Forensik Cloud Untuk Dropbox : Literatur Review

Shofie Mauladany Aziz
Program Studi Sarjana Informatika
Universitas Islam Indonesia
18523095@students.uii.ac.id

Erika Ramadhani
Jurusan Informatika
Universitas Islam Indonesia
erika@uii.ac.id

***Abstract*— Penyimpanan cloud digunakan sebagai media penyimpanan alternatif yang dapat diakses melalui jaringan internet yang telah tersedia pada perangkat cerdas seperti PC/Laptop, dan *smartphone*. Penggunaaan penyimpanan cloud dapat dimanfaatkan sesuai kebutuhan masing-masing individu baik untuk hal yang baik maupun buruk. Kejahatan dapat terjadi pada penyimpanan cloud ini seperti penyembunyian barang bukti curian, serta hal-hal yang dilarang lainnya. Dibutuhkannya forensik cloud ini untuk meminimalisir kejahatan yang telah terjadi. Kajian literatur dilakukan sebagai acuan bagi penulis untuk melakukan penelitian terkait analisis forensik pada aplikasi Dropbox. Kajian literatur ini mengguanakan pendekatan Systematic Literatur Review. Berdasarkan literatur yang telah di review, terdapat 2 metode atau model yang digunakan dalam proses forensik yaitu NIST dan McKemmish Model. Tools yang banyak digunakan pada analisis forensik yaitu SQLite.**

Keywords—Analisis forensik aplikasi dropbox

I. PENDAHULUAN

Penyimpanan cloud disediakan untuk menyimpan segala sesuatunya secara online. Penyimpanan cloud seperti ini sangat dibutuhkan karena dapat mengurangi hilangnya file yang kita simpan dalam bentuk flashdisk drive yang terjatuh, rusak, atau bahkan dicuri sehingga file tersebut disalahgunakan oleh pencuri tersebut. Banyak sekali penyedia penyimpanan cloud contohnya Dropbox, Google Drive, Microsoft Onedrive, Apple cloud. Cloud Storage adalah metafora dari internet, sebagaimana media penyimpanan yang sering digambarkan pada diagram jaringan komputer[1]. Dalam penanganan kasus kejahatan pada penggunaan penyimpanan cloud ini, maka dibutuhkannya forensik digital pada penyimpanan cloud.

Digital forensik pada umumnya adalah cabang ilmu yang berkaitan dengan hukum yang bukti hukum dapat ditemukan di komputer dan media penyimpanan digital baik fisik maupun cloud. Dapat diartikan Digital forensik adalah pemanfaatan teknologi untuk kepentingan hukum dan keadilan. Proses penyelidikan pada kasus kejahatan, melakukan observasi dalam bentuk digital maupun fisik. Pada dasarnya komputer forensik sangat dibutuhkan pada era digital ini karena semakin canggihnya teknologi mengakibatkan banyak kasus-kasus kriminal yang memanfaatkan teknologi. Sebagai bagian dari Keamanan Komputer (IT Security) digital forensik merupakan kajian yang menarik dengan menerapkan metode-metode tertentu dalam menelusuri bukti-bukti secara ilmiah dan dapat dipertanggung jawabkan secara hukum untuk mengungkap sebuah kasus kejahatan/criminal [2].

Penelitian ini berfokus pada kajian literatur yang berkaitan dengan cloud forensics pada aplikasi Dropbox. Diambil dari 2 jurnal nasional dan 1 jurnal internasional dengan topik yang sama yaitu forensik dropbox. Literatur review dilakukan untuk mengetahui bagaimana proses pengambilan barang bukti digital menggunakan tools dan metode yang berbeda dari setiap jurnalnya serta bertujuan untuk mengetahui barang bukti apa saja yang dapat diakuisisi.

II. METODE PENELITIAN

Metode yang digunakan pada penelitian ini yaitu SLR (*Systematic Literature Review*). SLR merupakan istilah yang digunakan untuk merujuk pada metodologi penelitian atau riset tertentu dan pengembangan yang dilakukan untuk mengumpulkan serta mengevaluasi penelitian yang terkait pada topik tertentu [7]. Metode ini digunakan untuk mengkaji literatur yang sesuai dengan topik penelitian secara sistematis. Tahapan pada metode ini yaitu :

A. Research Question (Pertanyaan Penelitian)

Pertanyaan penelitian ini dibuat berdasarkan topik utama yang dipilih pada penelitian ini. Berikut adalah pertanyaan penelitian yang disajikan pada penelitian ini:

1. Metode apa saja yang digunakan dalam proses forensik pada aplikasi Dropbox?
2. Perangkat apa yang digunakan dalam kegiatan forensik aplikasi Dropbox?
3. Tools apa yang digunakan proses forensik aplikasi Dropbox?

