TELEMATIKA, Vol. 14, No. 01, BULAN, TAHUN, Pp. 62 – 67
ISSN 1829-667X

KERANGKA INVESTIGASI FORENSIK PADA PELADEN PERTUKARAN BERKAS SAMBA BERDASARKAN SNI ISO/IEC 27037:2014

Dedy Hariyadi [(1)], Abdul Rohman Supriyono [(2)]
Komunitas Forensik Digital Indonesia (ForKID) [(1)]
Magister Teknik Informatika Universitas Islam Indonesia [(2)]
e-mail : milisdad@gmail.com [(1)], a.rohman.sy@gmail.com [(2)]

Abstract

Network File System (NFS) and Common Internet File System (CIFS) are commonly used protocols for exchange of files on a computer network connected to Network Attached Storage. The easy way to exchange files on a network does not close the possibility of illegal file exchanges or files containing crime. Therefore, a forensics investigation approach is required in the process of exchange of files on a computer network. The acquisition process in this research is done by 2 models, namely: direct acquisition on file-sharing and file acquisition system directly through the network. Acquisitions directly on a server are focused on the log acquisition process of a server that results from a samba service and a file exchange directory. Acquisition directly through the network focuses on the directory of file exchange accessed by the user. This acquisition model is based on SNI ISO / IEC 27037: 2014 concerning Guidelines on the Identification, Collection, Acquisition and Preservation of Digital Evidence that focuses on mission-critical systems are involved that cannot be shutdown.

Keywords : NFS, CIFS, Samba, SNI, Forensics

Abstrak

Network File System (NFS) dan *Common Internet File System (CIFS)* merupakan protokol yang biasa dipakai dalam melakukan pertukaran berkas di dalam sebuah jaringan komputer yang terhubung dengan *Network Attached Storage*. Mudahnya dalam bertukar berkas dalam sebuah jaringan tidak menutup kemungkinan adanya pertukaran berkas yang bersifat ilegal ataupun berkas yang mengandung tindak kejahatan. Oleh karena itu, diperlukan sebuah model pendekatan investigasi forensik dalam proses pertukaran berkas di sebuah jaringan komputer. Proses akuisisi dalam penelitian ini dilakukan dengan 2 model, yaitu: akuisisi secara langsung pada mesin peladen *file-sharing* dan akuisisi secara langsung melalui jaringan. Akuisisi secata langsung pada mesin peladen berfokus pada proses akuisisi log dari mesin peladen yang dihasilkan dari layanan samba dan direktori pertukaran berkas. Akusisi secara langsung melalui jaringan berfokus pada direktori pertukaran berkas yang diakses oleh pengguna. Model akuisisi ini berdasarkan SNI ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital yang fokus pada barang bukti elektronik kritis dengan kondisi tidak diperkenankan mati atau *shutdown*.

Kata Kunci : NFS, CIFS, Samba, SNI, Forensik

1. PENDAHULUAN

Protokol *file-sharing* atau pertukaran berkas yang diperkenalkan oleh Ward Christensen pada tahun 1978 merupakan titik awal pertukaran suatu berkas melalui jaringan. Pada saat itu jaringan yang digunakan adalah modem. Teknologi untuk pertukaran berkas melalui jaringan disebut XMODEM (Glossbrenner 1984).

Pertukaran berkas melalui jaringan memiliki manfaat secara umum diantaranya, mengurangi penggunaan kertas; meningkatkan produktivitas, kecepatan dan efisiensi pengambilan keputusan; visibilitas teknologi informasi, dan kemampuan eDiscovery (Shey 2014). Berdasarkan observasi protokol yang biasa digunakan dalam pertukaran berkas didalam

sebuah Network Attached Storage menggunakan Network File System (NFS) dan Common Internet File System (CIFS). NFS pertama kali diperkenalkan oleh Sun Microsystem, Inc. sebagai protokol yang menyediakan akses jarak jauh terhadap pertukaran berkas dalam jaringan (Sun Microsystems Inc. 1989)□. CIFS merupakan versi lain dari Server Message Block yang pertama kali diperkenalkan oleh Microsoft, selanjutnya dikenal sebagai protokol SMB/CIFS (Heizer et al. 1996)□.

