CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 1, No. 1, Mei 2018, hlm. 7-13

LIVE FORENSICS ACQUISITION FILE SHARING SAMBA PADA MIKROTIK ROUTEROS

Abdul Rohman Supriyono[1], Bambang Sugiantoro[2], Yudi Prayudi[3]

[1,3] Magister Teknik Informatika Fakultas Teknologi Industri
Universitas Islam Indonesia, Jl. Kaliurang Km 14.5 Sleman Yogyakarta
[2] Fakultas Sains dan Teknologi, UIN Sunan Kalijaga
Jl. Laksda Adisucipto Yogyakarta
Email: [1]a.rohman.sy@gmail.com, [2]bambang.sugiantoro@uin-suka.ac.id, [3]prayudi@uii.ac.id

Abstrak

Smart Router merupakan 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. Router jenis ini termasuk salah satu solusi dalam membangun jaringan lokal area yang dapat dijadikan sebagai file server dalam bertukar berkas. Tetapi terlepas dari manfaat yang ada tidak menutup kemungkinan adanya tindak kejahatan dengan memanfaatkan file sharing. Oleh karena itu, dalam bidang forensika digital dibutuhkan metode forensik live dan akuisisi live, mengingat smart router tergolong dalam kategori barang bukti elektronik yang bersifat kritis, dimana data (log) dapat hilang ketika perangkat dimatikan.

Kata kunci: *Forensik Live, Akuisisi Live, Berbagi File, RouterOS, SNI ISO/IEC 27037:2014*

LIVE FORENSICS ACQUISITION FILE SHARING SAMBA ON MIKROTIK ROUTEROS

Abstract

Smart Router is a router device that is equipped with Smart Wi-Fi software that allows us to easily manage and monitor the home network, and has more features or services than regular routers in general. Routers of this type include one solution in building a local area network that can be used as file server in file sharing. But regardless of the benefits it does not rule out the possibility of a crime by utilizing file sharing. Therefore, in the field of digital forensics required live forensic methods and live acquisitions, since the smart router belongs to a critical electronic item category, where data (log) can be lost when the device is turned off.

Keywords: *Live Forensics, Live Acquisition, File Sharing, RouterOS, SNI ISO/IEC 27037:2014*

1. PENDAHULUAN

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). 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). 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 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). Terdapatnya fasilitas penyimpanan dalam jaringan dapat membantu pengguna komputer dalam mengatasi kekurangan media penyimpanan serta 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). 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).

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. Untuk mendapatkan bukti digital apa saja yang diperoleh dari *file sharing* pada s*mart router*, maka dapat dilakukan dengan mensimulasikan berdasarkan skenario, serta menggunakan mekanisme *live forensics aquisition* untuk mendapatkan Bukti Digital dari aktivitas ilegal *file sharing.*

2. METODE PENELITIAN

Adapun bagan dari langkah-langkah yang akan ditempuh selama melakukan penelitian ini dapat dilihat pada Gambar 1 yaitu sebagai berikut:

Gambar 1. Tahapan dalam Metodologi Penelitian

2.1 Persiapan alat dan Bahan Penelitian

Adapun beberapa perangkat keras dan perangkat lunak yang dibutuhkan untuk melakukan uji simulasi dari skenario yang dibuat. Berikut ini beberapa alat dan bahan yang dipakai dalam melakukan penelitian, yang ditunjukan pada Tabel 1.

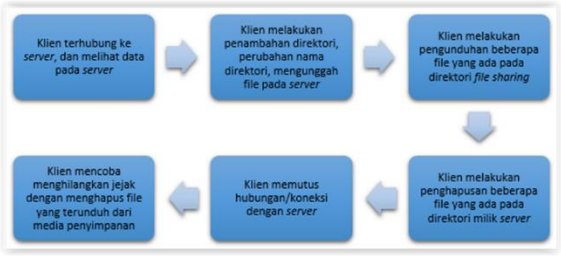
Tabel 1. Alat dan Bahan

No	***Hardware* dan *Software* (*Tools*)**	**Keterangan**
1	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)
2	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, yang sudah terpasang aplikasi Samba untuk menjalankan servis protokol SMB.
3	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.
4	*USB Thumb Drive* (JetFlash TS512MJFV30 USB Device) dengan kapasitas 512MB	Sebagai media penyimpanan pada perangakat Router MikroTik (RB951Ui-2HnD)

No	*Hardware* dan *Software* (*Tools*)	Keterangan
5	*USB Thumbdrive* (SanDisk Cruzer Edge) dengan kapasitas 32GB	Sebagai media penyimpanan klien, yang disimulasikan dengan menggunakan *thumbdrive* 32 GB.
6	AccessData® FTK® Imager 3.4.2.6	*Tools Image Forensic (Imagging Tools)*
7	DSi USB Write Blocker versi 1	*USB Write Blocker* untuk SO Windows
8	Notepad++ versi 7	Pembaca *File Log System*
9	FileZilla versi 3.30.0	Untuk mengakses Router MikroTik melalui protokol FTP
10	Autopsy 4.1.1 (RELEASE) Sleuth Kit Version: 4.2.0	Untuk melakukan membaca/membuka dan menganalisis *File Imagging*
11	Winbox-2.2.18	Untuk mengakses/me-*remote* perangkat MikroTik
12	- File gambar - File dokumen dengan autentikasi password - File MP3 - File Crack Sistem Operasi - File Aplikasi yang telah di-Crack	Beberapa file yang digunakan dalam proses pertukaran data

2.2 Skenario Kasus

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 alur dari skenario yang digunakan, yang ditunjukkan pada Gambar 2.