B. Search Process (Pengumpulan Literatur)

Pada tahap proses pengumpulan literatur, peneliti melakukan pencarian pada beberapa literatur terkait yang memiliki topik yang sesuai dengan kata kunci yaitu membahas tentang forensik pada aplikasi Dropbox. Pencarian ini dilakukan dengan bantuan *Google Scholar*, dan

Mendeley Desktop dengan kata kunci analisis forensik dropbox,

C. Inclusion and Exclusion Criteria (Pemilihan Literatur)

Pemilihan literatur dilakukan dengan menggunakan Mendeley dan juga Google Scholar, kemudian dipilih berdasarkan ketepatan topik penelitian yang sesuai dengan kata kunci yaitu forensik analisis forensik dropbox dengan tahun terbit minimal 2015. Terdapat 6 literatur yang telah dipilih, 6 di antaranya terdapat 2 literatur berstandar ISBN dan 4 berstandar ISSN. Dari 6 literatur tersebut dikategorikan berdasarkan metode, dan tools dan langkah yang dilakukan dalam proses analisis forensik pada aplikasi dropbox.

TABEL I. JUMLAH LITERATUR SESUAI DENGAN KATA KUNCI

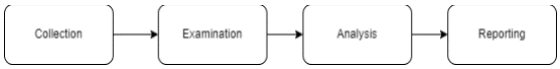
Kata kunci	Literatur	Jumlah Literatur
Analisis Forensik Dropbox	[2], [4], [5], [8], [9], [10]	6

Dari tabel di atas dapat disimpulkan bahwa literatur yang sesuai dengan kata kunci berjumlah 6 literatur.

III. HASIL DAN PEMBAHASAN

Literatur yang telah di analis dan di kaji mendapatkan sebuah hasil berupa data dan juga dijadikan referensi untuk dapat menjawab semua pertanyaan penelitian yaitu metode, tools dan perangkat yang digunakan dalam proses forensik aplikasi. Metode yang telah ditemukan pada 6 literatur berjumlah 2 metode yaitu :

1. NIST (*National Institute of Standard and Technology)* adalah badan nasional *non-regulator* dari bagian administrasi teknologi Amerika Serikat [12]. Metode ini mempunyai empat tahapan yang terlampir pada dibawah.



Gambar 1 Metode NIST

Tahap *Collection* meliputi pengambilan data-data untuk mendukung proses penyidikan dalam pencarian barang bukti [4]. Tahap *Examination* meliputi kegiatan pemeriksaan data yang dikumpulkan secara forensik dengan scenario otomatis atau manual, serta memastikan bahwa data tersebut memang unik atau asli sesuai dengan tempat kejadian perkara [4]. Tahap selanjutnya *Analysis* yaitu pemeriksaan untuk mendapatkan barang bukti terkait dengan kasus tersebut [12]. Tahap terakhir *Reporting* dilakukan dalam bentuk pembuatan laporan terkait hasil investigasi yang berisikan tentang hasil analisis barang bukti.

2. McKemmish Model memiliki empat tahapan yaitu *Identification, Preservation, Analysis, Presentation* [13]. Tahap pertama ada *Identification.* Tujuan utama pada langkah ini adalah untuk mengidentifikasi bukti lokasi dan desain untuk memilih metode yang tepat untuk memulihkan barang bukti yang ada. Bukti ini diambil melalui berbagai perangkat termasuk *smartphone*, laptop atau komputer, dan lain-lain [13]. Tahap selanjutnya adalah *Preservation.* Langkah ini mengarahkan upaya untuk melestarikan bukti yang diambil yang nantinya akan disajikan ke pengadilan. Dalam beberapa kasus, pelestarian barang bukti menjadi sangat menantang dan tidak dapat dihindari tetapi tetap harus diminimalkan melalui langkah-langkah yang memadai. Penjelasan diperlukan untuk membenarkan mengapa bukti gagal bertahan dengan bentuk aslinya [13]. Tahap *Analysis* ini terdiri dari mengekstrasi data digital dan memproses dan menafsirkannya melalui forensik teknik komputasi. Data yang dihasilkan cukup disederhanakan sehingga dapat dibaca oleh manusia [13]. *Presentation* adalah langkah terakhir dalam model McKemmish dan itu membutuhkan penyajian bukti yang tepat dan prosedur yang terlibat dalam pengadaan datanya [13].