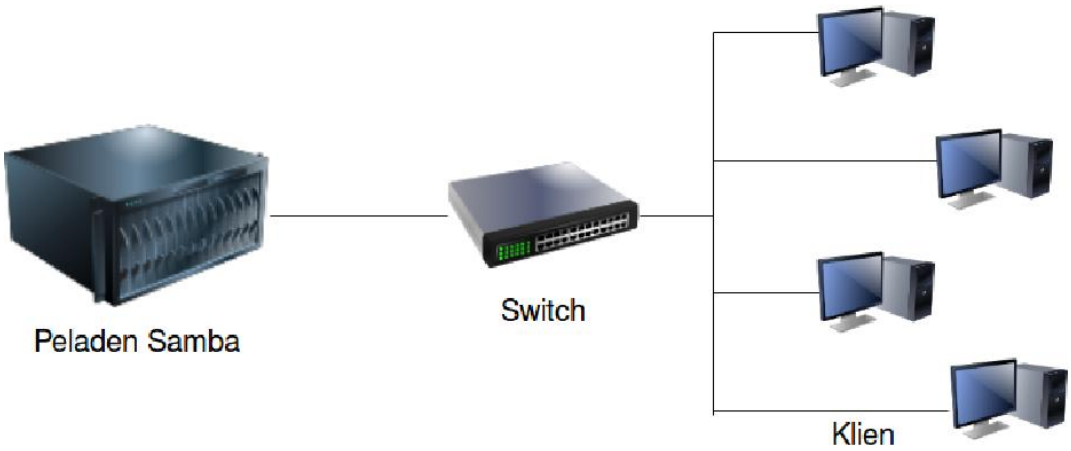
Adanya protokol tersebut sangat mudah pertukaran berkas dalam sebuah jaringan. Terutama pertukarangan berkas dalam jaringan lokal. Tidak menutup kemungkinan pertukaran berkas tersebut terdapat pertukaran berkas yang sifatnya ilegal atau pun berkas yang mendukung untuk tindak kejahatan. Oleh sebab itu diperlukan sebuah model pendekatan dalam menganalisis pertukaran berkas dalam sebuah peladen pertukaran berkas/*file-sharing* server.

2. *FILE-SHARING* SAMBA

Implementasi dari protokol SMB/CIFS pada platform sistem operasi GNU/Linux menggunakan Samba. Peladen Samba menyediakan dukungan pertukaran berkas dan printer yang bersifat cross-platform dengan sistem operasi seperti, Microsoft Windows, OS X, dan sistem Unix lainnya. Fungsi dari peladen Samba sebagai berikut (Ubuntu 2015)□:

1. Bertindak sebagai peladen untuk klien protokol SMB/CFIS yaitu: pertukaran berkas dalam satu direktori, berbagi printer, dan berkolaborasi dalam menulis sebuah berkas dokumen.
2. Bertindak sebagai Domain Controller pada jaringan lokal dengan sistem operasi Microsoft Windows maupun GNU/Linux dalam hal pengelola autentikasi pengguna.

Dalam penelitian ini dibangun sebuah lingkungan untuk pertukaran berkas yang terdiri dari peladen Samba sebagai penyedia konten atau berkas ilegal, switch sebagai penghubung dan 2 buah klien yang berfungsi sebagai pengunggah konten ilegal dan pengunduh konten ilegal. Topologi jaringan bersifat flat atau tidak menggunakan switch layer 2. Peladen Samba terinstall pada sistem operasi Ubuntu 16.04 dengan versi Samba 4.3. Adapun topologi yang dibangun tampak seperti pada Gambar 1.



