Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 293-299
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ pada Kasus Penyembunyian Berkas

Saleh Khalifah Saad[1], Rusydi Umar[2], Abdul Fadlil[3]
Universitas Ahmad Dahlan
Jl. Prof. Dr. Soepomo, S.H., Janturan, Umbul Harjo, Yogyakarta 55164, Indonesia
saleh90saad@gmail.com, rusydi_umar@rocketmail.com, fadlil@mti.uad.ac.id

Abstract

Smartphones are a testament to the development of digital technology. At this time the smartphone is also experiencing growth in storage media, one of which is the Cloud storage media. One cloud storage application is the Dropbox Application. The development of cloud storage media does not rule out the possibility of negative impact on the use or can be used as a medium for crime such as storing evidence of criminal transactions and cybercrime. This study uses conversation scenarios for application conditions, including data deletion in applications. Data for each experiment will be taken using the National Institute of Justice (NIJ) Method. The method used in dealing with crime with smartphone media evidence is the National Institute of Justice (NIJ) Method. The conclusion of this study is that the use of the National Institute of Justice (NIJ) method ranks the digital forensic stages starting with identification, collection, examination, analysis, and reporting very well. This method is widely used in handling digital crime cases. The results of the acquisition will then be analyzed by translating the hexsa codes resulting from the acquisition to produce evidence that can be understood by the judge later.

Keywords: *Forensics, Digital Evidence, cyber crime*

Abstrak

Smartphone adalah salah satu bukti perkembangan teknologi digital. Pada saat ini smartphone juga mengalami perkembangan pada media penyimpanan salah satunya adalah media penyimpanan Cloud. Salah satu aplikasi penyimpanan Cloud adalah Aplikasi Dropbox. Perkembangan media cloud storage ini tidak menutup kemungkinan akan mendapat dampak penggunaan yang bersifat negative atau dapat digunakan sebagai media untuk tindak kejahatan seperti penyimpanan bukti transaksi kriminal, dan cybercrime. Penelitian ini menggunakan skenario percakapan terhadap kondisi aplikasi, diantaranya penghapusan data pada aplikasi. Data setiap eksperimen akan diambil dengan menggunakan metode Metode National Institute of Justice (NIJ). Pengunaan metode yang di gunakan dalam menangani kejahatan dengan barang bukti media smartphone adalah Metode National Institute of Justice (NIJ). Kesimpulan pada peneitian ini adalah Penggunaan metode National Institute of Justice (NIJ) mengurutkan tahapan forensic digital dengan mulai dari identification, collection, examination, analysis, dan reporting dengan sangat baik. Metode ini banyak digunakan dalam menangani kasus kejahatan digital. Hasil akuisisi kemudian akan di analisa dengan cara menerjemahkan kode-kode hexsa hasil akuisisi sehingga menghasilkan barang bukti yang yang bisa di mengerti oleh hakim nantinya.

Kata kunci*: Forensik, Bukti Digital, cyber crime*

1. PENDAHULUAN

Pesatnya kemajuan teknologi mendorong berbagai macam peluang kejahatan didunia teknologi, baik penipuan berkedok hadiah (*phising)* ataupun dalam bentuk kejahatan peretasaan system yang biasa disebut

dengan *cyber crime, digital crime, computer crime* atau yang semisalnya [1]. Mesin pencari selalu menggunakna sebuah fitur layanan yang sangat cepat serta bersifat pribadi[2].

Keamanan pada sebuah pesan yang akna dikirim serta komunkias pada data sebuah informasi pada komunikasi dapat langsung serta tidak langsung pada teknologi yang ada pada sistem yang ada pada komputer [3]. Teknologi yang canggih akan menghasilkan sebuah kegiatan yang positif guna mencari sebuah celah dimana pada pengiriman mampu mengendalikan sebuah jaringan komunikasi yang sanagt baik dalam basis datanya tersebut. Penjahat yang dilakukan pada stretegi mampu untuk menargetkan media pada sebuha media sosial yang akan diawasi dengansangat ketat [4].

Teknologi memberikan manfaat bagi individu manusia pada sistem komunikasinya. Walaupun teknologi memberikan damapk yang baik namun terkadang teknologi juga memiliki dampak yang buruk bagi para penggunanya [5]. kejahatan yang terjadi biasanya berupa sebuah penyerangan yang akan dilakukna pada lembaga tertentu yang sering dilakukan [6].

