *Portable* sebagai media *File Sharing* dengan Sistem Operasi OpenWrt atau RouterOS** | ***Live Forensics*** | ***File Sharing* dengan Protokol SMB (*Server Message Block*)** | **SNI ISO/IEC 27037:2014** |
|---|---|---|---|---|
| (Handoko & Setiono, 2016) | Pemanfaatan router *wireless portable* sebagai sistem *Hotspot Portable* dan media *file sharing* dengan Sistem Operasi OpenWrt | --- | --- | --- |
| (Dharmendra et al., 2015) | Penerapan NAS dalam berbagi *file* pada jaringan dengan menggunakan perangkat *router access point* yang ter-*install* sistem operasi OpenWRT | --- | Memanfaatkan aplikasi Samba sebagai *server file sharing* pada NAS | --- |
| (Yudha & Prayudi, 2013) | --- | --- | Teknik Eksplorasi Bukti Digital Pada *File Sharing* Protokol SMB Untuk Mendukung Forensika Digital Pada Jaringan Komputer | --- |
| (Mazdadi et al., 2017) | --- | Melakukan proses akuisisi *log* pada RouterOS menggunakan metode *Live Forensics* | --- | --- |
| (Larasati & Hidayanto, 2017) | --- | Menerapkan dan pengimplementasian teknik *live forensics* untuk mendapatkan bukti digital dari aktivitas penggunaan | --- | --- |

| Paper Utama | Perangkat *Portable* sebagai media *File Sharing* dengan Sistem Operasi OpenWrt atau RouterOS | *Live Forensics* | *File Sharing* dengan Protokol SMB (*Server Message Block*) | SNI ISO/IEC 27037:2014 |
|---|---|---|---|---|
| | | aplikasi *Instant Messenger* pada sistem operasi windows 10 | | |
| (Soni et al., 2017) | --- | Mengakuisisi virtualisasi *server* dengan menggunakan metode *live forensics* tanpa mengganggu atau mematikan sistem operasi lainnya yang sedang berjalan | --- | --- |
| (Ahmad et al., 2017) | --- | Investigasi *Live Forensics* dari sisi pengguna untuk menganalisa serangan *Man In the Middle Attack* | --- | --- |
| (Aan Kurniawan & Prayudi, 2014) | --- | Penggunaan teknik *Live Forensics* pada aktivitas *Zeus Malware* untuk mendukung dalam investigasi *Malware Forensics* | --- | --- |
| (Sudyana et al., 2016) | --- | --- | --- | Instrumen evaluasi *framework* investigasi forensika digital menggunakan SNI ISO/IEC 27037:2014 |
| (Hariyadi et al., 2016) | --- | Teknik Akuisisi pada perangkat dalam kondisi | --- | Merancang aplikasi untuk mengakuisisi barang bukti digital |

| **Paper Utama** | **Perangkat *Portable* sebagai media *File Sharing* dengan Sistem Operasi OpenWrt atau RouterOS** | ***Live Forensics*** | ***File Sharing* dengan Protokol SMB (*Server Message Block*)** | **SNI ISO/IEC 27037:2014** |
|---|---|---|---|---|
| | | menyala dengan *Live Forensics* sesuai dengan SNI 27037:2014 Bagian7.1.2.1 | | pada Blackberry Messenger sesuai dengan SNI ISO/IEC 27037:2014 |
| (Hariyadi & Supriyono, 2017) | --- | --- | Server Samba sebagai objek dalam pembuatan kerangka investigasi pada *file sharing* | Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI ISO/IEC 27037:2014 |
| **Usulan Penelitian** | | | | |
| **Solusi yang diusulkan** | Perangkat elektronik *portable* yang memiliki fitur layanan sebagai *server file-sharing* seperti *smart* router | Dalam melakukan proses akuisisi data menggunakan metode *live forensics* | Melakukan eksplorasi bukti digital pada *file-sharing* dengan protokol SMB dan Samba sebagai aplikasi *file server* | Berdasarkan dari Standar Nasional Indonesia tentang Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital (SNI ISO/IEC 27037:2014) |
| **Usulan Penelitian** | Analisis Forensik pada perangkat *router access point portable* yang dapat dijadikan sebagai *server file-sharing*, yaitu dengan akuisisi secara langsung (*live forensics acquisition*) berdasarkan Standar Nasional Indonesia tentang Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital (SNI ISO/IEC 27037:2014). Dalam mendapatkan bukti digital dari aktivitas *file sharing* yang dapat dijadikan sebagai informasi pelengkap pada proses investigasi.<br>Akuisisi secara langsung (*live forensics*) pada perangkat yang sedang berjalan atau dalam kondisi hidup sangat dibutuhkan supaya barang bukti seperti *file log* tidak hilang dikarenakan adanya proses *wiping* pada saat proses *shutdown*.<br>Perangkat *smart* router *portable* yang menjadi bahan penelitian, yaitu perangkat router dengan sistem operasi OpenWrt dan MikroTik RouterOS. | | | |

## 1.8 Metodologi Penelitian

Adapun bagan dari langkah-langkah yang akan ditempuh selama melakukan penelitian ini yaitu sebagai berikut:




Gambar 1.3 Alur Metodologi Penelitian

1) Studi Pustaka

Penelitian ini dilakukan dengan melakukan studi kepustakaan yaitu dengan mengumpulkan bahan-bahan referensi yang terkait dengan penelitian, baik melalui buku, artikel, paper, jurnal, makalah, dan mengunjungi beberapa situs yang terdapat pada internet terkait dengan *Forensic Science*, *Digital Forensic*, *Network Forensic*, *Router*, *Smart Router*, *Router Forensic*, Referensi Model OSI (*Open System Interconnection*), Klasifikasi Barang Bukti Digital, Proses Investigasi, *Live Forensics*, *File Log*, *SAMBA*, Hak Cipta., serta beberapa referensi lain yang dapat menunjang kegiatan penelitian yang dilakukan.

2) Persiapan Alat dan Bahan Penelitian

Tahapan ini melakukan persiapan *tools* yang dipakai dalam melakukan *Live Forensics*. Sehingga dapat memahami bagaimana proses pencarian barang bukti digital pada kasus kejahatan yang berkaitan dengan *file sharing* serta *tools-tools* yang digunakan untuk kepentingan investigasi.

3) Persiapan Skenario

Tahapan ini melakukan pembuat skenario yang nantinya diterapkan dengan mensimulasikan berdasarkan kasus yang telah dibuat terkait adanya aktivitas ilegal yang melibatkan perangkat *smart router* sebagai media *file sharing*.

4) Simulasi Kasus

Simulasi digunakan untuk melakukan pengujian terhadap standar yang sudah dibuat, sehingga proses investigasi yang dibuat merupakan SOP yang efektif untuk melakukan investigasi pada kasus yang berkaitan dengan *file sharing*.

5) Investigasi Dan Olah TKP

Tahap Investigasi Dan Olah TKP pada penelitian ini dilakukan secara *live forensics acquisition* pada *Smart Router* dilakukan pada saat perangkat dalam kondisi menyala berdasarkan SNI ISO/IEC 27037:2014.

6) Analisis Forensik

Tahapan ini bertujuan untuk mengetahui keberhasilan dalam penarikan data dan informasi dari *Smart Router* kemudian dilakukan analisis forensik.

7) Laporan

Tahapan ini melakukan pembuatan laporan atas hasil yang telah diperoleh pada tahap analisis.

## 1.9 Sistematika Penulisan

Tahapan ini adalah tahapan yang memberikan gambaran secara umum terkait dengan sistematika penulisan, dengan tujuan memberikan penjelasan secara ringkas terhadap kerangka dalam penulisan.

BAB I: PENDAHULUAN

Tahapan ini adalah tahapan awal yang dilakukan dalam penelitian tahapan ini berisikan penjelasan terkait dengan latar belakang penelitian, penetapan judul, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, serta sistematika penulisan yang dilakukan.

BAB II: TINJAUAN PUSTAKA

Pada tahapan ini membahas tentang beberapa teori yang mendukung dalam penelitian yang dilakukan, terkait dengan *Forensics Science*; *Digital Forensics; Network Forensics;* Router, *Smart* Router; Referensi Model OSI (*Open System Interconnection*); Klasifikasi Barang Bukti Digital; Proses Investigasi; *Live Forensics*; *File Log;* Samba*;* Hak Cipta.

BAB III: METODOLOGI PENELITIAN

Tahapan ini berisikan gambaran secara umum tentang analisa yang dilakukan terhadap proses dan mekanisme forensik pada router forensik, serta melakukan implementasi terhadap akuisisi data pada *Smart* Router.

BAB IV: HASIL DAN PEMBAHASAN

Tahapan ini membahas tentang implementasi dari simulasi kasus, *live acquisition.* Pada tahapan ini yaitu melakukan pembahasan dari hasil yang telah diperoleh terkait penelitian yang dilakukan serta penyampaian kesimpulan secara teknis dari hasil yang telah dikerjakan.

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 di kemudian hari.

DAFTAR PUSTAKA

Daftar Pustaka berisi referensi yang terkait dengan penelitian, baik melalui buku, artikel, paper, jurnal, makalah, situs yang terkait yang dapat menunjang kegiatan penelitian yang dilakukan.

# BAB 2
# Tinjauan Pustaka

## 2.1 *Forensics Science*

Forensik adalah penerapan ilmu pengetahuan untuk memecahkan masalah secara hukum. Dalam forensik, hukum dan ilmu selamanya akan terintegrasi, dimana bukti ilmiah terbaik di dunia tidak ada gunanya jika itu tidak dapat diterima di pengadilan hukum(Sammons, 2012). Secara umum *Forensic Science* adalah pengumpulan, analisis, dan penyajian bukti elektronik untuk digunakan dalam masalah hukum dengan proses yang telah umum dilakukan, seperti alat – alat yang digunakan, dan teknik untuk analisa bukti.

## 2.2 *Digital Forensics*

Terdapat banyak cara untuk mendefinisikan digital forensics seperti yang diungkapkan oleh Zatyko, bahwa digital forensics merupakan "*The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation*"(Zatyko, 2007). Dari definisi tersebut dapat disimpulkan bahwa digital *forensics* merupakan penerapan dari ilmu komputer dan prosedur investigasi untuk tujuan hukum yang melibatkan analisis bukti digital setelah otoritas pencarian yang tepat, *chain of custody*, validasi dengan matematika, penggunaan alat-alat yang telah divalidasi, pengulangan, pelaporan, dan kemungkinan presentasi dari ahli. Dimana digital forensik meliputi lebih dari sekedar laptop dan komputer desktop, perangkat mobile, jaringan, dan "awan", juga mencakup analisis gambar, *video*, dan *audio* (dalam format analog dan digital). Fokus dari analisis ini umumnya keaslian, perbandingan, dan peningkatan. Secara khusus, *digital forensics* adalah aplikasi teknologi komputer untuk masalah hukum dimana bukti mencakup item – item yang berhubungan dengan objek atau barang yang bersifat digital yang merupakan hasil interaksi seseorang atau pelaku(Daniel & Daniel, 2012).

Dalam ilmu *digital forensics* terdapat beberapa prinsip – prinsip dasar. Adapun prinsip dasar *digital forensics* menurut Badan Standarisasi Nasional, tahun 2014 yang tertuang di dalam SNI ISO/IEC 27037:2014 (Badan Standarisasi Nasional, 2014)antara lain:

1. *Scope*: Berisi penjelasan tentang apa yang tercakup atau diatur dalam SNI 27037:2014. Pada bagian ini dijelaskan bahwa SNI merupakan panduan yang secara spesifik mengatur tentang aktivitas penanganan barang bukti digital.
2. *Normative Reference*: Pada bagian ini berisi tentang dokumen referensi yang digunakan untuk mengembangkan SNI ini. Ada 4 ISO atau standar internasional yang dijadikan dokumen referensi yaitu ISO/TR 15801, ISO/IEC 17020, ISO/IEC 17025:2005, dan ISO/IEC 27000.
3. *Terms and definitions*: Pada bagian ini berisi tentang istilah-istilah yang digunakan dan penjelasan dari istilah tersebut.
4. *Abbreviated Terms*: Pada bagian ini berisi tentang singkatan-singkatan yang digunakan. Sebagai contoh AVI yang merupakan singkatan dari *Audio Video Interleave*.
5. *Overview*: Pada bagian ini berisi tentang *overview* tentang penjelasan kegiatan penanganan barang bukti digital. *Overview* terdiri dari 4 bagian yaitu 1) konteks pengumpulan barang bukti, 2) prinsip barang bukti digital, 3) syarat-syarat penanganan barang bukti, dan 4) proses penanganan barang bukti digital.
6. *Key Components of identification, collection, acquisition, and preservation of digital evidence*: Pada bagian ini berisi penjelasan tentang kegiatan penting yang dilakukan dalam identifikasi, pengumpulan, akuisisi, dan preservasi. Bagian ini terdiri dari 9 pembahasan yaitu 1) *chain of custody*, 2) tindakan di tempat kejadian perkara, 3) peran dan tanggung jawab petugas, 4) kompetensi yang harus dimiliki petugas, 5) Hal yang harus dilakukan sewajarnya, 6) Dokumentasi, 7) *Briefing*, 8) Prioritas pengumpulan dan akuisisi, 9) Preservasi barang bukti digital yang berpotensi.
7. *Instance of identification, collection, acquisition, and preservation:* Bagian ini berisi tentang hal – hal atau kegiatan apa saja yang dilakukan dalam identifikasi, pengumpulan, akuisisi, dan preservasi.

## 2.3 *Network Forensics*

Istilah *network forensics* memang diambil dari terminologi yang berhubungan dengan kriminologi. *Network forensics* merupakan kegiatan untuk melakukan pencarian data yang berhubungan dengan kejahatan di lingkungan jaringan komputer. Kegiatan *network forensics* paling sering dilakukan ketika kegiatan kejahatan pada jaringan komputer telah terjadi. Namun demikian, kegiatan analisis *network forensics* juga dapat dilakukan untuk menangkal atau mendeteksi kegiatan yang mungkin akan terjadi pada jaringan komputer.

*Network forensics* bukanlah sebuah produk, namun proses yang cukup kompleks dimana kita dapat mengumpulkan data dan menganalisisnya, dan kemudian melakukan investigasi sesuai dengan kebutuhan. Ilmu *network forensics* sebenarnya adalah cabang ilmu baru yang merupakan bagian dari digital *forensics*, dan *network forensics* berfokus pada analisis dan investigasi data yang berasal dari paket jaringan (Agus Kurniawan, 2012).

Dalam mengidentifikasi komponen jaringan, perlu memahami bagaimana sistem forensik bekerja pada jaringan, menurut Linda Volonino dan Reynaldo Anzaldua dalam bukunya ***Computer Forensics For Dummies***, memaparkan beberapa perangkat keras jaringan yang telah distandarkan dan dapat dijadikan sebagai barang bukti meliputi (Volonino & Anzaldua, 2008):

1. Router

Router merupakan komputer dengan tujuan khusus yang memindahkan data ke jaringan dan memberikan informasi jalur kepada paket data serta jalur mana yang harus dilalui, Router menggunakan alamat IP untuk memindahkan data dan bekerja pada *layer* 3 (*Network Layer*) pada lapisan Model OSI. Perangkat router pada umumnya memiliki prosesor dan penyimpanan. Data yang dapat diambil dari perangkat router antara lain informasi *routing table*, informasi *log*, informasi jaringan yang terkoneksi ke router.

2. Switch

Komponen jaringan yang digunakan untuk menghubungkan *host – host* yang ada pada jaringan. Dalam lapisan Model OSI Switch bekerja pada *layer* 2 (*Datalink Layer*) dan menyimpan daftar *port* beserta identifikasi *MAC address host* pada jaringan dalam tabel *MAC Address*. Daftar ini digunakan oleh switch sebagai panduan dalam mengirimkan paket data, Informasi yang didapatkan adalah daftar *MAC address* yang pernah terkoneksi dengan switch pada jaringan tersebut.

3. Hub

Hub merupakan perangkat jaringan yang bekerja *layer* 1 (*Physical Layer*) pada model OSI. Hub tidak mengenal *MAC addressing/physical addressing*, sehingga tidak bisa memilah data yang harus ditransmisikan, sehingga *collision* tidak bisa dihindari pada metode kerja pada hub ini.

4. *Network Interface Card* (NIC)

*Network Interface Card* merupakan sebuah kartu yang fungsinya sebagai jembatan dari komputer ke sebuah jaringan komputer. Cara kerja NIC adalah untuk mengubah aliran data paralel dalam *bus* komputer menjadi bentuk data serial sehingga dapat ditransmisikan di atas media jaringan.

5. Host

Setiap perangkat komputasi, yang terpasang pada jaringan, yang memiliki beberapa bentuk pengalamatan, baik itu alamat IP atau alamat MAC. Beberapa perangkat *host* pada jaringan seperti: komputer, printer jaringan, mesin fotokopi jaringan, laptop, PDA, titik akses nirkabel (WAP), perangkat penyimpanan jaringan, kamera jaringan, router, switch, dan bahkan banyak perangkat mobile, seperti ponsel atau iPod, juga memiliki identifikasi alamat IP dan MAC.

6. *Wireless Access Point*

*Wireless Access Point* merupakan perangkat yang berfungsi untuk menyebarkan sinyal pada jaringan *wireless*. Informasi yang bisa didapatkan dari perangkat ini antara lain adalah *log* DHCP, *MAC address, username access point, password access point*, dan informasi *gateway*.

## 2.4 *Router, Smart Router*

Router merupakan perangkat jaringan yang meneruskan paket data dari satu jaringan ke jaringan lainnya. Berdasarkan alamat jaringan tujuan dalam paket yang masuk dan tabel *routing internal*, router menentukan *port* (jalur) untuk mengirimkan paket (*port* biasanya terhubung ke kabel *Ethernet*). Router memerlukan paket yang diformat dalam protokol *routable*, dengan standar global yaitu TCP/IP, atau hanya IP saja (Pcmag, 2017). Secara teknis, router adalah perangkat *gateway* jaringan *Layer* 3, yang berarti menghubungkan dua atau lebih jaringan dan router beroperasi pada lapisan jaringan model OSI (Rouse, 2016).

Router berisi prosesor (CPU), beberapa jenis memori digital, dan *input-output* (I/O) *interface*. Memori router menyimpan sistem operasi, sistem operasi router membatasi jenis aplikasi yang dapat dijalankan pada router dan juga memerlukan jumlah ruang penyimpanan yang jauh lebih kecil. Ada banyak sistem operasi yang dapat dijadikan sebagai router, baik sistem operasi yang berbayar maupun yang gratis dan/atau *open source*(Tengyuen, 2018)(Geier, 2018), serta ada beberapa sistem operasi jaringan yang sudah terpasang atau ter-*install* pada perangkat router (*embedded device*)(Jackson, 2018). Contoh sistem operasi router yang populer diantaranya Juniper Network Operating System (JunOS)(Juniper, 2018), Cisco Internetwork Operating System (IOS)(Cisco, 2018), MikroTik RouterOS(Mikrotik, 2018), DD-WRT(Dd-wrt, 2018), dan OpenWRT(OpenWrt, 2018). Sistem operasi ini diproduksi menjadi *image firmware* biner dan biasa disebut *firmware router*.

Router adalah bagian penting dari setiap penyelidikan karena router merupakan komponen utama yang menghubungkan dan memungkinkan semua perangkat lokal secara

bersama-sama di jaringan lokal yang dapat mengakses ke jaringan luar, dimana router akan menyimpan *log* tentang trafik jaringan yang terjadi. Bagi pengguna komputer rumahan dan bisnis yang memiliki koneksi internet berkecepatan tinggi seperti kabel, satelit atau DSL, router bisa bertindak sebagai *firewall* perangkat keras (Rouse, 2016). Router menjadi perangkat konsumen utama saat rumah tangga mulai mengumpulkan banyak komputer dan ingin berbagi koneksi *internet* di rumah. Router jenis ini biasa dipakai di rumah dan kantor skala kecil, router ini biasa disebut dengan "router nirkabel" atau "*Home Broadband Routers*" biasanya digunakan untuk mengelola lalu lintas *internet* atau berbagi koneksi *internet broadband* serta untuk *file sharing* dan pencetakan. Router jenis ini adalah perangkat kombinasi yang menampung *router, switch* jaringan dan *Wi-Fi Access Point* dalam satu perangkat.

*Smart Router,* sering disebut *Smart Wi-Fi Wireless Routers,* dimana router tersebut dilengkapi dengan perangkat lunak *Smart Wi-Fi* yang memungkinkan kita mengatur dan memantau jaringan rumah dengan mudah, serta memiliki fitur atau layanan yang lebih banyak dibandingkan dengan router biasa pada umumnya (Ideaing, 2016). Smart *Router* merupakan perangakat jaringan nirkabel yang menyediakan interaksi dengan aplikasi mobile. Misalnya, aplikasi dapat mengubah pengaturan router, memonitor perangkat jaringan, membatasi akses ke situs web tertentu, melihat kamera jaringan tinggal dan melihat-lihat atau melakukan streaming foto (Pcmag, 2018).

## 2.5 Referensi Model OSI (*Open System Interconnection*)

Model referensi jaringan terbuka OSI atau OSI *reference model for open networking* adalah model konseptual yang menjadi ciri dan standarisasi fungsi komunikasi dari sistem telekomunikasi atau komputasi tanpa memperhatikan struktur dan teknologi internal yang mendasarinya. Model ini merupakan produk dari proyek *Open System Interconnection* di *International Organization for Standardization*, yang dipelihara dengan identifikasi ISO / IEC 7498-1. Tujuannya adalah interoperabilitas sistem komunikasi yang beragam dengan protokol standar. Model partisi sistem komunikasi menjadi lapisan abstraksi. Versi asli dari model tersebut mendefinisikan tujuh lapisan (OSI *seven layer model*). Sebuah lapisan melayani lapisan di atasnya dan dilayani oleh lapisan di bawahnya.

OSI *Reference Model* pun digunakan sebagai titik awal untuk mempelajari bagaimana beberapa protokol jaringan di dalam sebuah kumpulan protokol dapat berfungsi dan berinteraksi. Fungsi dari tujuh lapisan OSI *Reference Model* diantaranya (Kistijantoro, 2007):

1. *Application Layer*: Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah DHCP (*Dynamic Host Configuration Protocol*), DNS (*Domain Name Server*), HTTP (*HyperText Transfer Protocol*), FTP (*File Transfer Protocol*), SMB (*Server Message Block*).
2. *Presentation Layer*: Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam Windows NT) dan juga *Network shell* (semacam *Virtual Network Computing* (VNC) atau *Remote Desktop Protocol* (RDP)).
3. *Session Layer*: Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama, protokol yang berada pada *layer* ini adalah NETBIOS (*Network Basic Input Output System*), SOCKET.
4. *Transport Layer*: Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (*acknowledgement*), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan, protokol yang berada pada lapisan ini adalah TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*).
5. *Network Layer*: Berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan *routing* melalui *internetworking* dengan menggunakan router dan switch *layer*-3, protokol yang berada pada lapisan ini adalah IP (*Internet Protocol*), RIP (*Routing Information Protocol*), ARP (*Address Resolution Protocol*), RARP (*Reverse ARP*).
6. *Data-link Layer*: Befungsi untuk menentukan bagaimana *bit-bit* data dikelompokkan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras, seperti halnya *MAC Address*, dan menetukan bagaimana perangkat-perangkat jaringan seperti hub, bridge, repeater, dan switch *layer* 2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi dua level anak, yaitu lapisan *Logical Link Control* (LLC) dengan protokol PPP (*Point to Point Protocol*) di dalamnya dan lapisan MAC dengan protokol SLIP (*Serial Line Internet Protocol*) di dalamnya.

7. *Physical Layer*: Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.(Kistijantoro, 2007) (Microsoft, 2018)

## 2.6 Klasifikasi Barang Bukti Digital

Berdasarkan ketentuan yang ada di dalam Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang termasuk bukti digital adalah informasi elektronik dan/atau dokumen elektronik. Dalam UU ITE tersebut dijelaskan pengertian tentang informasi elektronik dan dokumen elektronik, yaitu sebagai berikut (RI & RI, 2008):

1. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
2. Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Terdapat beberapa definisi tentang barang bukti yang diberikan oleh para ahli, diantaranya sebagai berikut:

Menurut Ruby Alamsyah dari hasil wawancara dengan media *online* Perspektif Baru dengan tema "**Teknik Forensik Meneliti Bukti Digital**", bahwa yang termasuk dalam barang bukti digital forensik merupakan semua barang bukti digital (*any digital evidence*) termasuk *handphone*, *notebook*, *server*, alat teknologi apapun yang mempunyai media penyimpanan dan bisa dianalisa (Alamsyah, 2009). Menurut Yudi Prayudi dalam publikasi jurnal Seminar Nasional Sains danTeknologi Informasi – ISSN : 2355-536X (2014) yang berjudul "**Problema dan Solusi *Digital Chain of Custody* Dalam Proses Investigasi *Cybercrime***", salah satu faktor penting dalam proses investigasi adalah hal terkait dengan barang bukti. Dalam hal ini terdapat dua istilah yang hampir sama, yaitu barang bukti

elektronik dan barang bukti digital. Barang bukti elektronik adalah bersifat fisik dan dapat dikenali secara visual (komputer, *handphone*, *camera*, *compact disk*, *harddisk*, dan lain-lain) sementara barang bukti digital adalah barang bukti yang diekstrak atau di-*recover* dari barang bukti elektronik (*file*, *email*, *sms*, *image*, *video*, *log*, *text*)(Prayudi, 2014).