Gambar 1. Topologi Jaringan pada Peladen Samba

3. PENELITIAN TERKAIT *FILE-SHARING* FORENSICS

Tindak kejahatan yang memanfaatkan pertukaran berkas telah banyak diteliti dengan berbagai model. Hal ini disebabkan model pertukaran berkas juga melalui berbagai macam protokol. Model investigasi forensik dalam proses analisis setiap protokol juga berbeda. Analisis forensik untuk protokol Gnutela yang diperhatikan adalah queries, swarming information, browse hosts, dan file downloads. Pda protokol BitTorrent yang perlu diperhatikan dalam analisis forensik adalah tracker messages, piece information exchange, Peer exchange, dan file downloads (Liberatore et al. 2010)□.

BitTorrent memiliki pola peer-to-peer yang berbeda jadi pendekatan analisis forensiknya tidak menggunakan model konvensional. Selain pendekatan analisis forensik dalam tindak kejahatan pertukaran berkas ilegal juga pendekatan secara hukum. Investigasi yang dapat dilakukan saat terjadi tindak kejahatan pertukaran berkas ilegal menggunakan protokol BitTorrent adalah mengakuisisi IP penyebar berkas, mengklasifikasi penyebar berkas berdasarkan aksi, identifikasi dan klasifikasi dari penyebar berkas, dan menganalisis komputer penyebar (Park et al. 2015).

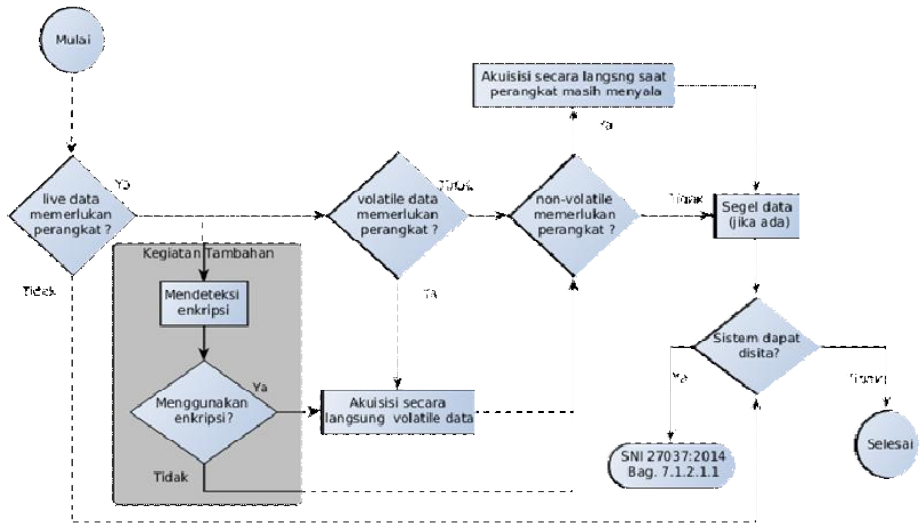
Pertukaran berkas saat ini tidak hanya pada jaringan perangkat komputer namun jaringan yang lebih majemuk seperti jaringan pada perangkat gemerak. Artefak dari aplikasi pertukaran berkas yang digunakan tindak kejahatan masih tetap tertinggal pada perangkat. Sebagai contoh ditemukan sebuah nama berkas dan data yang terkait dari sebuah aplikasi OneDrive dan Box yang dapat dipulihkan dari media penyimpanan internal ponsel bersistem operasi Android (Daryabar et al. 2016).

4. KERANGKA INVESTIGASI

Dalam penelitian ini mengadopsi Standar Nasional Indonesia (SNI) ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (Badan Standardisasi Nasional 2014). Pedoman ini memiliki cakupan yang luas diantaranya:

a. Media penyimpanan yang digunakan pada komputer
b. Perangkat gemerak
c. Perangkat navigasi
d. Citra digital dan kamera termasuk CCTV
e. Komputer yang terhubung dengan jaringan
f. Berbagai protokol jaringan seperti TCP/IP
g. Perangkat yang memiliki kemiripan fungsi sesuai hal diatas

Pada proses akuisisi 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. Secara umum diagram proses akuisisi secara logical dapat dilihat pada Gambar 2.