Dropbox adalah sebuah jaringan penyimpanan data yang dijalankan oleh Dropbox.inc. Dropbox merupakan sebuah penyimpanan data berkas dengan sistem internet. Sehingga Dropbox sangat memungkinkan sebagai sarana penyimpanan berkas transaksi barangcillegal atau *blackmarket.* Penggunaan metode *National Institute of Justice* (NIJ) mengurutkan tahapan *forensic digital* dengan mulai dari *identification, collection, examination, analysis,* dan *reporting* dengan sangat baik[7].

Adapun penelitian terdahulu yang dijadikan referensi dalam penelitian Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ pada Kasus Penyembunyian Berkas Rahasia diantara penelitian terdahulu yaitu, "Analisis *Live Forensics* Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital *Forensics Research Workshop* (DFRWS)", Penelitian ini menggunakan metode *DFRWS* yang terdiri dari tahap-tahap sebagai berikut: *Identification, Preservation, Collection, Examinition, Analysis* dan *Presentation*. Langkah selanjutnya adlaah menjalankan perangkat lunak (FTK Imager) sebagai bahan pendukung untuk mengetahui keamanan pada aplikasi Twitter. Dalam meyakinkan bahwa akun media sosial menjadi nilai yang merepresentasikan string asli atau akun asli dilakukan dengan analisis data pada direktori laptop. Berdasarkan beberapa hasil dari tahapan-tahapan metode yang telah dilakukan, proses analisis mengenai data pada media sosial Twitter dapat dikatakan bahwa bukti digital berupa barang bukti data yang valid [8].

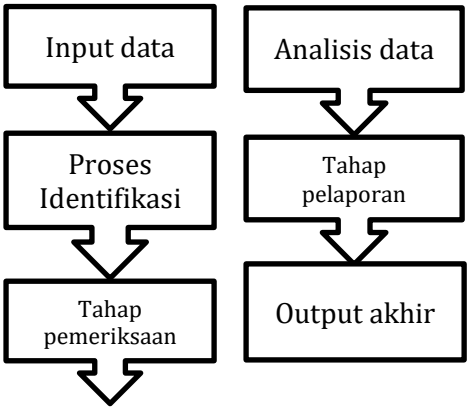
Berdasarkan pada analisa dan perbandingan bukti forensik aplikasi media sosial Facebook dan Twitter pada *Smartphone* Android, Hasil dari penelitian ini menunjukkan bahwa semua bukti forensik pada aplikasi media sosial Facebook berhasil ditemukan semua. Untuk aplikasi media social Twitter hanya berhasil ditemukan berupa nama akun, data lokasi, *photo profile*, *cover photo*, *posting* berupa teks dan *posting* berupa gambar [9].

"Anallisa Forensik Whatsapp dan Line *Messenger* pada *Smartphone* Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia", Adanya bkti digital pada aplikasi WhatsApp dan LINE *Messenger* berhasil didapatkan dari perangkat Android dengan menggunakan dua cara, yaitu cara manual dan menggunakan aplikasi tambahan. Data yang dapat diambil merupakan data utama dan data pendukung aplikasi. Data utama berupa *database* berisikan kontak dan percakapan dan artefak *file* penyusun aplikasi. Data pendukung aplikasi adalah *database* cadangan serta *file-file* terkait media seperti gambar, video, dan suara. Faktor yang mempengaruhi keberhasilan memperoleh bukti digital pada aplikasi WhatsApp dan LINE *Messenger* merupakan aktivitas perubahan kondisi aplikasi dan perangkat yang digunakan [10].

"Analisis Forensik Digital Aplikasi *Beetalk* untuk Penanganan *Cybercrime* Menggunakan Metode NIST", Penelitian ini diawali dengan membuat akun Beetalk pada dua handphone android yang sudah disiapkan, Selanjutnya melakukan skenario percakapan antara Akun A dan Akun B tentang prostitusi online melalui handphone android tersebut. Langkah Selanjutnya melakukan proses rooting pada salah satu *smartphone* Android yang akan akusisi, proses rooting ini menggunakan aplikasi KingRoot, aplikasi ini adalah aplikasi root android yang digunakan untuk membantu memperoleh akses rooting. Selanjutnya melakukan pemilihan *tool*s untuk mengambil data dari akun Beetalk. Pertama adalah melakukan proses backup data dalam perangkat *smartphone* agar tidak corrupted. *Tool*s yang digunakan untuk melakukan backup adalah MOBILedit Forensic. Setelaah itu melakukan Examination, tindakan ini bertujuan untuk menampilkan data yang telah di backup tadi untuk melihat bukti-bukti apasaja yang ada di dalam perangkat tersebut. *Tool*s yang akan digunakan untuk tahap Examination adalah OXYGEN Forensik, Alpikasi tersebut adalah aplikasi berbasis windows yang dapat digunakan untuk mengakusisi bukti digital pada *smartphone* Android yang telah di backup[11].