Menurut Yudi Prayudi dalam (Schatz, 2007), berbeda dengan barang bukti fisik pada umumnya, barang bukti digital akan sangat bergantung dari proses interpretasi terhadap kontennya. Oleh Karena itu, integritas dari barang bukti serta kemampuan *expert* dalam menginterpretasikannya akan berpengaruh terhadap pemilahan dokumen – dokumen digital yang tersedia untuk dijadikan sebagai barang bukti(Prayudi, 2014). Menurut Muhammad Nuh Al-Azhar bahwa bukti elektronik adalah bukti yang bersifat fisik dan dapat dikenali secara visual, sehingga investigator dan analis forensik harus sudah memahami serta mengerti masing-masing barang bukti elektronik ketika sedang melakukan pencarian (*searching*) barang bukti di TKP. Sedangkan bukti digital adalah bukti yang bersifat digital yang diekstrak atau di-*recover* dari bukti elektronik. Bukti ini di dalam Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah informasi elektronik dan dokuman elektronik. Janis barang bukti inilah yang harus dicari oleh investigator dan untuk kemudian dianalisis oleh analis forensik secara teliti keterkaitan masing-masing file dalam rangka mengungkap kasus kejahatan yang berkaitan dengan bukti elektronik (Al-Azhar, 2012).

## 2.7 Proses Investigasi

Hal penting yang harus diperhatikan oleh setiap petugas investigator forensika digital dalam menjalankan aktivitas forensika digital adalah diikutinya setiap tahapan dan prosedur dalam forensika digital, tahapan tersebut dikenal dengan istilah *frameworks*. SNI ISO/IEC 27037:2014 yang berjudul Teknologi Informasi – Teknik Keamanan – Pedoman identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital, merupakan *frameworks* atau standar forensika digital yang keseluruhan isi dokumennya diadopsi dari ISO 27037:2012 dengan metode republikasi-*reprint*. SNI ISO/IEC 27037:2014 merupakan standar nasional yang membahas tentang panduan spesifik terkait aktivitas investigasi forensika digital. Yang mana aktivitas tersebut meliputi identifikasi, pengumpulan, akuisisi, dan preservasi. Kesemua proses ini merupakan proses penting yang harus dilakukan secara hati-hati untuk tetap menjaga integritas barang bukti (Badan Standarisasi Nasional, 2014).

Ada 4 tahapan utama yang diatur dalam SNI ISO/IEC 27037:2014 yaitu tahapan identifikasi, pengumpulan, akuisisi, dan preservasi, diantaranya yaitu:

1. Identifikasi;
    a. Perencanaan Investigasi

        Perencanaan investigasi ini diatur oleh SNI pada bagian 6.7.2. Perencanaan dilakukan untuk menyusun strategi terkait investigasi yang akan dilakukan. Mulai dari perencanaan *tools* yang digunakan, perencanaan teknis investigasi, dan hal terkait lainnya.

    b. Persiapan dan Pengarahan *Team*

        Persiapan dan pengarahan *team* diatur oleh SNI pada bagian ke 6.7. Persiapan dilakukan dengan mempersiapkan seluruh kebutuhan baik itu hal administrasi maupun hal teknis untuk proses investigasi. Pengarahan team dilakukan untuk memastikan seluruh anggota tim investigasi paham dengan kasus yang akan ditangani, apa yang harus dilakukan dan tidak dilakukan selama investigasi, dan mengingatkan untuk selalu menjaga integritas barang bukti.

    c. Penilaian Resiko Keamanan TKP

        Penilaian resiko keamanan TKP diatur dalam SNI pada bagian ke 6.2.2. Penilaian resiko dilakukan untuk menjaga keamanan tim investigasi dan barang bukti. Sebagai contoh untuk menilai apakah di TKP terdapat senjata atau material yang dapat menyebabkan kerusakan fisik.

    d. Pengamanan TKP

        Hal ini diatur dalam SNI pada bagian ke 6.2.1. Pengamanan TKP dilakukan untuk melindungi barang bukti. Pengamanan juga dilakukan untuk membatasi tidak semua orang bisa masuk ke TKP dan hanya orang-orang yang telah diziinkan oleh tim.

    e. Pencarian Barang Bukti

        Hal ini diatur dalam SNI pada bagian ke 5.4.2. Pencarian barang bukti merupakan proses dimulainya melihat keseluruh TKP dan mencari apa saja yang berpotensi sebagai barang bukti.

    f. Identifikasi Barang Bukti

        Hal ini diatur dalam SNI pada bagian ke 5.4.2. Melakukan identifikasi baik itu dari sisi jenis, bentuk, dan fungsinya terhadap barang bukti yang ditemukan dari hasil pencarian apakah bisa menjadi barang bukti yang berpotensi. Identifikasi juga melakukan pengecekkan terhadap status barang bukti yang ditemukan semisal apakah dalam keadaan menyala atau tidak.

g. Menentukan Prioritas Barang Bukti

Hal ini diatur dalam SNI pada bagian ke 6.8. Memberikan prioritas terhadap barang bukti yang ditemukan terhadap aspek kerentanan data tersebut. Barang bukti yang mudah hilang seperti data dalam RAM yang hilang jika komputer mati harus diberikan prioritas. Sehingga barang bukti dengan prioritas tinggi diberikan tindakan yang lebih.

h. Dokumentasi

Hal ini diatur dalam SNI pada bagian ke 6.6. Segala aktivitias terkait penemuan barang bukti harus didokumentasikan. Dan dokumentasi disini juga mencakup keseluruhan aspek proses yang dilakukan mulai tahapan identifikasi sampai tahapan akhir investigasi yang harus selalu didokumentasikan. Dokumentasi dilakukan untuk menjaga integritas barang bukti.

i. Pencatatan Barang Bukti (*Chain of custody*)

Hal ini diatur dalam SNI pada bagian ke 6.1. *Chain of custody* merupakan catatan rantai perjalanan barang bukti. Jadi ketika barang bukti ditemukan, harus dicatat informasinya dan selanjutnya kemana saja barang bukti tersebut berpindah atau apa saja yang dilakukan terhadap barang bukti harus dicatat di *form chain of custody*. Hal ini juga dilakukan untuk menjaga integritas barang bukti.

2. Pengumpulan;

a. Menentukan barang bukti disita atau diakuisisi di TKP

Hal ini diatur dalam SNI pada bagian ke 6.8 dan 7.1.1.3. Dari hasil pemberian prioritas barang bukti, akan ditentukan apakah barang bukti yang ditemukan dapat langsung disita atau harus diakuisisi di TKP terkait datanya yang mudah hilang.

b. Melakukan penyitaan barang bukti

Hal ini diatur dalam SNI pada bagian ke 7.1.2. Penyitaan barang bukti dibagi menjadi dua tahapan yaitu prosedur penyitaan perangkat dalam keadaan menyala dan dalam keadaan mati.

(a) Barang bukti dalam keadaan menyala

1) Menganalisis apakah membutuhkan data *volatile* dari perangkat: Hal ini diatur dalam SNI pada bagian ke 7.1.2.1. Analisis dilakukan untuk menentukan apakah dari perangkat yang menyala tersebut membutuhkan data *volatile* yang akan hilang apabila perangkat dimatikan.;

2) Jika butuh lakukan prosedur *Live* akuisisi: Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Jika hasil analisis menyimpulkan dibutuhkan data *volatile*, maka lakukan prosedur *live* akuisisi terhadap perangkat.;
3) Jika tidak butuh lakukan pemeriksaan aspek keamanan dan kerentanan data terhadap listrik: Hal ini diatur dalam SNI pada bagian ke 7.1.2.1. Jika tidak butuh data *volatile*, atau proses *live* akuisisi telah selesai, lakukan pemeriksaan aspek keamanan data apakah data akan rusak apabila perangkat langsung dimatikan. Jika ternyata data akan rusak jika perangkat langsung dimatikan, lakukan prosedur *shutdown* secara sistem normal.
4) Melakukan prosedur *shutdown* perangkat: Hal ini diatur dalam SNI pada bagian ke 7.1.2.1. Jika data stabil atau tidak bermasalah apabila perangkat langsung dimatikan, cabut secara langsung kabel *power* untuk mematikan perangkat.

(b) Barang bukti dalam keadaan tidak menyala

Cabut semua kabel yang terkoneksi dan baterai (jika ada baterai) Hal ini diatur dalam SNI pada bagian ke 7.1.2.2. Cabut semua kabel dan amankan kabel tersebut, lalu label seluruh port yang terkoneksi dengan kabel untuk memudahkan proses rekonstruksi. Setelah prosedur ini selesai, maka lakukan prosedur selanjutnya yaitu memberikan label barang bukti.

c. Memberikan label barang bukti

Hal ini diatur dalam SNI pada bagian ke 7.1.2. Label seluruh barang bukti untuk memudahkan proses rekonstruksi dan memudahkan mengenali barang bukti tersebut.

d. Mempacking barang bukti

Hal ini diatur dalam SNI pada bagian ke 7.1.2. *Packing* atau lakukan proses pengemasan barang bukti dengan memasukkan barang bukti ke dalam alat pembungkus barang bukti. Perhatikan aspek keamanan barang bukti ketika akan dikemas. Sebagai contoh, perangkat yang terkoneksi ke jaringan *wireless* seperti *smartphone* harus dikemas dalam alat pembungkus khusus yang dapat menetralisir sinyal tersebut.

e. Mengumpulkan keterangan verbal dari saksi-saksi

Hal ini diatur dalam SNI pada bagian ke 7.1.1.2. Hal ini dilakukan untuk mendapatkan petunjuk lebih dan mencari informasi terkait barang bukti yang ditemukan. Sebagai contoh menanyakan *password* sistem yang ditemukan dalam barang bukti.

3. Akuisisi;

b. Pemeriksaan aspek keamanan barang bukti

Hal ini diatur dalam SNI pada bagian ke 7.1.1.1. Pemeriksaan aspek keamanan untuk memastikan bahwa proses akuisisi yang dilakukan tidak akan merusak barang bukti.

c. Penentuan model akuisisi yang dilakukan

Hal ini diatur dalam SNI pada bagian ke 7.1.3. Proses akuisisi terbagi menjadi 3 jenis yaitu akuisisi pada perangkat menyala, akuisisi pada perangkat yang tidak menyala dan partial akuisisi. Penentuan model akuisisi yang digunakan sesuai hasil identifikasi yang telah dilakukan terhadap barang bukti.

(a) Akuisisi pada perangkat yang menyala

1) Lakukan prosedur *live* akuisisi untuk mendapatkan data *volatile* Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Data *volatile* akan dapat hilang apabila perangkat digitalnya dimatikan, oleh karena itu live akuisisi dilakukan ketika perangkat masih dalam keadaan menyala. Beberapa contoh data *volatile* yaitu data di RAM, data proses yang berjalan, data koneksi jaringan. Petugas harus berkompetensi dan menggunakan *tools* yang valid untuk melakukan prosesdur ini.
2) Jika data *non volatile* juga dibutuhkan saat itu, lakukan juga prosedur akuisisi pada data *non volatile* Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Lakukan juga prosedur *live* akuisisi jika data *non volatile* seperti data yang tersimpan di *logical* juga dibutuhkan.
3) Jika perangkat bisa disita, lakukan prosedur pengumpulan barang bukti Hal ini diatur dalam SNI pada bagian ke 7.1.3.1. Jika setelah proses akuisisi pada data *volatile* selesai dan perangkat dapat disita lakukan prosedur pengumpulan barang bukti. Perangkat yang tidak dapat disita sebagai contoh komputer *server* yang sangat krusial terhadap sistem yang sedang berjalan.

(b) Akuisisi pada perangkat yang tidak menyala

Lakukan prosedur *static* akuisisi dengan melakukan *imaging* terhadap media penyimpanan data. Hal ini diatur dalam SNI pada bagian ke 7.1.3.2. Proses *static* akuisisi dijalankan dengan melakukan *bitstream copy*.

(c) *Partial* Akuisisi

Dapat dilakukan dengan menggunakan perpaduan prosedur *live* dan *static* akuisisi Hal ini diatur dalam SNI pada bagian ke 7.1.3.4. *Partial* akuisisi dilakukan untuk perangkat yang krusial dan tidak dimungkinkannya melakukan

akuisisi terhadap keseluruhan data seperti dikarenakan jumlah data yang sangat besar.

d. Pelaksanaan akuisisi

Setelah proses penentuan metode akuisisi dipilih, berikutnya adalah dilaksanakan proses akuisisi sesuai dengan metode akuisisi yang telah ditentukan sebelumnya.

e. Verifikasi hasil akuisisi

Hal ini diatur dalam SNI pada bagian ke 7.1.4. Verifikasi dilakukan untuk memastikan data hasil akuisisi identik dengan data aslinya. Verifikasi dapat dilakukan dengan menggunakan fungsi *hash*.

4. Preservasi.

a. Memberikan segel barang bukti

Hal ini diatur dalam SNI pada bagian ke 6.9.2. Barang bukti yang telah di-*packing*, harus disegel untuk memastikan selama proses pemindahan barang bukti tetap dalam kemasannya dan berguna menjaga integritas barang bukti.

b. Pemeriksaan aspek keamanan pemindahan barang bukti

Hal ini diatur dalam SNI pada bagian ke 6.9.2. Pemeriksaan aspek keamanan dilakukan untuk memastikan barang bukti aman selama proses pemindahan barang bukti dari TKP ke tempat penyimpanan ataupun laboratorium. Pemeriksaan aspek keamanan mencakup pemeriksaan pengemasan barang bukti untuk menjaga pengemasan yang dilakukan tidak merusak barang bukti.

c. Pemindahan barang bukti

Hal ini diatur dalam SNI pada bagian ke 6.9.2. Selama proses pemindahan barang bukti, petugas harus berhati-hati dan selalu memperhatikan keamanan barang bukti. Selain itu juga harus melakukan *update* di *form chain of custody*.

d. Penyimpanan barang bukti

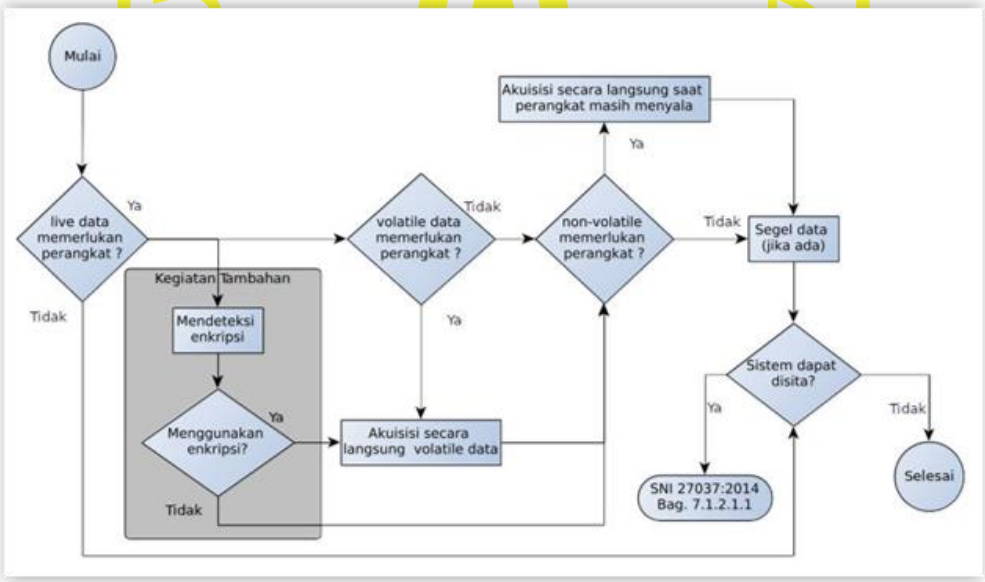
Hal ini diatur dalam SNI pada bagian ke 6.9.2. Barang bukti harus disimpan dalam tempat penyimpanan yang memiliki fasilitas keamanan yang baik dan fasilitas penyimpanan yang baik. Sebagai contoh harus memiliki fasilitas untuk menjaga suhu ruangan penyimpanan tidak terlalu panas atau tidak terlalu dingin sehingga dapat menyebabkan kerusakan barang bukti.

Prinsip – prinsip tersebut harus dipahami dalam melakukan proses *forensic*, bahwa:

1. Sebuah lembaga hukum atau petugasnya dilarang mengubah data digital yang tersimpan dalam media penyimpanan yang selanjutnya akan dibawa ke pengadilan.

2. Untuk seorang yang merasa perlu mengakses data digital yang tersimpan dalam media penyimpanan barang bukti, maka orang tersebut harus jelas kompetensi, relevansi, dan implikasi dari tindakan yang dilakukan terhadap barang bukti.
3. Terdapat catatan teknik dan praktis mengenai langkah-langkah yang dilakukan terhadap media penyimpanan selama proses pemeriksaan dan analisis berlangsung. Jika terdapat pihak ketiga yang melakukan investigasi terhadap media penyimpanan tersebut akan mendapatkan hasil yang sama.
4. *Person in charge* dari investigasi memiliki seluruh tanggung jawab dari keseluruhan proses pemeriksaan dan juga analisis dan dapat memastikan bahwa keseluruhan proses berlangsung sesuai dengan hukum yang berlaku.

Proses investigasi media penyimpanan diutamakan hasil verifikasi barang bukti digital sumber dan barang bukti hasil penggandaan harus sama. Hal ini dilakukan menggunakan metode akuisisi secara fisikal. Namun pada kondisi tertentu misalkan pada sebuah sistem yang sifatnya kritis dan tidak boleh dimatikan maka diperkenankan untuk melakukan akuisisi secara logikal. Proses akuisisi logikal hanya menyalin berkas yang aktif dan artefak lainnya termasuk diantaranya mengakuisisi partisi. Dalam proses akuisisi logikal tidak tersalin berkas yang telah terhapus. Menurut SNI ISO/IEC 27037:2014 juga telah mengatur prosedur akuisisi barang bukti elektronik dan barang bukti digital. Khusus untuk perangkat dalam kondisi menyala SNI ISO/IEC 27037:2014 telah mengaturnya pada bagian 7.1.3.1. Adapun ilustrasi proses akuisisi bukti digital pada perangkat dalam kondisi menyala dapat dilihat pada Gambar 2.1 (Badan Standarisasi Nasional, 2014).




Gambar 2.1 Akuisisi Bukti Elektronik dalam Kondisi Menyala

Lima hal yang dilakukan dalam mengakuisisi perangkat digital dalam kondisi menyala:

1. Memperhatikan bukti digital yang rentan hilang saat listrik padam seperti data yang tersimpan di RAM, daftar proses sistem operasi, informasi koneksi jaringan dan informasi terkait waktu. Bukti digital yang tidak mudah hilang jika listrik padam juga harus diperhatikan.
2. Dalam melakukan akuisisi secara langsung diperkenankan untuk mengakses sistem secara langsung baik secara fisik atau pun mengakses jarak jauh.
3. Disarankan menggunakan *tools* yang terpercaya atau tools yang dibawa sendiri. Saat menjalankan *tools* tersebut harus selalu dicatat.
4. Berkas yang diakuisisi sebaiknya dikompres dan tentukan nilah *hash*-nya.
5. Memastikan hasil akuisisi integritasnya terjaga dan tidak mudah rusak.

Akuisisi sebagian atau *partial acquisition* harus dicatat semua informasi yang terkait dengan barang bukti digital seperti, informasi direktori, informasi berkas atau informasi terkait sistem terakuisisi. Adapun hal yang diperkenankan akuisisi sebagian jika dalam kondisi: a. Sistem penyimpanan yang terlalu besar sebagai contoh peladen basis data; b. Sistem tidak boleh mati; c. Data yang tersalin dimungkinkan bukti digital yang tidak terkait dengan tindak kejahatan; atau d. Keterbatasan dengan aturan yang berlaku (Hariyadi & Supriyono, 2017).

## 2.8 *Live Forensics*

*Live forensics* merupakan suatu keadaan atau proses analisa *forensic* ketika sistem sedang berjalan. Metode yang dilakukan dan filosofi pendekatannya adalah sama dengan proses *forensic* tradisional yang ada, namun ketikan sistem mati proses terhenti dan dilanjutkan dengan menggunakan proses *forensic* tradisional/biasa. *Live forensics* dilakukan untuk mencari informasi dan barang bukti dalam sebuah perangkat komputer, artinya kita menghadapi keadaan dimana komputer atau alat bukti yang ditemui di TKP dalam keadaan *power on*(menyala/hidup). Hal ini memberikan keuntungan dari kekurangan proses *forensic* tradisional yang tidak dapat menganalisa sebuah komputer untuk mencari barang bukti serta informasi didalamnya. Kerugian melakukan *live forensics* adalah karena kecenderungan setiap komputer memiliki sistem operasi yang berbeda dan *invironment* yang tidak sama membuat investigator harus melakukan analisa ulang terhadap data mentah yang didapat, kemudian jika tidak dilakukan dengan benar, bukan tidak mungkin *live forensics* dapat merusak barang bukti yang ada(Artformatics, 2013), serta data yang dikumpulkan tersebut merupakan representasi dari sistem yang dinamis dan tidak mungkin untuk diproduksi ulang pada waktu berikutnya (Adelstein, 2006).

Pada dasarnya memiliki kesamaan pada teknik forensik tradisonal dalam hal metode yang dipakai yaitu identifikasi, penyimpanan, analisis, dan presentasi, hanya saja *live forensics* merupakan respon dari kekurangan teknik forensik tradisonal yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan misalnya aktivitas *memory*, *network* proses, *swap file*, *running system proses*, dan informasi dari file sistem dan ini menjadi kelebihan dari teknik *live forensics*(Lessing & Solms, 2008). Setiap metode maupun cara yang dilakukan pasti tetap ada kekurangan dan kelebihannya masing-masing, tidak terkecuali pada *live forensics*, kelemahan yang terdapat pada *live forensics* antara lain adalah sebagai berikut:

a) Berbedanya instalasi setiap komputer, keterbatasan pengetahuan ataupun keahlian yang dimiliki oleh seorang analisis *forensic* akan menjadi sebuah hambatan karena *environment* setiap komputer berbeda entah itu sistem operasinya, perangkat kerasnyanya,dll.
b) Kemungkinan data termodifikasi yang mempengaruhi akuisisi data untuk disajikan pada saat persidangan sangat berpengaruh pada sistem operasi yang dimiliki oleh tersangka.
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-forensic* yang dapat mengelabui seorang investigator.
e) Data yang diambil dalam sebuah jaringan menjadi sebuah data yang korup, sehingga mengurangi akuisisi barang bukti.

Sedangkan hal positif dari *live forensics* adalah ketika kekurangan pada teknik *forensic* biasa atau tradisional untuk melakukan analisa ataupun mengambil barang bukti dari sebuah arsitektur jaringan sistem informasi tidak dapat dilakukan, hal tersebut dapat diatasi dan dilakukan dengan teknik *live forensics*(Artformatics, 2013) (Jinkook, 2014). Dalam melakukan forensik pada perangkat dalam keadaan menyala (*on*), ada beberapa hal yang perlu dilakukan, diantaranya: Memeriksa perangkat pada bagian proses yang sedang berjalan (*running process*). Jika ditemukan ada proses yang bersifat destruktif (dapat menyebabkan kerusakan), investigator harus menghentikan proses tersebut dan mendokumentasikan aktivitas yang dilakukan.; Melakukan proses *capture* pada RAM dan data *volatile* lainnya

dari sistem operasi, seperti koneksi jaringan, *password*, status *file system*, user yang terkoneksi, dll.; Mendokumentasikan dan menghibernasi mesin virtual (*virtual machine*) yang sedang berjalan.; Mempertimbangkan adanya perangkat lunak enkripsi yang terpasang di komputer sebagai bagian dari sistem operasi. Jika ada, maka metode forensik yang tepat harus digunakan untuk mendapatkan data yang tidak terenkripsi sebelum komputer dimatikan.; Menyimpan file apapun yang sedang terbuka ke dalam media *trusted* (aman dan terpercaya).

## 2.9 *File Log*

*Log* dalam konteks komputasi adalah dokumentasi kejadian (aktivitas) yang diproduksi secara otomatis dengan pewaktuan (*time-stamps*) yang relevan dengan sistem tertentu. Hampir semua aplikasi dan sistem perangkat lunak menghasilkan file *log*, *log* dapat diartikan sebagai file yang berisi daftar tindakan yang telah terjadi. Sebuah timestamp adalah urutan karakter atau informasi yang dikodekan yang mengidentifikasi kapan suatu peristiwa terjadi, biasanya memberi tanggal dan waktu, kadang-kadang akurat sampai sepersekian detik, dengan standarisasi dari ISO 8601. *File log* adalah file yang berisi daftar acara, yang telah "*login*" oleh komputer. File *log* sering dihasilkan selama instalasi perangkat lunak dan dibuat oleh *server* Web, namun file tersebut juga dapat digunakan untuk berbagai tujuan lain. Sebagian besar file *log* disimpan dalam format teks biasa, supaya meminimalkan ukuran file dan memungkinkannya dapat dilihat melalui teks editor(Christensson, 2010).

*File log* yang dibuat oleh perangkat lunak biasanya berisi daftar file yang telah ditambahkan atau disalin ke *hard drive* selama proses instalasi. File *log* juga menyertakan tanggal dan waktu file-file itu terpasang, serta direktori tempat setiap file ditempatkan. File *log* penginstal memungkinkan pengguna melihat file apa yang terinstal di sistem menggunakan program tertentu. Hal ini berguna saat mengatasi masalah *crash program* atau saat menguninstall sebuah program(Christensson, 2010). *File log* juga dapat dihasilkan oleh utilitas perangkat lunak, program FTP, dan sistem operasi. Sebagai contoh, Mac OS X menyimpan *log* semua program dan sistem *crash*, yang dapat dilihat menggunakan aplikasi *Console*. Windows mencatat aplikasi, keamanan, dan *log* sistem, yang semuanya dapat dilihat menggunakan program *Event Viewer* yang sudah disertakan oleh Windows. Sebagian besar file *log* memiliki ekstensi file "***.log***", namun banyak yang menggunakan ekstensi standar "***.txt***" atau ekstensi *proprietary* lainnya(Christensson, 2010).