Gambar 2. Petunjuk Akuisisi Bukti Elektronik dalam Kondisi Menyala

Berdasarkan Gambar 1 dengan status sebagai mesin peladen yang tidak boleh mati maka proses akuisisi menggunakan ketentuan akuisisi perangkat digital dengan dalam kondisi menyala. Lima hal yang dilakukan dalam mengakuisisi perangkat digital dalam kondisi menyala:

a. 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.
b. Dalam melakukan akuisisi secara langsung diperkenankan untuk mengakses sistem secara langsung baik secara fisik atau pun mengakses jarak jauh.
c. Disarankan menggunakan tools yang terpercaya atau tools yang dibawa sendiri. Saat menjalankan tools tersebut harus selalu dicatat.
d. Berkas yang diakuisisi sebaiknya dikompres dan tentukan nilah hash-nya.
e. Memastikan hasil akuisisi integritasnya terjaga dan tidak mudah rusak.

Akuisisi sebagian atau partial acquisition harus dicatat semua infromasi 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.

5. AKUISISI *FILE-SHARING*

Proses akuisisi dalam penelitian ini dilakukan 2 model yaitu akuisisi secara langsung pada mesin peladen *file-sharing* dan akuisisi secara langsung melalui jaringan.

5.1. AKUISISI LANGSUNG PADA MESIN PELADEN

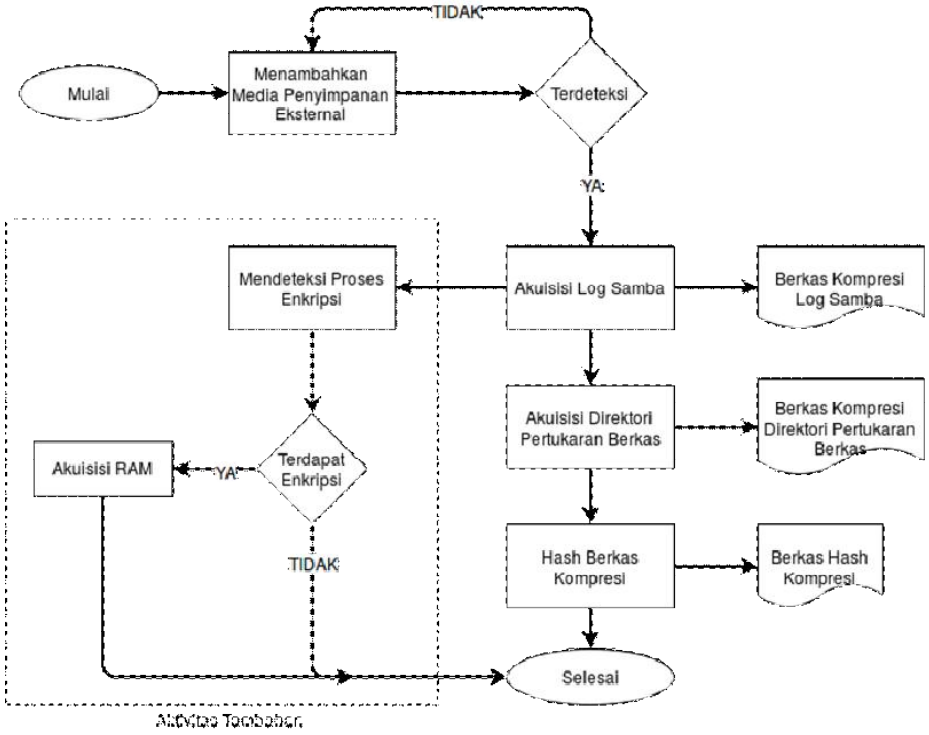
Akuisisi langsung pada mesin peladen *file-sharing* memerlukan sebuah media penyimpanan eksternal yang steril dan tidak mudah terkontaminasi. Tidak hanya media penyimpanan eksternal yang harus terjaga, berkas hasil dari akuisisi juga harus terjaga dengan baik. Proses akuisisi fokus pada log dari peladen yang dihasilkan dari layanan Samba dan direktori pertukaran berkas. Akusisi sebagian ini menghasilkan berkas yang terkompresi tentunya berkas tersebut harus melalui proses hash. Adapun tiga berkas yang dihasilkan, yaitu berkas kompresi log layanan Samba, berkas kompresi direktori pertukaran berkas dan berkas yang berisi nilai hash dari dua berkas tersebut.