2. METODOLOGI PENELITIAN

Tahap penelitian ini dibagi menjadi beberapa tahapdalam penyiapan data, ranangan, atau prosedur penelitian, serta bagaiamana pengujian yang kana terjadi pada bagian teori yang didasari pada teori.



Gambar 1. Alur Penelitian

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 293-299
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

2.1. Metode analisis forensik NIJ

Penggunaan metode penelitian ini mengadaftasi dari metode analisis forensik dari National Institute of Justice (NIJ). Metode ini menjelaskan bagaimana sebuah alur yang ada. Roni pada penjelasan pada keberhasilan hampir 100% pada data forensik.

2.2. Tahapan Metode NIJ

Tahap penelitian ini dibagi menjadi beberapa tahap yaitu tahap persiapan, tahap pengumpulan, tahap pemeriksaan, tahap analisis, dan tahap pelaporan, tahap metode NIJ dijelaskan secara lengkap sebagai berikut:

a) Tahap pertama adalah persiapan atau persiapan adalah kegiatan mempersiapkan peralatan untuk melakukan tugas-tugas yang diperlukan dalam proses investigasi. Pada tahap ini didalamnya terdapat proses mempersiapkan alat yang akan digunakan dalam proses investigasi.
b) Tahap kedua adalah pengumpulan atau pengumpulan adalah proses menemukan dokumen, dan mengumpulkan data atau membuat salinan benda fisik yang memiliki bukti digital di dalamnya. Tahap pengumpulan dalam proses ini pengumpulan data digital dilakukan dari sumber yang relevan agar dapat mempertahankan keaslian bukti digital dari kemungkinan perubahan.
c) Tahap ketiga adalah pemeriksaan, tahap ini adalah tahap untuk memeriksa bukti secara digital yang diperoleh melalui proses forensik secara manual atau secara otomatis dan untuk memastikan bahwa bukti digital yang diperoleh adalah asli seperti yang diperoleh di tempat terjadinya kejahatan.
d) Tahap keempat adalah analisis, setelah memperoleh bukti digital yang diperlukan dari tahap penyelidikan sebelumnya, maka bukti digital yang diperoleh dianalisis secara rinci menggunakan metode yang telah diakui secara ilmiah dan hukum untuk menentukan signifikansi bukti digital.
e) Tahap kelima adalah pelaporan, setelah melalui tahap analisis bukti digital yang diperoleh, Kemudian pelaporan dari hasil analisis terdiri dari deskripsi dari kegiatan yang telah dilakukan dilaksanakan dalam proses investigasi, penjelasan alat yang digunakan dalam proses investigasi, metode investigasi yang telah digunakan, penentuan tindakan pendukung investigasi yang telah dilakukan, serta memberikan beberapa rekomendasi sebagai bahan untuk mengevaluasi elemen pendukung yang terkandung dalam forensik digital

3. HASIL DAN PEMBAHASAN

Pada bagian ini akan dibahas mengenai anslisis forensic menggunakan metode NIJ.

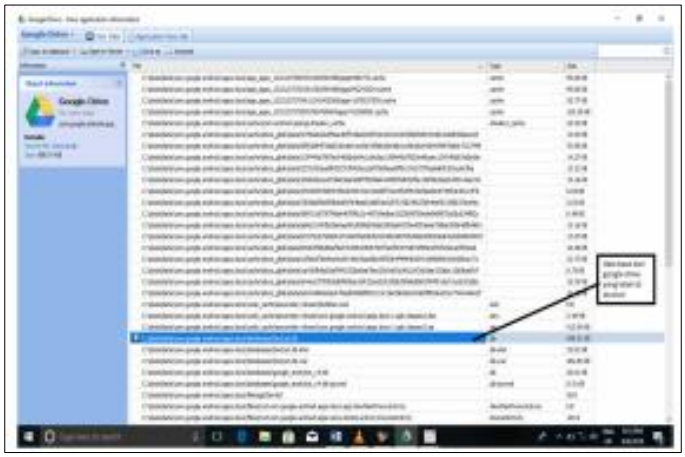
3.1. Aplikasi penunjang analisis forensik