Beberapa contoh *log* yang umum: Pada *server* web, *log* akses mencantumkan semua file individual yang diminta orang dari sebuah situs web. File-file ini akan menyertakan file

*html* dan gambar grafis yang melekat dan file terkait lainnya yang dapat dikirim. Dimana *server* web menyimpan file *log* yang mencantumkan setiap permintaan yang dilakukan ke *server*. Dari file *log server*, administrator dapat mengidentifikasi jumlah pengunjung, dari mana pengunjung berasal atau domain tempat mereka mengunjungi, seberapa sering pengunjung mengakses atau jumlah permintaan untuk setiap halaman dan pola penggunaan sesuai dengan variabel seperti waktu dalam sehari, minggu, bulan atau tahun(Rouse, 2010) (Beal, 2017). *Server web* menggunakan file *log* untuk merekam data tentang pengunjung situs. Informasi ini biasanya mencakup alamat IP setiap pengunjung, waktu kunjungan, dan halaman yang dikunjungi. *File log* juga dapat melacak sumber daya apa yang dimuat selama setiap kunjungan, seperti file gambar, JavaScript, atau CSS. Data ini bisa diolah oleh perangkat lunak statistik situs web, yang bisa menampilkan informasi dalam format yang *user-friendly*. Misalnya, pengguna mungkin dapat melihat grafik pengunjung harian selama bulan lalu dan klik setiap hari untuk melihat informasi lebih rinci(Christensson, 2010).

*Log audit* (juga dikenal sebagai jejak audit) mencatat dokumentasi kronologis dari setiap kegiatan yang dapat mempengaruhi operasi atau peristiwa tertentu. Rincian biasanya mencakup sumber daya yang diakses, alamat tujuan dan sumber, informasi tentang batas waktu pengguna yang masuk dan mengakses file sumber (*resource*)(Rouse, 2010).

## 2.10 Samba

Samba adalah sebuah perangkat *Open Source / Free Software* yang menyediakan layanan file dan layanan cetak untuk klien SMB/CIFS. Samba tersedia secara gratis, tidak seperti implementasi SMB/CIFS, dan memungkinkan interoperabilitas antara *server* Linux/Unix dan klien berbasis Windows(Samba.org, 2017). Samba adalah perangkat lunak yang bisa dijalankan di *platform* selain Microsoft Windows, misalnya UNIX, Linux, IBM System 390, OpenVMS, dan sistem operasi lainnya. Dalam perkembangan, SMB juga dapat diterapkan pada keluarga sistem operasi UNIX seperti MikroTik RouterOS dengan menggunakan program Samba. Mikrotik selain memiliki fungsi utama sebagai sebuah Router juga *support* SMB sehingga dapat difungsikan sebagai sebuah *file server*. Dukungan MikroTik RouterOS saat ini adalah SMB v1.0 serta SMB v2.002 (Citraweb, 2017). Samba menggunakan protokol TCP / IP yang diinstal pada *host server*, hal ini memungkinkan *host* tersebut berinteraksi dengan klien(Terpstra, 2006). Samba juga memberikan fleksibilitas dan kebebasan administrator jaringan dalam hal pengaturan, konfigurasi, dan pilihan sistem dan peralatan(Vernooij, Terpstra, & Carter, 2017).

## 2.11 Hak Cipta

Hak Cipta sebagai satu bagian dalam bidang Hak Kekayaan Intelektual (HKI) merupakan hak eksklusif atau yang hanya dimiliki oleh Pencipta atau Pemegang Hak Cipta untuk mengatur penggunaan hasil karya atau hasil olah gagasan atau informasi tertentu. Pada dasarnya, hak cipta merupakan "hak untuk menyalin suatu ciptaan" atau hak untuk menikmati suatu karya. Hak cipta juga sekaligus memungkinkan pemegang hak tersebut untuk membatasi pemanfaatan, dan mencegah pemanfaatan secara tidak sah atas suatu ciptaan(Munandar & Sitanggang, 2008).

Hal ini diatur dalam Pasal 1 ayat (1) Undang-Undang No. 19 Tahun 2002 tentang Hak Cipta yang berbunyi: “Hak Cipta adalah hak eksklusif bagi Pencipta atau penerima hak untuk mengumumkan atau memperbanyak Ciptaannya atau memberikan izin untuk itu dengan tidak mengurangi pembatasan-pembatasan menurut peraturan perundang-undangan yang berlaku”. Dan yang diperbaharui pada Undang-undang No.28 Tahun 2014 tentang Hak Cipta dalam Pasal 1 ayat (1) yang berbunyi: “Hak Cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan”.

# BAB 3
# Metodologi Penelitian

## 3.1 Studi Pustaka

Studi Pustaka merupakan kegiatan untuk mempelajari literatur – literatur dan teori yang mendukung dalam melakukan penelitian ini. Studi Pustaka dilakukan untuk mendapatkan informasi mengenai topik penelitian yang terkait dengan *Forensics Science*; *Digital Forensics; Network Forensics; Router*, *Smart Router*; Referensi Model OSI (*Open System Interconnection*); Klasifikasi Barang Bukti Digital; Proses Investigasi; *Live Forensics*; *File Log; SAMBA;* Hak Cipta., yang dapat bersumber dari dokumen, buku, paper, jurnal, laporan penelitian, artikel, atau bahan tertulis lainnya yang berupa teori, baik bersifat *online source* maupun *offline source*.

## 3.2 Persiapan Alat dan Bahan Penelitian

Pada tahap ini melakukan persiapan alat dan bahan untuk menunjang implementasi dalam penelitian. Adapun beberapa perangkat keras dan perangkat lunak yang dibutuhkan untuk melakukan uji simulasi dari skenario yang dibuat. Perangkat keras yang sudah disiapkan disusun sesuai dengan rancangan topologi jaringan yang sudah dibuat, serta pemasangan beberapa *tools* atau perangkat lunak yang diperlukan dalam melakukan simulasi. Berikut ini beberapa alat dan bahan yang dipakai dalam melakukan penelitian:

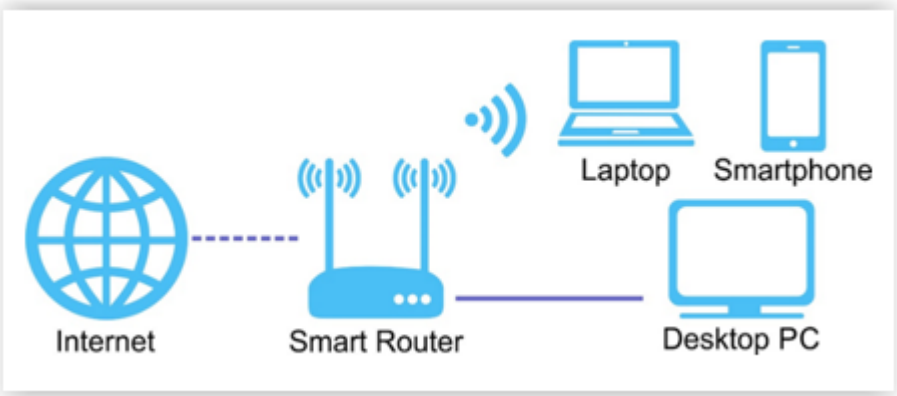
Tabel 3.1 Persiapan Alat dan Bahan Penelitian

| No | ***Hardware* dan *Software* (*Tools*)** | **Keterangan** |
|---|---|---|
| 01. | Laptop Lenovo ThinkPad E445, dengan spesifikasi Processor AMD A8-4500M, *Memory* RAM 4096MB | Sebagai komputer untuk melakukan penarikan data dan analisa, dengan Sistem Operasi Windows 10 Pro 64-bit. (PC Investigator) |
| 02. | Router GL-inet (GL-AR300) | Barang Bukti Elektronika *Smart Router*, yang bertindak sebagai *server file sharing*, yang dibangun dengan Sistem Operasi OpenWrt Chaos Calmer 15.05 r47065, yang sudah terpasang aplikasi Samba untuk menjalankan servis protokol SMB. |
| 03. | Router MikroTik (RB951Ui-2HnD) | Barang Bukti Elektronika *Smart Router*, yang bertindak sebagai *server file sharing*, yang dibangun dengan Sistem Operasi MikroTik RouterOS 6.39.2, |

| No | *Hardware* dan *Software* (*Tools*) | Keterangan |
|---|---|---|
| | | yang sudah terpasang aplikasi Samba untuk menjalankan servis protokol SMB. |
| 04. | Laptop SONY Vaio E-Series, dengan spesifikasi Processor AMD E2-2000, *Memory* RAM 2048MB | Perangkat Komputer sebagai *client*, yang bertindak sebagai tersangka. Komputer klien merupakan komputer yang melakukan akses fasilitas *file sharing* yang disediakan oleh *server*. Pada simulasi ini komputer klien berbasis sistem operasi Windows Professional 32-bit. Pada komputer klien, media penyimpanan klien disimulasikan dengan menggunakan *thumbdrive* 32 GB. |
| 05. | *USB Thumb Drive* (General USB Flash Disk USB Device) dengan kapasitas 4GB | Sebagai media penyimpanan pada perangkat Router GL-inet (GL-AR300) |
| 06. | *USB Thumb Drive* (JetFlash TS512MJFV30 USB Device) dengan kapasitas 512MB | Sebagai media penyimpanan pada perangkat Router MikroTik (RB951Ui-2HnD) |
| 07. | *USB Thumb Drive* (HP v155w USB Device) dengan kapasitas 4GB | Sebagai media penyimpanan Barang Bukti *Log system* |
| 08. | *USB Thumbdrive* (SanDisk Cruzer Edge) dengan kapasitas 32GB | Sebagai media penyimpanan klien, yang disimulasikan dengan menggunakan *thumbdrive* 32 GB. |
| 09. | AccessData® FTK® Imager 3.4.2.6 | *Tools Image Forensic (Imagging Tools)* |
| 10. | DSi USB Write Blocker versi 1 | *USB Write Blocker* untuk SO Windows |
| 11. | Notepad++ versi 7 | Pembaca *File Log System* |
| 12. | PuTTY Release 0.68 | Untuk mengakses Router GL-inet melalui protokol SSH |
| 13. | FileZilla versi 3.30.0 | Untuk mengakses Router MikroTik melalui protokol FTP |
| 14. | Autopsy 4.1.1 (RELEASE) Sleuth Kit Version: 4.2.0 | Untuk melakukan membaca/membuka dan menganalisis *File Imagging* |
| 15. | Winbox-2.2.18 | Untuk mengakses/me-*remote* perangkat MikroTik |

### 3.3 Persiapan Skenario

Untuk melakukan simulasi maka dibuat skenario dari penggunaan *Smart Router*. Tahapan skenario diperlukan untuk menggali informasi, melakukan ujicoba sistem, dan pendalaman dalam memahami karakteristik pada *Smart Router*. Pembuatan skenario dibuat agar simulasi dapat berjalan sesuai yang diharapkan dan dapat memenuhi target yang diinginkan. Berikut ini merupakan topologi yang diterapkan pada penelitian ini yang digambarkan pada Gambar 3.1.




Gambar 3.1 Topologi Jaringan

**Keterangan:**

Router: Dalam penelitian ini jenis router yang dipakai *Smart Router*, dimana router tersebut selain dapat difungsikan sebagai *access point*, juga dapat dijadikan sebagai mesin peladen (*server*) *file sharing*.

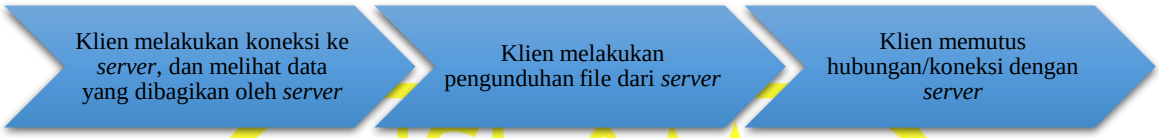
*Client*: Berfungsi sebagai pengakses *file sharing* yang dibagikan oleh server, client dapat melakukan proses pengunduhan file dan pengunggah file, klien dapat berupa Desktop PC, Laptop dan *Smartphone*.

Topologi ini merupakan topologi umum yang biasa digunakan pada pengguna rumah maupun perkantoran berskala kecil. Supaya *client* terhubung ke jaringan dapat menghubungkan secara langsung menggunakan kabel LAN dari router. Smart Router juga dapat berfungsi sebagai *Access Point* yang berfungsi untuk menghubungkan jaringan tanpa kabel/nirkabel, dengan AP (*Access Point*) memungkinkan *smartphone* dan laptop (*client*) dapat terhubung dengan Router menggunakan koneksi *WiFi*. *Smart Router* juga dapat dijadikan sebagai peladen (*server*) yang dapat dibagikan cukup dengan menambahkan media *storage* seperti *USB Thumb Drive* yang dipergunakan sebagai media penyimpanannya.

Skenario yang dibuat berawal dari adanya pelaporan dari pelapor, bahwa ada indikasi perubahan data atau file yang terdapat pada media penyimpanan *file sharing*. Terdapat beberapa file yang hilang atau terhapus oleh klien yang terhubung dalam jaringan lokal. Media *file sharing* tersebut terdapat di dalam perangkat *smart router*, dimana perangkat *smart router* tersebut selain dapat dijadikan sebagai *wireless access point* juga dapat berfungsi sebagai media *file sharing* dengan SMB sebagai protokol pengembangnya. Untuk mempermudah dalam simulasi kasus, maka dibuat 2 (dua) skenario terkait kasus yang ada.

### 3.3.1 Skenario 1 (satu)

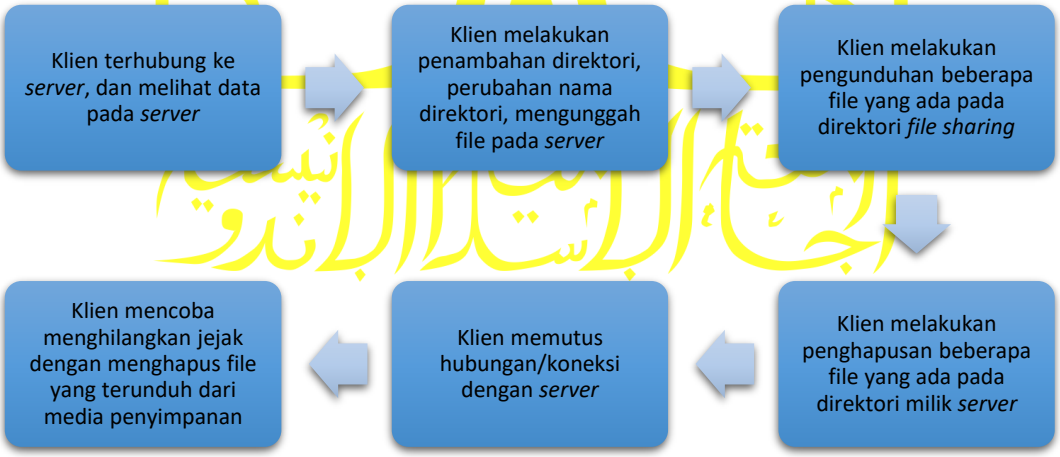
Pada skenario 1 (satu) klien bergabung dengan jaringan yang memiliki fasilitas *file sharing* dengan protokol SMB, klien tersebut melakukan koneksi ke *server* dan melihat isi data-data yang dibagikan oleh *server*. Klien tersebut melakukan transfer data dari *server* ke komputer klien dan juga sebaliknya, kemudian klien mengakhiri atau memutus koneksi dari *server*. Alur pada skenario 1 (satu) dapat dilihat pada Gambar 3.2




Gambar 3.2 Alur Skenario 1 (satu)

### 3.3.2 Skenario 2 (dua)

Pada skenario 2 (dua) klien bergabung dengan jaringan yang memiliki fasilitas *file sharing* dengan protokol SMB, klien tersebut melakukan koneksi ke *server* dan melihat data-data yang dibagikan oleh *server*, klien mencoba melakukan penambahan direktori, melakukan perubahan nama salah satu direktori yang tersimpan di *server*, klien juga melakukan pengunggahan beberapa file ke direktori *file sharing* pada *server*, klien tersebut melakukan penghapusan beberapa file yang terdapat pada media *file sharing* yang sebelumnya telah diunduh terlebih dahulu, kemudian klien mengakhiri atau memutus koneksi dari *server*. Dan untuk menghilangkan jejak klien melakukan penghapusan file yang telah didapat dari *server*, dengan menghapus file pada media penyimpanan klien. Alur pada skenario 2 (dua) dapat dilihat pada Gambar 3.3




Gambar 3.3 Alur Skenario 2 (dua)

### 3.4 Simulasi Kasus

Simulasi bertujuan untuk melakukan pembuktian terhadap hipotesa yang dibuat. Simulasi dilakukan karena tidak memungkinkan untuk melakukan investigasi pada kasus sebenarnya. Simulasi dilakukan untuk menimbulkan jejak aktivitas pada router dimana kemudian akan dicari sebagai temuan dalam proses investigasi forensik. Tahap pembuatan simulasi untuk mendukung proses pengambilan data agar penelitian yang dirancang mendapatkan hasil yang sesuai dengan rumusan yang sudah dibuat.

### 3.5 Investigasi dan Olah TKP

Pada tahap ini dilakukan proses olah TKP dan pengamanan terhadap barang bukti, proses ini dilakukan supaya barang bukti yang didapat terhindar dari kontaminasi dari luar. Barang bukti yang didapat diambil gambarnya dengan kamera foto dan diberi label penamaan, proses pada olah TKP mengacu pada SNI ISO/IEC 27037:2014. Ada beberapa aktifitas seperti identifikasi, pengumpulan, akuisisi, dan preservasi.

#### 3.5.1 Identifikasi

Dalam dokumen SNI ISO/IEC 27037:2014, Identifikasi adalah proses yang meliputi pencarian, mengenali, dan mendokumentasikan semua yang berpotensial menjadi barang bukti digital. Proses identifikasi yang dilakukan seperti mengenali informasi *digital storage media* dan *processing devices* yang mengandung potensi barang bukti digital yang relevan terhadap kasus. Proses ini juga termasuk melakukan aktifitas untuk memberikan prioritas terhadap barang bukti yang dikumpulkan berdasarkan tingkat *volatility* atau tingkat barang bukti digital yang mudah rusak atau hilang. Data *volatility* atau data yang mudah rusak dan hilang harus diidentifikasikan untuk memastikan bahwa data tersebut mendapatkan prioritas utama dalam proses pengumpulan dan akusisi agar meminimalisir kerusakaan terhadap barang bukti digital yang berpotensi tersebut dan memastikan mendapatkan barang bukti yang terbaik.

#### 3.5.2 Pengumpulan

Dalam dokumen SNI ISO/IEC 27037:2014, Pengumpulan adalah proses penanganan barang bukti digital dimana peralatan yang diindikasikan menjadi barang bukti yang berpotensi, dipindahkan dari lokasi aslinya (TKP) ke laboratorium atau lokasi lain yang dapat dikontrol untuk kemudian akan diakusisi dan dianalisis, supaya barang bukti dari TKP dapat dipastikan aman. Peralatan yang ditemukan di TKP dan berpotensi menjadi barang bukti digital dibagi menjadi dua jenis yaitu  peralatan dalam keadaan hidup dan peralatan dalam

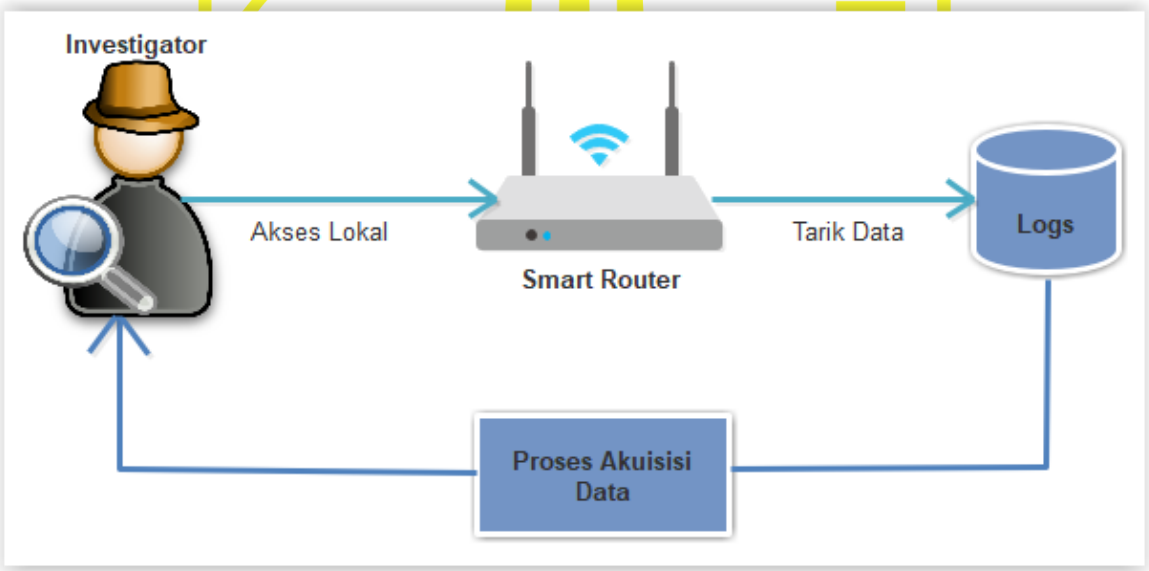
keadaan mati. Perbedaan kedua hal tersebut menjadi penting karena akan menentukan perbedaan tindakan yang harus dilakukan. Proses pengumpulan ini juga harus didokumentasikan dan juga proses ini termasuk mempaketkan atau membungkus barang bukti yang ditemukan ke dalam alat pembungkus barang bukti untuk kemudian dikirimkan ke laboratorium.

### 3.5.3 Akuisisi

Dalam dokumen SNI ISO/IEC 27037:2014, Akuisisi adalah sebuah proses untuk membuat salinan barang bukti digital dan mendokumentasikan metodologi yang digunakan serta aktifitas yang dilakukan. Dalam melakukan akuisisi harus memilih metode yang paling sesuai berdasarkan situasi, biaya dan waktu, dan mendokumentasikan keputusan yang dipilih untuk menggunakan metode tertentu dan *tool* yang sesuai. Tahap akuisisi pada penelitian ini dilakukan secara *live acquisition*, untuk model akuisisi pada *Smart Router* mengacu pada penelitian yang dilakukan oleh Dedi Hariyadi dan Abdul Rohman, yaitu dengan melakukan proses akuisisi secara langsung pada perangkat melalui jaringan komputer.

1. Akuisisi Data *Live Acquisition*

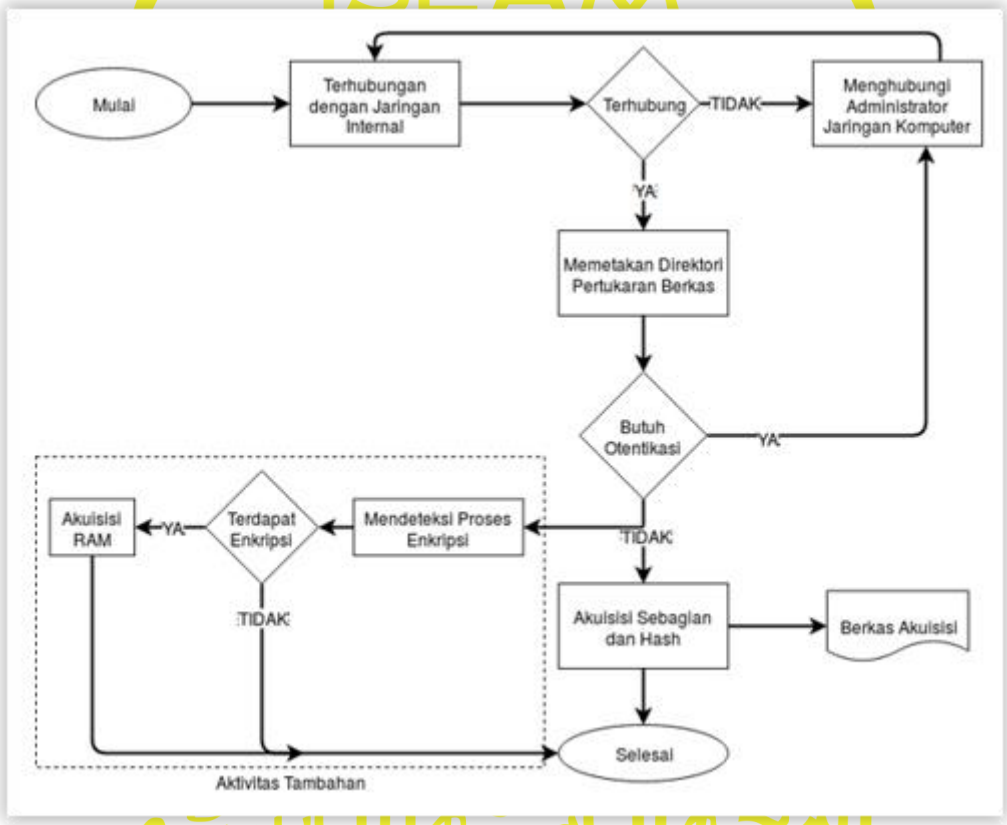
Kondisi utama yang harus dipenuhi dalam *live Acquisition* adalah kondisi dimana sistem sedang dalam keadaan beroperasi/*running* dikarenakan beberapa informasi jaringan pada router akan hilang jika sistem dimatikan ataupun dilakukan *reboot*. Oleh karena itu, pengambilan data pada router perlu dilakukan sesegera mungkin. Untuk mekanisme akuisisi data secara *live Acquisition* dapat dilihat pada Gambar 3.4