TABEL II. METODE YANG DIGUNAKAN BERDASARKAN TAHUN

Tahun	Metode		
	NIST	***McKemmish***	***Tidak disebutkan***
2015	[10]		
2019			[8]
2020	[4]	[9]	[2],[5]

Hasil pengelompokan jurnal sesuai dengan tabel di atas disimpulkan bahwa metode yang tidak disebutkan pada literatur lebih banyak yaitu berjumlah 3 literatur. Adapun yang menggunakan metode NIST berjumlah 2 dan yang menggunakan metode McKemmish Model berjumlah 1 literatur.

Pengambilan barang bukti yang dilakukan oleh Walter Buyu [9] adalah artefak pada Dropbox versi desktop yang dijalankan menggunakan sistem operasi Windows 10. Penulis menemukan tools yang digunakan : *VMWare, Access Data FTK Imager, Regshot, DB Browser for SQLite, GlassWire, HxD, EaseUS Data Recovery Wizard, Autopsy* dengan langkah Identifikasi artefak pada virtual machine yang dibuat menggunakan *VMWare.* Langkah ini dilakukan mulai dari tahap pemasangan dropbox pada virtual machine, unggah file kedalam folder dropbox, menghapus file, dan pencopotan aplikasi dropbox pada virtual machine [9]. Kemudian melakukan penyimpanan barang bukti yang dibantu oleh *Access Data FTK Imager* yang digunakan untuk membuat salinan VM (*virtual machine*) yang telah dibuat [9]. Kemudian pengambilan artefak berikutnya yaitu registri pada aplikasi dropbox yang terpasang pada VM (*virtual machine).* Artefak berikutnya yaitu diambil menggunakan registri yang dapat mengetahui apa saja fungsi yang ada pada aplikasi dropbox. Langkah berikutnya yang dilakukan yaitu pengembalian file yang telah dihapus dengan bantuan tools *Autopsy,* dan *EaseUS Data Recovery Wizard.*

Analisis forensik yang dilakukan oleh Aye Chan Ko, dan Wint Thida Zaw [10], menggunakan *VMWare* dan melakukan pemasangan Windows pada VM (*Virtual Machine)*. Adapun tools yang digunakan yaitu : *VMWare,* Windows 7, Dropbox Client, Mozilla Firefox 33.0, Google Chrome 38.0, CCleaner 4.19 [10]. Pada saat pemasangan Dropbox Client pada VM ditemukan artefak berupa path file pada Dropbox Client mulai dari *Install file path, Sync Folder, Default file, Link file, Libraries, Prefetch files,* dan *Database File.* Setelah ditemukannya path file yang menunjukkan dimana lokasi

Dropbox Client berada. Penulis menemukan artefak penting yaitu database Dropbox. Database ini berisikan Host id, Email pengguna, *PC Display Name*, *Dropbox Path* [10]. Database ini dapat menampilkan apa saja yang telah terekam pada database berdasarkan kegiatan yang telah dilakukan. Database dapat dibaca menggunakan tools SQLite yang kemudian dapat menampilkan secara rinci isi dari database tersebut. Database ini lah yang diakuisisi sebagai barang bukti.

