Buletin Profesi Insinyur 6(1) (2023) 014–019
http://dx.doi.org/10.20527/bpi.v6i1.176

ISSN 2654-5926

Analisis Investigasi Forensik Digital pada Layanan *Private Cloud Computing* Menggunakan SNI 27037:2014

Didik Sudyana[1] Irwan Hadi[1] Fietyata Yudha[2]

[1] Program Studi Teknik Informatika, STMIK Amik Riau

[2] Program Studi Informatika, Universitas Islam Indonesia

✉ didik.sudyana@sar.ac.id

***Cloud computing* telah memberikan banyak manfaat bagi pengguna. Terdapat beberapa jenis model adopsi *cloud computing*, salah satunya adalah model *private* yang memberikan perlindungan lebih terhadap privasi, dan telah banyak digunakan oleh pelaku industri. Tingginya angka penggunaan *cloud computing* memberikan peluang bagi para perilaku kriminal untuk melakukan tindak kejahatan siber. Ketika kejahatan siber telah terjadi, dibutuhkan penanganan dengan metode forensik digital untuk menganalisis barang bukti digital dan menemukan bukti-bukti kejahatan. Namun, teknik investigasi terhadap *cloud computing* berbeda, karena masalah reliabilitas data. Melakukan investigasi dari sisi pengguna merupakan salah satu metode yang dapat dilakukan. Oleh karena itu perlu dilakukan penelitian untuk melakukan proses investigasi kejahatan terhadap sisi pengguna yang terhubung layanan *private cloud* dan menganalisis barang bukti yang bisa didapatkan dari proses investigasi. Untuk mendukung proses investigasi dan analisis barang bukti digital yang dilakukan telah sesuai dengan kaidah forensik digital, digunakan *framework* Standar Nasional Indonesia (SNI) 27037:2014 yang merupakan standar nasional untuk analisis forensik digital. Dari hasil penelitian yang dilakukan, framework SNI 27037:2014 berhasil digunakan untuk menuntun proses investigasi terhadap barang bukti digital dari sisi pengguna dan berhasil menemukan beberapa barang bukti digital, seperti data yang telah dihapus, riwayat akses penggunaan *cloud*, dan riwayat akses file.**

Kata kunci: investigasi forensik digital, *cloud computing*, SNI 27037:2014

Diajukan: 21 November 2022
Direvisi: 9 Desember 2022
Diterima: 18 Januari 2023
Dipublikasikan online: 23 Januari 2023

Pendahuluan

Pemanfaatan *cloud computing* telah memberikan berbagai kemudahan dan peningkatan produktivitas bagi pengguna. Dengan berbagai manfaat yang ditawarkan oleh *cloud computing*, membuat adopsi *cloud computing* oleh perusahaan atau organisasi begitu cepat demi memenuhi kebutuhan perusahaan ataupun organisasi tersebut, salah satunya untuk mendukung keperluan bisnis (Marwi, 2021).

Seluruh perangkat lunak dan data yang berada di layanan *cloud,* disimpan pada *server* yang dapat diakses melalui internet. Sehingga, penggunaan *cloud computing* memudahkan pengguna dalam melakukan akses terhadap data ataupun perangkat lunak mereka (Irwanto et al., 2022).

Terdapat empat jenis model layanan *cloud computing* yaitu *Private*, *Public*, *Community*, dan *Hybrid* (Umar & Sudrajat, 2017). *Private Cloud Computing* merupakan model infrastruktur *cloud* yang dioperasikan dan dipergunakan oleh suatu organisasi untuk kepentingan internal (Kartolo & Negara, 2022).

Perkembangan penggunaan *cloud computing* semakin meningkat setiap tahunnya. Dalam sebuah survey yang dilakukan oleh *Flexera* melaporkan bahwa data perkiraan jumlah pengguna *cloud* pada 2014 lalu sebesar 1,136 juta. Jumlahnya terus mengalami peningkatan hingga 2016 yang mencapai 1,561 juta. Pada 2017, jumlah pengguna *cloud computing* telah mencapai 1,8 juta. Kemudian sebanyak 84% perusahaan telah menggunakan layanan *private cloud computing* (Flexera, 2021).

