# FORENSIK CLOUD UNTUK GOOGLE DRIVE:*LITERATURE REVIEW*

Syafiq Irfan Isnaindar
Program Studi Sarjana Informatika
Universitas Islam Indonesia
18523134@students.uii.ac.id

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

***Abstract*— Seiring dengan perkembangan zaman, media penyimpanan di sekitar kita terus berkembang mengikuti perkembangan teknologi dan tren yang ada di masyarakat. Jika pada zaman dahulu kita memerlukan penyimpanan berwujud fisik seperti *harddisk*, CD maupun disket, kini penyimpanan melalui media cloud menjadi yang populer di masyarakat. Pengguna cukup memerlukan jaringan internet guna mengakses dan menyimpan file mereka pada *cloud storage*. Namun, menyimpan file pada *cloud storage* menimbulkan resiko kejahatan seperti pencurian data mengingat file yang disimpan dalam jaringan cloud sehingga perlu dilakukan tindakan digital forensik untuk mencegah kejahatan pada *cloud storage* dan menyusun tindakan pencegahan di masa mendatang. Pada jurnal ini digunakan metode *literature review* dengan menganalisis jurnal yang telah didapatkan kemudian dipilih kembali sehingga didapatkan kesimpulan berdasarkan hasil literasi pada jurnal yang didapat sebelumnya. Adapun hasil dari *literature review* ini adalah pembahasan dan kesimpulan dari proses melakukan forensik cloud yang diambil dari jurnal peneliti yang telah melakukan percobaan forensik cloud, jurnal yang digunakan merupakan jurnal berbahasa Indonesia dan berbahasa inggris.**

**Keywords—penyimpanan, forensik cloud, Google Drive, *Literature review*.**

## I. PENDAHULUAN

Media penyimpanan yang dulu memiliki kapasitas terbatas dengan ukuran media besar, kini seiring dengan perkembangan teknologi hadir dengan ukuran media yang kecil dengan kapasitas yang jauh lebih besar. Namun, media penyimpanan kini hadir dengan bentuk non fisik yang disebut *cloud storage*, dimana data milik pengguna disimpan di dalam server. Kehadiran *cloud storage* atau penyimpanan cloud memberikan alternatif penyimpanan bagi pengguna yang mana akses data dapat dilakukan dimana saja dan kapan saja dengan bermodalkan perangkat untuk mengakes dan jaringan internet tanpa harus membawa perangkat penyimpanan fisik. *Cloud storage* sendiri mengubah kebiasan orang-orang yang mana sebelumnya saat akan menyimpan file perlu membawa perangkat penyimpanan macam *flashdrive,CD* maupun *Hard disk* sehingga kehadiran *cloud storage* memberikan kemudahan bagi penggunanya. Beberapa layanan *cloud storage* yang secara umum banyak digunakan salah satunya adalah Google Drive. Google Drive sendiri tersedia dalam bentuk *website, desktop* serta *mobile aplication.* Layanan ini memungkinkan para penggunanya untuk menyimpan data di server mereka, mensinkronisasi data dengan perangkat lain, dan saling berbagi file atau data dengan pengguna lainnya. Pengguna Google Drive sendiri dapat mengedit dokumen yang dimiliki karena platform ini terhubung dengan produk Google lainnya seperti Google docs, Google form, Spreadsheet, dll. Tercatat pada Mei 2017 terdapat 2 triliun file yang disimpan dalam layanan tersebut dan 1 miliar pengguna yang memakai layanan ini yang tercatat pada Juli 2018 memperlihatkan bahwa banyak peminat pengguna produk Google tersebut.

Namun dibalik banyaknya pengguna dan data yang tersimpan tersebut menimbulkan resiko besar mengenai jaminan kemanan data pribadi dan file milik para pengguna tersebut sehingga diperlukan keamanan pada sistem layanan tersebut. Berdasarkan permasalahan tersebut dapat dibuat rumusan masalah sebagai berikut :

a. Bagaimana proses penyelidikan forensik cloud pada Google Drive ?
b. Apakah dengan forensik cloud dapat mengumpulkan barang bukti dari hasil penyelidikan ?

Rumusan masalah diatas tersebut yang mendorong dilakukannya forensik cloud guna mengetahui prosedur dalam melakukan forensik cloud pada Google Drive mengingat platform tersebut memiliki pengguna dan data yang tersimpan dengan jumlah yang banyak.