Gambar 2. Skenario Kasus

2.3 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.

2.4 Investigasi dan Olah TKP

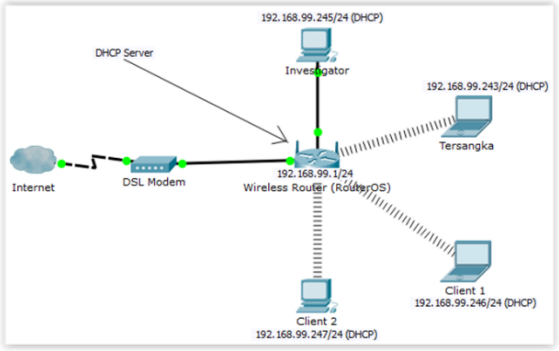
Proses olah TKP dan pengamanan terhadap barang bukti dilakukan supaya barang bukti yang didapat terhindar dari kontaminasi dari luar. Barang bukti yang didapat diambil gambarnya dengan kamera foto dan diberi label penamaan, proses pada olah TKP mengacu pada SNI ISO/IEC 27037:2014 (Badan Standarisasi Nasional 2014).

2.5 Analisis Forensik

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.

3. HASIL DAN PEMBAHASAN

Topologi yang akan digunakan pada skenario dan simulasi dijalankan pada sebuah jaringan *workstation* dengan perangkat *smart router* sebagai *file server* yang sudah terpasang aplikasi samba. Jaringan yang dirancang menggunakan alokasi IP kelas C 192.168.99.0/24, dengan jangkuan alamat IP yang digunakan untuk DHCP 192.168.99.2 – 192.168.99.254. Desain jaringan pada simulasi yang dilakukan dapat dilihat pada Gambar 3.



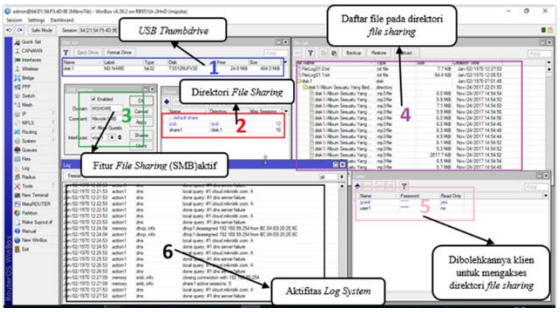
Gambar 3. Simulasi Topologi Jaringan

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.

3.1. Akuisisi Barang Bukti

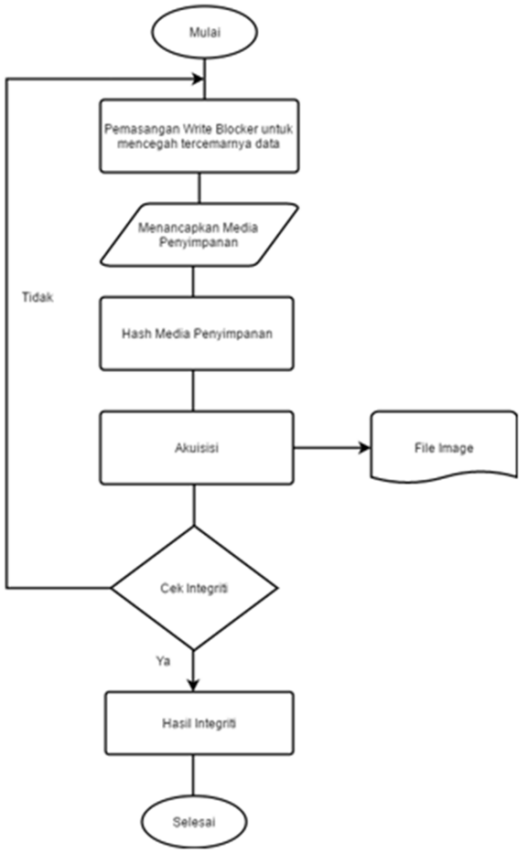
Sesuai dengan SOP pada SNI ISO/IEC 27037:2014 pada bagian ke 6.8 dan 7.1.1.3 terkait barang bukti yang menjadi prioritas dan yang akan disita atau diakuisisi, berdasarkan kondisi barang bukti elektronik pada saat ditemukan masih dalam keadaan menyala (*on*), maka dalam proses akuisisi pada barang bukti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

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.



Gambar 4. Tampilan Proses pada Perangkat Smart Router MikroTik

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. Proses akuisisi barang bukti elektronik berupa *USB Thumbdrive* berdasarkan alur pada proses akuisisi media penyimpanan, seperti pada Gambar 5.