Aplikasi-aplikasi yang sudah di siapakan untuk menunjang penelitian ini berupa Aplikasi USB *Connector* digunakan sebagai menghubungkan antara *smartphone* dengan PC kemudian dilakukan ekstraksi dengan bantuan *tool-tool* forensik. Pada gambar 2 menjelaskan tampilan dari *tool Oxygen Forensics*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 293-299
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

yang dihubungkan dengan *smartphone* Samsung Galaxy V Plus. Spesifikasi dari *smartphone* juga di tunjukkan pada gambar di bawah ini:

Gambar 2. Tampilan data forensics



Gambar 3. *Google drive*

3.2. Hasil Analisis *Tools* Forensik

Hasil penelitian yang dilakukan maka didapatkan perbandingan hasil dari kedua buah *tool* forensik dengan data sebagai berikut:

Tabel 1. Hasil Analisis *Tools* Forensik

Tool	*Account*	Ekstensi file	Gambar yang bisa dimunculkan	Folder zip yang terdeteksi
Oxygen forensic	Yes	Yes	Yes	Yes
Mobile edit forensic	Yes	No	No	No

Dari data tabel di atas menjelaskan bahwa data dari kedua *tool* forensik tersebut ada yang bisa membaca *account* pengguna media penyimpanan *Google drive* sisanya dari ekstensi file dan jenis file yang bisa di buka hanya di miliki satu *tool* saja yaitu *Oxygen Forensics* Pada kajian peneliti terdahulu hanya sampai pada sebuah *account* email dari *google drive* tidak bisa memunculkan data digital yang menjadi bahasan utama dari sebuah kode hexsa dari proses akuisisi data digital dari *smartphone*, penelitian ini telah

sampai pada kajian dimana ketika data diakuisisi dari sebuah perangkat *smartphone* dan menerjemahkan kode hexsadesimal akan meghasilkan berbagai data, untuk penelitian ini, peneliti baru bisa menerjemahkan kode hexsa menjadi sebuah gambar.

4. SIMPULAN

Penggunaan metode National Institute of Justice (NIJ) mengurutkan tahapan *forensic digital* dengan mulai dari *identification, collection, examination, analysis*, dan *reporting* dengan sangat baik. Metode ini banyak digunakan dalam menangani kasus kejahatan digital.

Dari hasil penelitian diketahui bahwa dari kedua *tool* forensik yaitu Oxygen dan Mobile edit forensic ada yang bisa membaca *account* pengguna media penyimpanan *Google drive* sisanya dari ekstensi file dan jenis file yang bisa di buka hanya di miliki satu *tool* saja yaitu *Oxygen Forensics*.

Saran dari penulis ada banyak *tool-tool* forensik yang belum dicoba penulis, penelitian selanjutnya akan lebih baik dengan *tool*s dan metode yang berbeda. Penggunaan *tool* forensik yang berbeda diharapkan bisa memberikan banyak informasi dari data hasil akuisisi, karena *tool-tool* forensik memiliki kekurangan dan keunggulan masing-masing.

DAFTAR PUSTAKA

[1] A. Yudhana, I. Riadi, and F. Ridho, "DDoS classification using neural network and naïve bayes methods for network forensics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, pp. 177–183, 2018.

[2] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental analysis of web browser sessions using live forensics method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 2951–2958, 2018.

[3] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid-State Drive Dengan Metode National Institute of Justice (Nij)," vol. 3, no. 1, pp. 70–82, 2018.

[4] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 1, 2017.

[5] I. Zuhriyanto *et al.*, "Perancangan Digital Forensik Pada Aplikasi," vol. 2018, no. November, pp. 86–91, 2018.

[6] I. Riadi, A. Yudhana, and M. C. F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute of Justice (Nij)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 219–227, 2018.

[7] Forensik, Dropbox, National Institute of Justice (NIJ), Pornografi. 1) 2)," vol. 13, pp. 37–54, 2019.

[8] A. Yudhana, I. Riadi, and I. Zuhriyanto, "Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," vol. 20, no. 2, pp. 125–130, 2019.

[9] W. A. Mukti, S. U. Masruroh, and D. Khairani, "Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android," *J. Tek. Inform.*, vol. 10, no. 1, pp. 73–84, 2018.

[10] S. Ikhsani and B. C. Hidayanto, "Analisa Forensik Whatsapp dan LINE Messenger Pada Smartphone Android Sebagai Rujukan Dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia," *J. Tek. ITS*, vol. 5, no. 2, 2016.

[11] M. I. Syahib, I. Riadi, and R. Umar, "Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan," *Semin. Nas. Inform. 2018 (semnasIF 2018) UPN" V e t e r a n " Yogyakarta, 24 November. 2018*, vol. 2018, no. November, p. 134, 2018.