Gambar 3.4 Mekanisme Investigasi *Live Acquisition*

2. Akuisisi secara langsung pada *Smart Router* melalui jaringan

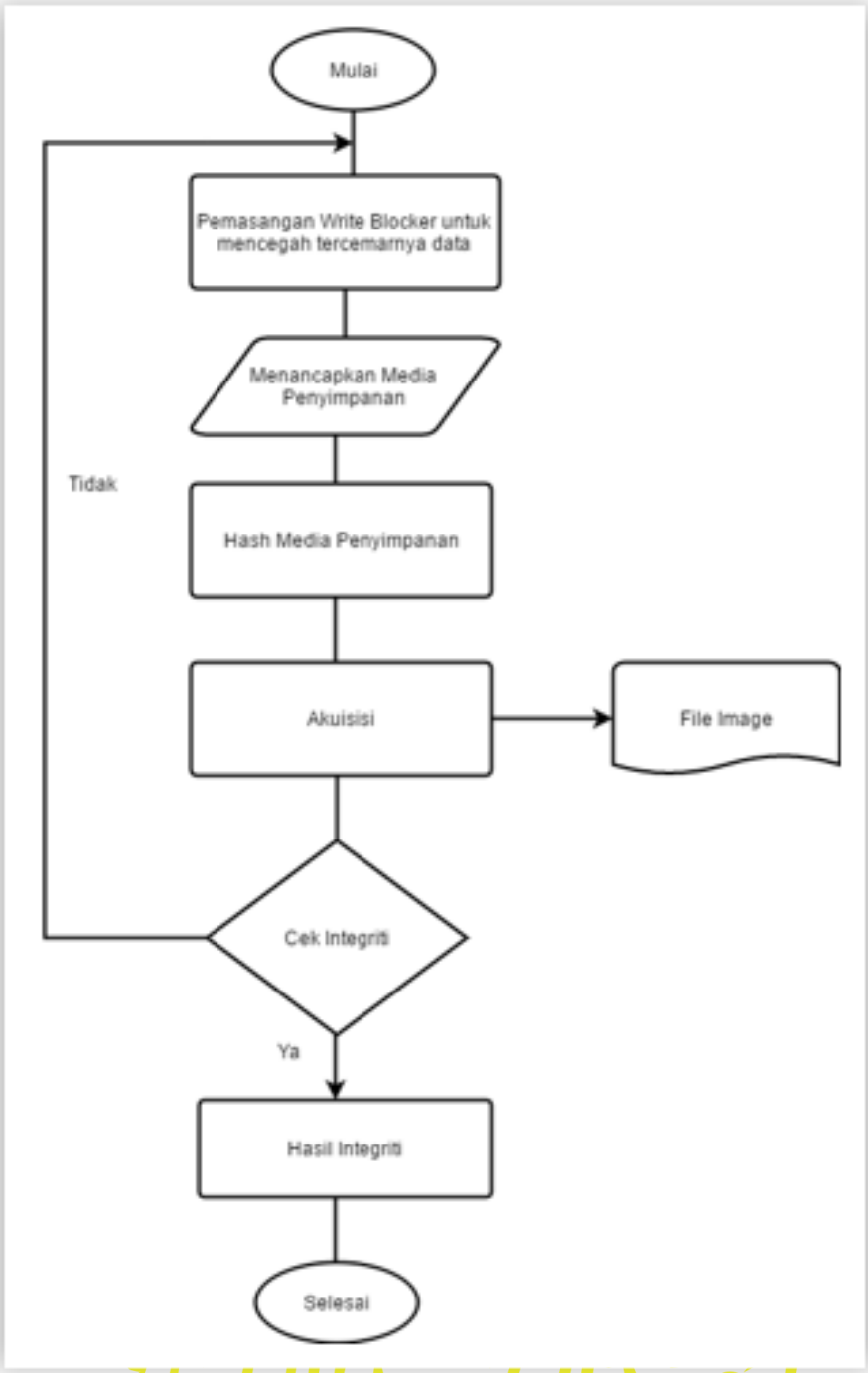
Dalam melakukan akuisisi secara langsung pada *Smart Router* diperlukan sebuah media penyimpanan eksternal yang steril dan tidak mudah terkontaminasi. Proses akuisisi fokus pada *log* dari *Smart Router* yang dihasilkan dari layanan Samba dan direktori pertukaran berkas. Ada beberapa berkas yang dihasilkan seperti *log* layanan Samba, direktori pertukaran berkas, dan berkas yang berisi nilai *hash* dari kedua berkas tersebut. Untuk beberapa kasus tertentu misalkan adanya proses enkripsi maka dilakukan akuisisi data *volatile* karena ada peroses sistem operasi dan enkripsi yang tercatat di RAM. Untuk proses akuisisi perangkat Router melalui jaringan dapat dilihat pada Gambar 3.5




Gambar 3.5 Akuisisi Perangkat Router Melalui Jaringan

3. Akuisisi *storage* (*USB Thumb Drive*)

Dalam proses akuisisi *storage* dilakukan dengan menggunakan *tools* FTK Imager, yaitu dengan menduplikasi *bit-for-bit* atau *bit-stream copy* sehingga hasil imaging akan sama persis dengan barang bukti. Hasil yang didapat dari proses akuisisi berupa *file image* dengan format **.dd**. File *image* yang telah berhasil didapatkan kemudian harus diverifikasi dengan menggunakan fungsi "*hash*" seperti **SHA-1** atau **MD5**. Hal ini dilakukan untuk menguji keaslian dari hasil file *image* yang didapatkan sama dengan data aslinya, secara umum alur dari proses akuisisi *storage* dapat dilihat pada Gambar 3.6




Gambar 3.6 Akuisisi pada *Storage* (*USB Thumb Drive*)

4. Akuisisi *Log File*

*Log file* merupakan file yang berisi aktivitas yang terjadi pada sebuah komputer. *Log file* tersimpan pada direktori tertentu pada sebuah sistem operasi. Pada tahap ini *log file* diambil secara langsung atau *live acquisition*, mengingat bahwa ada beberapa tipikal dari sistem operasi yang mengharuskan untuk mengakuisisi *log file* secara langsung atau *live acquisition*, mengingat bahwa *log file* akan hilang atau terhapus ketika perangkat elektronik tersebut tidak menyala/mati (*off*). File *log* yang diperoleh dari hasil akuisisi disimpan dan

dilakukan teknik kompresi file dan dilakukan verifikasi *hashing* supaya meminimalisir adanya perubahan yang terjadi pada file *log* tersebut dan kemudian disimpan pada *USB Thumbdrive* tersendiri.

### 3.5.4 Preservasi

Dalam dokumen SNI ISO/IEC 27037:2014, Preservasi adalah proses untuk melakukan pengamanan terhadap barang bukti digital yang potensial dan perangkat digital yang memuat barang bukti digital yang juga berpotensial dari kerusakan dan hal-hal yang menyebabkan barang bukti tersebut bisa hilang. Proses preservasi harus dimulai dan dilakukan diseluruh proses penanganan barang bukti digital, yang dimulai dari proses identifikasi perangkat digital yang memuat barang bukti digital yang potensial.

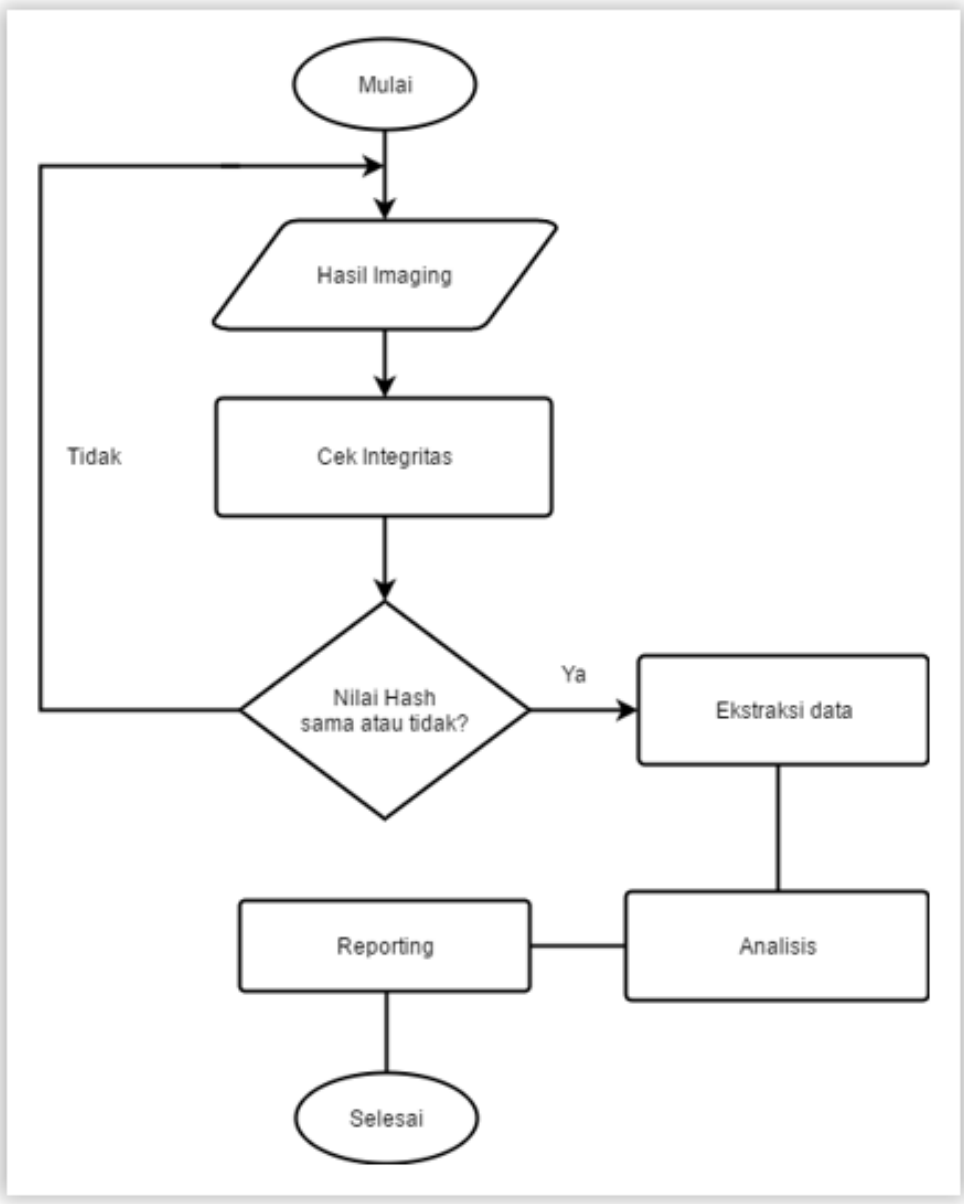
## 3.6 Analisis Forensik

Analisis merupakan tahap untuk mendapatkan berbagai informasi yang dibutuhkan untuk memecahkan kasus. Analisis dilakukan dengan menggunakan bantuan *tools* – *tools* forensik. Analisis terhadap *log* pertama kali dilakukan untuk melihat aktivitas-aktivitas yang terjadi pada sistem/*server*, seperti diketahuinya aktivitas yang terjadi pada sebuah komputer yang dilakukan oleh klien terkait kejanggalan yang terjadi pada sistem tersebut. Setelah mendapatkan hasil analisa dari file *log*, dapat diketahui dari mana kejahatan yang terjadi berasal. Jika asal kejahatan sudah bisa diketahui, maka proses analisa dapat mengerucut kepada dua file hasil *imaging* yaitu, file *image* media penyimpanan yang dijadikan sebagai *file sharing* pada *server* dan file *image* dari komputer klien sebagai pelaku kejahatan.

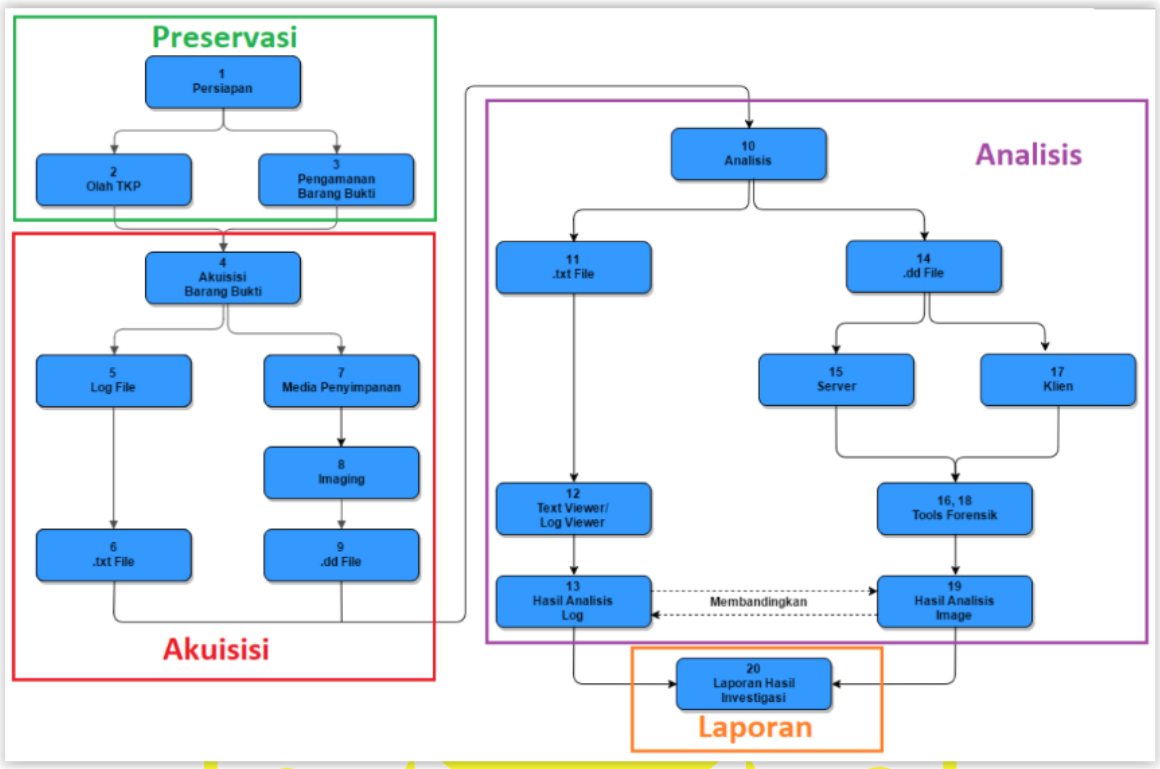
Adapun analisa forensik yang lain, seperti menganalisa ***dd file***, dimana "***dd file***" merupakan file hasil dari proses *imaging* media penyimpanan yang telah diakuisisi secara *pysical device*. Analisa ***dd file*** ini berfungsi untuk mengetahui file-file apa saja yang tersimpan di dalam media penyimpanan yang dijadikan sebagai direkttori *file sharing*, adapun jenis file yang diperoleh seperti file – file yang sudah terhapus, ataupun file yang sudah termodifikasi berdasarkan *timestamp*-nya. Hasil analisa yang didapat pada proses analisa *log file* dicocokkan dengan hasil pada proses analisa media penyimpanan milik *server*. Selain dicocokkan dengan hasil analisa media penyimpanan *server*, hasil analisa file *log* juga dicocokkan dengan hasil analisa media penyimpanan klien.

Komponen-komponen tersebut merupakan informasi yang dapat digabungkan untuk bisa menjawab kebutuhan informasi terkait dari mana sumber tindak kejahatan, dan waktu kejadian kejahatan. Adapun alur kerja forensik secara umum yang dilakukan pada penelitian

ini dapat dilihat pada Gambar 3.7, sedangkan untuk alur dari proses investigasi forensik dengan mengadopsi dari Bagan Proses Investigasi Forensik pada Protokol SMB hasil dari penelitian dengan judul “Teknik Eksplorasi Bukti Digital Pada *File Sharing* Protokol SMB Untuk Mendukung Forensika Digital Pada Jaringan Komputer” (Yudha & Prayudi, 2013). Berdasarkan bagan tersebut, maka untuk alur dari investigasi forensik dapat ditunjukan pada Gambar 3.8.




Gambar 3.7 Alur kerja Forensik




Gambar 3.8 Alur Proses Investigasi Forensik

Berdasarkan dokumen SNI ISO/IEC 27037:2014, untuk tahap preservasi pada alur investigasi penelitian ini dilakukan pada proses (1,2)Persiapan Olah TKP dan (1,3)Persiapan Pengamanan Barang Bukti; untuk tahap akuisisi dilakukan pada proses (4,5)Akuisisi *Log* File berupa (4,5,6)file ekstensi **.txt** dan (4,7)Akuisisi Media Penyimpanan dengan melakukan proses (4,7,8)*Imaging* berupa (4,7,8,9)file ekstensi **.dd**; pada tahap analisis dilakukan pada proses (10,11,12)Analisis file ***log.txt*** dan (10,14,15,16)Analisis file barang bukti media penyimpanan pada file **.dd** *server*, dan (10,14,17,18)Analisis file barang bukti media peyimpanan pada file **.dd** klien; tahap berikutnya melakukan (13,19)perbandingan atau membandingkan hasil analisa pada file ***log.txt*** dengan file hasil analisa media penyimpanan; untuk tahap terakhir melakukan proses (20)Pelaporan.

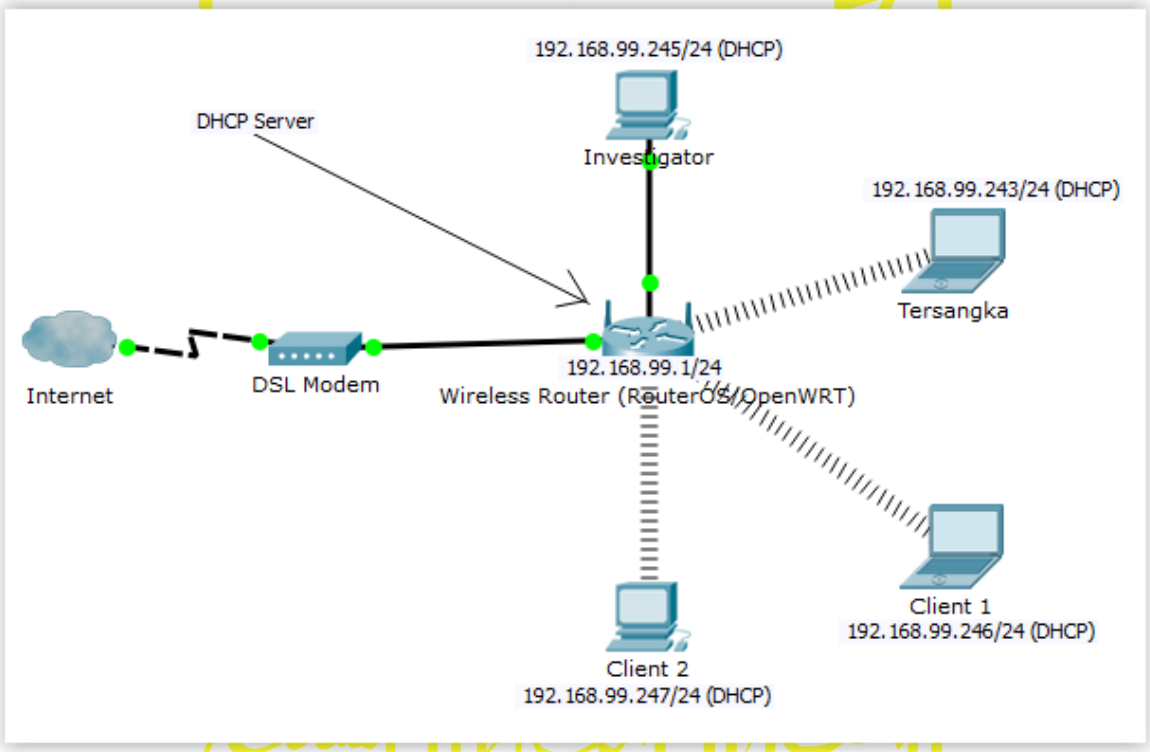
## 3.7 Laporan

Laporan hasil investigasi merupakan bentuk tertulis dari keseluruhan proses analisis yang dilakukan dan juga berisi temuan-temuan dari proses analisis. Segala aktivitias terkait penemuan barang bukti harus didokumentasikan. Dan dokumentasi disini juga mencakup keseluruhan aspek proses yang dilakukan mulai tahapan identifikasi sampai tahapan akhir investigasi yang harus selalu didokumentasikan. Dokumentasi dilakukan untuk menjaga integritas barang bukti.

# BAB 4
# Hasil dan Pembahasan

## 4.1 Hasil Rancangan / Desain

Pada bagian ini dijelaskan tahapan persiapan dalam implementasi topologi yang akan digunakan pada skenario dan simulasi akuisisi. Perancangan topologi dilakukan dengan menggunakan aplikasi *Cisco Packet Tracer*. Aplikasi ini memiliki kemampuan untuk melakukan simulasi jaringan terhadap rancangan topologi. Manfaat dari perancangan dengan aplikasi ini adalah untuk mengetahui apakah rancangan yang telah dibangun dapat terkoneksi secara *logical* dan terhubung antara satu sama lain.




Gambar 4.1 Rancangan Topologi Jaringan dengan Packet Tracer

Topologi yang dirancang pada Gambar 4.1 sudah berhasil terhubung secara *logical* antara komponen yang digunakan terbukti dengan adanya warna hijau antar *node* yang dihubungkan. Komponen yang digunakan terdiri dari *Cloud(internet), Modem, Router Wireless Access Point* dengan *IP Address* 192.168.99.1/24, PC Investigator dengan *IP Addess* 192.168.99.245/24, Laptop Tersangka dengan *IP Address* 192.168.99.243/24, Laptop *Client* 1 dengan *IP Address* 192.168.99.246/24, dan PC *Client* 2 dengan *IP Address* 192.168.99.247/24.

## 4.2 Data

Data yang dipakai dalam simulasi skenario merupakan data data digital, seperti:

1. File gambar
2. File dokumen dengan autentikasi password
3. File MP3
4. File *Crack* Sistem Operasi
5. File Aplikasi yang telah di-*Crack*

## 4.3 Skenario

Pada bagian ini dilakukan penerapan skenario yang telah dirancang pada Bab 3 dan pada tahapan Persiapan. Skenario yang dilakukan seperti penerapan topologi jaringan, adapun penerapan uji coba aktivitas pada jaringan dalam pemanfaatan *smart router* sebagai *file sharing* dengan fasilitas protokol SMB dilakukan pada tahap simulasi kasus, serta penerapan *log* akuisisi yang ada pada perangkat *smart router* dilakukan pada tahap simulasi investigasi perangkat.

Penerapan topologi jaringan menggunakan topologi yang umum digunakan, yaitu topologi jaringan hirarki. Terdapat dua perangkat yang dijadikan objek pada penelitian ini, yaitu *smart router* GL-inet AR300, dimana perangkat ini memiliki 1 *port WAN* dan 4 *port LAN*, 2 *port USB*. Serta perangkat *smart router* MikroTik RB951Ui-2HnD, perangkat ini memiliki 5 *port LAN*, dan 1 *port USB*. Dua perangkat ini selain dapat dijadikan sebagai *wireless router access point* juga dapat berfungsi sebagai *media file sharing*, dengan cara menambahkan media penyimpanan seperti *USB Thumbdrive*. Perangkat fisik yang digunakan ditunjukan pada Gambar 4.2.




Gambar 4.2 Perangkat *Smart Router* (kiri GL-inet AR300, kanan MikroTik RB951Ui-2HnD)

## 4.4 Simulasi Kasus

Simulasi dilakukan dengan menerapkan skenario yang sudah dibuat yaitu dengan adanya aktivitas pada jaringan. Skenario yang dibuat berawal dari adanya pelaporan dari pelapor, bahwa ada indikasi perubahan data atau file yang terdapat pada media penyimpanan *file sharing*. Terdapat beberapa file yang hilang atau terhapus oleh klien yang terhubung dalam jaringan lokal. Media *file sharing* tersebut terdapat di dalam perangkat *smart router*, dimana perangkat *smart router* tersebut selain dapat dijadikan sebagai *wireless access point* juga dapat berfungsi sebagai media *file sharing* dengan aplikasi Samba. Berdasarkan skenario ada beberapa aktivitas terkait pemanfaatan *file sharing* dengan menggunakan aplikasi Samba, dan untuk mendapatkan bukti digital pada *log system* dan *log Samba*, maka diberi aksi sebagai berikut:

1. Aktivitas pengunduhan file dari *server*
2. Aktivitas penyimpanan file ke *server*
3. Aktivitas perubahan file pada *server*
4. Aktivitas penghapusan file pada *server*
5. Aktivitas menghilangkan bukti digital dari media penyimpanan

## 4.5 Investigasi dan Olah TKP

Berdasarkan pada dokumen pada SNI ISO/IEC 27037:2014, tahapan dalam proses investigasi dan Olah TKP yang dilakukan pertama kali adalah proses identifikasi. Sesuai dengan dokumen SNI ISO/IEC 27037:2014 tentang tahapan identifikasi, pada bagian 6.2.1 yaitu mengenai pengamanan TKP. Pengamanan TKP dilakukan untuk melindungi barang bukti. Pada tahap identifikasi juga dilakukan pencarian barang bukti, dalam hal ini berdasarkan dokumen SNI ISO/IEC 27037:2014 bagian 5.4.2. Pada tahap identifikasi juga dilakukan pencatatan barang bukti (*Chain of custody*).

### 4.5.1 Pengamanan Barang Bukti

Barang bukti yang didapatkan diamankan dari kontaminasi data sebelum dilakukan akuisisi. Terdapat beberapa barang bukti elektronik diantaranya Perangkat *Smart Router*, *USB Thumbdrive*, dimana untuk barang bukti perangkat *Smart Router* didapatkan masih dalam kondisi menyala (*on*) dengan bukti elektonik berupa media penyimpanan *USB Thumbdrive* yang masih menancap pada perangkat *Smart Router*. Dalam simulasi kasus ini terdapat dua perangkat router yang dijadikan objek penelitian, diantaranya: perangkat router GL-inet AR300 dan perangkat router MikroTik RB951Ui-2HnD.

Kondisi perangkat GL-inet AR300 pada saat ditemukan, dimana perangkat ini memiliki 1 *port WAN* dan *4 port LAN*, 2 *port USB*, pada waktu ditemukan *USB Thumbdrive* dengan kondisi merek yang sudah tidak bisa terbaca menamcap pada salah satu *port USB* (USB 1), diasumsikan *USB Thumbdrive* tersebut dijadikan sebagai media penyimpanan *file sharing*, dan terdapat kabel *UTP* yang menancap pada *port LAN* (*LAN* 2), serta lampu indikator seperti indikator *LAN*, *WAN*, dan *POWER* dalam keadaan menyala, dari indikator tersebut menandakan bahwa baik perangkat (router) maupun fitur koneksi *LAN* dan koneksi *WAN* dalam keadaan normal.