## II. TINJAUAN PUSTAKA

Menurut Mell dan Grance dijelaskan bahwa cloud computing atau penyimpanan awan adalah adalah *bentuk yang dapat memungkinkan akses jaringan dimana pun sesuai permintaan kepada sumber daya jaringan yang dapat dikonfigurasi dengan cepat tersedia dari interaksi penyedia layanan* [1].

Ancaman yang secara umum dapat terjadi pada *cloud storage* antara lain, peretasan akun oleh pihak tidak bertanggung jawab yang dapat membuka celah terhadap pencurian data pengguna, pencurian identitas pengguna maupun *trace location* secara illegal.

Secara umum forensik Cloud sendiri diartikan sebagai cabang ilmu Digital Forensik dilingkungan *Cloud storage*. Menurut penjelasan Ruan, dkk dijelaskan bahwa kesulitan dalam mendefinisikan forensik cloud terletak pada kenyataan bahwa tidak ada definisi forensik cloud yang diterima secara universal [2]. Namun berdasarkan NIST Cloud storage Reference Architecture, forensik cloud adalah aplikasi *ilmu forensik digital* di lingkungan *cloud computing*. Secara teknis, ini terdiri dari pendekatan forensik hibrida menuju generasi barang bukti digital. Secara organisasi melibatkan interaksi antara aktor *cloud* untuk memfasilitasi investigasi baik internal maupun eksternal. Secara hukum sering menyiratkan multi-yurisdiksi dan situasi multi-penyewa [2].

Perlu dilakukan sebuah penelitian mengenai *forensik cloud* untuk mengentahui prosedur dan cara kerja dalam melakukan tindakan *forensik cloud* mengingat potensi ancaman yang ada sehingga diperlukan juga jurnal-jurnal maupun artikel ilmiah yang membahas mengenai *forensik cloud*. Dalam penyusunan jurnal terdapat sebuah metode yang dapat digunakan yaitu *literature review*. *Literature review* sendiri merupakan kegiatan survei terhadap artikel ilmiah, buku, jurnal atau informasi yang diterbitkan dengan tujuan untuk memberikan deskripsi, ringkasan maupun petunjuk terhadap suatu bidang penelitian. *Literature review* juga digunakan untuk membuat analisis dan sintesis terhadap pengetahuan yang sudah ada terkait topik yang akan diteliti untuk menemukan ruang kosong bagi penelitian yang akan dilakukan [6].

Umumnya *literature review* berisi mengenai ulasan, rangkuman maupun pemikiran dari penulis tersebut dari jurnal, buku maupun artikel ilmiah sesuai bidang dan topik yang dibahas. *Literature review* juga bisa dijadikan sebagai kegiatan mencari landasan teori yang digunakan sebagai bahan penelitian.

## III. METODE PENELITIAN

Metode yang digunakan pada jurnal ini adalah *literature review*, yaitu dengan melakukan analisa dari beberapa literatur yang telah didapat dari beberapa sumber kemudian dipilih kembali sehingga menghasilkan kesimpulan berdasarkan hasil literasi pada jurnal yang didapat sebelumnya.

Adapun jurnal yang digunakan sebagai bahan *literature review* ini adalah 3 jurnal yang membahas mengenai kegiatan forensik cloud pada Google Drive baik itu jurnal berbasa Indonesia maupun jurnal berbahasa Inggris. Alasan penulis memilih ketiga jurnal tersebut karena pembahasan dari isi ketiga jurnal tersebut menurut penulis sesuai dengan apa yang penulis cari sehingga ketiga jurnal tersebut dirasa bisa memenuhi materi yang akan digunakan penulis untuk melakukan *literature review*.

