Jurnal Infotekmesin
Vol.10, No.02, Juli 2019
p-ISSN: 2087-1627, e-ISSN: 2685-9858

EKSPLORASI BUKTI DIGITAL PADA SMART ROUTER MENGGUNAKAN METODE LIVE FORENSICS

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

[1]Program Studi D3 Teknik Informatika, Politeknik Negeri Cilacap, Indonesia
[2]Program Studi Teknik Informatika, UIN Sunan Kalijaga, Indonesia
[3]Program Studi Teknik Informatika, Universitas Islam Indonesia
a.rohman.sy@pnc.ac.id[1], bambang.sugiantoro@uin-suka.ac.id[2], prayudi@uii.ac.id[3]

Abstrak

Kata Kunci:
Akuisisi Live;
Berbagi File;
Bukti Digital;
Forensik Live;
Smart Router.

Perangkat jaringan sebagai media file sharing serta dapat dijadikan menjadi file server mulai bermunculan, sepertihalnya perangkat smart router dapat dijadikan sebagai file server dengan menambahkan USB Thumbdrive sebagai media penyimpanannya. Dengan beragamnya perangkat router, maka menjadi tantangan tersendiri di dalam ilmu forensika digital ketika terjadi kasus dengan memanfaatkan perangkat smart router terkait dengan layanan file sharing. Maka perlu dilakukan kajian mengenai metode yang tepat dalam menginvestigasi perangkat smart router. Makalah ini membahas tentang pemakaian metode live forensics acquisition dalam menginvestigasi perangkat smart router, terhadap file log sistem terkait aktifitas pada file sharing. Dalam identifikasi dilakukan proses pencarian, mengenali, mendokumentasi hal yang berpotensi sebagai barang bukti digital terhadap processing device dan digital media storage. Dalam proses akuisisi menggunakan dua metode, yaitu menggunakan metode live acquisition pada perangkat router, dan physical acquisition pada device yang dijadikan media penyimpanan pada smart router.

Abstract

Keywords:
Live acquisition;
File Sharing;
Digital Proof;
Forensics Live;
Smart Router.

Network devices as media file sharing and can be used as file servers have begun to appear, just as smart router devices can be used as file servers by adding USB Thumb drive as storage media. With the diversity of router devices, it becomes a challenge in digital forensic science when a case occurs by utilizing a smart router device related to file-sharing services. Then it is necessary to study the right method in investigating smart router devices. This paper discusses the use of the live forensics acquisition method in investigating smart router devices, against system log files related to file-sharing activities. In identifying the process of searching, recognizing, and documenting potential things as digital evidence of processing devices and digital media storage. The acquisition process uses two methods, namely the live acquisition method on the router device and physical acquisition on the device that is used as storage media on the smart router.

✉Alamat korespondensi:
E-mail : a.rohman.sy@pnc.ac.id
p-ISSN: 2087-1627, e-ISSN: 2685-9858

1. Pendahuluan

Dengan kemajuan teknologi yang dimiliki oleh perangkat *smart router*, maka perangkat *smart router* pun banyak diterapkan di kalangan perumahan dan kantor kecil untuk dijadikan sebagai *file server*, hanya dengan menambahkan perangkat *USB Thumbdrive* sebagai *media* penyimpanan. Terdapat beberapa jenis *smart router* dengan sistem operasi OpenWrt yang dapat dimanfaatkan untuk *file sharing* menggunakan aplikasi Samba.