Dengan tingginya angka penggunaan *cloud computing*, dapat memberikan dampak negatif terhadap penyalahgunaan untuk kejahatan. Dampak negatif itupun tidak dapat dihindari dan menimbulkan konsekuensi berupa terjadinya kejahatan siber (Fadilla et al., 2022). Indonesia merupakan salah satu negara dengan tingginya angka kejahatan siber. Dalam periode 2017-2020, terdapat 16.845 laporan tidak pidana siber yang masuk ke Direktorat Tindak Pidana Siber Polri (Dob, 2021).

Ketika kejahatan siber telah terjadi, maka diperlukan metode untuk menangani kejahatan tersebut dengan teknik digital forensik untuk menganalisis dan menelusuri bukti-bukti digital dari tindakan kejahatan (Sudyana, 2016). Namun di *cloud computing*, teknik investigasi berbeda antara satu layanan dengan yang lainnya karena masalah reliabilitas data dan perbedaan jenis *cloud* itu sendiri. (Sudyana et al., 2019)

Cara mensitasi artikel ini:
Sudyana, D., Hadi, I., Yudha, F. (2023) Analisis Investigasi Forensik Digital pada Layanan *Private Cloud Computing* Menggunakan SNI 27037:2014. *Buletin Profesi Insinyur* 6(1) 014-019

 ISSN 2654-5926

Beberapa peneliti terdahulu telah melakukan beberapa penelitian terkait investigasi pada *cloud computing* ini. Wulandari (2018) melakukan penelitian untuk menginvestigasi teknik forensik di layanan *public cloud computing*. Penulis menggunakan teknik *k-means clustering* untuk melakukan *profiling* terhadap serangan *DDoS*. Hasil *profiling* dapat digunakan untuk melakukan investigasi forensik digital. Hemdan & Manjaiah (2021) menganalisis *virtual machine* sebagai barang bukti digital yang digunakan sebagai *server cloud computing*. Helmi et al. (2019) melakukan penelitian investigasi forensik pada layanan *cloud computing* menggunakan metode *live* forensik dalam standar NIST 800-86. Penulis berhasil menemukan barang bukti digital dalam simulasi kasus yang telah direncanakan sebelumnya. Sudyana et al. (2019) melakukan penelitian terhadap sisi server *private cloud computing* dan berhasil menemukan petunjuk barang bukti digital. Soni et al. (2019) melakukan investigasi pada server dengan melakukan akuisisi virtual server yang menggunakan sistem proxmox. Jayanti & Dewi (2020) melakukan investigasi terhadap perangkat jaringan yang terkoneksi ke sistem *owncloud* untuk menemukan barang bukti digital.

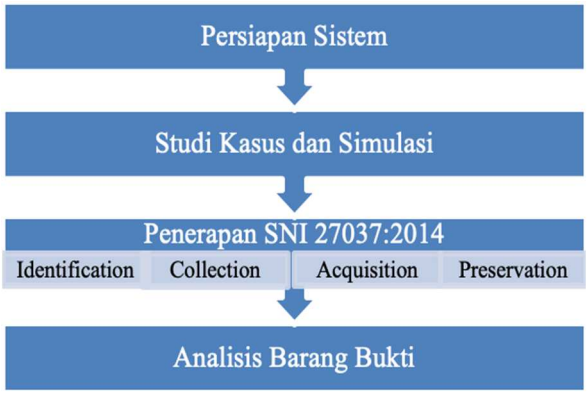
Dalam penelitian ini, dilakukan proses investigasi kejahatan yang terjadi di *cloud computing* pada sisi pengguna yang terhubung layanan *private cloud*, serta menganalisis barang bukti yang bisa didapatkan dari proses investigasi menggunakan SNI 27037:2014. Berdasarkan penelitian sebelumnya yang telah dijabarkan pada paragraph diatas, teknik investigasi dari sisi pengguna seperti dalam penelitian ini masih belum dilakukan.