Sedangkan kondisi perangkat MikroTik RB951Ui-2HnD pada saat ditemukan, dimana perangkat ini memiliki 5 *port LAN*, dan 1 *port USB*, dengan *USB Thumbdrive* sudah tidak terbaca mereknya menancap pada *port USB* diasumsikan *USB Thumbdrive* tersebut dijadikan sebagai media penyimpanan *file sharing*, dan terdapat kabel *UTP* yang menancap pada salah satu *port LAN* (*LAN* 2), serta lampu indikator *LAN*, *WAN*, dan *POWER* dalam keadaan menyala, dari indikator lampu tersebut menandakan bakwa perangkat tersebut dalam keadaan normal, baik untuk koneksi *LAN*, koneksi *WAN*, maupun kondisi dari perangkat itu sendiri. Berikut ini adalah gambar dari barang bukti elektronik yang ditunjukan pada Gambar 4.3.




Gambar 4.3 Barang Bukti Elektonik

### 4.5.2 Akuisisi Barang Bukti

Sesuai dengan SOP pada SNI ISO/IEC 27037:2014 pada bagian ke 6.8 dan 7.1.1.3 terkait barang bukti yang menjadi prioritas dan yang akan disita atau diakuisisi, berdasarkan kondisi barang bukti elektronik pada saat ditemukan masih dalam keadaan menyala (*on*), maka dalam proses akuisisi pada barang bukti router dilakukan secara langsung (*live acquisition*).

Dalam kasus yang terjadi barang bukti elektronik berupa perangkat *router board portable*, dimana perangkat tersebut tidak terdapatnya monitor yang dapat digunakan untuk melihat proses yang sedang berjalan.

Oleh karena itu, maka dibutuhkan perangkat komputer untuk mengakses atau me-*remote* guna melihat *log* dari aktivitas yang ada pada perangkat tersebut yang terhubung ke dalam jaringannya. Prosedur akuisisi bukti elektronik yang masih dalam kondisi menyala dan dilakukan akuisisi melalui jaringan, berdasarkan acuan seperti pada Gambar 3.5. Berikut ini merupakan perangkat komputer yang dipakai untuk mengakses perangkat router, yang ditunjukan pada Gambar 4.4. Perangkat komputer ini merupakan perangkat yang dijadikan sebagai komputer investigator.



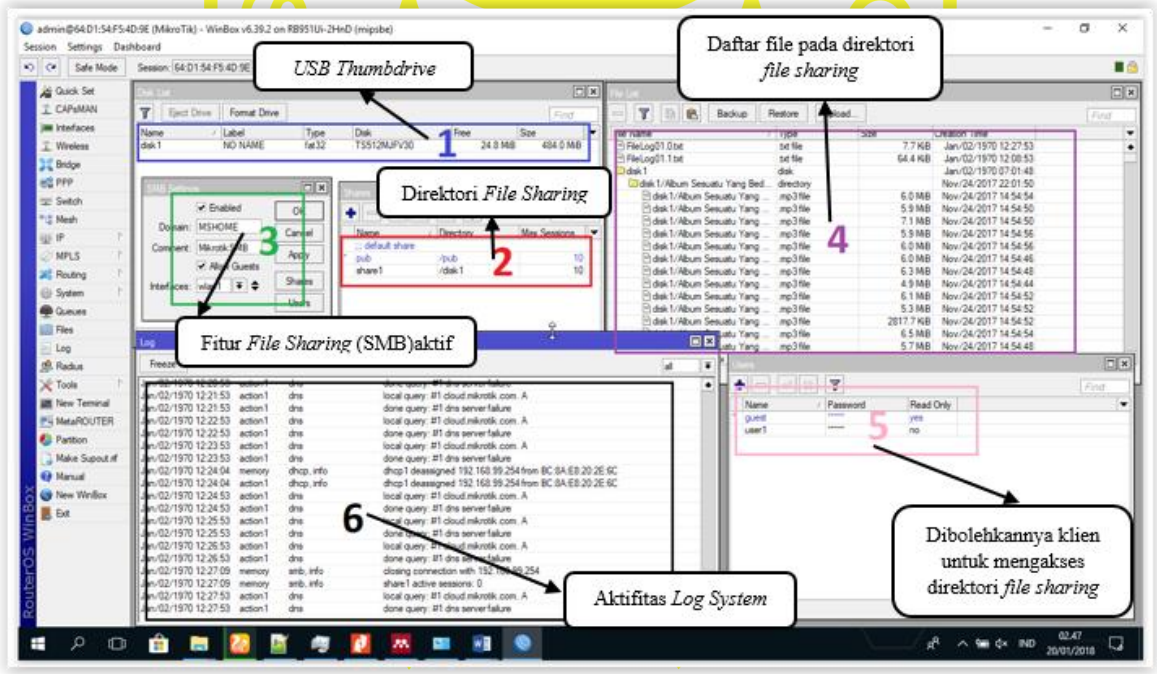

Gambar 4.4 Perangkat Komputer Akuisisi Barang Bukti

**1. *Live Forensics* pada Perangkat *Smart Router* MikroTik RB951Ui-2HnD**

Adapun proses akuisisi barang bukti dilakukan secara langsung melalui koneksi jaringan atau *remote access*, bukan dilakukan akuisisi langsung pada perangkat router tersebut, dikarenakan barang bukti elektronik tidak memiliki monitor yang dapat dijadikan media atau fasilitas untuk dapat melihat proses apa saja yang sedang dijalankan. Berdasarkan pada SNI ISO/IEC 27037:2014 ketika ditemukannya kondisi barang bukti yang dalam keadaan

menyala, maka perlu dicatat semua proses atau beberapa proses program aplikasi atau *service* yang sedang berjalan dan yang diindikasikan berpotensi sebagai barang bukti digital.

Berikut gambaran dari beberapa proses yang sedang berjalan pada perangkat router terkait pemanfaatan *file sharing*, bahwa perangkat router dilakukan proses *live forensics* dengan cara investigator mengakses perangkat router menggunakan *tool* Winbox. Untuk tampilan proses yang sedang berjalan dapat dilihat pada Gambar 4.5, dimana pada gambar tersebut terlihat ada beberapa fitur yang dapat menjadi bahan acuan terkait penggunaan *Smart Router* sebagai *file sharing*, pada gambar terlihat adanya media penyimpanan *USB Thumbdrive* dengan kapasitas penyimpanan 484 MB dengan tipe *file system* FAT32 yang ditandai dengan nomor 1 dan nomor 2, dan terdapat beberapa file di dalamnya yang ditandai dengan nomor 4; *USB Thumbdrive* tersebut dapat diakses oleh klien yang ditandai dengan nomor 5, yang dapat diakses dengan menggunakan koneksi *WiFi* (`wlan1`) yang ditandai dengan nomor 3; serta adanya beberapa *log* yang tercatat dengan beberapa *ip address* klien yang mengakses direktori *file sharing* yang ditandai dengan nomor 6.




Gambar 4.5 Tampilan Proses pada MikroTik

## 2. *Live Forensics* pada Perangkat *Smart Router* GL-inet AR300

Pada tahap akuisisi barang bukti elektronik dengan kasus perangkat router GL-inet AR300 yang dijadikan barang bukti elektronik juga sama penanganannya, bahwa perangkat yang tidak terdapatnya akses monitor, maka dilakukan *remote access* melalui jaringan. Adapun gambaran dari proses yang sedang berjalan pada perangkat router GL-inet AR300 yang diakses dari perangkat komputer investigator menggunakan *browser*, untuk tampilan proses

yang sedang berjalan dapat dilihat pada Gambar 4.6. Dimana pada gambar tersebut terlihat ada beberapa fitur yang dapat menjadi bahan acuan terkait penggunaan *smart router* sebagai *file sharing*, pada gambar yang ditandai dengan nomor 1 terlihat adanya info seperti *firmware*, *MAC Address*, model, dan beberapa fitur lainnya; terlihat ada beberapa klien yang terkoneksi dengan perangkat tersebut dengan pengaturan *IP Address* secara *DHCP* terlihat pada gambar yang diberi nomor 2; terlihat pada gambar juga aktifnya akses *WAN* dengan menggunakan *port* 83 terlihat pada gambar yang diberi nomor 3; pada gambar terlihat adanya media penyimpanan *USB Thumbdrive* dengan kapasitas penyimpanan 3.73 GB yang ditunjukan dengan nomor 5a; dengan aktif direktori *writable* dan dapat diakses menggunakan jaringan *LAN* dan *WAN*, yang ditandai dengan nomor 4; dimana *USB Thumbdrive* tersebut terdapat beberapa file di dalamnya terlihat pada gambar yang ditandai dengan nomor 5b, 5c.

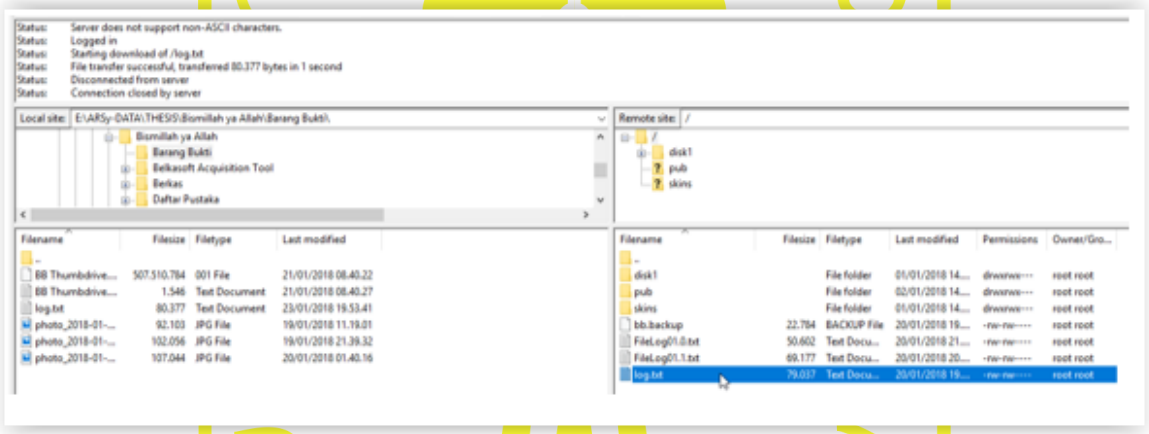
Tampilan yang didapat pada perangkat router GL-inet AR300 jauh lebih sederhana dibandingkan dengan perangkat router MikroTik RB951Ui-2HnD, pada perangkat GL-inet AR300 tidak ditampilkannya menu atau fitur untuk mengakses *Log system*. Oleh karena itu, investigator harus mengakses direktori "*root*" untuk dapat menemukan atau melihat *log system* yang berjalan.




Gambar 4.6 Tampilan Proses pada GL-inet

### 3. *Live Acquisitions Log System* pada MikroTik RB951Ui-2HnD

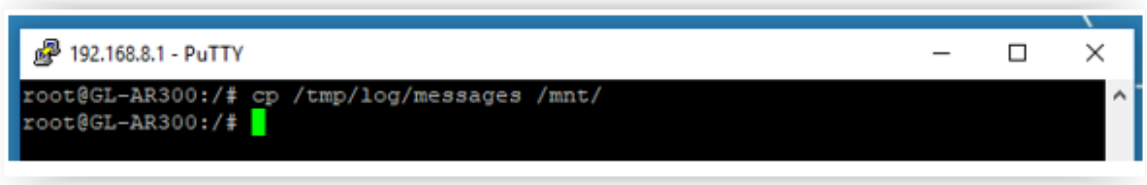
Dalam kasus dengan barang bukti elektronik yang masih dalam keadaan menyala (*on*), maka sebagai investigator tidak diperkenankan untuk mematikan barang bukti elektronik tersebut. Dalam penelitian ini barang bukti elektronik berupa perangkat router, maka investigator dapat langsung melakukan akuisisi dengan mengakses langsung ke perangkat melalui jaringan. Ketika investigator telah melakukan proses identifikasi dengan menggunakan *live forensics*, maka langkah selanjutnya adalah melakukan *live acquisition* terkait aktivitas yang ada seperti melakukan akuisisi *log system* dan juga *log* samba. Adapun untuk mengakses perangkat router tersebut menggunakan koneksi FTP (*File Transfer Protocol*) untuk perangkat *smart router* MikroTik, dengan alasan untuk meminimalisir adanya tindakan atau akses yang dapat mempengaruhi kondisi dari barang bukti elektronik dan barang bukti digital. Gambaran proses akuisisi yang dilakukan menggunakan koneksi FTP *(File Transfer Protocol*) dapat dilihat pada Gambar 4.7.



Gambar 4.7 Akses File *Log* Menggunakan FTP

### 4. *Live Acquisitions Log System* pada GL-inet AR300

Sama halnya seperti yang dilakukan pada perangkat smart router MikroTik RB951Ui-2HnD, pada perangkat *smart router* GL-inet AR300 dalam mendapatkan aktivitas yang terjadi terkait kasus yang ada, maka untuk mendapatkan *log system* dan *log* samba dilakukan menggunakan *live acquisition* dengan cara melakukan proses copy paste file *log* tersebut. Koneksi yang digunakan untuk mengakses direktori "*root*" menggunakan akses koneksi SSH (*Secure Shell*). Gambaran proses akuisisi yang dilakukan menggunakan koneksi SSH (*Secure Shell*) dapat dilihat pada Gambar 4.8.

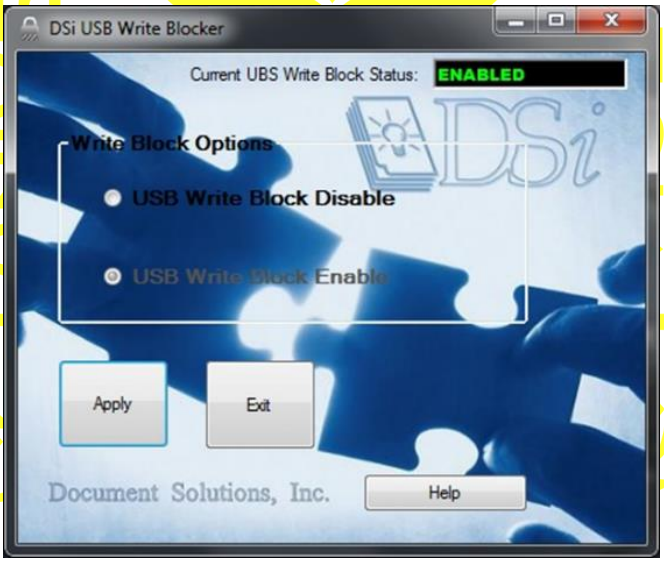



Gambar 4.8 Akses File *Log* Menggunakan SSH

Berdasarkan bukti digital yang didapat berupa perangkat elektronik *smart router*, dimana terdapat barang bukti elektronik berupa *USB Thumbdrive* yang diindikasi sebagai media penyimpanan *file sharing*, maka pada tahap akuisisi barang bukti juga dilakukan proses imagging pada bukti elektronik *USB Thumbdrive*.

**5. Akuisisi Barang Bukti Digital pada Media Penyimpanan (*USB Thumbdrive*)**

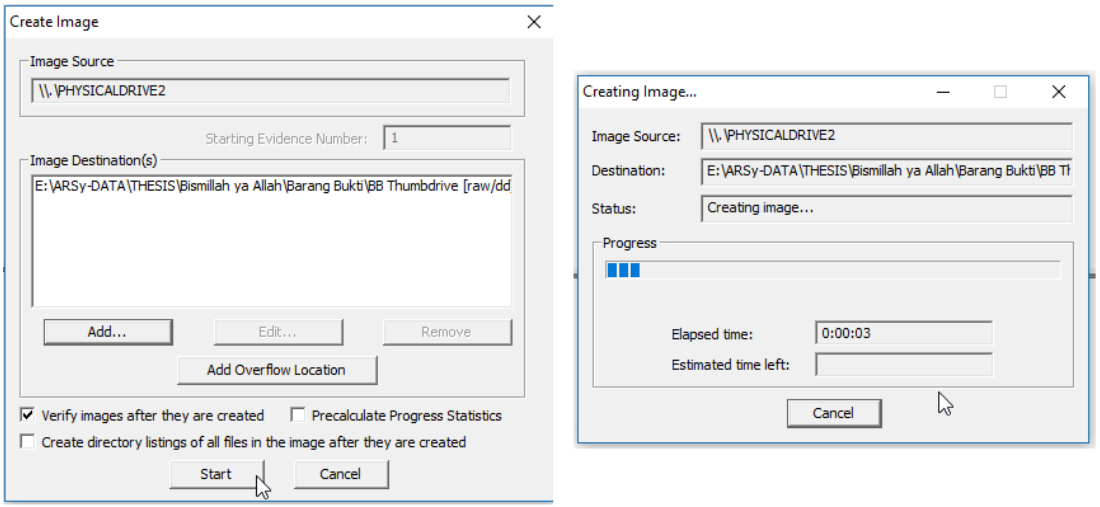
Proses akuisisi barang bukti elektronik berupa *USB Thumbdrive* berdasarkan alur pada proses akuisisi media penyimpanan dengan mengacu pada Gambar 3.6. Akuisisi barang bukti media penyimpanan dilakukan dengan melakukan proses *imaging* dengan menggunakan aplikasi FTK Imager yang berjalan pada sistem operasi windows pada komputer investigator, dan untuk menghindari kontaminasi barang bukti digital maka diperlukan *tools USB Write Blocker* seperti yang terlihat pada Gambar 4.9. Penggunaan *tools* ini dimaksudkan untuk mencegah terjadinya perubahan isi data.




Gambar 4.9 *USB Write Blocker*

Proses akuisisi pada media penyimpanan *USB Thumbdrive* dilakukan dengan cara *physical* (*sector per sector atau bit-stream copy*) sehingga hasil *imaging* akan sama persis dengan barang bukti secara *physical*. File hasil *imaging* disimpan dengan ekstensi **.dd**, untuk berikutnya dilakukan proses analisis. Informasi yang didapat dari proses *imaging* dicatat secara detail. Hal-hal yang perlu dicatat antara lain waktu memulai imaging dan mengakhiri

*imaging*, nilai *hash* file hasil *imaging*, dan besar file hasil *imaging*. Detail file hasil *imaging* dapat dilihat pada Tabel 4.1. Seluruh file yang sudah dilakukan *imaging* diuji keaslian file dengan menggunakan metode *hashing*. Metode *hashing* yang digunakan adalah MD5 dan SH1. Berikut proses akuisisi *USB Thumbdrive* yang diperlihatkan pada Gambar 4.10.




Gambar 4.10 Proses *Imaging* media penyimpanan *USB Thumbdrive* pada MikroTik

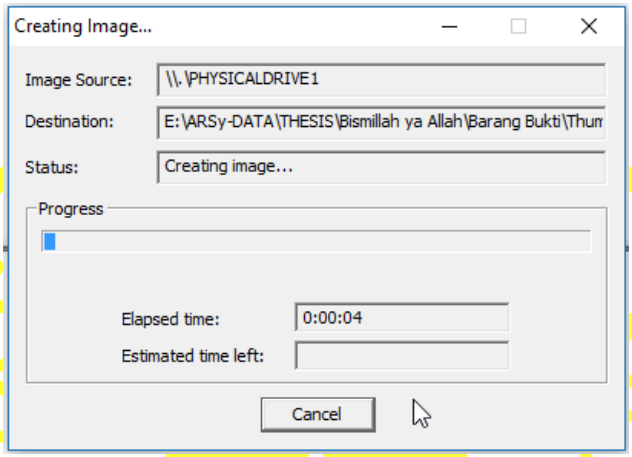
Tabel 4.1 Detail Akuisisi *USB Thumbdrive* MikroTik RB951Ui-2HnD

| **Case Information** | |
|---|---|
| Case Number | USB01 |
| Evidence Number | 06-02-2018 |
| Source Type | Physical Drive |
| Unique description | BB USB Thumbdrive MikroTik RB951Ui-2HnD |
| Examiner | Abdul Rohman |
| Drive Model | JetFlash TS512MJFV30 USB Device |
| Drive Serial Number | 5R0STVDH |
| Bytes per Sector | 512 |
| Sector Count | 991.232 |
| Source data size | 484 MB |
| Time Acquisition | Acquisition started: Tue Feb 06 13:09:28 2018 |
| | Acquisition finished: Tue Feb 06 13:10:10 2018 |
| Computed Hashes | MD5 checksum: b4e7eda5b8f64fced88882dc26ae4c49 |
| | SHA1 checksum: 0b95fb7c7d7f1b8eba2e5556974e86962c48f73e |
| Tools | AccessData® FTK® Imager 3.4.2.6 |
| Notes | BB USB Thumbdrive yang belum mengalami perubahan isi baik penambahan, pengurangan, atau manipulasi/modifikasi. |

Pada Tabel 4.1 tersebut dapat dilihat detail dari proses akuisisi yang dilakukan. File detail akuisisi *USB Thumbdrive* merupakan file hasil dari proses *imaging* media penyimpanan *USB Thumbdrive* yang dijadikan sebagai media penyimpanan pada layanan *file sharing* pada perangkat *smart router* MikroTik RB951Ui-2HnD.

Proses akuisisi pada media penyimpanan *USB Thumbdrive* pada perangkat *smart router* GL-inet AR300 juga dilakukan untuk mandapatkan file *image* yang nantinya

dilakukan analisa dengan menggunakan *tools* forensik. Detail informasi mengenai file hasil *imaging* dapat dilihat pada Tabel 4.2. Seluruh file yang sudah dilakukan *imaging* diuji keaslian file dengan menggunakan metode *hashing*. Metode *hashing* yang digunakan adalah MD5 dan SH1. Berikut proses akuisisi *USB Thumbdrive* yang diperlihatkan pada Gambar 4.11.




Gambar 4.11 Proses *Imaging* media penyimpanan *USB Thumbdrive* pada GL-inet

Tabel 4.2 Detail Akuisisi *USB Thumbdrive* GL-inet AR300

| **Case Information** | |
|---|---|
| Case Number | USB02 |
| Evidence Number | 06-02-2018 |
| Source Type | Physical Drive |
| Unique description | BB USB Thumbdrive GL-inet AR300 |
| Examiner | Abdul Rohman |
| Drive Model | General USB Flash Disk USB Device |
| Drive Serial Number | 0854000000009450 |
| Bytes per Sector | 512 |
| Sector Count | 7.831.552 |
| Source data size | 3824 MB |
| Time Acquisition | Acquisition started: Tue Feb 06 13:16:01 2018 |
| | Acquisition finished: Tue Feb 06 13:19:48 2018 |
| Computed Hashes | MD5 checksum: 96075a07d64dd2fe1b4a077507740337 |
| | SHA1 checksum: 327e8397d9a9645df21edf641be9ce64b4f9961b |
| Tools | AccessData® FTK® Imager 3.4.2.6 |
| Notes | BB USB Thumbdrive yang belum mengalami perubahan isi baik penambahan, pengurangan, atau manipulasi/modifikasi. |

## 4.6 Pengujian

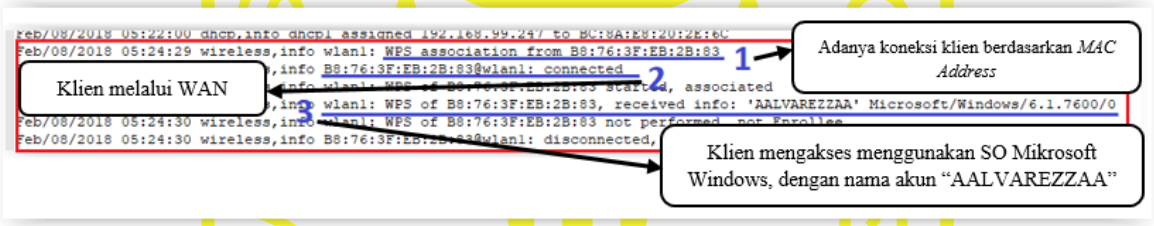
Pada tahap pengujian yang dilakukan pada penelitian ini, yaitu dengan melakukan pengujian terhadap aktivitas (*log*) yang terjadi pada perangkat *smart router* terkait pemanfaatan perangkat *smart router* yang dapat dijadikan sebagai media *file sharing*. Pengujian dilakukan berdasarkan skenario kasus, terdapat 2 (dua) skenario seperti yang sudah dipaparkan pada bab sebelumnya (BAB 3), pengujian juga dilakukan dengan membandingkan perangkat

*wireless access point* atau *smart wireless router* yang dapat difungsikan sebagai media *file sharing* terkait bagaimana mendapatkan file *log* yang ada pada perangkat tersebut, yang dapat dijadikan sebagai sumber informasi dalam proses investigasi.

Pengujian pertama dilakukan pada perangkat *smart router* MikroTik RB951Ui-2HnD, untuk pengujian berikutnya dilakukan pada perangkat *smart router* GL-inet AR300.

### 4.6.1 MikroTik RB951Ui-2HnD

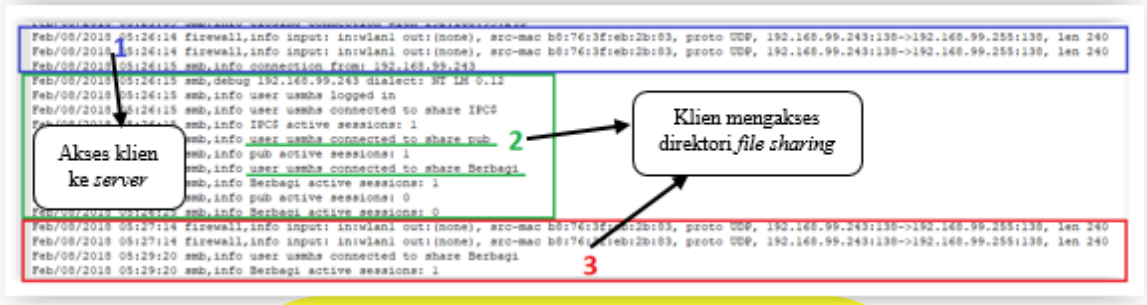
Dilakukan pengujian berdasarkan skenario 1 (satu), yaitu terdapatnya beberapa klien terhubung ke *server*, dan masing-masing dari klien melakukan aktivitas seperti biasa, yaitu dengan melihat atau mengakses beberapa direktori yang di-*share* oleh *server*, pada skenario ini terdapat klien yang mencoba melakukan aktivitas pengunduhan beberapa file dari *server*, kemudian klien mencoba untuk memutus hubungan atau memutus koneksi dengan *server*. Berikut ini tampilan *screen shot* dari aktivitas *log* yang tercatat pada *log system* perangkat *smart router* MikroTik RB951Ui-2HnD berdasarkan skenario 1 (satu), yang ditunjukan pada Gambar 4.12.