File sharing merupakan sebuah metode dalam pendistribusian dan pertukaran *file* atau menyediakan akses informasi yang tersimpan secara digital, seperti program komputer, *file* teks, *video, audio, image*, grafik dan buku elektronik dari satu komputer ke komputer lain melalui jaringan yang memungkinkan pertukaran *file* secara lokal maupun global. Terdapat beberapa cara diantaranya dengan penggunaan *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* [1]. Adapun manfaat yang dimiliki oleh *file sharing* diantaranya: Nyaman; Hemat Biaya; Hemat Waktu; Hemat Ruang Penyimpanan; Integritas Data Meningkat; Meningkatnya Aksesibilitas; Mudah dalam mengakses *File* [2]. Terdapat dampak negatif yang ditimbulkan dari fasilitas ini, seperti pertukaran konten – konten ilegal yang dapat menimbulkan tindak kejahatan serta melanggar hukum dalam kepemilikan hak cipta [3].

Menurut Seth Rosenblatt memaparkan bahwa setidaknya terdapat 13 dari router nirkabel jenis *smart* wifi router dapat diambil alih dari jaringan lokal oleh peretas melalui jaringan LAN maupun jaringan WAN [4]. Hal seperti ini yang menjadikan tantangan dalam bidang forensika digital dalam mencari informasi pada perangkat router yang dapat berpotensi sebagai bukti elektronik yang semakin beragam jenisnya. *Smart router* termasuk bukti elektronik yang bersifat kritis, dimana perangkat membutuhkan sistem dalam keadaan menyala (*running*) pada saat dilakukan proses investigasi, dan harus ditangani secara. Melihat adanya potensi kejahatan pada aktifitas *file sharing* yang melibatkan perangkat *smart router* sebagai *file server*, sehingga perlu dilakukannya proses investigasi forensik dengan menggunakan metode *live forensics* dan *live acquisition* pada sistem yang masih dalam keadaan menyala supaya barang bukti seperti *file* log tidak hilang. Serta bagaimana proses investigasi yang efektif pada perangkat *Smart Router* dalam kasus – kasus kejahatan yang memanfaatkan fitur atau media *file sharing*.

2. Tinjauan Pustaka

Sebelumnya [5], telah melakukan analisis mengenai tindak kejahatan yang melibatkan protokol *file sharing*, terutama pada protokol SMB, dengan menguji terhadap metode yang digunakan untuk mendapatkan barang bukti digital pada *file sharing*. Sementara itu [6], menggunakan metode *live forensics* dalam mengakuisisi aktivitas serangan pada perangkat router. Metode *live forensics* juga dipakai oleh [7] dalam menemukan informasi digital pada aplikasi *instan messenger*. Selain metode yang digunakan dalam melakukan investigasi, prosedur juga sangat dibutuhkan, seperti [8] melakukan evaluasi pada dokumen SNI ISO/IEC 27037:2014 tentang prosedur forensika digital yang harus sesuai dengan aturan hukum dan mekanisme. SOP SNI ISO/IEC 27037:2014 juga digunakan oleh [9] untuk menganalisis konten pada aplikasi *Blackberry Messenger*. Sementara itu[10], merancang kerangka investigasi pada perangkat *server* yang berdasarkan dokumen SNI ISO/IEC 27037:2014.

Penelitian pada makalah ini berfokus pada metode *live forensics* dan *live acquition* yang digunakan untuk menganalisis perangkat *smart router* yang tidak diperkenankan untuk dimatikan dalam melakukan proses investigasi.

3. Tinjauan Pustaka

3.1 Digital Forensics

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 [11]. Terdapat beberapa prinsip dasar dalam *digital forensics* yang tertuang di dalam SNI ISO/IEC 27037:2014, antara lain: *Scope; Normative Reference; Terms and definitions; Abbreviated Terms; Overview; Key Components of identification, collection, acquisition, and preservation of digital evidence; Instance of identification, collection, acquisition, and preservation* [12].