Jurnal-jurnal yang dijadikan acuan dalam menulis *literature review* tersebut didapatkan dengan melakukan pencarian di website yang menyediakan berbagai jurnal *online* seperti *Sciendirect*, *Google Scholar* dan *Researchgate.*

Adapun langkah-langkah dalam melakukan *literature review* bisa dilakukan sebagai berikut :

- Membaca artikel ilmiah atau jurnal terkait sesuai dengan topik yang dibahas.
- Memperhatikan seksama isi jurnal tersebut meliputi daftar isi, abstrak maupun informasi yang terdapat didalamnya.
- Mengevaluasi bahan literasi dari jurnal atau artikel ilmiah yang telah dibaca.
- Menyusun ringkasan dan catatan dari artikel atau jurnal tersebut meliputi tahun dan tanggal, penulus, metode penelitian, referensi, hipotesis maupun informasi penting dari jurnal tersebut.
- Menyusun kembali artikel dan buat kesimpulan dari hasil *literature review* yang telah dilakukan.

| NO. Jurnal | Jurnal Forensik Cloud Pada Google Drive | | |
|---|---|---|---|
| | Penulis | Tahun | Judul |
| 1 | Anton Yudhana, Rusydi Umar Ahwan Ahmadi | 2019 | Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method |
| 2 | Ming Sang Chang | 2016 | Forensic Investigation of Google Drive on Android |
| 3 | Anton Yudhana, Rusydi Umar, Ahwan Ahmadi | 2018 | Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ) |

| NO. Jurnal | Analisis jurnal forensik cloud pada Google Drive |
|---|---|
| | Prosedur dan hasil |
| 1 | Penulis menggunakan perangkat smartphone Samsung Galaxy V Plus dan Notebook AMD A10-9600P RADEON R5 HP, Windows 10 64 Bit dengan *tools* untuk akuisisi data forensik MOBILedit FORENSIC EXPRESS, Axiom Magnet untuk mengekstrak data foto dan USB Connector sebagai penghubung smartphone dan . Peneliti juga membuat skenario dengan asumsi pelaku kejahatan menyimpan foto barang bukti di Google Drive lalu dilakukan forensik sesuai metode NIST, sehingga didapatkan bukti berupa file foto, Video, Zip, Rar, PDF, Docx, Pptx, Aplication, Database. |
| 2 | Peneliti menggunakan software Android V4.2.2, Google Chrome V31.0.1650.59, Firefox V45.0.1, and Google Drive App V2.3.631.15.34 serta *tools* forensik dan analysis data menggunakan AccessData FTK Imager V3.1.1.8, MANDIANT Memoryze V3.0, WinHex V18.5, SQLite V2.0.1, dan CCleaner V1.13.50. Peneliti membuat lima skenario yaitu Base, Upload, Acces, Download, CCleaner. File sementara yang di upload pada Google Drive dihapus sementara dengan CCleaner berikut file ujicoba dan Riwayat penelusuran. Nama file, akun dapat terlihat pada SQLite dan nama file juga terlihat pada FTK Imager. |

| | |
|---|---|
| 3 | Pada proses akuisisi data menggunakan *tools* Oxygen Forensics dengan objek berupa smartphone Samsung Galaxy V plus didapatkan data yang berupa kode hexsa yang terdeteksi sebagai *account* email berhasil diakuisisi. Peneliti tersebut juga membandingkan kembali dengan menggunakan *tools* MOBILedit Forensics, dimana saat proses akuisisi berlangsung ditunjukan kode-kode hexsa yang terdeteksi sebagai akun email dari Google Drive. |

## IV. PEMBAHASAN

Proses melakukan literature review yang telah penulis lakukan dengan dimulai tahapan mencari jurnal maupun artikel online sesuai dengan topik yang penulis butuhkan. Setelah didapat, penulis membaca isi dari jurnal tersebut guna mendapatkan informasi yang dibutuhkan seperti judul jurnal, metode forensik cloud, proses forensik cloud, *tools* yang digunakan, dan studi kasus yang diangkat. Lalu membuat poin-poin berdasarkan informasi dari jurnal yang telah dibaca untuk menentukan informasi yang akan ditampilkan dalam jurnal. Terakhir dilkakukan penyusunan kembali poin-poin yang telah didapat menjadi kesatuan informasi sehingga menjadi artikel baru.

Dari hasil *literature review* jurnal yang telah didapat baik jurnal berbahasa Indonesia maupun Jurnal berbahasa Inggris prosedur dan skenario yang dibuat tidak jauh berbeda. Seperti skenario yang dimisalkan terjadi penghapusan data, pelacakan username dan password, dan proses pemulihan data. Pada pembahasan ini akan dibahas secara lebih lanjut dari hasil *literature review* yang telah dilkukan sebagai berikut :

