Jurnal CoreIT, Vol.X, No.X, Bulan Tahun
ISSN 2460-738X (Print)
ISSN 2599-3321 (Online)

Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)

Anton Yudhana [1], Rusydi Umar [2], Ahwan Ahmadi [3]
[1] Teknik Elektro, Fakultas Teknik, Universitas Ahmad Dahlan
[2,3] Teknik Informatika, Fakultas Teknik, Universitas Ahmad Dahlan

Jl. Prof. Soepomo, SH, Janturan Yogyakarta 55164
eyudhana@ee.uad.ac.id[1], rusydi_umar@rocketmail.com[2], ahwanahmadi71@gmail.com[3]

***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*. Penyimpanan awan yang ada pada android dan menjadi bawaan dari sebuah smartphone dengan sistem operasi andoid. Perkembangan media cloud storage ini tidak menutup kemungkinan akan mendapat dampak penggunaan yang bersifat negative atau dapat di gunakan sebagai media untuk tindak kejahatan. Hal ini merupakan tantangan baru bagi IT *forensic* dan penegak hukum untuk melakukan penyelidikan terhadap tindak kejahatan digital pada media cloud storage google drive pada android. Akuisisi digunakan untuk tahap yang penting dalam proses analisis tetapi tetap di rujuk dari metode yang sudah disepakati. Pengunaan metode yang di gunakan dalam menangani kejahatan dengan barang bukti media smartphone adalah *Metode National Institute of Justice* (NIJ) .**

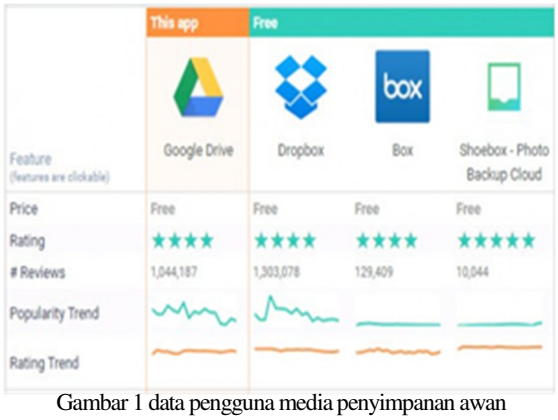
Kata Kunci* – *smartphone, penyimpanan, forensik mobile, google drive, NIJ

PENDAHULUAN

Perkembengan teknologi smartphone sudah sangat pesat. Smartphone kini telah berkembang dengan fitur-fitur yang disesuaikan dengan perkembangan zaman dan kebutuhan dari penggunanya [1]. Perangkat seluler juga lambat laun mulai menggantikan peran komputer dengan semakin banyaknya fitur yang disediakan [2]. Smartphone dengan sistem operasi Android yang mempunyai aplikasi yang semakin canggih berdasarkan perkembangan era digital [3].

Smartphone pada saat ini sudah banyak megambil teknologi komputer PC terutama dalam hal media penyimpanan. Banyaknya pilihan aplikasi penyimpanan awan yang ada dismartphone sekarang ini yang memberikan kapasitas penyimpanan besar dan gratis untuk di gunakan sebagai media menyimpan data [4] .

Pada gambar 1 menjelaskan rating dari beberapa jenis penyimpanan *cloud stronge, google drive* memiliki posisi ke dua dengan jumlah ulasan 1.044.187, posisi pertama adalah *dropbox* dengan jumlah ulasan 1.303.087 kali.



Gambar 1 data pengguna media penyimpanan awan

Model analisis tradisional digital forensik antara penyidik dengan barang bukti saling terkait, penyidik bekerja dengan bukti fisik, seperti media penyimpanan atau perangkat komputasi tertentu [5]. Akses barang bukti melalui perangkat seperti smartphone telah banyak membantu dalam proses investigasi layanan penyimpanan awan.

Popularitas komputasi awan telah menimbulkan pertanyaan mengenai keamanan data yang di simpan dalam media *cloud storage* [6]. Forensik digital pada layanan penyimpanan awan akan selalu memunculkan tantangan baru bagi para peneliti forensik digital dan penguji dalam menangani kasus *cyber crime* [7]. Karakteristik kompleks bagi komputer forensik yang sedang bekerja membawa tantangan besar, dalam rangka beradaptasi dengan perubahan digital sekarang ini, komputer forensik dalam komputasi awan telah menjadi topik penting, seiring berkembangnya era digital dan tidak lepas juga keterkaitannya dengan *forensic mobile* [8].