Penelitian yang dilakukan oleh Gandewa Bayu Satrya [8] menggunakan perangkat android dengan tipe Oppo A37 dengan sistem operasi Android Lolipop, dan Samsung A7 dengan sistem operasi Android Nougat [8]. Tools yang digunakan yaitu *Android Debug Bridge*, *Busybox Pro* v27, *VRoot* v1.7.3, *Dropbox* v150.2.4, *SQLite Browser* v3.7.0, *SQLite* v3.8.11[8]. Langkah pertama yang dilakukan yaitu melakukan rooting pada kedua perangkat Oppo A37 dan Samsung A7. Rooting adalah proses yang memungkinkan pengguna untuk mendapatkan hak kontrol tertinggi [8]. Rooting itu penting karena ada folder dan data tertentu yang hanya bisa diakses ketika smartphone sudah di root [8]. Analisis yang dilakukan meliputi analisis pada instalasi data, *sign up data, login data, logout data, uploading data, downloading data, File operation data (Open), File operation data (New Folder), File operation data (New file), File operation data (Move), File operation data (Rename), File operation data (Share), File operation data (Delete), Uninstall data* [8]. Seluruh file dianalisis dalam bentuk database. Masing-masing database di identifikasi apa saja informasi yang terdapat pada database tersebut.

Berdasarkan Saleh Khalifa Saad, Rusydi Umar, dan Abdul Fadlil [4] dalam penelitiannya melakukan analisis forensik aplikasi Dropbox pada Android Samsung Galaxy V Plus dan Samsung Galaxy Trend Plus [4]. Adapun tools yang digunakan dalam penelitian yaitu : *Android Debug Bridge (ADB)*, dan *Busybox.* Pengambilan barang bukti dilakukan dengan cara mencari database yang berisikan kegiatan pada penggunaan aplikasi dropbox pada android. Database tersebut merekam kegiatan mulai dari *Install, Sign up, login, logout, Upload, Download, File operation data (Open), File operation data (New Folder), File operation data (New file), File operation data (Move), File operation data (Rename), File operation data (Share), File operation data (Delete), Uninstall data* [4]. Setelah semua telah terkumpul, dapat disimpulkan pencarian artefak pada Samsung Galaxy Trend dapat dilakukan dengan mudah dengan cara membandingkan direktori dan database yang berasal dari aktivitas-aktivitas tersebut [4].

Menurut Shu Yun Lim, Alfonso Johan, Paridah Daud, Noor Azma Ismail [5] pada penelitiannya melakukan pengambilan artefak pada aplikasi Dropbox berbasis desktop yang berupa Registri aplikasi Dropbox, Database, dan Jaringan Aktivitas yang ada pada aplikasi Dropbox. Tools yang digunakan yaitu : Winlogon Registry, *Wireshark*, *CurrPorts*, *LiveTcpUdpWatch*, dan *SQLite DB.* Langkah pertama yang dilakukan yaitu melakukan pemasangan aplikasi Dropbox pada windows, dan melakukan pengecekan registri dengan bantuan Winlogon Registry. Registry Banyak perubahan menarik yang terjadi selama proses instalasi. Beberapa nilai pendaftar dibuat selama proses instalasi Dropbox [5]. Registri Winlogon adalah komponen sistem operasi Microsoft Windows yang tersedia untuk digunakan di berbagai aplikasi, seperti profil kecil, dan screen saver komputer (bahasa memori yang dapat diakses) opsional yang dibuat oleh komputer [5]. Kemudian setiap kegiatan yang dilakukan pada aplikasi Dropbox akan membuat suatu registry. Aktivitas jaringan pada saat mengakses Dropbox merupakan bagian dari artefak yang bagus untuk diakuisisi. Aktivitas jaringan dianalisis menggunakan *Wireshark* dan *LiveTcpUdpWatch* yang menampilkan IP, Server, Address, serta alamat HTTP yang ada pada Dropbox tersebut. Pengambilan artefak berikutnya yaitu database yang terdapat pada aplikasi Dropbox. Database tersebut berisikan seluruh aktivitas yang telah dilakukan pada aplikasi Dropbox.

Penelitian terakhir yang ditulis oleh Josua Pujion Lasnihora, Setia Juli Irzal Ismail, dan Gandeva Bayu Satrya [2] melakukan analisis forensik aplikasi Dropbox pada Android. Perangkat yang digunakan berupa *smartphone* dengan tipe Xiaomi Redmi 4A (Android 9). Tools yang digunakan yaitu : Dropbox v198.2.2, Ressurection Remix Pie, Root Explorer v4.7.1, dan SQL DB Browser v3.8.0 [2]. Langkah pertama yang dilakukan yaitu pemasangan aplikasi Dropbox pada ponsel, kemudian ponsel tersebut dipastikan dalam keadaan telah melakukan proses root. Proses selanjutnya yaitu melakukan aktivitas pada aplikasi dropbox mulai dari *Sign In, Sign Out, Download*. Aktivitas yang telah dilakukan akan membentuk suatu file database yang kemudian akan di periksa integritas pada file database tersebut menggunakan checksum SHA-1 [2]