a. Pertama dari jurnal yang ditulis Anton Yudhana, Rusydi Umar dan Ahwan Ahmadi(2019) dalam jurnal yang berjudul Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method tersebut peneliti menggunakan metode NIST dengan melakukan proses skenario forensik cloud dengan asumsi pelaku kejahatan menyimpan foto barang bukti di Google Drive lalu dilakukan forensik sesuai metode NIST pada Google Drive tersebut dengan menggunakan perangkat smartphone Samsung Galaxy V Plus dan Notebook AMD A10-9600P RADEON R5 HP, Windows 10 64 Bit dengan *tools* untuk akuisisi data forensik yaitu MOBILedit FORENSIC EXPRESS, Axiom Magnet untuk mengekstrak data foto dan USB Connector sebagai penghubung smartphone dan notebook. Dari hasil kegiatan forensik didapatkan 59 data entri pada file Entry227 dengan *tools* Axiom Magnet dan 46 file dengan rincian 8 file gambar, 3 video , 2 file zip , 4 file rar , 20 file pdf,, 4 file docx ,2 file pptx ,1 Application ,2 Database File dan 15 folder yang tidak memiliki data.

b. Lalu jurnal kedua yang ditulis Ming Sang Chang 2016 dengan judul Forensic Investigation of Google Drive on Android peneliti melakukan skenario Peneliti membuat lima skenario yaitu Base, Upload, Acces, Download, CCleaner dimana peneliti menggunakan AccessData FTK Imager, SQLite, dan WinHex untuk menemukan sisa-sisa data dari semua skenario untuk mengetahui sisa sisa data Android dari Google Drive untuk menemukan *username*, kata sandi, akses *browser*, akses perangkat lunak, dan file yang disimpan dalam akun dengan menggunakan keyword untuk mencari sisa-sisa data tersebut.

Skenario pertama yaitu Base dilakukan dengan menginstall perangkat lunak berupa *browser* Google Chrome, Firefox dan aplikasi Google Drive lanjut dengan skenario kedua yakni Upload untuk mengunggah file uji coba pada Google Drive lalu dihapus melalui smartphone lalu mengakses dari Google Drive, lalu menutup aplikasi Google Drive dan browser tersebut. Kemudian langkah ketiga melakukan akses dengan menggunakan *browser* atau perangkat lunak klien yang berbeda untuk masuk ke Google Drive dan hanya secara online membuka file uji yang diunggah sebelumnya lalu peneliti logout dan menutup browser atau aplikasinya. *Keywords* tersebut menurut peneliti dapat digunakan untuk mencari sisa-sisa data. Peneliti menggunakan GDA-Access sebagai contoh untuk menunjukkan temuan seperti nama file, akun, dan *timestamp* yang dapat ditemukan oleh SQLite.

Skenario keempat peneliti menggunakan browser atau perangkat lunak yang berbeda untuk masuk ke Google Drive dan mengunduh file uji coba yang diunggah sebelumnya. Peneliti kemudian logout dan menutup browser atau perangkat lunak klien. *Keywords* tersebut dapat digunakan untuk mencari sisa-sisa data.GDA-Download digunakan peneliti sebagai contoh untuk menunjukkan temuan. Nama file, akun, dan *timestamp* juga dapat ditemukan oleh SQLite. Peneliti juga menemukan nama file dengan FTK Imager. Percobaan ini juga menemukan akun uji coba, berkas uji, isi berkas uji, dan *timestamp* dapat ditemukan dengan SQLite, dan WinHex

Skenario terakhir yaitu CCleaner dimana skenario ini menggunakan *software* CCleaner untuk melakukan antiForensik. Skenario ini menurut peneliti sama seperti skenario unduhan. Kemudian CCleaner dijalankan untuk menghapus file sementara, file uji, dan riwayat penelusuran, kata sandi, *cookies, cache, history*, dll. *Keywords* tersebut dapat digunakan untuk mencari sisa-sisa data. Lalu digunakan GDA-CCleaner sebagai contoh untuk menunjukkan hasil temuan. Nama file, dan *timestamp* dapat ditemukan oleh SQLite seperti. Nama file juga dapat ditemukan dengan FTK Imager.

c. Jurnal terakhir adalah jurnal yang ditulis oleh Anton Yudhana, Rusydi Umar, Ahwan Ahmadi (2018) dengan judul Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ). Peneliti menggunakan metode NIJ ( National Institute of Justice ) dengan perangkat software dan hardware berupa Laptop HP A10-9600P, USB konektor, Oxygen Forensic, MOBILedit Forensic, Handphone SAMSUNG Galaxy V Plus. Peneliti menghubungkan *smartphone* dengan pc

kemudian melakukan ekstraksi dengan bantuan *tools* yang telah disiapkan. Penulis mengakuisisi data menggunakan Oxygen Forensic sehingga didapat data yang salah satunya terdeteksi sebagai *account* email yang diterjemahkan dari kode hexsa. Peneliti juga mendeteksi sebuah data sebagai gambar dari kode hexsa yang didapat dan file zip dari analisis media Google Drive.