3.2 Kerangka Investigasi

Setiap investigator harus memperhatikan dan mengikuti prosedur atau kerangka kerja dalam forensika digital. Investigasi forensik harus dilakukan secara ilmiah dan harus sesuai dengan semua persyaratan hukum yang berlaku[13]. Penelitian awal dibidang ini difokuskan pada pembahasan Kerangka Investigasi forensik *file-sharing* samba pada mesin peladen berdasarkan SNI ISO/IEC 27037:2014, bahwa penanganan investigasi forensik harus lebih hati – hati terutama pada sistem kritis yang memiliki karakteristik sistem yang tidak diperkenankan untuk dimatikan, seperti halnya pada mesin peladen *file-sharing* berbasis Samba, pada perangkat ini proses investigasi dapat dilakukan akuisisi secara langsung pada perangkat dan akuisisi secara langsung melalui jaringan klien[10].

3.3 *Live Forensics*

Di era komputasi moderen, *live forensics* merupakan pelengkap dalam proses analisis statis, dimana *live forensics* memungkin kan untuk memulihkan dan menganalisis konten memori, proses dan data tanpa mematikan sistem. *Live forensics* memainkan peran yang penting selama pemeriksaan sistem karena potensi ketersediaan bukti digital yang mudah hilang, seperti proses yang sedang berjalan, koneksi jaringan, *port*, yang terbuka dan kinci enkripsi, dan lain-lain [14].

3.4 *Log File*

Di dalam komputasi *file log* adalah *file* yang mencatat informasi, kejadian, dan kondisi yang dibuat secara otomatis, baik yang terjadi pada sistem operasi atau perangkat lunak komunikasi yang sedang berjalan yang sesuai dengan sistem tersebut (perangkat jaringan). *File log* ini tidak adanya standar untuk lokasi, penggunaan, format, dan ukuran *file log* untuk masing-masing sistem dan perangkat, dan biasanya berupa *file* teks [15].

3.5 Samba

Samba adalah sebuah perangkat *Open Source/Free Software* yang menyediakan layanan berbagi *file* dan layanan untuk mencetak yang dapat dilakukan oleh klien SMB/CIFS. Samba tersedia secara gratis dan memungkinkan interoperabilitas antara *server* Linux/Unix dan klien berbasis Windows [16]. Dalam aplikasinya, layanan berbagi *file* dalam jaringan dapat memungkinkan terjadinya perpindahan konten ilegal dan pelanggaran hukum dalam kepemilikan hak cipta ataupun perpindahan suatu konten yang dapat menimbulkan suatu tindak kejahatan [3]. Beberapa tindak kejahatan yang diakibatkan penyalahgunaan berbagi *file* antara lain: kurang amannya dalam mengakses suatu file, penyebaran *worm*, *virus*, tindakan *phising*, plagiarisme atau pelanggaran hukum kepemilikan hak cipta seperti mengambil gagasan orang lain dan menjadikannya milik sendiri, hilangnya privasi individu atau perusahaan yang memungkinkan informasi sensitif individu atau perusahaan dapat diakses dengan mudah oleh pihak lain yang tidak sah [2], [5].

3.6 *Smart 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 dapat memudahkan kita dalam mengatur dan memantau jaringan rumah, dengan fitur atau layanan yang dimiliki lebih banyak dibandingkan dengan router biasa pada umumnya [17]. Kelebihan lain yang dimiliki oleh router jenis ini, seperti memonitor perangkat jaringan, membatasi akses ke dalam situs tertentu, memantau kamera jaringan secara *live*, dan *streaming foto* atau *video* [18]. Fitur lain yang dapat dimanfaatkan dalam memenuhi keperluan rumah seperti menjadikan router sebagai *media file sharing* dimana hanya menambahkan perangkat penyimpanan atau *media storage*, dan menjadikan sebagai penyimpanan file bersama [19].