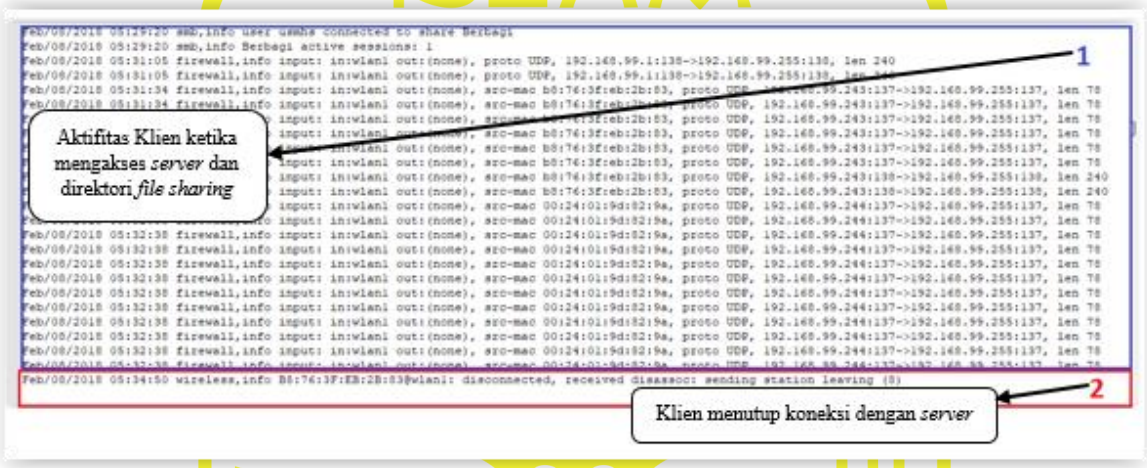

Gambar 4.12 Koneksi *client* ke *server*

Berdasarkan skenario yang telah dibuat, dimana ada beberapa aktivitas yang dilakukan oleh klien ketika mengakses *file sharing* yang ada pada *smart router*. Seperti pada skenario 1 (satu) maka aktivitas yang terjadi pada *log* seperti tampak pada Gambar 4.12 yaitu adanya aktivitas koneksi dari *client* ke *server* melalui koneksi *port wlan* pada router ditandai pada nomor 1 (satu), klien berhasil terhubung dengan *server*, dan didapat informasi *MAC Addess* dari klien yaitu **B8:76:3F:EB:2B:83** nampak klien menggunakan Sistem Operasi Windows dengan user akun '**AALVAREZZAA**', pada gambar ditandai dengan nomor 2,3 (dua,tiga). Pada Gambar 4.13 terlihat aktivitas yang dilakukan klien seperti mencoba melakukan akses terhadap *file sharing*, seperti pada gambar yang diberi tanda nomor 1 (satu) terlihat adanya pemakaian protokol UDP, klien mencoba untuk mengakses direktori *file sharing* sebagai *user* "**usmhs**", ada dua direktori yang disharing, yaitu "pub" dan direktori "Berbagi", pada gambar ditandai dengan nomor 2 (dua), klien terlihat mengakses salah satu file pada direktori *sharing*, pada gambar ditandai dengan nomor 3 (tiga). Pada Gambar 4.14 terlihat adanya aktivitas yang dilakukan klien seperti mengakses beberapa file yang ada pada direktori *file*

*sharing* yang diberi tanda 1 (satu), dan klien mencoba untuk memutus koneksi dari *server* yang ditandai dengan nomor 2 (dua).




Gambar 4.13 Aktivitas Klien




Gambar 4.14 Aktivitas *client* pada *File Sharing*

Pengujian berikutnya dilakukan berdasarkan skenario 2 (dua), yaitu: terdapatnya beberapa klien terhubung ke *server*, dan masing-masing dari klien melakukan aktivitas seperti biasa yaitu melihat atau mengakses beberapa direktori yang di-*share* oleh *server*. Pada skenario ini terdapat satu klien yang melakukan penambahan direktori pada *file sharing*, klien juga melakukan perubahan nama dari salah satu direktori yang tersimpan di *server*, klien tersebut melakukan penghapusan beberapa file yang terdapat pada media *file sharing* yang sebelumnya telah diunduh terlebih dahulu, kemudian klien mengakhiri atau memutus koneksi dari *server*. Dan untuk menghilangkan jejak klien melakukan penghapusan file yang telah didapat dari *server*, dengan menghapus file pada media penyimpanan klien. Berikut ini potongan tampilan *screen shot* dari aktivitas *log* yang tercatat pada *log system* perangkat *smart router* MikroTik RB951Ui-2HnD berdasarkan skenario 2 (dua), yang ditunjukan pada Gambar 4.15.




Gambar 4.15 Aktivitas *Log* pada *smart router* MikroTik RB951Ui-2HnD_skenario2

Pada tahap pengujian juga dilakukan pencatatan mengenai informasi dari hasil imaging pada media penyimpanan, baik media penyimpanan milik *server* maupun media penyimpanan milik klien. Adapun alur dari proses ini mengacu pada Gambar 3.8. Untuk detail hasil dari proses *imaging* untuk media penyimpanan milik *server* tampak seperti pada Tabel 4.3.

Tabel 4.3 Akuisisi *USB Thumbdrive* MikroTik RB951Ui-2HnD [skenario2]

| **Case Information** | |
|---|---|
| Case Number | USBSken02 |
| Evidence Number | 08-02-2018 |
| Source Type | Physical Drive |
| Unique description | BB USB Thumbdrive MikroTik RB951Ui-2HnD |
| Examiner | Abdul Rohman |
| Drive Model | JetFlash TS512MJFV30 USB Device |
| Drive Serial Number | 5R0STVDH |
| Bytes per Sector | 512 |
| Sector Count | 991.232 |
| Source data size | 484 MB |
| Segment | BB_USB_Thumbdrive_MikroTik_RB951Ui-2HnD.001 |
| Time Acquisition | Acquisition started: Thu Feb 08 22:57:37 2018 |
| | Acquisition finished: Thu Feb 08 22:58:19 2018 |
| Computed Hashes | MD5 checksum: 59ffded23f80a54a25ff3ac4feb5a262 |
| | SHA1 checksum: f2453da538802beb8bf4ad96d9a62c15793dccc2 |
| Tools | AccessData® FTK® Imager 3.4.2.6 |
| Notes | BB Thumbdrive yang digunakan untuk menyimpan *file sharing* pada server smart router untuk perangkat MikroTik RB951Ui-2HnD yang telah mengalami perubahan seperti pada skenario 2. |

Pada Tabel 4.3 diatas dapat dilihat detail dari proses akuisisi yang dilakukan. File **BB_USB_Thumbdrive_MikroTik_RB951Ui-2HnD.001** merupakan file hasil dari proses *imaging* media penyimpanan *server*. Media penyimpanan pada *server* berukuran 484 MB. Media penyimpanan *server* diakuisisi dalam waktu 82 detik. Metode *hashing* yang digunakan adalah MD5 dengan nilai *hash* **59ffded23f80a54a25ff3ac4feb5a262** dan SHA1 dengan nilai *hash* **f2453da538802beb8bf4ad96d9a62c15793dccc2**.

Media penyimpanan milik klien (tersangka) juga dilakukan proses akuisisi dengan dilakukannya *imaging*, untuk detail hasil dari *imaging* pada media penyimpanan klien (tersangka) dapat dilihat pada Tabel 4.4.

Tabel 4.4 Akuisisi Media Penyimpanan Klien(Tersangka) MikroTik [skenario2]

| **Case Information** | |
|---|---|
| Case Number | USBSken02 |
| Evidence Number | 08-02-2018 |
| Source Type | Physical Drive |
| Unique description | BB Media Penyimpanan Tersangka MikroTik RB951Ui-2HnD |
| Examiner | Abdul Rohman |
| Drive Model | SanDisk Cruzer Edge USB Device |
| Drive Serial Number | 4C530499930328123404 |
| Bytes per Sector | 512 |
| Sector Count | 61.489.152 |
| Source data size | 30024 MB |
| Segment | BB_Tersangka_Sken02_MikroTik_RB951Ui-2HnD.001 |
| Time Acquisition | Acquisition started: Thu Feb 08 23:20:44 2018 |
| | Acquisition finished: Thu Feb 08 23:29:50 2018 |
| Computed Hashes | MD5 checksum: b3eae18a9529324ed2b87c7ab16f543b |
| | SHA1 checksum: 8731b92f2a74f74955b2641e1706b492064b9713 |
| Tools | AccessData® FTK® Imager 3.4.2.6 |
| Notes | BB Media Penyimpanan yang digunakan untuk menyimpan file hasil download dari server pada skenario 2 untuk perangkat MikroTik RB951Ui-2HnD |

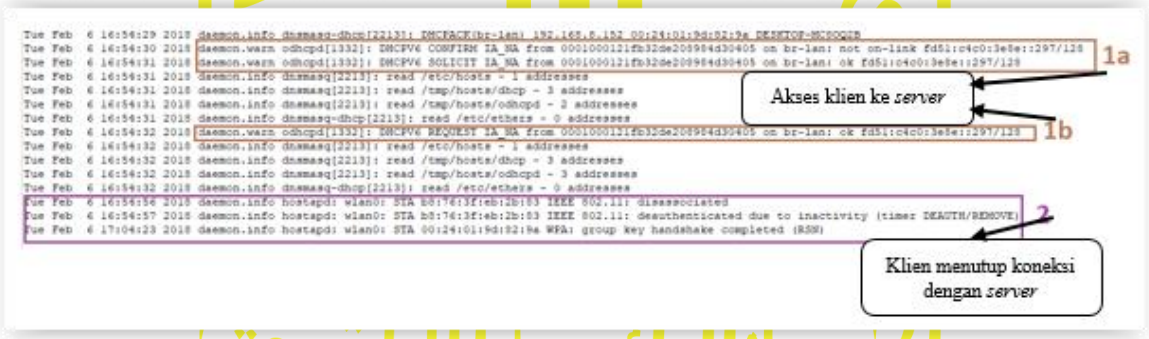
Pada Tabel 4.4 diatas dapat dilihat detail dari proses akuisisi yang dilakukan. File **BB_Tersangka_Sken02_MikroTik_RB951Ui-2HnD.001** merupakan file hasil dari proses *imaging* media penyimpanan milik klien(tersangka). Media penyimpanan pada klien berukuran 30024 MB. Media penyimpanan milik klien diakuisisi dalam waktu 9 menit 16 detik. Metode *hashing* yang digunakan adalah MD5 dengan nilai *hash* **b3eae18a9529324ed2b87c7ab16f543b** dan SHA1 dengan nilai *hash* **8731b92f2a74f74955b2641e1706b492064b9713**.

### 4.6.2 GL-inet AR300

Pada perangkat GL-inet juga dilakukan pengujian berdasarkan skenario 1 (satu), yaitu terdapatnya beberapa klien terhubung ke *server*, dan masing-masing dari klien melakukan aktivitas seperti biasa, yaitu dengan melihat atau mengakses beberapa direktori yang di-*share* oleh *server*, pada skenario ini terdapat klien yang mencoba melakukan aktivitas pengunduhan beberapa file dari *server*, kemudian klien mencoba untuk memutus hubungan atau memutus koneksi dengan *server*. Berikut ini potongan tampilan *screen shot* dari aktivitas *log* yang tercatat pada *log system* perangkat *smart router* GL-inet AR300 berdasarkan skenario 1 (satu), yang ditunjukan pada Gambar 4.16, dan pada Gambar 4.17.




Gambar 4.16 a. Aktivitas *Log* pada *smart router* GL-inet AR300_skenario1




Gambar 4.17 b. Aktivitas *Log* pada *smart router* GL-inet AR300_skenario1

Pengujian berikutnya dilakukan berdasarkan skenario 2 (dua), yaitu: terdapatnya beberapa klien terhubung ke *server*, dan masing-masing dari klien melakukan aktivitas seperti biasa yaitu melihat atau mengakses beberapa direktori yang di-*share* oleh *server*. Pada skenario ini terdapat satu klien yang melakukan penambahan direktori pada *file sharing*, klien juga melakukan perubahan nama dari salah satu direktori yang tersimpan di *server*, klien tersebut melakukan penghapusan beberapa file yang terdapat pada media *file sharing* yang sebelumnya telah diunduh terlebih dahulu, kemudian klien mengakhiri atau

memutus koneksi dari *server*. Dan untuk menghilangkan jejak klien melakukan penghapusan file yang telah didapat dari *server*, dengan menghapus file pada media penyimpanan klien. Berikut ini potongan tampilan *screen shot* dari aktivitas *log* yang tercatat pada *log system* perangkat *smart router* GL-inet AR300 berdasarkan skenario 2 (dua), yang ditunjukan pada Gambar 4.18.




Gambar 4.18 Aktivitas *Log* pada *smart router* GL-inet AR300_skenario2

Pada tahap pengujian juga dilakukan pencatatan mengenai informasi dari hasil *imaging* pada media penyimpanan, baik media penyimpanan milik *server* maupun media penyimpanan milik klien. Adapun alur dari proses ini mengacu pada Gambar 3.8. Untuk detail hasil dari proses *imaging* untuk media penyimpanan milik *server* tampak seperti pada Tabel 4.5.

Tabel 4.5 Akuisisi *USB Thumbdrive* GL-inet AR300 [skenario2]

| **Case Information** | |
|---|---|
| Case Number | USBSken02 |
| Evidence Number | 08-02-2018 |
| Source Type | Physical Drive |
| Unique description | BB USB Thumbdrive GL-inet AR300 |
| Examiner | Abdul Rohman |
| Drive Model | General USB Flash Disk USB Device |
| Drive Serial Number | 0854000000009450 |

| **Case Information** | |
|---|---|
| Bytes per Sector | 512 |
| Sector Count | 7.831.552 |
| Source data size | 3824 MB |
| Segment | BB_USB_Thumbdrive_GL-inet_AR300.001 |
| Time Acquisition | Acquisition started: Thu Feb 08 06:26:36 2018 |
| | Acquisition finished: Thu Feb 08 06:30:36 2018 |
| Computed Hashes | MD5 checksum: 3a3901569cb3331478070ca178e6800a |
| | SHA1 checksum: cd4a4038af7619cfabac7cf13bd8c5dc84a6752c |
| Tools | AccessData® FTK® Imager 3.4.2.6 |
| Notes | BB Thumbdrive yang digunakan untuk menyimpan *file sharing* pada server smart router untuk perangkat GL-inet AR300 yang telah mengalami perubahan seperti pada skenario 2. |

Pada Tabel 4.5 diatas dapat dilihat detail dari proses akuisisi yang dilakukan. File **BB_USB_Thumbdrive_GL-inet_AR300.001** merupakan file hasil dari proses *imaging* media penyimpanan *server*. Media penyimpanan pada *server* berukuran 3824 MB. Media penyimpanan *server* diakuisisi dalam waktu 4 menit 0 detik. Metode *hashing* yang digunakan adalah MD5 dengan nilai *hash* **3a3901569cb3331478070ca178e6800a** dan SHA1 dengan nilai *hash* **cd4a4038af7619cfabac7cf13bd8c5dc84a6752c**.

Media penyimpanan milik klien (tersangka) juga dilakukan proses akuisisi dengan dilakukannya *imaging*, untuk detail hasil dari *imaging* pada media penyimpanan klien (tersangka) dapat dilihat pada Tabel 4.6.

Tabel 4.6 Akuisisi Media Penyimpanan Klien(Tersangka) GL-inet [skenario2]

| **Case Information** | |
|---|---|
| Case Number | USBSken02 |
| Evidence Number | 08-02-2018 |
| Source Type | Physical Drive |
| Unique description | BB Media Penyimpanan Tersangka GL-inet |
| Examiner | Abdul Rohman |
| Drive Model | SanDisk Cruzer Edge USB Device |
| Drive Serial Number | 4C530099910328123414 |
| Bytes per Sector | 512 |
| Sector Count | 61.489.152 |
| Source data size | 30024 MB |
| Segment | BB_Tersangka_Sken02_GL-inet.001 |
| Time Acquisition | Acquisition started: Thu Feb 08 02:15:24 2018 |
| | Acquisition finished: Thu Feb 08 02:31:25 2018 |
| Computed Hashes | MD5 checksum: 88809368ea93b7ab35921729fb369583 |
| | SHA1 checksum: 6e224bc364e6ffbf0d0dbc174665635fa05df9e8 |
| Tools | AccessData® FTK® Imager 3.4.2.6 |
| Notes | BB Media Penyimpanan yang digunakan untuk menyimpan file hasil download dari server pada skenario 2 untuk perangkat GL-inet AR300 |

Pada Tabel 4.6 diatas dapat dilihat detail dari proses akuisisi yang dilakukan. File **BB_Tersangka_Sken02_GL-inet.001** merupakan file hasil dari proses *imaging* media penyimpanan milik klien(tersangka). Media penyimpanan pada klien berukuran 30024 MB. Media penyimpanan milik klien diakuisisi dalam waktu 16 menit 1 detik. Metode *hashing* yang digunakan adalah MD5 dengan nilai *hash* **88809368ea93b7ab35921729fb369583** dan SHA1 dengan nilai *hash* **6e224bc364e6ffbf0d0dbc174665635fa05df9e8**.

## 4.7 Analisis Hasil dari Pengujian

Barang bukti yang sudah didapat melalui proses akuisisi akan dianalisa untuk menemukan kejanggalan atas aktivitas yang terjadi terkait dengan kejahatan. Hasil dari analisa yang dilakukan serta temuan yang didapat ditulis dalam laporan hasil dari investigasi dan menjadi panduan atau informasi tambahan dalam memutuskan suatu perkara. Alur dari proses analisis mengacu pada Gambar 3.8 tentang alur dari analisis forensik.

### 4.7.1 Analisis pada *smart router* MikroTik RB951Ui-2HnD

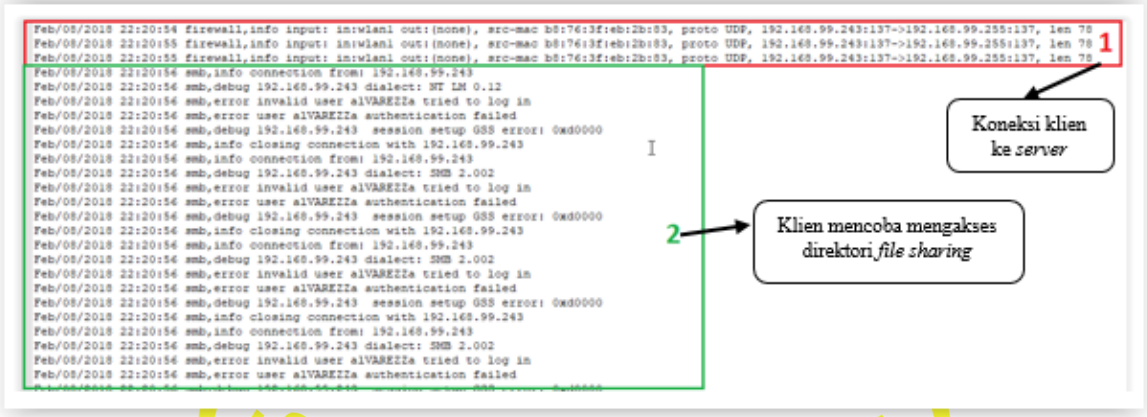
Informasi yang diperoleh pada proses akuisisi dicatat sebagai kelengkapan laporan. Terdapat beberapa catatan yang merupakan detail informasi dari barang bukti yang didapatkan, serta deskripsi singkat mengenai aktivitas terkait tindak kejahatan yang terjadi. Detail informasi dari proses akuisisi dapat dilihat pada Tabel 4.7.

Tabel 4.7 Detail Informasi Kasus pada Perangkat MikroTik

| **Detail Informasi** | |
|---|---|
| Jenis Pelanggaran | - Penghapusan file oleh klien dari direktori server<br>- Pengunggahan file pada direktori server |
| Jumlah Barang Bukti | 3 (tiga) file: 2 file *image*; 1 file text |
| Tipe Barang Bukti Digital | - File .001<br>- File .txt |
| Ukuran Barang Bukti Digital | - BB_USB_Thumbdrive_MikroTik_RB951Ui-2HnD.001: 484 MB<br>- BB_Tersangka_Sken02_MikroTik_RB951Ui-2HnD.001: 30024 MB<br>- LogSken02-MikroTik.txt : 87.4 KB |
| Deskripsi: Ditemukannya kejanggalan pada direktori server seperti hilangnya beberapa file dan terdapatnya file baru. | |

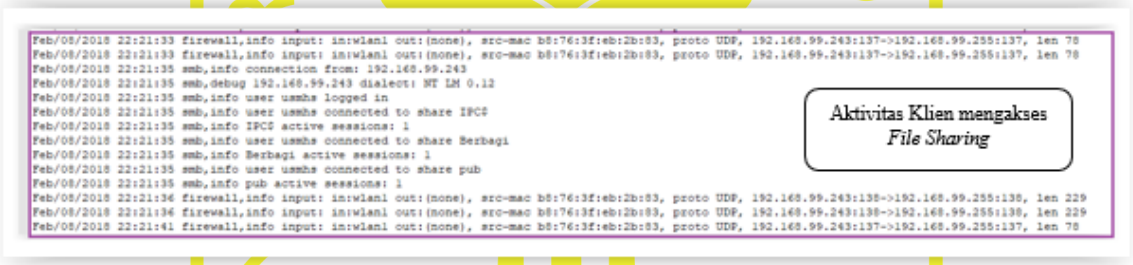
Analisis pertama dilakukan pada file *log* yang diperoleh, yaitu file "**LogSken02-MikroTik.txt**" yang didapatkan dari perangkat *smart router* MikroTik RB951Ui-2HnD. Akuisisi file *log* dilakukan karena perangkat yang didapatkan masih dalam kondisi menyala, dengan harapan dapat memperoleh informasi terkait penggunaan SMB sebagai protokol *file sharing* yang sudah ter-*install* pada perangkat *smart router* tersebut. Pada *log* terlihat adanya

aktivitas klien yang mencoba melakukan koneksi ke *server*, seperti terlihat pada Gambar 4.13.



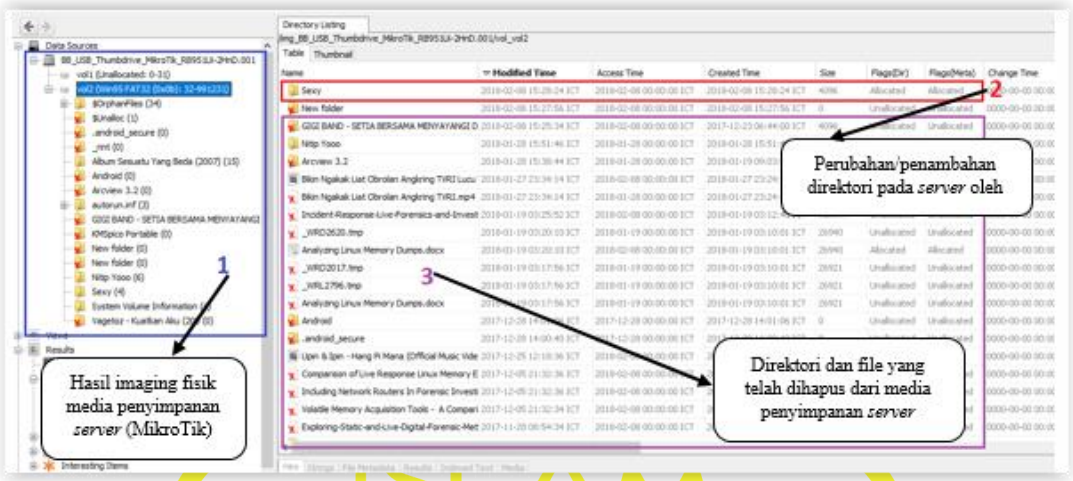

Gambar 4.19 Aktivitas Klien

Pada Gambar 4.19 tampak adanya klien yang mencoba melakukan koneksi ke *server*, pada gambar ditandai dengan nomor 1 (satu), dengan adanya *src-mac* **b8:76:3f:eb:2b:83** menggunakan protokol UDP yang mengakses *server*, klien mencoba mengakses direktori *file sharing*, tampak pada gambar yang diberi nomor 2 (dua).