Digital forensik juga sabagai suatu ilmu untuk menemukan barang bukti dari suatu tindak kejahatan yang telah terjadi [9]. Ilmu digital forensik telah mempelajari berbagai hal terutama untuk pemecahan kasus kejahatan yang memanfaatkan teknologi informasi atau lebih sering disebut dengan *cyber crime* [10]. Dalam rangka melakukan investigasi yang tepat dan sesuai, tidak hanya menggunakan komputer forensik saja tetapi juga berkembang forensik untuk mobile atau ponsel yang perlu dilakukan untuk memproleh barang bukti digital [11]. Mengunakan metode forensik yang sesuai merupakan

faktor penting untuk mendukung proses investigasi tindak kejahatan yang lebih efektif dan efisien dalam menangani sebuah kasus *cyber crime* [12]. Dalam model forensik tradisional, penyidik bekerja dengan barang bukti fisik tetapi ketika melakukan analisis digunakan hasil duplikasi dari sebuah barang bukti sistem, seperti penyimpanan media, atau perangkat komputasi terpadu (misalnya, smartphone)[13].

Mobile forensik dapat diterapkan diberbagai macam perangkat smartphone dengan berdasrkan metode dan jenis sistem perangkat lunak yang di gunakan [14]. Menurut dokumen SNI 27037:2014, akuisisi merupakan proses untuk membuat salinan barang bukti digital dan mendokumentasikan metodologi yang digunakan serta aktifitas yang dilakukan [15]. Digital forensik merupakan salah satu cara menemukan suatu bukti digital. Akuisisi pada media smartphone merupakan cara mengeluarkan file sistem yang ada di storage smartphone.

METODE PENELITIAN

Penggunaan metode penelitian ini mengadaftasi dari metode analisis forensik dari *National Institute of Justice* (NIJ). Metode ini digunakan untuk menjelaskan bagaimana tahapan penelitian yang dilakukan sehingga alur penelitian bisa selesai secara sistematis dan dapat dijadikan pedoman dalam menyelesaikan permaslahan yang ada. Menurut Roni Anggara disebutkan melakukan teknik forensik dan analisa forensik berdasarkan metode yang benar akan memiliki keberhasilan hampir 100% dalam mengumpulkan data forensik [16].

Tahapan metode dari *National Institute of Justice* (NIJ) ini terbagi menjadi lima tahapan yakni *identification, collection, examination, analysis, dan reporting* [17], secara lengkap dipaparkan sebagai berikut:

1. Tahap *Identification*

Tahap *identification* atau tahap identifikasi merupakan kegiatan pemilahan barang bukti tindak kejahatan digital dan pemilahan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses identifikasi, pelabelan, perekaman, untuk menjaga keutuhan barang bukti.

2. Tahap *Collection*

Tahap *collection* atau tahap pengumpulan merupakan serangkaian kegiatan mengumpulkan data-data untuk mendukung proses penyidikan dalam rangka pencarian barang bukti kejahatan digital. Pada tahap ini didalamnya terdapat proses pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti dari perubahan.

3. Tahap *Examination*

Tahap *examination* atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa file tersebut asli sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, untuk itu pada file digital perlu dilakukan identifikasi dan validasi file dengan teknik hashing.

4. Tahap *Analysis*

Tahap *analysis* atau tahap meneliti ini dilakukan setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, selanjutnya data tersebut dianalisis secara detail dan komprehensif dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut. Hasil analisis terhadap data digital selanjutnya disebut digunakan sebagai barang bukti digital serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.

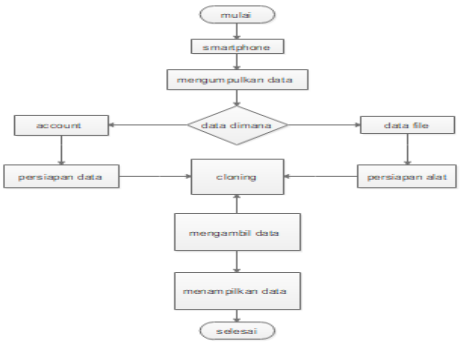
5. Tahap *Reporting*

Tahap *reporting* atau tahap pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan dan dianalisis. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai tool, dan metode yang digunakan, penentuan tindakan pendukung yang dilakukan, dan memberikan rekomendasi untuk perbaikan kebijakan, metode, *tool*, atau aspek pendukung lainnya pada proses tindakan digital forensik

Alat dan bahan yang di butuhkan dalam penelitian ini adalah

a. Laptop HP A10-9600P
b. USB konektor
c. *Oxygen Forensic*
d. *MOBILedit Forensic*
e. Handphone SAMSUNG Galaxy V Plus

Perancangan sistem berdasrkan metode National Institute of Justice (NIJ) yang akan dilakukan dapat di lihat di gambar 1.