SNI 27037:2014 merupakan standar nasional yang membahas tentang panduan spesifik terkait aktivitas dalam menangani bukti digital (Badan Standarisasi Nasional, 2014). Aktivitas tersebut meliputi *Identification*, *Collection*, *Acquisition*, dan *Preservation*. Standar ini dapat menjamin dan memberikan panduan untuk keempat aktor tersebut mengelola barang bukti dengan baik dan agar metodo*log*i yang digunakan dapat diterima di Indonesia. Metodo*log*i yang digunakan dalam pengumpulan barang bukti akan berpengaruh terhadap diterima atau tidaknya barang bukti tersebut di pengadilan (Sudyana, 2016).

Penelitian ini ditujukan pada salah satu layanan *private cloud* yaitu *Owncloud*. *Owncloud* merupakan perangkat lunak *opensource* yang digunakan sebagai media penyimpanan data dan berbagi data. Dengan adanya masalah siber terhadap layanan *cloud computing*, maka penelitian ini perlu dilakukan proses investigasi kejahatan pada sisi pengguna yang terhubung layanan *private cloud* dan menganalisis barang bukti yang didapatkan dari proses investigasi menggunakan SNI 27037:2014, sehingga penelitian ini dapat membantu *investigator* dalam melakukan investigasi serta dapat dipergunakan sebagai barang bukti dipengadilan.

Metode

Tahapan yang dilakukan dalam melakukan investigasi terhadap *owncloud* sebagai *private cloud* menggunakan SNI 27037:2014 terdiri atas empat tahapan utama seperti yang dapat dilihat pada Gambar 1, yaitu: persiapan sistem, studi kasus dan simulasi, penerapan SNI 27037:2014, dan analisis barang bukti.



Gambar 1 Tahapan Penelitian

Persiapan Sistem

Pada tahapan ini, seluruh persiapan sistem dilakukan. Dimulai dari persiapan *software* dan *hardware*. Adapun seluruh kebutuhan *software* dan *hardware* dalam penelitian ini, terangkum dalam Tabel 1.

Tabel 1 Kebutuhan *hardware* dan *software*

No	Hardware / *Software*	*Notes*
1	*PC Server* untuk *Owncloud*	*Hardware*
2	PC Client to Access *OwnCloud*	*Hardware*
3	*OwnCloud Server* 10.0.3	*Software*
4	*OwnCloud Client*	*Software*

Studi Kasus dan Simulasi

Tahapan ini dilakukan untuk mempersiapkan sebuah skenario kasus yang akan disimulasikan pada sisi pengguna. Dengan skenario seorang karyawan berinisial "A" diduga melakukan pembocoran informasi internal perusahaan. *File* rahasia perusahaan tersebut diduga disimpan pelaku pada *cloud* storage milik perusahan. Akan tetapi pelaku berkilah bahwa tidak pernah melakukan hal tersebut.

Pada tahapan ini, dipersiapkan 4 buah *file* berekstensi .pdf dan dilakukan perhitungan kode *hash* dengan rincian data seperti terlihat pada Tabel 2.

Tabel 2 Rincian Data Kasus

No	***File* Name**	**MD5**
1.	Audit Report MBTO.pdf	62e35a290c990b441f5 1d72ecdbbc80d
2.	Company Pro*file* Wirausaha.pdf	89d333b3526bc6ca475 87f71bf352f24
3.	Laporan Audit Intern.pdf	11ea7c0019200b8e5a0 a9cf44af4b3a3
4.	Laporan Keuangan Auditor.pdf	c21bb7dc6588bba7f09 08dbff3eee09c

Kemudian *file* Nomor 3 dan 4 dihapus terlebih dahulu. Dari kasus tersebut, perlu dilakukan forensik pada laptop tersangka untuk mencari bukti yang terkait dengan *file* perusahaan tersebut.

Penerapan SNI 27037:2014

Identification

Proses *identification* melibatkan pencarian dokumentasi bukti digital. Proses ini mengidentifikasi media penyimpanan digital yang mungkin mengandung bukti digital yang relevan dengan suatu insiden. Bukti yang

 ISSN 2654-5926

didapat harus diurutkan dengan benar untuk meminimalkan kerusakan pada bukti digital.

Collection

Collection adalah proses dalam pengumpulan bukti digital. Perangkat yang mungkin mengandung bukti digital bisa saja dihapus. Perangkat yang mengandung bukti digital bisa berada dalam dua keadaan, keadaan pertama saat sistem nyala, keadaan kedua saat sistem mati. Diperlukan berbagai pendekatan dan alat tergantung pada kondisi perangkat. Pada penelitian ini peneliti membuat contoh kasus pada keadaan saat sistem mati. Gambar 2 memperlihatkan tahapan dari proses *collection*.

Acquisition

Proses *Acquisition* merupakan tahapan akuisisi barang bukti digital seperti partisi hardisk, atau *file* yang dipilih. Kemudian akan didokumentasikan dengan metode yang digunakan serta kegiatan yang akan dilakukan. Akuisisi ini dilakukan agar dapat memverifikasi bahwa bukti tersebut akurat. Akurat dalam artian sumber asli dan setiap salinan bukti digital harus menghasilkan output fungsi verifikasi yang sama. Tahapan dari *acquisition* terlihat pada Gambar 3.

Preservation

Preservation merupakan tahap menjaga integritas barang bukti untuk memastikan barang bukti digital hasil akuisisi sama dan identik dengan barang bukti asli. Seorang investigator harus dapat menunjukkan bahwa bukti tersebut belum dimodifikasi sejak dikumpulkan atau sejak didapatkan.

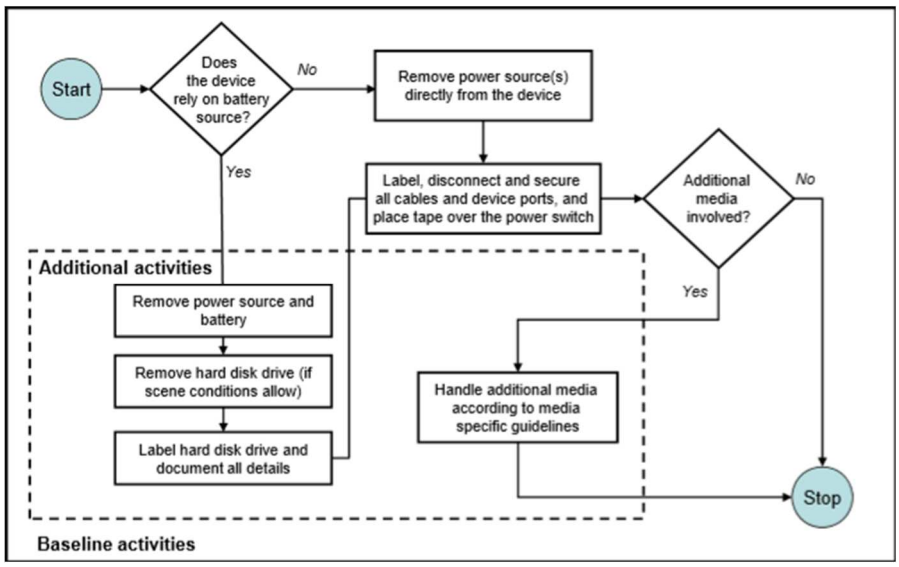
Analisis Barang Bukti

Pada tahap ini, hasil akuisisi akan digunakan untuk pencarian barang bukti digital. Dalam tahap ini, tidak diperbolehkan menggunakan media penyimpanan asli. Sehingga dilakukan duplikasi terhadap *file* hasil akuisisi dan melakukan proses investigasi menggunakan *file* hasil duplikasi tersebut. Pada penelitian ini, juga digunakan *Autopsy* sebagai *software* analisis.

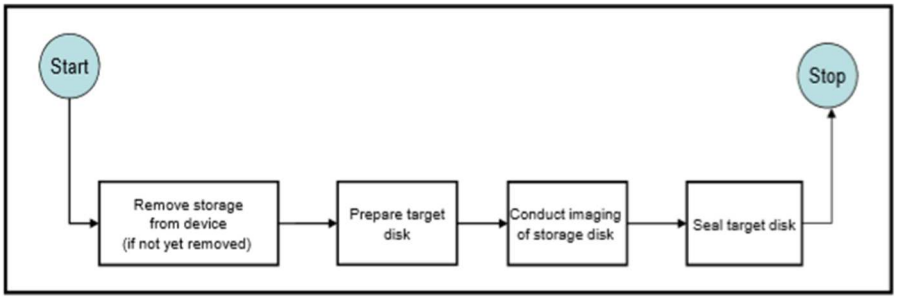
Hasil dan Pembahasan

Dalam proses menganalisis barang bukti digital, terdapat beberapa fokus pencarian yang dapat dilakukan. Alsadhan & Alhussein (2018) mengutarakan bahwa menemukan data-data yang telah dihapus dan melakukan proses pengembalian data tersebut merupakan salah satu fokus yang dapat dilakukan. Helmi et al. (2019) dan Sudyana et al. (2019) mengutarakan bahwa perangkat yang terkoneksi ke jaringan, akan menghasilkan beberapa riwayat akses yang juga dapat dijadikan sebagai barang bukti. Sehingga, berdasarkan fokus yang telah diutarakan penelitian sebelumnya, proses analisis barang bukti digital yang dilakukan dalam penelitian ini juga berfokus pada dua hal tersebut.

Dalam penelitian ini, adapun hasil yang didapatkan tidak hanya berupa data yang telah terhapus dan riwayat akses



Gambar 2 Tahapan Proses *Collection*



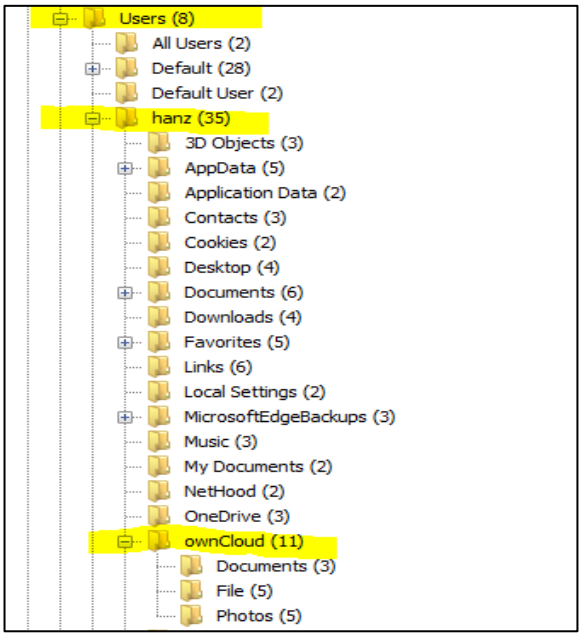
Gambar 3 Tahapan Proses *Acquisition*

Buletin Profesi Insinyur 6(1) (2023) 014–019
http://dx.doi.org/10.20527/bpi.v6i1.176
ISSN 2654-5926

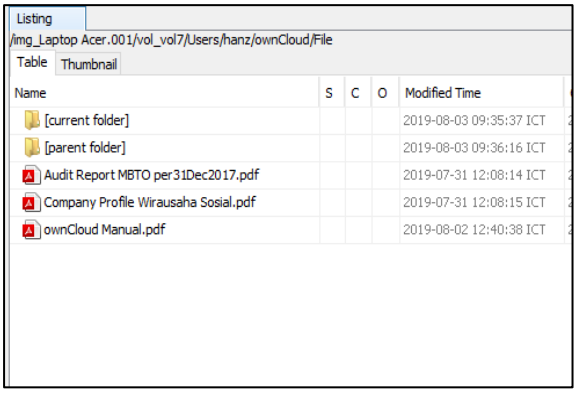
jaringan, akan tetapi riwayat akses file dan riwayat penggunaan *cloud* juga berhasil didapatkan.

Berikut adalah uraian dari hasil proses analisis yang telah dilakukan dalam proses pencarian barang bukti digital:

1. Pada proses analisis ditemukan sebuah *folder* penyimpanan *cloud* pada direktori c:/*users*/*user*name seperti yang terlihat pada Gambar 4. Setelah dilakukan penelusuran, ditemukan 2 dari 4 *file* penting yang dicuri seperti yang terlihat pada Gambar 5.

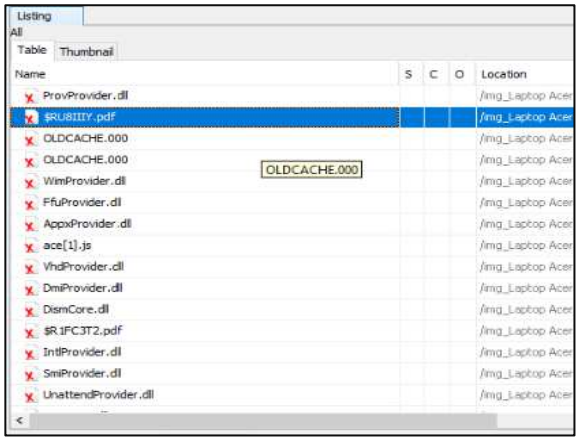


Gambar 4 *Folder* Penyimpanan Data *Cloud*



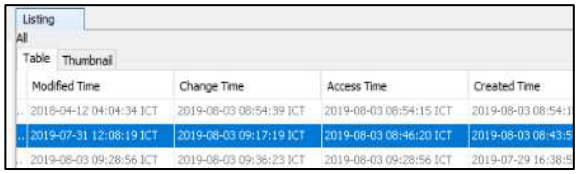
Gambar 5 Sub-*Folder* Penyimpanan Data *Cloud*

2. Tahapan berikutnya adalah melakukan penelusuran *deleted file* pada hasil analisis. Ditemukan 2 *file* perusahaan yang dicari, $R1FC3T2.pdf dan $RU8IIIY.pdf seperti yang terlihat pada Gambar 6, perubahan nama *file* ini terjadi karena proses penghapusan yang dilakukan secara permanen. Untuk memastikan bahwa *file* yang ditemukan adalah *file* yang sama dengan *file* sebelum dihapus, maka dilakukan proses ekstraksi *file* dari *deleted folder* dan dilakukan perhitungan kode *hash* pada *file* yang ditemukan, kemudian membandingkan dengan *file* awal. Dari hasil perhitungan kode *hash* yang dilakukan, *file* hasil ekstraksi merupakan *file* yang sama dengan *file* awal berdasarkan nilai kode hash yang identik.



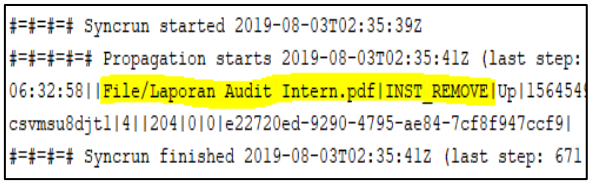
Gambar 6 *Folder* Deleted *File*

3. Pada proses analisis didapatkan waktu *file* diupload dan dihapus (Gambar 7).



Gambar 7 Waktu upload *file* dan penghapusan

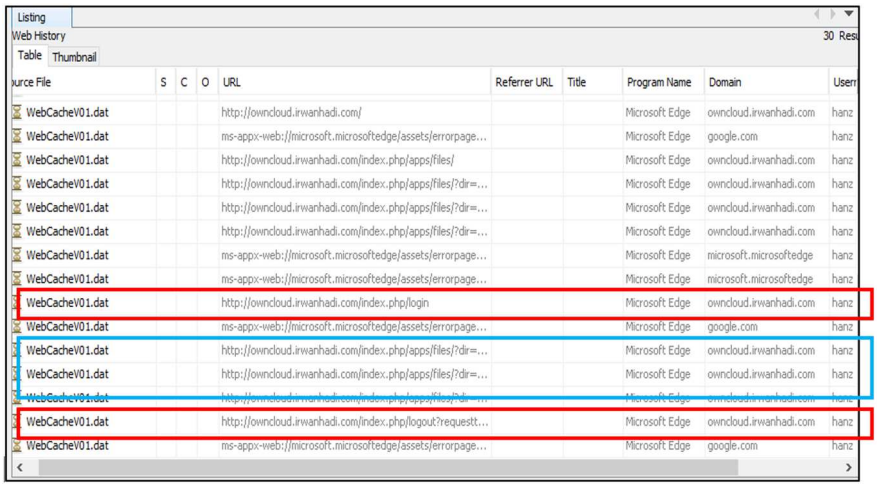
4. Dalam *folder owncloud*, ditemukan juga *log system* yang dibuat secara otomatis oleh *owncloud* dengan nama *file Owncloud*sync.*log*. *File* tersebut merupakan *file* dokumen yang menjadi catatan secara otomatis terhadap apa saja yang lakukan didalam *folder owncloud* tersebut. Berdasarkan pemeriksaan terhadap *file log* tersebut, ditemukan catatan penghapusan *file* yang telah dilakukan sebelumnya seperti yang terlihat pada Gambar 8 di bawah ini. *Log* tersebut mencatat proses sinkronisasi otomatis yang berada pada *folder* bernama "*File*", dengan nama *file* LaporanAuditInter.pdf dan aksi INST_REMOVE yang berarti *file* tersebut dihapus



Gambar 8 *Log OwnCloud*

5. Selanjutnya adalah mencari bukti lainnya seperti *history browsing*. Jika tersangka pernah melakukan akses *owncloud* lewat *interface web browser*, aktifitas tersebut akan tercatat pada *log web history*. *Autopsy* telah melakukan analisis terhadap aktivitas *browsing* dan menemukan barang bukti digital bahwa pelaku pernah mengakses layanan *private cloud computing* menggunakan media *web browser* beserta waktu aksesnya, seperti yang terlihat pada Gambar 9.

Gambar 8 merupakan bukti bahwa tersangka pernah melakukan akses *owncloud* tampilan interface melewati Web Browser Microsoft Edge. Pada bagian yang diberi tanda merah merupakan aktifitas *login* dan *logout* pada *owncloud*. Pada bagian yang diberi tanda biru dengan URL



Gambar 9 Waktu Akses Web History

http://*owncloud*.irwanhadi.com/index.php/apps/*files*/?dir=/*File* merupakan aktifitas browser. Index.php/apps/*files* menunjukkan sekumpulan *file*s ataupun *folder* didalam halaman utama sebuah *user owncloud*, selanjutnya pada /?dir menunjukkan *folder*, lalu =/*File* adalah *folder* yang diakses dengan nama *folder File*. Kesimpulan pada *URL* tersebut adalah *user* melakukan akses *log*in kemudian mengakses *folder* bernama *File*.

Berdasarkan hasil analisis, keseluruhan proses kejadian dapat dirangkum kedalam kronologi urutan peristiwa berdasarkan waktu didalam tabel *timeline* yang dapat dilihat pada Tabel 3. Tabel kronologi urutan peristiwa merupakan salah satu simpulan barang bukti digital terbaik yang dapat menjelaskan secara detail tahapan demi tahapan kejadian.

Tabel 3 Krono*logi* Urutan Peristiwa

Waktu	Aktifitas
2019-08-03 08:46:02	Membuat Folder " File" pada owncloud
2019-08-03 08:43:52	Upload File Audit Report MBTO
2019-08-03 08:43:53	Upload File Company Profile Wirausaha
2019-08-03 08:43:53	Laporan Audit Intern
2019-08-03 08:43:55	Laporan Keuangan
2019-08-03 09:17:15	Hapus Laporan Keuangan
2019-08-03 09:35:37	Hapus Laporan Audit Intern
2019-08-03 09:36:20	Akses owncloud Login Web

Kesimpulan

Dari hasil penelitian yang telah dilakukan, maka dapat disimpulkan bahwa investigasi forensik digital pada layanan *private cloud computing* dapat dilakukan dan berhasil menemukan barang bukti digital yang diperlukan. Penggunaan metode SNI 27037:2014 juga membantu proses pencarian barang bukti menjadi terstandar dan terstruktur.

Adapun beberapa barang bukti digital yang dapat ditemukan dalam proses investigasi berupa 2 *file* yang dihapus, beberapa *log* yang ditemukan seperti: waktu upload *file*, waktu hapus *file*, *log* sync, dan waktu akses *web browsing.*

Referensi

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

Dob. (2021). Ada 5.000 Kasus Perbulan, Indonesia Emergency Kejahatan Siber. *CNBC Indonesia*. https://www.cnbcindonesia.com/tech/20211011205453-37-283113/ada-5000-kasus-perbulan-indonesia-emergency-kejahatan-siber

Fadilla, M. K., Sugiantoro, B., & Prayudi, Y. (2022). Membangun Framework Konseptual Terintegrasi Menggunakan Metode Composite Logic untuk Cloud Forensic Readiness pada Organisasi. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *6*(1), 144–153. https://doi.org/10.30865/mib.v6i1.3427

Flexera. (2021). *State of The Cloud Report*.

Helmi, I., Widiyasono, N., & Gunawan, R. (2019). Simulasi Analisis Bukti Digital Pada Layanan Cloud Computing Menggunakan Metode NIST 800-86. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *3*(3), 217–224. https://doi.org/10.30865/mib.v3i3.1193

Hemdan, E. E.-D., & Manjaiah, D. H. (2021). An efficient digital forensic model for cybercrimes investigation in cloud computing. *Multimedia Tools and Applications*, *80*(9), 14255–14282. https://doi.org/10.1007/s11042-020-10358-x

Jayanti, & Dewi, E. (2020). Analisis Forensik Digital Storage pada Owncloud Drive. *Jurnal Repositor*, *2*(8). https://doi.org/10.22219/repositor.v2i8.968

Kartolo, R., & Negara, E. S. (2022). Analisis Kinerja Private Cloud Computing Menggunakan Metode Reability, Maintanability, Availability dan Security. *Inovtek Polbeng*, *7*(1), 135–145.

Marwi, H. C. (2021). Peranan Cloud Computing Dalam Bisnis Perusahaan. *Tematika*, *9*(1), 27–34.

Soni, Prayudi, Y., Sugiantoro, B., Sudyana, D., & Mukhtar, H. (2019). *Server Virtualization Acquisition Using Live Forensics Method*. 18–23. https://doi.org/10.2991/iccelst-st-19.2019.4

Sudyana, D. (2016). *Belajar Mengenali Forensika Digital*. Diandra Kreatif.

Sudyana, D., Lizarti, N., & Erlin, E. (2019). Forensic Investigation Framework on Server Side of Private Cloud

 ISSN 2654-5926

Computing. *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, *10*(3), 181. https://doi.org/10.24843/lkjiti.2019.v10.i03.p06

Umar, R., & Sudrajat, A. F. (2017). Penerapan Cloud Computing Pada Sistem Reservasi Homestay Dieng Berbasis Web. *Jurnal Sistem Informasi*, *1*(2), 40–48.

Vitasari Irwanto, E., Fitriandani, C. R., & Izzalqurny, T. R. (2022). Kenapa Perlu Menggunakan Cloud Untuk Audit di Masa Depan? *Prosiding National Seminar on Accounting, Finance, and Economics (NSAFE)*, 106–114.

Winda Andrini Wulandari. (2018). Analisis Network Forensics Menggunakan Honeypot Pada Jaringan Layanan Public Cloud Computing. *Jurnal Teknologi Informasi Universitas Lambung Mangkurat (JTIULM)*, *3*(1), 18–25. https://doi.org/10.20527/jtiulm.v3i1.24