3.7 OpenWrt

OpenWrt adalah sistem operasi Linux yang menargetkan perangkat *embedded* dengan menyediakan *filesystem* yang dapat ditulis sepenuhnya dengan manajemen paket, sehingga pengguna dari vendor dapat leluasa untuk memilih dan mengkonfigurasi aplikasi sehingga dapat melakukan perubahan *device* melalui penggunaan aplikasi yang sesuai [20]. Berangkat dari hal tersebut maka OpenWrt dapat digunakan untuk jenis perangkat router, seperti produk router GL-inet [21]. Jenis router ini dapat disebut sebagai perangkat *smart router* dikarenakan router jenis ini selain dapat berfungsi layaknya perangkat router pada umumnya, perangkat ini dapat difungsikan sebagai *media file sharing* hanya dengan menambahkan perangkat *USB Thumbdrive* atau *hard drive* eksternal dengan Samba sebagai aplikasi *file sharing*-nya [22], [23].

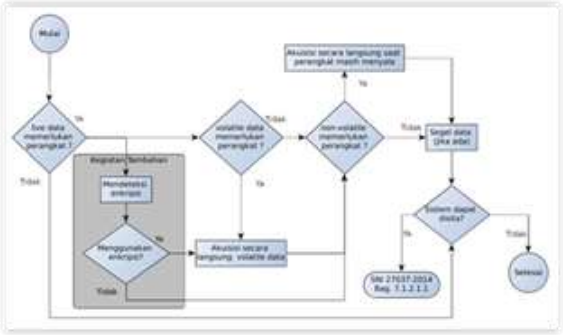
4. Metodologi

Standar Nasional Indonesia (SNI) ISO/IEC 27037:2014 yang mengatur prosedur akuisisi barang bukti elektronik dan barang bukti digital khusus untuk perangkat dalam kondisi menyala, telah mengaturnya menjadi 4 tahap pada bagian 7.1.2.1.1. Dimana tahapan tersebut diantaranya [12]:

1) **Identifikasi:** terdapat beberapa proses yang dilakukan pada tahap identifikasi, seperti: perencanaan investigasi, persiapan dan pengarahan team, penilaian resiko keamanan TKP, pengamanan TKP, pencarian barang bukti, identifikasi barang bukti, menentukan prioritas barang bukti, dokumentasi, pencatatan barang bukti.
2) **Pengumpulan:** terdapat beberapa proses yang dilakukan pada tahap pengumpulan, seperti: penentuan barang bukti yang disita atau diakuisisi di TKP, melakukan penyitaan barang bukti, memberikan label barang bukti, mempacking barang bukti, mengumpulkan keterangan-keterangan verbal dari saksi-saksi.
3) **Akuisisi:** terdapat beberapa proses yang dilakukan pada tahap akuisisi, seperti: pemeriksaan aspek keamanan barang bukti, penentuan model akuisisi yang dilakukan, pelaksanaan akuisisi, verifikasi hasil akuisisi.
4) **Preservasi:** terdapat beberapa proses yang dilakukan pada tahap preservasi, seperti: memberikan segel barang bukti, melakukan

pemeriksaan aspek keamanan pemindahan barang bukti, pemindahan barang bukti, penyimpanan barang bukti.

Adapun ilustrasi proses akuisisi bukti digital pada perangkat dalam kondisi yang masih menyala dapat dilihat pada Gambar 1.



Gambar 1. Akuisisi Bukti Elektronik dalam Kondisi Menyala

5. Hasil dan Pembahasan

5.1. Identifikasi

Identifikasi merupakan suatu proses dalam melakukan pencarian, penggalian, dan pendokumentasian semua hal yang bisa berpotensial menjadi sebuah barang bukti digital. Dalam penelitian ini bukti berupa *smart router* berbasis OpenWrt. Hasil dari tahap ini dapat dilihat pada Tabel 1 dan Gambar 2:

Tabel 1. Spesifikasi Alat

No	Tipe Spesifikasi	Spesifikasi Barang Bukti
1	Brand	GL-inet
2	Brand Model	GL-AR300
3	OS	OpenWrt Chaos Calmer 15.05 r47065
4	ROM	16 MB
5	Thumbdrive	3824 MB