Pada kasus tertentu misalkan adanya proses enkripsi maka dilakukan akuisisi data volatile karena ada proses sistem operasi dan enkripsi tercatat di RAM. Gambar 3 menjelaskan alur dari akuisisi langsung pada mesin peladen *file-sharing*.

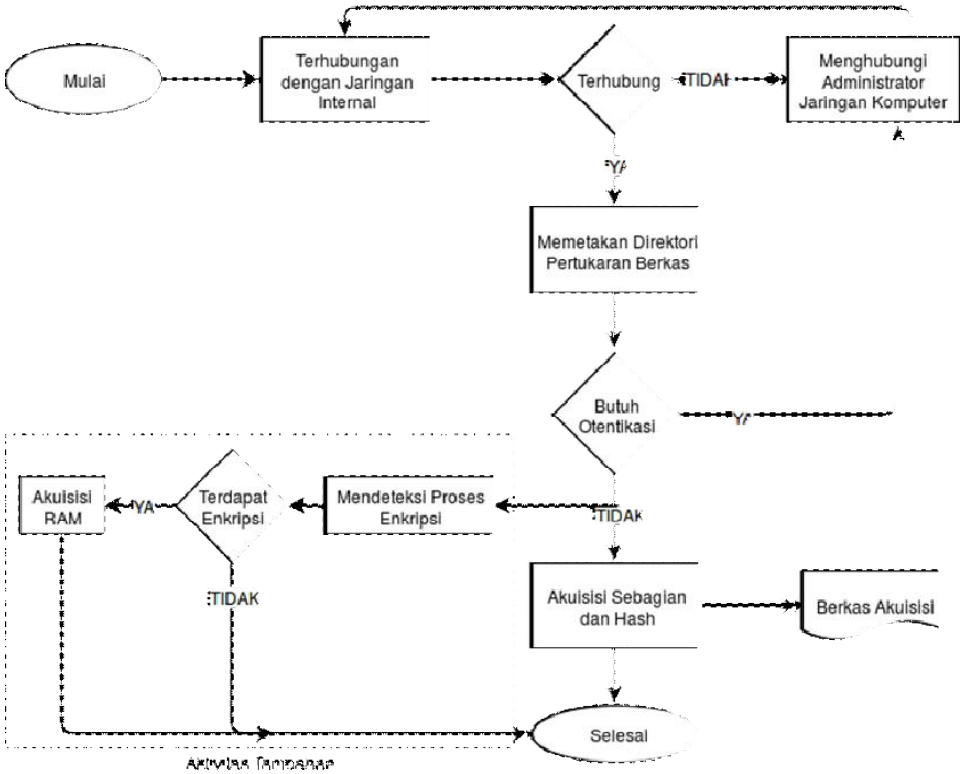
5.2. AKUISISI LANGSUNG MELALUI JARINGAN

Akuisisi secara langsung melalui jaringan dilakukan pada dua lingkungan sistem operasi, yaitu MS Windows dan Linux. Sistem operasi MS Windows yang digunakan adalah MS Windows 7 sedangkan Linux menggunakan Linux Mint 17.3. Baik MS Windows dan Linux Mint memiliki kesamaan prosedur saat pertama kali melakukan akuisisi, yaitu peladen *file-sharing* yang menggunakan samba dipetakan terlebih dahulu. Teknik di MS Windows menggunakan Map network drive sedangkan di Linux Mint atau sistem operasi Linux lainnya menggunakan mounting. Sedangkan teknik akuisisi pada sistem operasi MS Windows adalah mengakuisisi drive yang terdeteksi hasil Map network drive. Untuk teknik akuisisi pada sistem operasi Linux adalah mengkompresi berkas yang telah ter-mounting perangkat lunak kompresi seperti tar.

Tidak berbeda jauh dengan akuisisi pada mesin peladen *file-sharing*, deteksi proses enkripsi diperlukan. Jika terdapat indikasi enkripsi maka dilakukan proses akuisisi data volatile pada RAM. Gambar 4 menunjukan alur dari proses akuisisi langsung melalui jaringan internal.



Gambar 3: Alur Akuisisi Langsung pada Mesin Peladen *File-Sharing*



Gambar 4: Alur Akuisisi Langsung melalui Jaringan

6. KESIMPULAN DAN SARAN

Penanganan investigasi forensik pada sistem kritis harus hati-hati karena memiliki karakteristik sistem yang tidak diperkenankan *shutdown.* Mesin peladen *file-sharing* berbasis Samba merupakan bagian sistem yang kritis. Dalam penelitian ini diusulkan model investigasi forensik khusus mesin peladen *file-sharing* berbasis Samba, yaitu akuisisi secara langsung pada mesin peladen *file-sharing* dan akuisisi secara langsung melalui jaringan klien. Kedua model ini berdasarkan dari Standar Nasional Indonesia tentang Pedoman Identifikasi, Pengumpulan, Akuisisi, dan Preservasi Bukti Digital (SNI ISO/IEC 27037:2014).