Penulis telah mengumpulkan data dari ke enam literatur berupa perangkat apa saja yang digunakan pada penelitian, tools, dan juga metode. Untuk perangkat yang digunakan ditemukan 2 yaitu PC/Desktop dan juga Android. Berdasarkan analisis pada 6 literatur, secara keseluruhan analisis forensik yang dilakukan yaitu pengambilan artefak baik itu dalam bentuk database maupun registry. Tools yang digunakan untuk membaca isi dari database secara keseluruhan menggunakan SQLite.

KESIMPULAN

Literatur review yang telah dilakukan sebagai bahan acuan untuk penulis dalam melakukan proses forensik pada aplikasi Dropbox. Analisis forensik yang dilakukan memiliki langkah, tools, serta hasil yang berbeda dari setiap jurnalnya. Dari 6 literatur secara keseluruhan membahas tentang bagaimana cara pengambilan barang bukti atau artefak yang dapat diperoleh melalui aplikasi Dropbox. Berdasarkan literatur yang telah di review, terdapat 2 perangkat berbeda yang dilakukan pada proses forensik aplikasi dropbox yaitu PC/Desktop, dan Android. Tools yang sering digunakan pada saat proses analisis forensik yaitu SQLite, dan metode yang digunakan yaitu NIST, dan McKemmish model. Saran untuk peneliti pada masa yang akan datang dapat mengkaji literatur mengenai analisis forensik pada aplikasi dropbox yang menggunakan metode lain seperti NIJ, dan DFRWS Forensics Investigation Models serta menggunakan tools forensics yang lainnya.

REFERENSI

[1] Santiko, I., & Rosidi, R. (2017). Pemanfaatan private cloud storage sebagai media penyimpanan data e-learning pada lembaga pendidikan. *Jurnal Teknik Informatika*, *10*(2), 137-146.

[2] Lasniroha, J. P., Ismail, S. J. I., & Satrya, G. B. (2020). Mengidentifikasi Artefak Pada Aplikasi Dropbox Untuk Mendukung Forensic Android. *eProceedings of Applied Science*, *6*(3).

[3] Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital investigation*, *13*, 38-57.

[4] Saad, S. K., Umar, R., & Fadlil, A. (2020, April). Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIST. In *Seri Prosiding Seminar Nasional Dinamika Informatika* (Vol. 4, No. 1).

[5] Lim, S. Y., Johan, A., Daud, P., & Ismail, N. (2020). Dropbox forensics: forensic analysis of a cloud storage service. *Int. J. Eng. Trends Technol*, 45-49.

[6] Sulung, N. (2020). Analisis pembelajaran di masa pandemik covid 19 (literatur review). *Jurnal Endurance: Kajian Ilmiah Problema Kesehatilean*, *5*(3), 496-513.

[7] Triandini, E., Jayanatha, S., Indrawan, A., Putra, G. W., & Iswara, B. (2019). Metode systematic literature review untuk identifikasi platform dan metode pengembangan sistem informasi di Indonesia. *Indonesian Journal of Information Systems*, *1*(2), 63-77.

[8] Satrya, G. B. (2019). Digital forensics study of a cloud storage client: a dropbox artifact analysis. *CommIT (Communication and Information Technology) Journal*, *13*(2), 57-66.

[9] Buyu, W. (2020). *Forensic Analysis of Dropbox Data Remnants on Windows 10* (Doctoral dissertation, University of Nairobi).

[10] Ko, A. C., & Zaw, W. T. (2015). Digital forensic investigation of Dropbox cloud storage service. *Network Security and Communication Engineering (Ed: Kennis Chan), CRC Press: İngiltere*, 147-150.

[11] Dewi, B. T. K., & Setiawan, M. A. (2022). Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web. *AUTOMATA*, *3*(1).

[12] Mushlihudin, M., & Nofiyan, A. (2021). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology. *CYBERNETICS*, *4*(02), 79-92.

[13] Xu, J., Cooke, F. L., Gen, M., & Ahmed, S. E. (Eds.). (2018). *Proceedings of the Twelfth International Conference on Management Science and Engineering Management*. Springer.