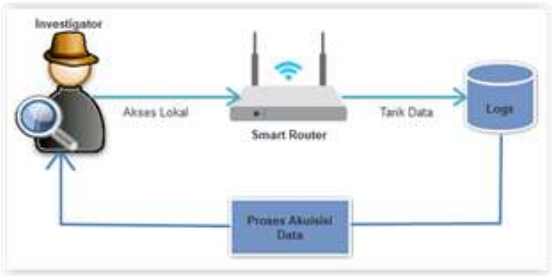
Gambar 2. GL-inet sebagai Barang Bukti Fisik

5.2. Pengumpulan

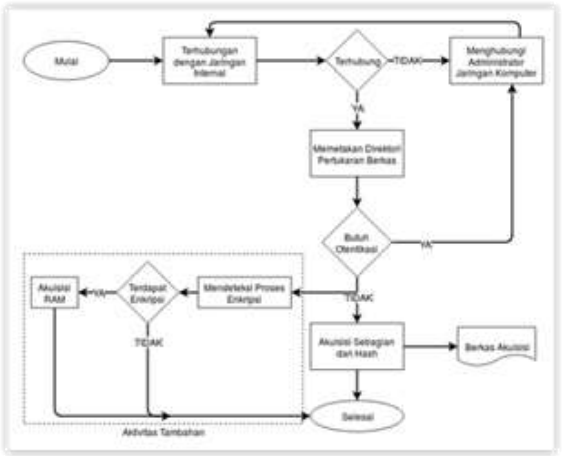
Pengumpulan yaitu suatu proses penanganan barang bukti digital seperti peralatan yang terindikasi menjadi barang bukti, dipindahkan dari lokasi TKP ke laboratorium untuk kemudian diakusisi dan dianalisis, supaya barang bukti dapat dipastikan aman.

5.3. Akuisisi

Akuisisi merupakan sebuah proses dengan menggandakan barang bukti digital dan mendokumentasikannya setiap aktifitas yang dilakukan. Pada penelitian ini dilakukan melalui jaringan lokal secara *live acquisition*. Untuk mekanisme akuisisi data secara *live acquisition* dapat dilihat pada Gambar 3 dan untuk alur dari akuisisi melalui jaringan dapat dilihat pada Gambar 4.



Gambar 3. Mekanisme *Investigasi Live Acquisition*

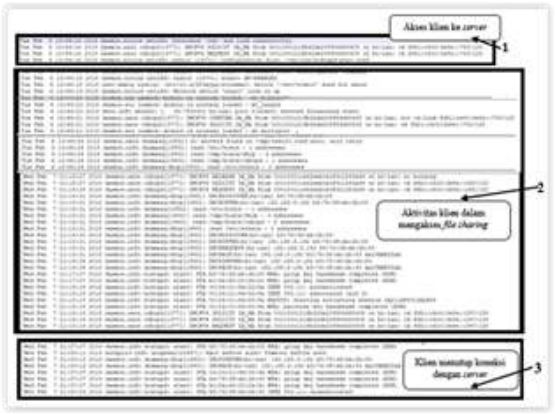


Gambar 4. Akuisisi Perangkat Router Melalui Jaringan

Berikut ini merupakan tampilan dari proses yang terjadi pada perangkat GL-inet, terlihat pada Gambar 5.

Gambar 5. Tampilan Proses pada GL-inet

Dalam mendapatkan aktivitas yang terjadi terkait pemanfaatan perangkat sebagai *media file sharing*, maka untuk mendapatkan *log system* dilakukan menggunakan *live acquisition* dengan cara melakukan proses copy paste *file log* tersebut. L*og system* yang diperoleh pada perangkat *smart router* GL-inet AR300 dapat dilihat pada Gambar 6.



Gambar 6. Aktivitas Log pada *smart router* GL-inet AR300

Akuisisi juga dilakukan pada *media* penyimpanan *USB Thumbdrive* yang dijadikan sebagai *media file sharing*. Berikut hasil dari imaging pada *USB Thumbdrive* menggunakan tools FTK Imager dapat dilihat pada Tabel 2 dan Gambar 7.