Gambar 5. Alur Akuisisi pada Storage (USB Thumb Drive)

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. Detail *file* hasil *imaging* dapat dilihat pada Tabel 2.

Tabel 2. Detail Akuisisi USB Thumbdrive MikroTik RB951Ui-2HnD

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

Case Information	
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.

Pada Tabel 2 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 3.

Tabel 3. Akuisisi Media Penyimpanan Klien(Tersangka)

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 untuk perangkat MikroTik RB951Ui-2HnD

Pada Tabel 3 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.

3.2. Analisis

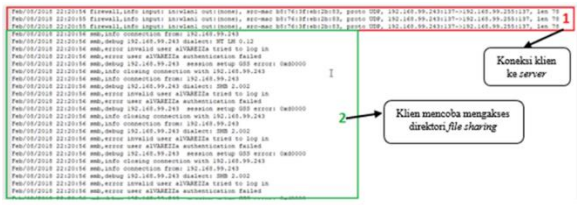
Informasi yang diperoleh pada proses akuisisi dicatat sebagai kelengkapan laporan. Terdapat beberapa catatan yang merupakan detail informasi dari barang bukti yang didapatkan, serta deskripsi singkat mengenai aktivitas terkait tindak kejahatan yang terjadi. Detail informasi dari proses akuisisi dapat dilihat pada Tabel 4.

Tabel 4. Detail Informasi Kasus

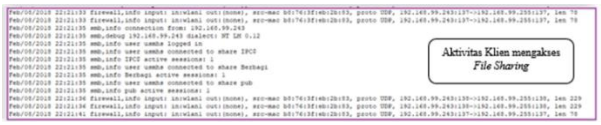
Detail Informasi	
Jenis Pelanggaran	- Penghapusan file oleh klien dari direktori server - Pengunggahan file pada direktori server
Jumlah Barang Bukti	3 (tiga) file: 2 file *image*; 1 file text
Tipe Barang Bukti Digital	- File .001 - File .txt
Ukuran Barang Bukti Digital	- BB_USB_Thumbdrive_MikroTik_RB951Ui-2HnD.001: 484 MB - BB_Tersangka_Sken02_MikroTik_RB951Ui-2HnD.001: 30024 MB - 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 6 dan Gambar 7, dimana 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), seperti tampak pada Gambar 6.

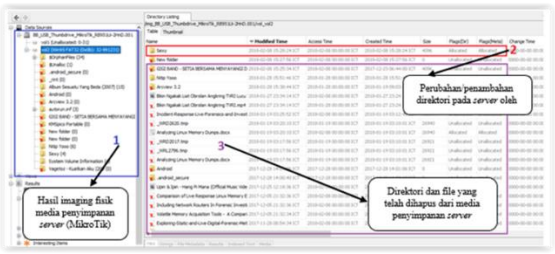


Gambar 6. Aktivitas Klien



Gambar 7. 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 8.



Gambar 8. Bukti perubahan isi dari file sharing pada USB Thumbdrive MikroTik

Pada Gambar 8 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* atau *timestamp*. 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 9.

Gambar 9. List Direktori Root pada Media Penyimpanan Klien MikroTik

Analisis dilakukan seperti pada Gambar 9 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 8. 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. 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:

a. 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.
b. 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.

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

a. Perlu 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.*
b. Diperlukan metode khusus untuk mendapatkan informasi mengenai barang bukti yang dapat diperoleh dari memori fisik pada perangkat *smart router*.

DAFTAR PUSTAKA

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

Cutter, T.C., 2017. The Best Router for Streaming on Multiple Devices. *The Cord Cutting Report*. Available at: https://cordcuttingreport.com/2017/01/21/best-router/ [Accessed January 25, 2018].

Desk, I.S., 2017. File Sharing and Piracy. *Information Systems and Technology*. Available at: https://ist.mit.edu/security/file_sharing [Accessed August 11, 2017].

Ideaing, T., 2016. These Smart Routers Solve the Biggest Wi-Fi Problems: Range & Speed. *ideaing.com*. Available at: https://ideaing.com/ideas/best-wifi-router-smart-home [Accessed February 5, 2018].

Lee, C., 2017. Benefits and Risks of File Sharing for Enterprises. *ezTalks*. Available at: https://www.eztalks.com/file-sharing/benefits-and-risks-of-file-sharing-for-enterprises.html.

Telematika, T.L., 2013. Sejarah dan Perkembangan Wireless LAN. *LSP TELEMATIKA*, pp.1–16. Available at: http://www.lsp-telematika.or.id/blog/halaman/post/sejarah-dan-perkembangan-wireless-lan.html [Accessed January 24, 2018].

Yudha, F., 2013. *PENGEMBANGAN PROSES INVESTIGASI UNTUK ANALISIS FORENSIKA DIGITAL PADA JARINGAN DENGAN PROTOKOL SERVER MESSAGE BLOCK (SMB)*. UNIVERSITAS ISLAM INDONESIA.