Gambar 4.20 Aktivitas Klien mengakses *File Sharing*

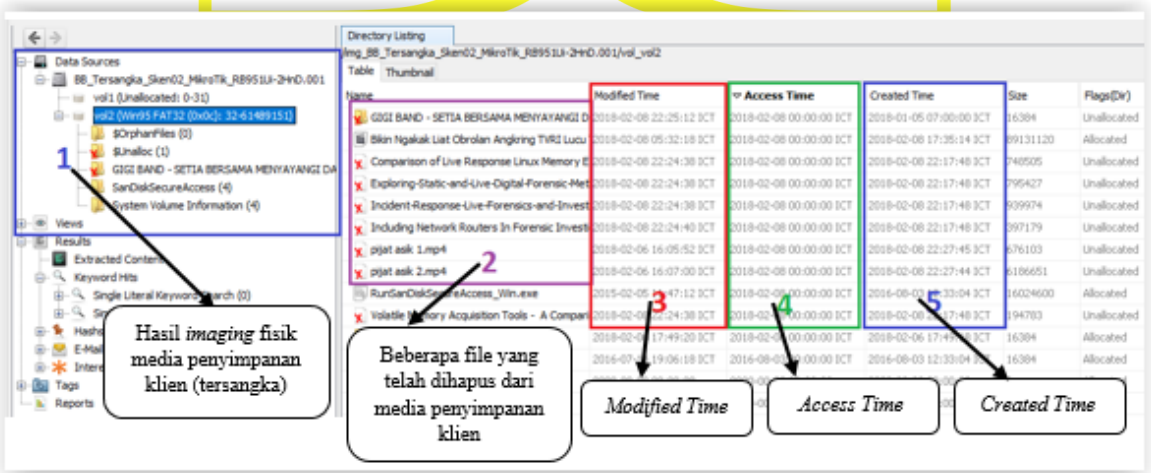
Berdasarkan informasi dari *log* yang diperoleh, untuk menguatkan dalam menganalisis maka perlu dilakukannya analisa terhadap hasil *image* media penyimpanan *server* untuk membuktikan aktivitas yang dilakukan klien. Untuk menganalisa hasil *image* dilakukan dengan menggunakan *tools* forensik. Berikut merupakan tampilan hasil *image* dari media penyimpanan *server*, yang ditunjukan pada Gambar 4.21.




Gambar 4.21 Bukti perubahan isi dari *file sharing* pada *USB Thumbdrive* MikroTik

Pada Gambar 4.21 didapat informasi adanya perubahan seperti terlihat pada gambar yang diberi nomor 1 (satu) terkait penambahan direktori file pada *server* dan aktivitas penghapusan direktori dan beberapa file pada *server*, pada gambar yang diberi tanda 2 (dua) terlihat ada direktori "**Sexy**" yang diindikasi sebagai direktori yang dibuat oleh klien, dan pada gambar yang diberi tanda 3 (tiga) terlihat ada beberapa file yang diindikasi telah dilakukan penghapusan oleh klien, yang ditandai dengan tanda "**silang**" yang berarti direktori tersebut telah dihapus (*unallocated*), berdasarkan informasi *timeline*.

Proses analisis berikutnya juga dilakukan pada hasil *image* media penyimpanan klien, hasil dari analisis pada media penyimpanan klien nantinya akan dilakukan pencocokan terkait kasus yang dilakukan oleh tersangka dengan hasil *image* dari media penyimpanan klien, berikut tampilan hasil *image* media penyimpanan klien yang dapat dilihat pada Gambar 4.22.




Gambar 4.22 *List* Direktori *Root* pada Media Penyimpanan Klien MikroTik

Pada Gambar 4.22 terlihat adanya penambahan direktori dan beberapa file yang diindikasi didapat dari hasil *download* dari *server*, dan klien berusaha untuk menghapus direktori dan file tersebut dari media penyimpanan milik klien. Untuk mencocokan informasi yang diperoleh dari hasil *image* media peyimpanan *server* dengan hasil *image* media penyimpanan klien, dilakukan dengan mencocokan *timeline* dari direktori dan file yang ada pada media penyimpanan *server* dengan *timeline* dari direktori dan file yang ada pada media penyimpanan klien.

Analisis dilakukan pada Gambar 4.22 terdapatnya file "**Comparison...**" pada media penyimpanan klien seperti yang ditandai dengan nomor 1 (satu), pada *timeline* tercatat *Modified Time* 2018-02-08 22:24:38 ICT, ditandai dengan nomor 3 (tiga), *Access Time* 2018-02-08 00:00:00 ICT yang ditandai dengan nomor 4 (empat), *Created Time* 2018-02-08 22:17:48 ICT yang ditandai dengan nomor 5 (lima). Direktori ini dicocokan berdasarkan *timeline* yang ada pada media penyimpanan *server*, seperti terlihat pada Gambar 4.21. Pada direktori *server* didapat informasi timeline terlihat bahwa terdapat file "**Comparison...**", pada *timeline* tercatat *Modified Time* 2017-12-05 21:32:36 ICT, *Access Time* 2018-02-07 00:00:00 ICT, dan *Created Time* 2018-01-19 09:11:51 ICT.

### 4.7.2 Analisis pada *smart router* GL-inet AR300

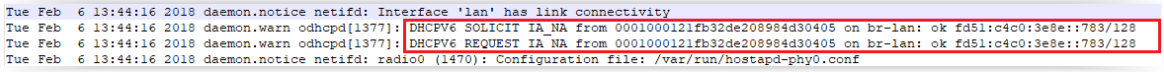
Informasi yang diperoleh pada proses akuisisi dicatat sebagai kelengkapan laporan. Terdapat beberapa catatan yang merupakan detail informasi dari barang bukti yang didapatkan, serta deskripsi singkat mengenai aktivitas terkait tindak kejahatan yang terjadi. Detail informasi dari proses akuisisi dapat dilihat pada Tabel 4.8.

Tabel 4.8 Detail Informasi Kasus pada Perangkat GL-inet

| **Detail Informasi** | |
|---|---|
| Jenis Pelanggaran | - Penghapusan file oleh klien dari direktori server<br>- Pengunggahan file pada direktori server |
| Jumlah Barang Bukti | 3 (tiga) file: 2 file *image*; 1 file text |
| Tipe Barang Bukti Digital | - File .001<br>- File .txt |
| Ukuran Barang Bukti Digital | - BB_USB_Thumbdrive_GL-inet_AR300.001: 3824 MB<br>- BB_Tersangka_Sken02_GL-inet.001: 30024 MB<br>- LogSken02-GL-inet.txt : 14.3 KB |
| Deskripsi: Ditemukannya kejanggalan pada direktori server seperti hilangnya beberapa file dan terdapatnya file baru. | |

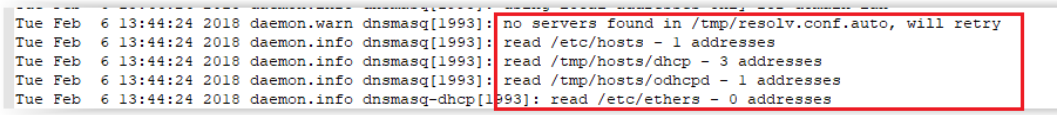
Analisis pertama dilakukan pada file *log* yang diperoleh, yaitu file "**LogSken02-GL-inet.txt**" yang didapatkan dari perangkat *smart router* GL-inet AR300. Akuisisi file *log* dilakukan karena perangkat yang didapatkan masih dalam kondisi menyala, dengan harapan dapat memperoleh informasi terkait penggunaan SMB sebagai protokol *file sharing* yang

sudah ter-*install* pada perangkat *smart router* tersebut. Pada *log* terlihat adanya aktivitas klien yang mencoba melakukan koneksi ke *server*, dan didapat IP DHCPV6 **fd51:c4c0:3e8e::783/128**, seperti terlihat pada Gambar 4.23.

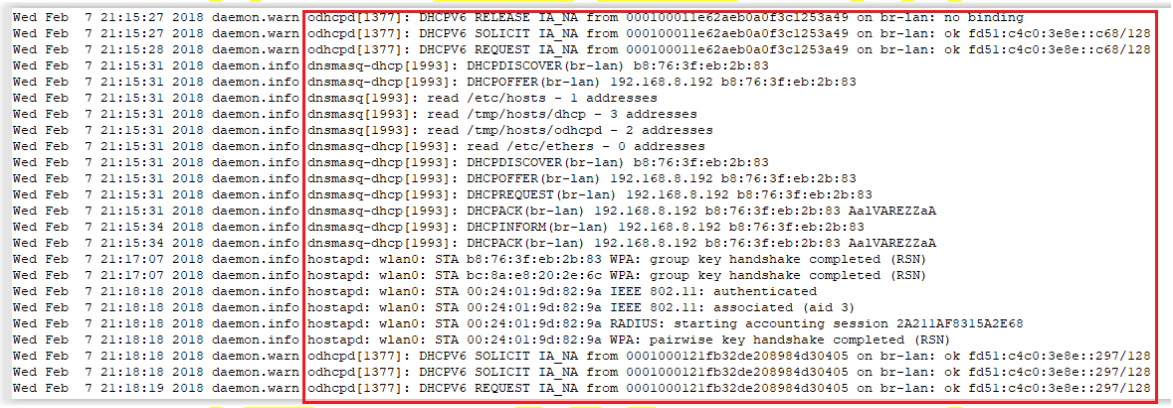



Gambar 4.23 Proses Koneksi Klien ke *Server*

Pada Gambar 4.24 memperlihatkan bahwa klien mencoba untuk mengakses beberapa direktori yang ada di *server*, dan terlihat ada aktivitas yang dicurigai bahwa klien melakukan beberapa aktivitas seperti menambah direktori, mengganti nama direktori, dan menghapus direktori pada *server*. Hal ini dapat dilihat pada Gambar 4.25.

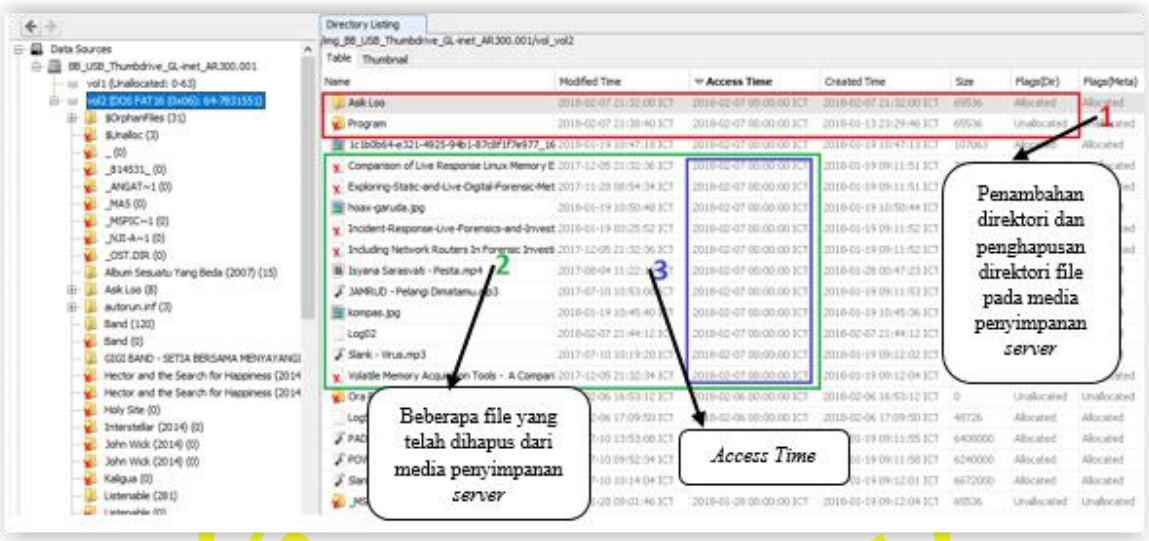



Gambar 4.24 Klien Melihat Isi Direktori *Server*




Gambar 4.25 Aktivitas Klien terkait tindakan ilegal *file sharing*

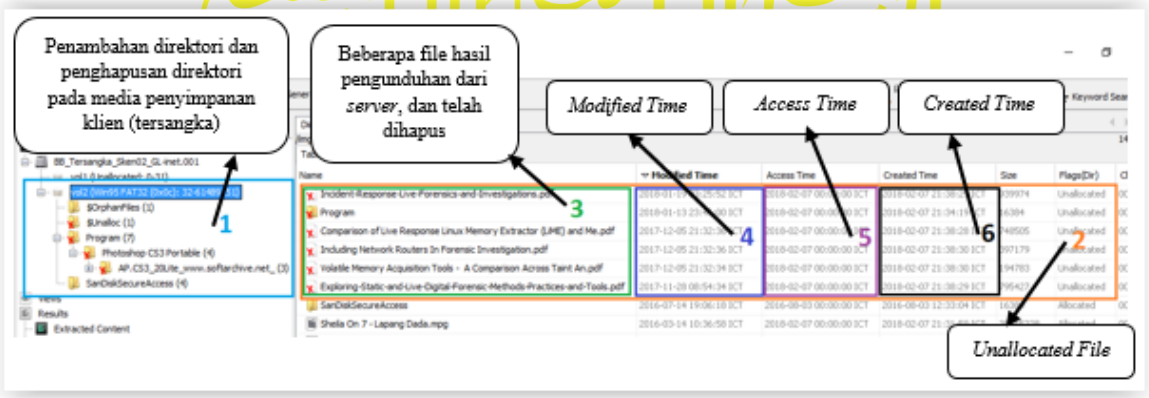
Berdasarkan informasi dari *log* yang diperoleh, untuk menguatkan dalam menganalisis maka perlu dilakukannya analisa terhadap hasil *image* media penyimpanan *server* untuk membuktikan aktivitas yang dilakukan klien. Untuk menganalisa hasil *image* dilakukan dengan menggunakan *tools* forensik. Berikut merupakan tampilan hasil *image* dari media penyimpanan *server*, yang ditunjukan pada Gambar 4.26




Gambar 4.26 *List* Direktori *Root* pada Media Penyimpanan *Server* GL-inet

Pada Gambar 4.26 didapat informasi adanya perubahan terkait penambahan direktori file pada *server*, dan aktivitas penghapusan direktori dan beberapa file pada *server*, pada gambar yang diberi tanda 1 (satu) terlihat ada direktori "**Asik Loo**" yang diindikasi sebagai direktori yang dibuat oleh klien, dan pada gambar yang diberi tanda 1 (satu) terlihat ada direktori "**Program**" diindikasi telah dilakukan penghapusan oleh klien, yang ditandai dengan tanda "**silang**" yang berarti direktori tersebut telah dihapus (*unallocated*), serta penghapusan beberapa file pada *server* yang ditandai dengan nomor 2 (dua), berdasarkan informasi *timeline* seperti pada gambar yang diberi tanda 3 (tiga).

Proses analisis berikutnya juga dilakukan pada hasil *image* media penyimpanan klien, hasil dari analisis pada media penyimpanan klien nantinya akan dilakukan pencocokan terkait kasus yang dilakukan oleh tersangka dengan hasil *image* dari media penyimpanan klien, berikut tampilan hasil *image* media penyimpanan klien yang dapat dilihat pada Gambar 4.27.




Gambar 4.27 *List* Direktori *Root* pada Media Penyimpanan Klien

Pada Gambar 4.27 terlihat adanya penambahan direktori dan beberapa file yang diindikasi didapat dari hasil *download* dari *server*, dan klien berusaha untuk menghapus direktori dan file tersebut dari media penyimpanan milik klien. Untuk mencocokan informasi yang diperoleh dari hasil *image* media peyimpanan *server* dengan hasil *image* media penyimpanan klien, dilakukan dengan mencocokan *timeline* dari direktori dan file yang ada pada media penyimpanan *server* dengan *timeline* dari direktori dan file yang ada pada media penyimpanan klien.

Analisis dilakukan pada Gambar 4.27 terdapatnya direktori "**Program**" pada media penyimpanan klien seperti yang ditandai dengan nomor 1 (satu), pada *timeline* tercatat *Modified Time* 2018-01-13 23:46:00 ICT, ditandai dengan nomor 4 (empat), *Access Time* 2018-02-07 00:00:00 ICT yang ditandai dengan nomor 5 (lima), *Created Time* 2018-02-07 21:34:19 ICT yang ditandai dengan nomor 6 (enam). Direktori ini dicocokan berdasarkan timeline yang ada pada media penyimpanan *server*, seperti terlihat pada Gambar 4.26. Pada direktori *server* didapat informasi *timeline* terlihat bahwa terdapat direktori "**Program**", pada *timeline* tercatat *Modified Time* 2018-02-07 21:38:40 ICT, *Access Time* 2018-02-07 00:00:00 ICT, dan *Created Time* 2018-01-13 23:29:46 ICT.

## 4.8 Analisis Hasil Penelitian

Hasil analisa forensik yang dilakukan pada barang bukti berupa file *log* dapat dilakukan analisis secara umum terhadap aktivitas yang terjadi. Berdasarkan atas kasus yang terjadi, pada jaringan dengan perangkat *smart router* yang dapat dijadikan sebagai file *server* dengan protokol SMB dan adanya aktivitas seperti yang ada pada kasus, maka diperoleh beberapa informasi maka perlu dilakukannya analisis pada media penyimpanan *file sharing*. Berdasarkan hasil temuan yang didapatkan pada proses analisis forensik, maka dapat ditemukan beberapa simpulan sebagai berikut:

1. Bukti digital apa yang dapat diperoleh dari *file sharing* pada *Smart Router*.
2. Mekanisme *live forensics acquisition* untuk mendapatkan Bukti Digital dari aktivitas ilegal *file sharing*.
3. Proses investigasi yang efektif untuk kasus – kasus kejahatan *file sharing* pada perangkat *smart router*.

### 4.8.1 Bukti digital yang diperoleh dari aktifitas *file sharing* pada *Smart Router*

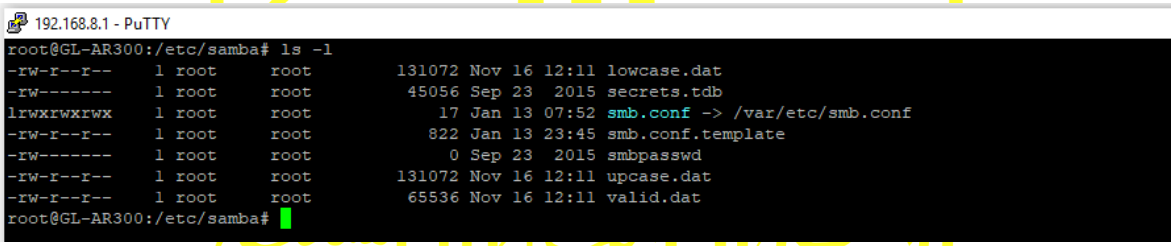
Analisis *log* dilakukan untuk mencari bukti digital terkait pada perangkat *smart router* yang memanfaatkan protokol SMB sebagai media *file sharing*. Dalam kasus yang melibatkan

adanya aktivitas pada *file sharing* ada beberapa kondisi yang dapat dijadikan parameter, seperti adanya akses pengunduhan file dari *server* ke klien, pengunggahan file dari klien ke *server*, serta penghapusan beberapa file yang terdapat di dalam direktori *file sharing*, bahwa aktivitas yang ada pada *system log* tidak mencatat kejadian terkait parameter dari kondisi yang terjadi.

Dari hasil pengujian yang dilakukan aktivitas *log* pada perangkat *smart router* terkait pemanfaatan protokol SMB yang dapat dijadikan sebagai media *file sharing*, baik perangkat *smart router* GL-inet AR300 dan MikroTik RB951Ui-2HnD tidak ditemukannya informasi tentang *log* dari aktivitas mengenai *file sharing* seperti yang ada pada skenario kasus, bahwa klien yang terhubung ke dalam jaringan melakukan berbagai aktivitas seperti mengunduh file, mengunggah file dan menghapus file. Bahwa aktivitas tersebut tidak terekam atau tercatat pada sistem *log* (*syslog*) dan juga pada *log* samba. Untuk bukti digital yang diperoleh terkait pemanfaatan *file sharing* dapat dilihat pada Tabel 4.9 pada kolom **Informasi yang diperoleh pada Syslog (terkait *file sharing*)**.

### 4.8.2 Mekanisme untuk mendapatkan Bukti Digital dari aktivitas *file sharing*.

Mekanisme yang dilakukan untuk mendapatkan bukti digital dari aktivitas *file sharing* dilakukan secara *live* akuisisi, mengingat bahwa aktivitas yang terekam pada *log* sistem dapat hilang ketika perangkat dalam kondisi mati (*off*). Perangkat *smart router* jenis ini juga tidak dilengkapi fitur untuk mendapatkan informasi mengenai aktivitas *log* pada samba, pada gambar terlihat bahwa pada direktori samba tidak ditemukan *log*.




Gambar 4.28 Direktori File Samba pada *smart router* GL-inet AR300

Pada Gambar 4.28 menunjukan tidak terdapatnya *log* samba yang dapat dijadikan sebagai bahan informasi terkait bukti digital dengan memanfaatkan protokol SMB sebagai media *file sharing* pada perangkat *smart router* GL-inet AR300. Sedangkan pada perangkat *smart router* MikroTik RB951Ui-2HnD untuk direktori *log* samba tidak dapat ditemukan.

Dalam melakukan analisis bukti digital pada perangkat *smart router* terkait adanya aktivitas *file sharing* perlu dilakukannya komparasi atau perbandingan bukti digital yang terdapat pada media peyimpanan pada perangkat router dengan *system log* terkait aktivitas waktu yang tercatat pada media penyimpanan dan waktu pada *system log*.

### 4.8.3 Proses investigasi untuk kasus kejahatan *file sharing* pada *smart router*

Berdasarkan pada barang bukti yang diperoleh dan juga hasil analisa yang dilakukan, maka untuk melakukan proses investigasi terkait kejahatan *file sharing* pada perangkat *smart router*, perlu dilakukan proses investigasi yang efektif yang digunakan untuk melakukan investigasi protokol SMB adalah dengan terlebih dahulu melakukan analisa pada *system log*. Hal ini dilakukan karena *system log* memberikian informasi tentang hal-hal yang dilakukan terkait aktivitas ilegal *file sharing*. Sehingga investigator dapat mengetahui apa saja yang harus dianalisa pada media penyimpanan *server* maupun klien. Berangkat dari informasi yang didapat dari proses analisa *system log*, maka dilakukan analisa media penyimpanan *server* dan klien. Hasil analisa media penyimpanan tersebut dicocokan kembali dengan hasil analisa *log*. Bagan proses investigasi efektif yang dapat digunakan untuk investigasi terkait kejahatan *file sharing* dapat dilihat pada Gambar 3.8.

Berdasarkan dokumen SNI ISO/IEC 27037:2014, untuk tahap preservasi pada alur investigasi penelitian ini dilakukan pada proses (1,2)Persiapan Olah TKP dan (1,3)Persiapan Pengamanan Barang Bukti; untuk tahap akuisisi dilakukan pada proses (4,5)Akuisisi *Log* File berupa (4,5,6)file ekstensi **.txt** dan (4,7)Akuisisi Media Penyimpanan dengan melakukan proses (4,7,8)*Imaging* berupa (4,7,8,9)file ekstensi **.dd**; pada tahap analisis dilakukan pada proses (10,11,12)Analisis file **log.txt** dan (10,14,15,16)Analisis file barang bukti media penyimpanan pada file **.dd** *server*, dan (10,14,17,18)Analisis file barang bukti media peyimpanan pada file **.dd** klien; tahap berikutnya melakukan (13,19)perbandingan atau membandingkan hasil analisa pada file **log.txt** dengan file hasil analisa media penyimpanan; untuk tahap terakhir melakukan proses (20)Pelaporan.

Berikut merupakan tabel perbandingan Analsis Forensik untuk *Smart Router* yang ditunjukan pada Tabel 4.9.

Tabel 4.9 Analisis Forensik untuk *Smart Router*

| No | Merk Perangkat | Sistem Operasi | Teknik Akuisisi *Log* | | Temuan pada Bukti Digital | | Informasi yang diperoleh pada *Syslog* (terkait *file sharing)* |
|---|---|---|---|---|---|---|---|
| | | | *System log* | Samba *log* | Skenario 1 | Skenario 2 | |
| **1.** | MikroTik RouterBoard (RB951Ui 2HnD) | MikroTik RouterOS 6.39.2 | Dapat diunduh secara langsung melalui web browser atau menggunakan *tools* WinBox atau FTP, dan SCP | Tidak dapat membaca *log* samba secara langsung | Tidak diperolehnya informasi *log* file Samba terkait pemanfaatan *file sharing*, baik pada *log* smb maupun *log* pada *system log*. | Adanya perubahan aktivitas koneksi dari *client* ke *server* dengan adanya penambahan direktori komputer *client* pada *log system*. | - info input: in:wlan1<br>- src-mac b8:76:3f:eb:2b:83<br>- proto UDP<br>- ip address 192.168.99.243<br>- smb,info connection from: 192.168.99.243<br>- user alVAREZZa authentication<br>- smb,info connection from: 192.168.99.243<br>- smb,info user usmhs logged in<br>- smb,info user usmhs connected to share Berbagi<br>- wireless,info B8:76:3F:EB:2B:83@wlan1: disconnected, received disassoc: sending station leaving |
| **2.** | GL-inet (AR300) | OpenWrt Chaos Calmer 15.05 r47065 | Tidak dapat diunduh secara langsung melalui web browser. Diunduh dengan *tools* putty melalui protokol SSH, menggunakan teknik *copy-paste log*. | Dapat mengakses direktori Samba, tetapi tidak dapat membaca *log* samba | Tidak diperolehnya informasi *log* file Samba terkait pemanfaatan *file sharing*, baik pada *log smb* maupun *log* pada *system log*. | Adanya perubahan aktivitas koneksi dari *client* ke *server* dengan adanya penambahan direktori komputer *client* pada *log system*. | - daemon.info hostapd: wlan0: STA b8:76:3f:eb:2b:83 IEEE 802.11: authenticated<br>- daemon.info hostapd: wlan0: STA b8:76:3f:eb:2b:83 IEEE 802.11: associated<br>- daemon.info hostapd: wlan0: STA b8:76:3f:eb:2b:83 WPA: pairwise key handshake completed<br>- daemon.warn odhcpd[1377]: DHCPV6 SOLICIT IA_NA from 000100011e62aeb0a0f3c1253a49 on br-lan: ok fd51:c4c0:3e8e::c68/128<br>- daemon.warn odhcpd[1377]: DHCPV6 REQUEST IA_NA from 000100011e62aeb0a0f3c1253a49 on br-lan: ok fd51:c4c0:3e8e::c68/128<br>- daemon.info dnsmasq-dhcp[1993]: DHCPDISCOVER(br-lan) b8:76:3f:eb:2b:83<br>- daemon.info dnsmasq-dhcp[1993]: DHCPOFFER(br-lan) 192.168.8.192 b8:76:3f:eb:2b:83 |

| No | Merk Perangkat | Sistem Operasi | Teknik Akuisisi *Log* | | Temuan pada Bukti Digital | | Informasi yang diperoleh pada *Syslog* (terkait *file sharing)* |
|---|---|---|---|---|---|---|---|
| | | | *System log* | Samba *log* | Skenario 1 | Skenario 2 | |
| | | | | | | | - daemon.info dnsmasq-dhcp[1993]: DHCPREQUEST(br-lan) 192.168.8.192 b8:76:3f:eb:2b:83<br>- daemon.info dnsmasq-dhcp[1993]: DHCPACK(br-lan) 192.168.8.192 b8:76:3f:eb:2b:83 AalVAREZZaA<br>- daemon.info hostapd: wlan0: STA b8:76:3f:eb:2b:83 IEEE 802.11: disassociated |

Dari Tabel 4.9 bahwa perangkat *smart router* MikroTik RB951Ui 2HnD, untuk *Syslog*-nya dapat diunduh secara langsung melalui *web browser* atau menggunakan *tools* WinBox atau FTP, dan SCP, sedangkan untuk Samba *log*-nya tidak dapat dibaca *log* samba-nya secara langsung. Pada skenario 2 (dua) terlihat adanya perubahan aktivitas koneksi dari *client* ke *server* dengan adanya penambahan direktori komputer *client* pada *log system*. Ada beberapa informasi yang tercatat pada *syslog*, seperti:

1) *info input*: in:wlan1

   Terdapatnya informasi klien yang terhubung melalui koneksi WLAN

2) *src-mac* b8:76:3f:eb:2b:83

   Tercatatnya *mac address* dari klien yang terkoneksi

3) proto UDP

   Koneksi yang terbentuk menggunakan protokol UDP pada *Layer Transport*

4) *ip address* 192.168.99.243

   Dari klien yang terhubung (b8:76:3f:eb:2b:83) diberi *ip address* 192.168.99.243

5) smb,*info connection from*: 192.168.99.243

   Klien dengan *ip address* 192.168.99.243 melakukan koneksi ke *file sharing* menggunakan protokol SMB.