5.4. Preservasi

Preservasi merupakan suatu proses pengamanan terhadap barang bukti digital yang berpotensi dan perangkat digital yang dapat memuat barang bukti digital yang juga berpotensi dari kerusakan dan hal-hal yang menyebabkan barang bukti tersebut bisa hilang.

Tabel 2. Akuisisi *USB Thumbdrive* GL-inet AR300

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
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.

Gambar 7. Hasil Imaging *Media* Penyimpanan GL-inet AR300

5.5. Analisis Forensik

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 terlihat pada Tabel 3.

Tabel 3. Detail Informasi Kasus pada Perangkat GL-inet

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_GL-inet_AR300.001: 3824 MB - BB_Tersangka_Sken02_GL-inet.001: 30024 MB - 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* pada perangkat tersebut. Pada *log* terlihat adanya aktivitas klien yang mencoba melakukan koneksi ke *server*, dan didapat IP DHCPV6 fd51:c4c0:3e8e::783/128, dapat dilihat pada Gambar 8, dan 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*, dapat dilihat pada Gambar 9 dan Gambar 10.

Gambar 8. Koneksi Klien ke *Server*

Gambar 9. Klien Melihat Isi Direktori *Server*

Gambar 10. Aktivitas Klien terkait tindakan ilegal *file sharing*

Untuk menguatkan dalam menganalisis maka perlu dilakukannya analisa terhadap hasil image *media* penyimpanan *server* untuk membuktikan aktivitas yang dilakukan klien. Berikut merupakan tampilan hasil image dari *media* penyimpanan *server*, yang ditunjukan pada Gambar 11.

Gambar 11. List Direktori Root pada *Media* Penyimpanan *Server* GL-inet

Pada Gambar 11 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 seperti terlihat pada Gambar 12.

Gambar 12. List Direktori *Root* pada *Media* Penyimpanan Klien

Pada Gambar 12 tampak terdapat 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*, yang dapat dilihat pada Gambar 11. 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.

6. Kesimpulan

Terdapat dua metode yang digunakan dalam melakukan proses akuisisi, yaitu menggunakan metode *live acquisition* atau *logical acquisition* pada perangkat router, dan *pysical acquisition* pada device yang dijadikan sebagai *media file sharing* pada perangkat *smart router*.

Membutuhkan pengembangan lebih lanjut mengenai teknik ataupun metode yang digunakan dalam menginvestigasi perangkat *smart router*, dikarenakan semakin beragamnya perangkat *smart router* dari berbagai vendor dan sistem operasi yang ada di dalamnya. Serta membutuhkan pengujian lebih lanjut dari metode *live forensics acquisition* terhadap kasus *cybercrime* yang terjadi.

Daftar Pustaka

[1] M. Rouse, "Definition peer-to-peer (P2P)," *Techtarget*, 2014. [Online]. Available: http://searchnetworking.techtarget.com/definition/peer-to-peer. [Accessed: 24-Jan-2018].

[2] C. Lee, "Benefits and Risks of File Sharing for Enterprises," *ezTalks*, 18-Jan-2017.

[3] T. ISU, "File Sharing & Copyrighted Materials," *Iowa State University*, 2017. [Online]. Available: https://www.it.iastate.edu/policies/filesharing/. [Accessed: 11-Aug-2017].

[4] S. Rosenblatt, "Top Wi-Fi routers easy to hack, says study," *cnet*, 2013. [Online]. Available: https://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/. [Accessed: 21-Feb-2018].

[5] F. Yudha and Y. Prayudi, "Teknik Eksplorasi Bukti Digital Pada File Sharing Protokol SMB Untuk Mendukung Forensika Digital Pada Jaringan Komputer," *Konf. Nas. Inform.*, no. November, 2013.