Peneliti juga melakukan perbandingan dengan *tools* MOBILedit Forensics pada perangkat Samsung Galaxy V plus dan dilakukan proses akuisisi. Saat dilakukan akuisisi penulis mendapatkan kode hexsa seperti sebelumnya yang salah satunya terdeteksi sebagai *account* email pengguna Google Drive. Lebih lanjut peneliti membandingkan secara singkat perbedaan Oxygen Forensic dengan MOBILedit Forensics dimana menurut penulis, kemampuan Oxygen Forensic dalam melakukan penelitian lebih banyak seperti mampu mendeteksi *account*, ekstensi file, mendeteksi gambar, mendeteksi folder zip. Sedangkan dari hasil penelitian MOBILedit Forensics hanya dapat melakukan deteksi *account*.

## V. KESIMPULAN

Dari hasil *literature review* pada ketiga jurnal diatas dapat disimpulkan bahwasanya dengan asumsi data-data yang hilang di Google Drive merupakan bukti tindak kejahatan kemungkinan bisa dipulihkan melalui proses *forensik cloud* sesuai prosedur yang berlaku sehingga bisa menjadi barang bukti yang berlaku di mata hukum. Informasi lain seperti *username*, kata sandi, maupun informasi file yang diunggah dapat dilacak yang mana berguna dalam pelaksanaan *forensik cloud*. *Tools* yang digunakan peneliti seperti Axiom Magnet, FTK Imager, Oxygen Forensic, MOBILedit Forensic memiliki kelebihan dan kekurangan nya sendiri. Dimana sebagai pembaca kita bisa mengetahui dan menyimpulkan sendiri dari hasil yang dilakukan oleh peneliti dalam melakukan kegiatan forensik cloud.

Lebih lanjut hasil *literature review* diatas, pada percobaan forensik cloud disimpulkan dapat mengakuisisi atau memulihkan data pada *cloud storage* Google drive. Adapun dari percobaan diatas menggunakan Google Drive versi *mobile* dari dua percobaan dan satu versi *website.* Dari hasil percobaan forensik cloud oleh peneliti didapatkan beberapa hasil antara lain foto, akun email, video, zip, rar, PDF, docx, pptx, aplikasi, database.

Peran Forensik Cloud pada era digital saat ini sangatlah penting mengingat pada era ini semua orang bisa mengakses berbagai informasi melalui internet. Penyimpanan cloud memang memberikan manfaat yang besar karena cukup dengan akses jaringan internet dan perangkat mobile seperti smartphone maupun laptop pengguna bisa mengakses layanan penyimpanan cloud. Dengan adanya jurnal maupun artikel ilmiah yang membahas mengenai forensik cloud membuat pembaca yang berminat dalam bidang ini bisa mendapatkan gambaran maupun landasan sebelum melakukan kegiatan forensik cloud.

## VI. REFERENSI


[1] Mell P, Grance T. The NIST definition of *cloud storage* version 15. National Institute of Standards and Technology; 2010.

[2] Ruan K, Carthy J, Kechadi T, Baggili I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results.Digital Investigation; 2013

[3] M. S. Chang, "Forensic Investigation of Google Drive on Android," *International Journal of Software & Hardware Research in Engineering,* vol. 4, 2016.

[4] R. Umar. A. Ahmadi. Anton Yudhana, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institue of Justice(NIJ)," vol. 4, 2018.

[5] R. Umar. A. Ahmadi. A. Yudhana, "Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method," *Scientific Jurnal of Informatics,* vol. 6, 2019.

[6] M. Rahmayanti. Zulvikar Syambani Ulhaq, "Panduan Penulisan Skripsi Literature Review," *Fakultas Kedokteran dan Ilmu Kesehatan Universitas Islam Negeri Maulana Malik Ibrahim Malang,* p. 4, 2020.