Kerangka invenstigasi forensik pada penelitian ini belum mencakup pada perangkat elektronik dengan fungsi sebagai peladen *file-sharing* yang sifatnya portabel dan tidak kritis seperti perangkat *Access Point* terbaru. *Access Point* saat ini tidak hanya berfungsi sebagai transmisi dan penerima sinyal secara nirkabel namun telah dilengkapi dengan fitur layanan *file-sharing*. Cukup menambahkan media penyimpanan eksternal seperti *SD Card* maka *Access Point* tersebut dapat berfungsi sebagai mesin peladen *file-sharing*. Oleh sebab itu penelitian ini dapat dikembangkan lebih lanjut pada perangkat *Access Point* yang memiliki fitur layanan *file-sharing*.

7. DAFTAR PUSTAKA

Badan Standardisasi Nasional, 2014. *Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (ISO/IEC 27037:2012, IDT)*, Jakarta.

Daryabar, F. et al., 2016. Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. *Australian Journal of Forensic Sciences*, 618(June 2017), hal.1–28. Available at: http://dx.doi.org/10.1080/00450618.2015.1110620.

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

Heizer, I. et al., 1996. *Common Internet File System Protocol (CIFS/1.0)*, Available at: https://tools.ietf.org/html/draft-heizer-cifs-v1-spec-00.

Liberatore, M. et al., 2010. Forensic investigation of peer-to-peer file sharing networks. *Digital Investigation*, (October), hal.1–11. Available at: http://www.sciencedirect.com/science/article/pii/S1742287610000393.

Park, S. et al., 2015. Methodology and implementation for tracking the file sharers using BitTorrent. , hal.271–286.

Shey, H., 2014. Market Trends□: Secure File Sharing And Collaboration In The Enterprise , Q1 2014.

Sun Microsystems Inc., 1989. *NFS: Network File System Protocol Specification*, Available at: https://tools.ietf.org/html/rfc1094.

Ubuntu, 2015. Samba - Community Help Wiki. Available at: https://help.ubuntu.com/community/Samba [Diakses Oktober 3, 2016].