[6] M. I. Mazdadi, I. Riyadi, and A. Luthfi, "Live Forensics on RouterOS using API Services to Investigate Network Attacks," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 2, pp. 406–410, 2017.

[7] T. D. Larasati and B. C. Hidayanto, "ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN APLIKASI INSTANT MESSENGER PADA SISTEM OPERASI WINDOWS 10," *SESINDO*, vol. 6, no. November, pp. 456–256, 2017.

[8] D. Sudyana, B. Sugiantoro, and A. Luthfi, "Instrumen Evaluasi Framework Investigasi Forensika Digital Menggunakan SNI 27037 : 2014," *JISKa*, vol. 1, no. September, pp. 75–83, 2016.

[9] D. Hariyadi, W. W. Winarno, and A. Luthfi, "Analisis Konten Dugaan Tindak Kejahatan Dengan Barang Bukti Digital Blackberry Messenger," *Teknomatika*, vol. 9, no. 1, pp. 81–89, 2016.

[10] D. Hariyadi and A. R. Supriyono, "Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI ISO/IEC 27037:2014," *TELEMATIKA*, vol. 14, no. 01, pp. 62–67, 2017.

[11] L. Daniel and L. Daniel, *Digital Forensic For Legal Profesionals*. 225 Wyman Street, Waltham, MA 02451, USA: Syngress, 2012.

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

[13] M. Kohn, J. Eloff, and M. S. Olivier, "Framework for a Digital Forensic Investigation," *Proc. ISSA 2006 from Insight to Foresight Conf. Sandt.*, 2006.

[14] M. Bashir and M. Khan, "Triage in Live Digital Forensic Analysis," *Int. J. Forensic Comput. Sci.*, vol. 8, no. 1, pp. 35–44, 2013.

[15] A. La Rosa, "Log Monitoring: not the ugly sister," *Pandorafms*, 2018. [Online]. Available: https://blog.pandorafms.org/log-monitoring/. [Accessed: 02-Mar-2018].

[16] Samba.org, "What is Samba," *Samba.org*, 2017. [Online]. Available: https://www.samba.org/samba/what_is_samba.html. [Accessed: 30-Apr-2017].

[17] T. Ideaing, "These Smart Routers Solve the Biggest Wi-Fi Problems: Range & Speed," *ideaing.com*, 2016. [Online]. Available: https://ideaing.com/ideas/best-wifi-router-smart-home. [Accessed: 05-Feb-2018].

[18] Pcmag, "Smart Wi-Fi router," 2018. [Online]. Available: https://www.pcmag.com/encyclopedia/term/65987/smart-wi-fi-router. [Accessed: 11-Jan-2018].

[19] T. C. Cutter, "The Best Router for Streaming on Multiple Devices," *The Cord Cutting Report*, 2017. [Online]. Available:

https://cordcuttingreport.com/2017/01/21/best-router/. [Accessed: 25-Jan-2018].
[20] OpenWrt, "Welcome to the OpenWrt Project," *openwrt.org*, 2018. [Online]. Available: https://openwrt.org/. [Accessed: 02-Mar-2018].
[21] Alzhao, "Build your own openwrt for GL.iNet," *gl-inet.com*, 2014. [Online]. Available: https://www.gl-inet.com/build-your-own-openwrt-for-gl-inet/. [Accessed: 03-Mar-2018].
[22] OpenWrt, "Share USB Hard-drive with Samba using the Luci web-interface," *wiki.openwrt.org*, 2018. [Online]. Available: https://wiki.openwrt.org/doc/recipes/usb-storage-samba-webinterface. [Accessed: 03-Mar-2018].
[23] ClauzClauz, "How to make a Samba NAS with an OpenWrt router," *wiki.ninux.org*, 2011. [Online]. Available: http://wiki.ninux.org/OpenWrtNAS. [Accessed: 03-Mar-2018].