6) *user* alVAREZZa *authentication*

   Diperolehnya informasi mengenai nama akun atau *user* dari sistem yang dipakai klien, nama akun ini biasanya melekat pada sistem operasi yang dipakai klien.

7) smb,*info connection from*: 192.168.99.243

   Adanya akses koneksi ke *file sharing* dari *ip address* 192.168.99.243

8) smb,*info user usmhs logged in*

   Diperolehnya informasi terdapat *user* yang melakukan proses *login* sebagai user "**usmhs**", dimana *user* "**usmhs**" digunakan sebagai otentikasi ketika mengakses *file sharing*.

9) smb,*info user usmhs connected to share* Berbagi

   *User* berhasil *login* dengan *user* "**usmhs**" dan berhasil mengakses direktori *file sharing* "**Berbagi**". "**Berbagi**" merupakan direktori yang di-share atau dibagikan.

10) *wireless,info* B8:76:3F:EB:2B:83@wlan1: *disconnected, received disassoc*: *sending station leaving*

    Klien dengan *mac address* B8:76:3F:EB:2B:83 melakukan pemutusan atau mengakhiri koneksi dengan *server*, yang sebelumnya terkoneksi melalui jaringan WLAN.

Sedangkan para perangkat *smart router* GL-inet AR300, bahwa untuk *Syslog* tidak dapat diunduh secara langsung melalui *web browser*. Untuk mendapatkannya diunduh dengan *tools putty* melalui protokol SSH, menggunakan teknik *copy-paste log*, sedangkan untuk *log* samba dapat diakses untuk direktori Samba-nya, tetapi tidak dapat membaca *log* samba. Untuk informasi yang diperoleh pada syslog terkait *file sharing* pada *smart router* GL-inet AR300 diantaranya:

1) *daemon.info hostapd*: wlan0: STA b8:76:3f:eb:2b:83 IEEE 802.11: *authenticated*
   Informasi adanya klien dengan *mac address* b8:76:3f:eb:2b:83 yang melakukan koneksi ke *server* melalui WLAN
2) *daemon.info hostapd*: wlan0: STA b8:76:3f:eb:2b:83 IEEE 802.11: *associated*
   Penambahan informasi *mac address* b8:76:3f:eb:2b:83 pada tabel *mac address server*
3) *daemon.info hostapd*: wlan0: STA b8:76:3f:eb:2b:83 WPA: *pairwise key handshake completed*
   Klien b8:76:3f:eb:2b:83 malukan koneksi pada jaringan *hotspot* dan berhasil terkoneksi ke *server*
4) *daemon.warn odhcpd*[1377]: DHCPV6 SOLICIT IA_NA *from* 000100011e62aeb0a0f3c1253a49 *on br-lan*: *ok* fd51:c4c0:3e8e::c68/128
   Klien b8:76:3f:eb:2b:83 berhasil terkoneksi ke *server* DHCP dan mendapatkan *ip address* secara otomatis dengan IPv6 fd51:c4c0:3e8e::c68/128
5) *daemon.warn odhcpd*[1377]: DHCPV6 REQUEST IA_NA *from* 000100011e62aeb0a0f3c1253a49 *on br-lan*: *ok* fd51:c4c0:3e8e::c68/128
   *Server* melakukan *request ip address* untuk klien yang terkoneksi
6) *daemon.info dnsmasq-dhcp*[1993]: DHCPDISCOVER(br-lan) b8:76:3f:eb:2b:83
   Klien dengan *mac address* b8:76:3f:eb:2b:83 berhasil terkoneksi dan menunggu respon dari *server*
7) *daemon.info dnsmasq-dhcp*[1993]: DHCPOFFER(br-lan) 192.168.8.192 b8:76:3f:eb:2b:83
   Klien dengan *mac address* b8:76:3f:eb:2b:83 berhasil mendapatkan *ip address dhcp*, dengan *ip address* 192.168.8.192
8) *daemon.info dnsmasq-dhcp*[1993]: DHCPREQUEST(br-lan) 192.168.8.192 b8:76:3f:eb:2b:83
   *Request ip address* untuk klien dengan *mac address* b8:76:3f:eb:2b:83 berhasil mendapatkan *ip address dhcp*, dengan *ip address* 192.168.8.192
9) *daemon.info dnsmasq-dhcp*[1993]: DHCPACK(br-lan) 192.168.8.192 b8:76:3f:eb:2b:83 AalVAREZZaA

Didapat informasi mengenai klien yang berhasil terkoneksi ke *server*, bahwa klien yang terkoneksi dengan *ip address* 192.168.8.192, diperoleh dari klien dengan *mac address* b8:76:3f:eb:2b:83, dimana akun atau username yang dipakai klien pada sistem operasi yang digunakan adalah "**AalVAREZZaA**"

10) *daemon.info hostapd*: wlan0: STA b8:76:3f:eb:2b:83 IEEE 802.11: *disassociated*

Klien dengan *mac address* b8:76:3f:eb:2b:83 melakukan pemutusan atau megakhiri koneksi dengan *server*, yang sebelumnya terkoneksi pada jaringan WLAN.

Dari beberapa informasi yang diperoleh pada masing – masing perangkat *smart router*, terkait pemakaian fitur *file sharing*, memiliki karakteristik yang berbeda pada masing – masing informasi yang tercatat pada *system log*-nya. Baik pada skenario 1 (satu) maupun skenario 2 (dua) untuk informasi dari *log* samba sendiri tidak diperoleh secra lebih rinci, dimana informasi yang ditemukan pada *syslog* hanya berupa catatan dari klien yang terkoneksi pada *server* dan aktivitas klien yang mengakses direktori *file sharing* saja. Untuk informasi terkait aktivitas ilegal yang dilakukan oleh klien pada direktori *file sharing* di *server* tidak dapat terbaca. Oleh karena itu, untuk mendapatkan bukti yang kuat terkait pemanfaatan *file sharing* pada perangkat *smart router* perlu dilakukannya pencocokan atau perbandingan antara file yang terdapat pada direktori *file sharing* milik *server* dengan file yang terdapat pada direktori *file sharing* milik klien yang terindikasi sebagai tersangka.

# BAB 5
# Kesimpulan dan Saran

## 5.1 Kesimpulan

Berdasarkan hasil yang didapat pada proses implementasi, hasil dan pembahasan, maka pada penelitian studi dan analisa forensika digital pada perangkat smart router sebagai media *file sharing* dengan protokol SMB dapat ditarik beberapa kesimpulan:

1. Bukti digital yang diperoleh dari aktivitas *file sharing* pada perangkat *smart router* dengan sistem operasi yang berbeda dan vendor yang berbeda didapat *log system* yang beragam/berbeda, dikarenakan setiap sistem operasi atau vendor pengembang memiliki otoritas. Aktivitas *log* yang ada pada *log* sistem (*syslog*) hanya mencatat atau merekam aktivitas dari sistem, dan aktivitas yang berkaitan dengan *file sharing* seperti *log* pada *file* samba tidak tercatat dengan detail. Maka potensi kejahatan dengan memanfaatkan perangkat *smart router* sebagai media *file sharing* sangat mungkin terjadi dan sulit untuk mendapatkan bukti digital terkait pemanfaatan protokol SMB dengan aplikasi samba pada perangkat *smart router* MikroTik RB951Ui-2HnD dan GL-inet AR300.
2. Mekanisme untuk mendapatkan bukti digital pada perangkat *smart* router terkait aktivitas *file sharing* dimana perangkat dalam kondisi menyala dilakukan sesuai dengan SNI ISO/IEC 27037:2014, dengan dilakukannya identifikasi seperti melakukan proses pencarian, mengenali, mendokumentasi hal yang berpotensi sebagai barang bukti digital terhadap *processing device* dan digital media *storage*, terdapat dua metode yang digunakan untuk melakukan proses akuisisi, yaitu menggunakan metode *live acquisition* atau *logical acquisition* pada perangkat router, dan *pysical acquisition* pada *device* yang dijadikan media *file sharing* pada perangkat router tersebut.
3. Proses investigasi yang efektif untuk kasus kejahatan *file sharing* pada *smart* router, berdasarkan dokumen SNI ISO/IEC 27037:2014, terbagi menjadi 4 (empat) bagian, yaitu: (1) Preservasi, pada tahap preservasi alur investigasi dilakukan pada proses "Persiapan Olah TKP dan Persiapan Pengamanan Barang Bukti"; (2) Akuisisi, pada tahap akuisisi dilakukan proses "Akuisisi *Log File*" berupa *file log* dengan ekstensi **.txt**, dan tahap akuisisi juga dilakukan pada "Media Penyimpanan" dengan melakukan proses "*Imaging*" berupa *file* dengan ekstensi **.dd**; (3) Analisis, pada tahap analisis dilakukan pada proses "Analisis file **log.txt** dan Analisis *file* barang bukti media penyimpanan

*server* berupa *file* **.dd**, dan Analisis *file* barang bukti media peyimpanan klien berupa *file* **.dd**"; pada tahap analisis juga melakukan perbandingan atau membandingkan hasil analisa pada *file* **log.txt** dengan *file* hasil analisa media penyimpanan; (4) Pelaporan, tahap pelaporan merupakan tahap terakhir dalam melakukan proses investigasi.

## 5.2 Saran

Untuk penelitian lebih lanjut mengenani forensik pada perangkat seperti halnya *smart* router yang dapat dijadikan sebagai media *file sharing* diberikan beberapa saran, saran tersebut adalah:

1. Merode *live forensics* pada *smart* router tidak cukup membantu dalam mendapatkan informasi mengenai bukti digital terkait pemanfaatan protokol SMB, sehingga perlu dilakukan proses *tapping* atau *sniffing* dengan menggunakan metode *network forensic*, dan metode statis dengan melakukan pencarian bukti digital pada media peyimpanan yang sebelumnya telah dilakukan proses *imaging*.
2. Diperlukan dilakukan pengujian dan analisis pada perangkat *smart* router dengan sistem operasi yang sama tetapi dengan vendor yang berbeda untuk menemukan karakteristik terkait bukti digital pada *file sharing*.
3. Diperlukan metode khusus untuk mendapatkan informasi mengenai barang bukti yang dapat diperoleh dari memori fisik pada perangkat *smart* router.

# Daftar Pustaka


Adelstein, F. (2006). Live forensics: diagnosing your system without killing it first. *Communications of the ACM*, 63–66. Retrieved from https://cacm.acm.org/magazines/2006/2/6016-live-forensics/abstract#

Ahmad, M. S., Riadi, I., & Prayudi, Y. (2017). Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man in the Middle Attack Berbasis Evil Twin. *ILKOM Jurnal Ilmiah*, *9*(April), 1–8. Retrieved from http://jurnal.fikom.umi.ac.id/index.php/ILKOM/article/view/103/60

Al-Azhar, M. N. (2012). *Digital Forensic: Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek.

Alamsyah, R. (2009). Teknik Forensik Meneliti Bukti Digital. Retrieved March 26, 2017, from http://www.perspektifbaru.com/wawancara/708

Artformatics. (2013). Live Forensic. Retrieved March 26, 2017, from https://artformatics.wordpress.com/2013/02/16/live-forensic/

Aslam, S. (2018). The 10 Best Wifi Routers for 2018. Retrieved February 6, 2018, from https://www.omnicoreagency.com/best-wifi-routers/

Badan Standarisasi Nasional. (2014). *SNI 27037:2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital*. Jakarta.

Bandara, H. M. N. D., & Jayasumana, A. P. (2013). Collaborative applications over peer-to-peer systems-challenges and solutions. *Peer-to-Peer Networking and Applications*, *6*(3), 257–276. https://doi.org/10.1007/s12083-012-0157-3

Bastounis, O. (2018). Best wireless routers 2018: the best routers for your home network. Retrieved February 6, 2018, from http://www.techradar.com/news/networking/routers-storage/best-router-9-top-wireless-routers-on-test-1090523

Beal, V. (2017). log file. Retrieved April 30, 2017, from http://www.webopedia.com/TERM/L/log_file.html

Carmack, C. (2005). How BitTorrent Works. Retrieved August 11, 2017, from http://computer.howstuffworks.com/bittorrent1.htm

Christensson, P. (2010). Log File Definition. Retrieved April 30, 2017, from

https://techterms.com/definition/logfile

Cisco, T. (2018). Products IOS Cisco IOS Software Releases. Retrieved January 25, 2018, from https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-software-releases-listing.html

Citraweb, T. (2017). File Server SMB pada Mikrotik. Retrieved January 31, 2018, from http://www.mikrotik.co.id/artikel_lihat.php?id=94

Cutter, T. C. (2017). The Best Router for Streaming on Multiple Devices. Retrieved January 25, 2018, from https://cordcuttingreport.com/2017/01/21/best-router/

Daniel, L., & Daniel, L. (2012). *Digital Forensic For Legal Profesionals*. (R. Maxwell, Ed.). 225 Wyman Street, Waltham, MA 02451, USA: Syngress.

Dd-wrt, T. (2018). Latest DD-WRT Releases. Retrieved January 25, 2018, from http://www.dd-wrt.com/site/support/router-database

Desk, I. S. (2017). File Sharing and Piracy. Retrieved August 11, 2017, from https://ist.mit.edu/security/file_sharing

Dharmendra, I. K., Putu, L., & Desiani, A. (2015). Penerapan Network Attached Storage Menggunakan Openwrt Studi Kasus : Bagian Kemahasiswaan STIKOM Bali. In *Konferensi Nasional Sistem & Informatika 2015* (pp. 1016–1020). Bali: STIMIK STIKOM Bali.

Fuller, S. (2017). Internet/Media Piracy: Statistics & Facts. Retrieved December 26, 2017, from https://www.statista.com/topics/3493/media-piracy/

Geel, M. (2013). Cloud Storage: File Hosting and Synchronisation 2.0, 11–14. Retrieved from https://www.vis.ethz.ch/de/visionen/pdfs/2012/visionen_2012_3.pdf?end=15&start=11

Geier, E. (2018). Four Ways to Transform That Old PC Into a Powerful Router. Retrieved January 25, 2018, from http://www.practicallynetworked.com/networking/convert_old_pc_to_new_router.htm

Glossbrenner, A. (1984). XMODEM: A Standard is Born. *PC Mag*, 451–452.

Handoko, L. B., & Setiono, O. (2016). Rancang Bangun Sistem Hotspot Portable dengan OpenWRT Engineering of Portable Hotspot System using OpenWRT. *Jurnal Ilmiah SISFOTENIKA*, *Vol.6*, *No.*, 182–193.

Hariyadi, D., & Supriyono, A. R. (2017). Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI ISO/IEC 27037:2014. *TELEMATIKA*,

*14*(1), 62–67. Retrieved from http://jurnal.upnyk.ac.id/index.php/telematika/article/view/1967

Hariyadi, D., Winarno, W. W., & Luthfi, A. (2016). Analisis Konten Dugaan Tindak Kejahatan Dengan Barang Bukti Digital Blackberry Messenger. *Teknomatika*, *9*(1), 81–89.

Ideaing, T. (2016). These Smart Routers Solve the Biggest Wi-Fi Problems: Range & Speed. Retrieved February 5, 2018, from https://ideaing.com/ideas/best-wifi-router-smart-home

Internet Live Stats. (2016). *Internet users in the world*. Retrieved from http://www.internetlivestats.com/internet-users/

ISU, T. (2017). File Sharing & Copyrighted Materials. Retrieved August 11, 2017, from https://www.it.iastate.edu/policies/filesharing/

Jackson, G. S. (2018). Network Operating Systems Vs. Embedded Operating Systems. Retrieved January 25, 2018, from http://smallbusiness.chron.com/network-operating-systems-vs-embedded-operating-systems-46508.html

Jinkook, K. (2014). Live Response vs Traditional. Retrieved January 18, 2018, from https://www.symantec.com/connect/blogs/live-response-vs-traditional-forensics-0

Jones, R. (2007). Safer Live Forensic Acquisition. *Computer Science Laboratory*. Retrieved from http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf

Juniper, T. (2018). Junos OS Overview. Retrieved January 25, 2018, from https://www.juniper.net/us/en/products-services/nos/junos/

Kistijantoro, A. I. (2007). *Pengantar Jaringan Komputer*. (Dw. Prabantini, Ed.) (1st ed.). Yogyakarta: Andi Offset.

Kurniawan, A. (2012). *Network Forensics "Panduan Analisis & Investigasi Paket Data Jaringan Menggunakan Wireshark."* (N. WK, Ed.) (1st ed.). Yogyakarta: C.V ANDI OOSET.

Kurniawan, A., & Prayudi, Y. (2014). Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics. *HADFEX (Hacking and Digital Forensics Exposed)*, (JUNE 2014), 1–5.

Larasati, T. D., & Hidayanto, B. C. (2017). ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN APLIKASI INSTANT MESSENGER PADA SISTEM OPERASI WINDOWS 10. *SESINDO*, *6*(November), 456–256.

Lee, C. (2017, January 18). Benefits and Risks of File Sharing for Enterprises. *ezTalks*.

Retrieved from https://www.eztalks.com/file-sharing/benefits-and-risks-of-file-sharing-for-enterprises.html

Lessing, M., & Solms, B. Von. (2008). Live Forensic Acquisition as Alternative to Traditional Forensic Processes. *Proceedings of the Conference on IT Incident Management & IT Forensics (IMF 2008)*, 1–9. Retrieved from http://hdl.handle.net/10204/3141

Mag, T. P. (2017a). Definition of: Access Point. Retrieved January 25, 2018, from https://www.pcmag.com/encyclopedia/term/37393/access-point

Mag, T. P. (2017b). Definition of: Wireless Router. Retrieved January 25, 2018, from https://www.pcmag.com/encyclopedia/term/54783/wireless-router

Mazdadi, M. I., Riyadi, I., & Luthfi, A. (2017). Live Forensics on RouterOS using API Services to Investigate Network Attacks. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(2), 406–410. Retrieved from https://sites.google.com/site/ijcsis/

Media, K. (2017). *Use of peer-to-peer services to consume or share digital content in the United Kingdom ( UK ) from 2012 to 2017 , by legality group* *. Retrieved from https://www.statista.com/statistics/291481/use-of-peer-to-peer-services-to-consume-or-share-digital-content-uk/

Microsoft, T. (2018). The OSI Model's Seven Layers Defined and Functions Explained. Retrieved January 17, 2018, from https://support.microsoft.com/en-us/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

Mikrotik, T. (2018). RouterOS is the operating system of RouterBOARD. Retrieved January 25, 2018, from https://mikrotik.com/software

Multipage. (2015, May 21). 5 Benefits of the Cloud for File Sharing. *MyWorkDrive*. Retrieved from https://www.myworkdrive.com/5-benefits-of-the-cloud-for-file-sharing/

Munandar, H., & Sitanggang, S. (2008). *Mengenal Hak Kekayaan Intelektual. Hak Cipta, Paten, Merek dan Seluk – beluknya.* Jakarta: Erlangga Group.

Namrata, N. (2013). NETWORK ATTACHED STORAGE DIFFERENT FROM TRADITIONAL FILE SERVERS & IMPLEMENTATION OF WINDOWS BASED NAS. *International Journal of Computer Engineering and Technology (IJCET)*, *4*(3), 539–549. Retrieved from www.iaeme.com/ijcet.asp

Nikiforakis, N., Balduzzi, M., Van Acker, S., Joosen, W., & Balzarotti, D. (2011). Exposing the Lack of Privacy in File Hosting Services. *USENIX Workshop on Large-*

*Scale Exploits and Emergent Threats*, 1–8. Retrieved from http://www.usenix.org/events/leet11/tech/%5Cnpapers3://publication/uuid/F9CFF630-4FFD-4199-A8BA-73A560D741A8

OpenWrt, T. (2018). What is OpenWrt? Retrieved January 25, 2018, from https://openwrt.org/

Pcmag. (2017). Definition of: router. Retrieved December 14, 2017, from https://www.pcmag.com/encyclopedia/term/50637/router

Pcmag. (2018). Smart Wi-Fi router. Retrieved January 11, 2018, from https://www.pcmag.com/encyclopedia/term/65987/smart-wi-fi-router

Prayudi, Y. (2014). Problema dan Solusi Digital Chain Of Custody. *Seminar Nasional Aplikasi Teknologi Informasi (Senasti)*, (2011), 197–204.

RI, D., & RI, P. (2008). *UU No.11 Tahun 2008, tentang Informasi dan Transaksi Elektronik*. Jakarta.

Rosenblatt, S. (2013). Top Wi-Fi routers easy to hack, says study. Retrieved February 21, 2018, from https://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/

Rouse, M. (2010). log (log file). Retrieved April 30, 2017, from http://whatis.techtarget.com/definition/log-log-file

Rouse, M. (2014). Definition peer-to-peer (P2P). Retrieved January 24, 2018, from http://searchnetworking.techtarget.com/definition/peer-to-peer

Rouse, M. (2015). network-attached storage (NAS). Retrieved August 11, 2017, from http://searchstorage.techtarget.com/definition/network-attached-storage

Rouse, M. (2016). Definition Router. Retrieved January 18, 2018, from http://searchnetworking.techtarget.com/definition/router

Samba.org. (2017). What is Samba. Retrieved April 30, 2017, from https://www.samba.org/samba/what_is_samba.html

Sammons, J. (2012). *THE BASICS OF DIGITAL FORENSIC The Primer for Getting Started in Digital Forensics*. (Rajewski Jonathan, Ed.), *The Basics of Digital Forensics*. Wyman Street, Waltham, MA 02451, USA: Syngress. https://doi.org/10.1016/B978-1-59749-661-2.00001-2

Sandberg, R., Goldberg, D., Kleiman, S., Walsh, D., & Lyon, B. (1985). Design and Implementation of the Sun Network Filesystem.

Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. *Proceedings - 1st International Conference on Peer-to-Peer Computing, P2P 2001*, (September 2001), 101–102.

https://doi.org/10.1109/P2P.2001.990434

Soni, Prayudi, Y., & Sugiantoro, B. (2017). Teknik Akuisisi Virtualisasi Server Menggunakan Metode Live Forensic. *Teknomatika*, *9*(2).

Sudyana, D., Sugiantoro, B., & Luthfi, A. (2016). Instrumen Evaluasi Framework Investigasi Forensika Digital Menggunakan SNI 27037 : 2014. *JISKa*, *1*(September), 75–83.

TechNet, M. (2017). Common Internet File System. Retrieved August 12, 2017, from https://technet.microsoft.com/en-us/library/cc939973.aspx

Telematika, T. L. (2013). Sejarah dan Perkembangan Wireless LAN. Retrieved January 24, 2018, from http://www.lsp-telematika.or.id/blog/halaman/post/sejarah-dan-perkembangan-wireless-lan.html

Tengyuen, N. (2018). 4 Free Router OS Turns Old PC Into High Performance Router And Enterprise Network Switch. Retrieved January 25, 2018, from https://www.geckoandfly.com/24015/router-os-enterprise-network-switch/

Terpstra, J. H. (2006). Samba-3 by Example Practical Exercises in Successful Samba Deployment. Retrieved April 30, 2017, from https://www.samba.org/samba/docs/man/Samba-Guide/

Vernooij, J. R., Terpstra, J. H., & Carter, G. (Jerry). (2017). The Official Samba 3.5.x HOWTO and Reference Guide. Retrieved April 30, 2017, from https://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/

Volonino, L., & Anzaldua, R. (2008). *Computer Forensics For Dummies*. Indianapolis: Wiley Publishing, Inc.

Yudha, F. (2013). *PENGEMBANGAN PROSES INVESTIGASI UNTUK ANALISIS FORENSIKA DIGITAL PADA JARINGAN DENGAN PROTOKOL SERVER MESSAGE BLOCK (SMB)*. UNIVERSITAS ISLAM INDONESIA. https://doi.org/10.13140/RG.2.1.2144.0402

Yudha, F., & Prayudi, Y. (2013). Teknik Eksplorasi Bukti Digital Pada File Sharing Protokol SMB Untuk Mendukung Forensika Digital Pada Jaringan Komputer. *Konferensi Nasional Informatika*, (November).

Zatyko, K. (2007). Commentary:Defining Digital Forensics. Retrieved March 25, 2017, from https://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics