CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 2, No. 2, November 2019, hlm. 65-68

DETEKSI BUKTI DIGITAL PADA ADRIVE CLOUD STORAGE MENGGUNAKAN LIVE FORENSIK

Tri Rochmadi

Program Studi Sistem Informasi, Universitas Alma Ata
Email: trirochmadi@almaata.ac.id

Abstrak

Era revolusi industri 4.0 yang serba digital seperti sekarang ini, teknologi *cloud* tidak bisa dilepaskan dalam kehidupan kita. *Cloud computing* juga menjadi salah satu teknologi yang cepat berkembang dan transformatif. Disamping beberapa kemudahan dan kenyaman dalam menggunakan *cloud*, menimbulkan masalah baru yaitu *cybercrime*. Kejahatan *cyber* akan semakin beraneka macam dan memungkinkan pelaku kejahatan akan berinovasi dengan adanya *cloud*. *Cloud forensik* tetap menjadi kendala dan tantangan bagi investigator dikarenakan setiap penyedia *cloud* memiliki arsitektur yang berbeda sehingga diperlukan investigasi yang berbeda dalam melakukan *cloud forensik.* Dalam penelitian ini dilakukan penelitian *cloud storage forensik* dari layanan Adrive. Penelitian ini dilakukan melalui sebuah simulasi atas skenario kasus penggunaan *cloud* kemudian dilakukan tahapan-tahapan dalam proses investigasi dari metode *digital forensik* yang meliputi *acquisition*, *examination*, *analysis* dan *conclusion*. Berdasarkan hasil penelitian dengan *live forensik* dengan akuisisi dan analisis memori RAM, bukti digital dapat dideteksi dan didapatkan bukti digital berupa file dokumen yang didapatkan dari sebuah tautan yang digunakan untuk berbagi file.

Kata kunci: Bukti Digital, Live Forensik, Cloud Storage

DIGITAL EVIDENCE DETECTION IN ADRIVE CLOUD STORAGE USING LIVE FORENSICS

Abstract

The era of digital industry revolution 4.0 as it is today, cloud technology cannot be released in our lives. Cloud computing is also one of the fastest-growing and transformative technologies. Besides some convenience and comfort in using the cloud, it raises a new problem namely cybercrime. Cybercrime will be more diverse and allow criminals to innovate with the cloud. Cloud forensics remains an obstacle and challenge for investigators because each cloud provider has a different architecture so different investigations are needed in conducting cloud forensics. In this study, forensic cloud storage research was conducted from Adrive services. This research was conducted through a simulation of cloud use case scenarios and then carried out the stages in the investigation process of the digital forensic method which included acquisition, examination, analysis, and conclusion. Based on the results of research with live forensics with the acquisition and analysis of RAM memory, digital evidence can be detected and digital evidence obtained in the form of document files obtained from a link used to share files.

Keywords: *Digital Evidence, Live Forensics, Cloud Storage*

1. PENDAHULUAN

Era revolusi industri 4.0 menuntut hampir semua lini kehidupan menggunakan *internet of things* (Surbiryala and Rong, 2018) yang tidak akan terlepas dengan *cloud computing*.

Cloud computing menurut *National Institute of Standards and Technology* (NIST) terbagi menjadi 3 yaitu *cloud* dengan *software*, *platform* dan infrastruktur sebagai layanan. Namun karena banyak layanan *cloud* sebagai penyimpanan kemudian disebut juga *STaaS/Storage as a Service* (Mohtasebi, Dehghantanha and Choo, 2016).

Cloud saat ini sangat berkembang dan *cloud computing* menjadi solusi karena berbagai kelebihan diantaranya data-data dapat diakses dimana saja, kapan saja dan menghemat anggaran untuk pengadaan infrastruktur (Shariati, Dehghantanha and Choo, 2016).

Di balik kelebihan menggunakan *cloud* tersebut, ternyata menimbulkan masalah baru yaitu kejahatan *cyber* misalkan untuk melakukan

penyimpanan data ilegal ataupun penyebarannya yang mudah. Dari kasus tersebut penelitian di bidang *cloud* menjadi tantangan untuk mendeteksi bukti digital pada cloud karena *cloud storage* banyak digunakan dan semakin banyak vendor penyedianya.

Cloud storage Adrive karena juga dapat digunakan berbasis web untuk melakukan aktifitas dalam pengelolaan data, maka akuisisi bukti digitalnya menggunakan metode live forensik ketika laptop atau sistem masih dalam keadaan hidup (Rochmadi, Riadi and Prayudi, 2017). Hal ini diperlukan agar bukti digital yang ditemukan dapat diketahui lebih detail.

2. LANDASAN TEORI

2.1. Digital Forensik

Digital forensik adalah sebuah metode yang digunakan dalam proses investigasi dari barang bukti elektronik ataupun digital dengan tujuan untuk rekonstruksi kejahatan *cyber* ataupun membantu dalam proses tindakan analisis kasus kejahatan (Umar, Riadi and Zamroni, 2018).

2.2. Live Forensik

Live forensik merupakan pengembangan dari forensik tradisional yang dilakukan ketika system masih hidup (Rochmadi, Riadi and Prayudi, 2017). Tujuan dari live forensik melakukan forensik pada memori, file swap, jaringan dan proses sistem yang berjalan untuk mendapatkan informasi lebih detail.

2.3. Cloud Storage Forensik

Cloud forensik (Hemdan and Manjaiah, 2017) adalah forensik digital yang dilakukan di lingkungan cloud. Secara khusus *cloud forensik* berhubungan dengan *internet of things* karena sifatnya yang virtual, remote, jaringan, klien server dan berhubungan juga dengan big data karena tidak terlepas dari data yang saling tersinkron dan terjadi proses kirim data antara klien ke *cloud server*.

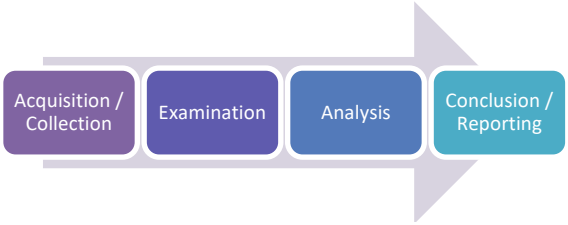
2.4. Penelitian Terkait

Penelitian dengan vendor ownCloud oleh (Martini and Choo, 2013) pada sistem operasi Windows 7 berhasil dengan baik dengan akuisisi dan analisis baik dari klien maupun server. Kemudian pada sistem operasi yang sama Windows 7 (Federici, 2014) meneliti objek cloud lainnya yaitu Dropbox, Google Drive dan Skydrive dengan membuat aplikasi untuk melakukan forensik *cloud* dengan cara *remote*.

3. METODOLOGI PENELITIAN

3.1. Metode

Metode pada penelitian ini menggunakan metode NIST *National Institute of Standar and Technology* yang terdiri dari 4 tahap seperti pada gambar 1.



Gambar 1. Proses Metode NIST

1. *Acquisition/Collection*

Tahap ini melakukan akuisisi barang bukti elektronik ataupun bukti digital yang mungkin ada kaitannya dengan sumber tindak kejahatan. Tahap ini wajib memperhatikan sifat dari barang bukti digital yang sangat komplek.

2. *Examination*

Tahap ini merupakan tahapan untuk mengekstraksi data atau bukti digital yang harus dijaga integritasnya terhadap keaslian barang bukti agar dapat dipertanggungjawabkan di pengadilan.

3. *Analysis*

Analisa ini dilakukan setelah didapatkan bukti digital dari hasil examination. Tahap ini bisa menggunakan dari beberapa ahli yang terkait dengan kasus yang ditangani agar hasil analisis menjadi lebih detail.

4. *Conclusion/Reporting*

Semua tahapan di atas harus terdokumentasikan dengan baik agar memudahkan proses pembuatan laporan dan mudah dipahami oleh orang lain dari kegiatan investigasi yang dilakukan.

3.2. Rancangan Simulasi

Penelitian ini menggunakan simulasi yang bertujuan untuk mendapatkan bukti digital sesuai yang diskenariokan seperti pada gambar 2.

Gambar 2. Simulasi Kasus Adrive

Simulasi ini tersangka menggunakan Adrive melalui aplikasi Adrive dan menshare file yang telah diupload ke *cloud storage* melalui web Adrive.

4. PEMBAHASAN

Penelitian ini pada proses akuisisinya menggunakan tool akuisisi FTK Imager 3.1.1.8 pada saat laptop yang digunakan tersangka masih dalam

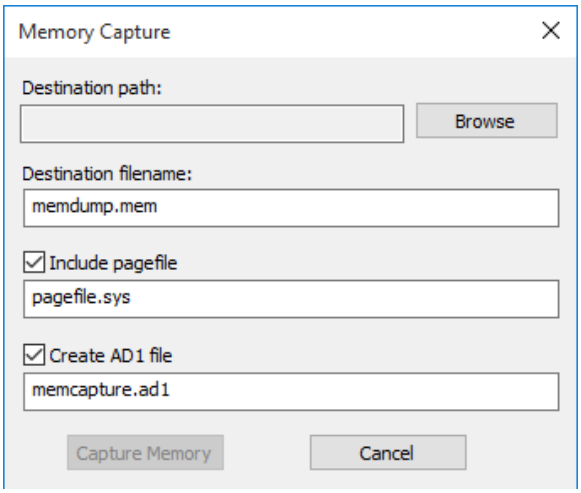
keadaan hidup. Laptop yang digunakan tersangka menggunakan sistem operasi Windows 7 32 bit dengan memori RAM sebesar 2 GB. Proses analisis deteksi bukti digital yang digunakan adalah tool forensik *open source* yaitu Autopsy 4.11.0.

Tabel 2. Tool Forensik

Tool Software	Fungsi
FTK Imager 3.1.1.8	Akuisisi file digital dari memori RAM dan file digital dari Drive lokasi instalasi Adrive pada computer tersangka.
Autopsy 4.11.0	Tool untuk menganalisa file image dari akuisisi bukti digital RAM dan Storage.

4.1. Akuisisi Bukti Digital

Proses akuisisi bukti digital menggunakan tool FTK Imager 3.1.1.8 dapat dilihat seperti pada gambar 3. Pada proses ini akuisisi bukti digital difokuskan pada RAM dari laptop tersangka yang digunakan.



Gambar 3. Proses Akuisisi Bukti Digital

Dari hasil akuisisi tersebut didapatkan file dengan ekstensi .mem dan hashnya berekstensi .ad1. Hasil akuisisi tersebut didapatkan bukti digital seperti pada tabel 2.

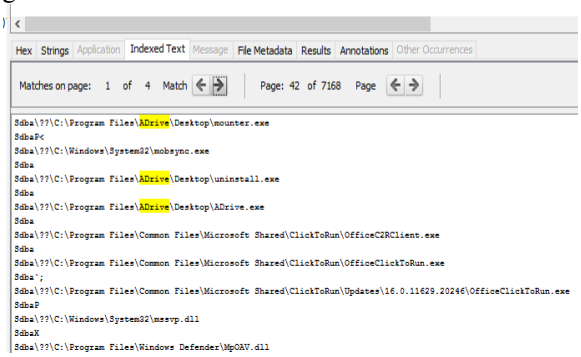
Tabel 2. Hasil Akuisisi Bukti Digital

Hasil Akuisisi	Keterangan
memcapture.ad1 memcapture.ad1 .txt memdump.mem pagefile.sys	Created By AccessData® FTK® Imager 3.1.1.8 Case Information: Case Number: 1 Evidence Number: 2 Unique Description: adrive memori Examiner: Tri Rochmadi Notes: akuisisi --- Information for I:\PDP\memcapture.ad1: [Computed Hashes] MD5 checksum: 497ea5b89eb3701e89ad7535a5255a36
	SHA1 checksum: aaa434b469b3f9b01f245a2820dcf09f0a7523fb Image information: Acquisition started: Thu Jun 27 19:31:41 2019 Acquisition finished: Thu Jun 27 19:51:09 2019 Segment list: I:\PDP\memcapture.ad1

Dari hasil akuisisi tersebut juga terdapat file dengan ekstensi .sys yaitu file pagefile.sys yang merupakan file paging dari sistem Windows yang digunakan sebagai virtual memori dalam sistem operasi Windows.

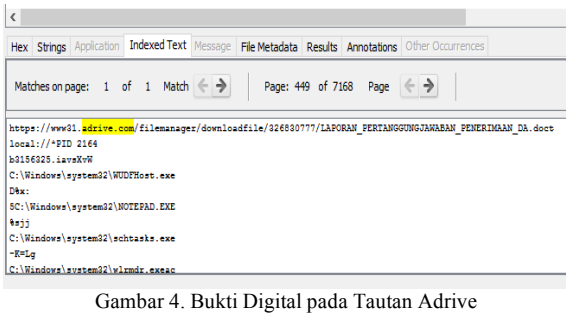
4.2. Hasil Deteksi Bukti Digital

Setelah dilakukan akuisisi dan dilanjutkan dengan tahapan analisis dengan menggunakan Autopsy 4.11.0, bukti digital dapat terdeteksi yaitu menggunakan cloud dari vendor Adrive dan aplikasi tersebut terinstal pada computer tersangka terletak di direktori C:\\Program Files\Adrive seperti pada gambar 4.



Gambar 4. Deteksi Bukti Digital Adrive

Pada proses analisis berikutnya bukti digital dapat ditemukan sebuah link yang digunakan untuk berbagi file ke orang lainnya. File tersebut berupa file dokumen dengan nama LAPORAN_PERTANGGUNGJAWABAN_PENERIMAAN_DA.doct dan file tersebut dengan tautannya adalah http://www31.adrive.com/filemanager/downloadfile/326830777/LAPORAN_PERTANGGUNGJAWABAN_PENERIMAAN_DA.doct terlihat pada gambar 5.



Gambar 4. Bukti Digital pada Tautan Adrive

Hasil analisis ini didapatkan bukti digital bahwa tersangka menggunakan cloud storage dengan vendornya adalah Adrive. Penggunaan Adrive oleh tersangka diinstal pada laptop yang dibuktikan bahwa ada instalasi di direktori C:\\Program Files\Adrive. Sedangkan untuk berbagi file tersangka mengakses web dan file tersebut dibagikan dengan tautan http://www31.adrive.com/filemanager/downloadfile/326830777/LAPORAN_PERTANGGUNGJAWABAN_PENERIMAAN_DA.doct.

5. KESIMPULAN

Berdasarkan hasil yang diperoleh dalam penelitian ini dengan live forensik bukti digital pada penggunaan *cloud* Adrive dapat terdeteksi dari akuisisi dan analisis pada RAM. Dari hasil penelitian tersebut bukti digital berupa lokasi instalasi Adrive. Hasil pendeteksian Adrive tersebut ditemukan sebuah file dokumen yang dibagikan setelah file tersebut diunggah ke *cloud storage* Adrive. Bukti digital tersebut berdasarkan identifikasi bisa digunakan sebagai bukti digital yang sah.

DAFTAR PUSTAKA

FEDERICI, C. (2014) 'Cloud Data Imager: A unified answer to remote acquisition of cloud storage areas', Digital Investigation. Elsevier Ltd, 11(1), pp. 30–42. doi: 10.1016/j.diin.2014.02.002.

HEMDAN, E. E. D. AND MANJAIAH, D. H. (2017) 'A cloud forensic strategy for investigation of cybercrime', Proceedings of IEEE International Conference on Emerging Technological Trends in Computing, Communications and Electrical Engineering, ICETT 2016. doi: 10.1109/ICETT.2016.7873667.

MARTINI, B. AND CHOO, K. K. R. (2013) 'Cloud storage forensics: OwnCloud as a case study', Digital Investigation. Elsevier Ltd, 10(4), pp. 287–299. doi: 10.1016/j.diin.2013.08.005.

MOHTASEBI, S. H., DEHGHANTANHA, A. AND CHOO, K. K. R. (2016) Cloud Storage Forensics: Analysis of Data Remnants on SpiderOak, JustCloud, and pCloud, Contemporary Digital Forensic Investigations of Cloud and Mobile Applications. doi: 10.1016/B978-0-12-805303-4.00013-7.

ROCHMADI, T., RIADI, I. AND PRAYUDI, Y. (2017) 'Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser', International Journal of Computer Applications. doi: 10.5120/ijca2017913717.

SHARIATI, M., DEHGHANTANHA, A. AND CHOO, K. K. R. (2016) 'SugarSync forensic analysis', Australian Journal of Forensic Sciences, 48(1), pp. 95–117. doi: 10.1080/00450618.2015.1021379.

SURBIRYALA, J. AND RONG, C. (2018) 'Secure customer data over cloud forensic reconstruction', 2018 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–4. doi: 10.1109/ICCE.2018.8326324.

UMAR, R., RIADI, I. AND ZAMRONI, G. M. (2018) 'Mobile Forensic Tools Evaluation for Digital Crime Investigation', International Journal on Advanced Science, Engineering and Information Technology, 8(3), p. 949. doi: 10.18517/ijaseit.8.3.3591.