Gambar 1. Rancangan sistem

Penjelasan gambar 1 adalah sebagai berikut :

a. Menyediakan bahan Pada tahap ini adalah penyediaan bahan berupa sebuah smartphone

SAMSUNG Galaxy V Plus yang dijadikan sebagai subjek penelitian

b. Mengumpulkan data Pengumpulan data dimasudkan untuk mengumpulkan informasi-informasi tentang smartphone tersebut dan mengumpulkan informasi data yang akan diforensik.
c. Mencari informasi data Pada tahap ini adalah pencarian bentuk data *account*, ekstensi data, dan data yang bisa di buka dari sebuah kode hexsa yang tersimpan pada *smarphone.*
d. Melakukan persiapan alat
e. Setelah proses pencarian selesai dan ditentukan bentuk file yang akan dikembalikan selanjutnya mempersiapkan alat dan bahan serta teknik yang bisa dilakukan untuk meng*akuisisi* data. Hal ini dimaksudkan untuk memudahkan kegiatan mengeluarkan data dengan cepat dan efisien.
f. Melakukan *cloning* Tahap selanjutnya yaitu melakukan *cloning* terhadap data yang sudah dikeluarkan.
g. Mengambil data Pada tahap ini yaitu pengambilan data hasil dari kegiatan cloning
h. Menampilkan data untuk dilaporkan Pada tahap akhir yaitu data yang sudah diambil dari hasil cloning selanjutnya dilaporkan sebagai hasil temuan dalam penelitian ini

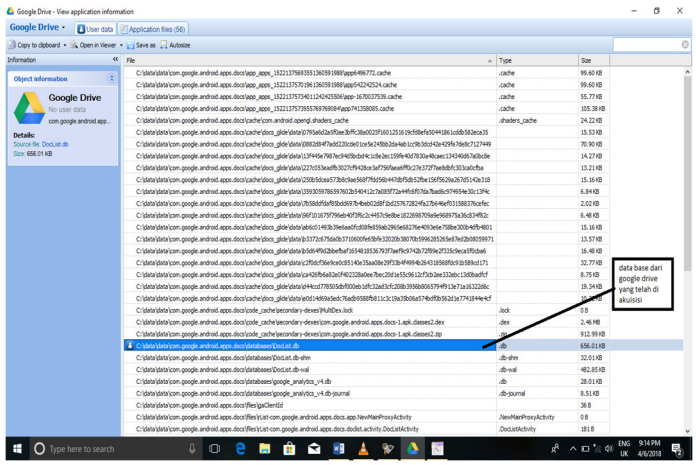
HASIL DAN PEMBAHASAN

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

Gambar 2 tampilan data di Oxygen Forensics

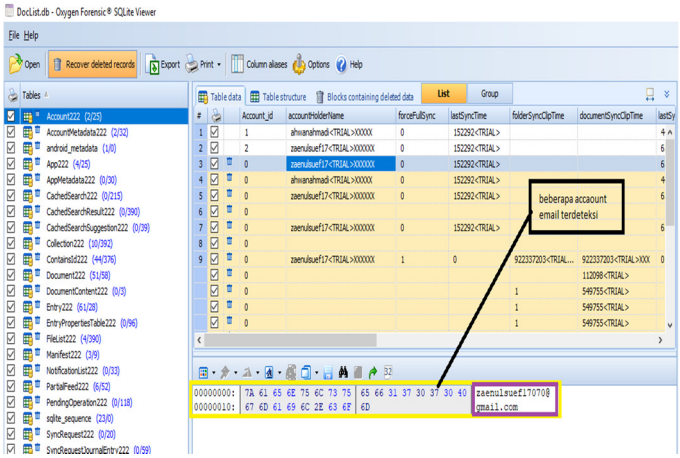
Gambar 3 menunjukkan data-data yang berhasil di*akuisisi* dari sebuah peyimpanan *Google Drive*.



Gambar 3 data pada *Google Drive*

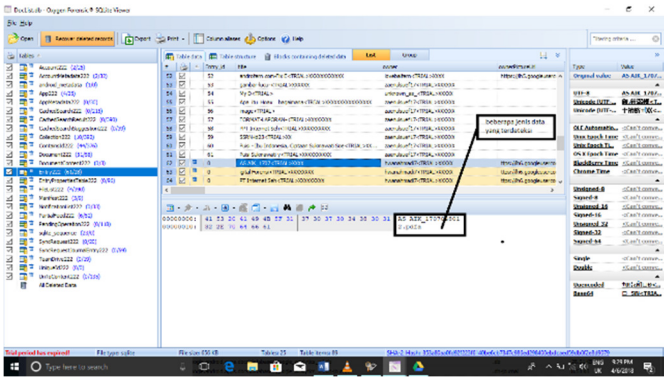
Salah satu data yang terdeteksi adalah sebuah *account email* dari penyimpanan *Google Drive* yang

kemudian di terjemahkan dari kode hexsa dapat dilihat dari gambar 4.



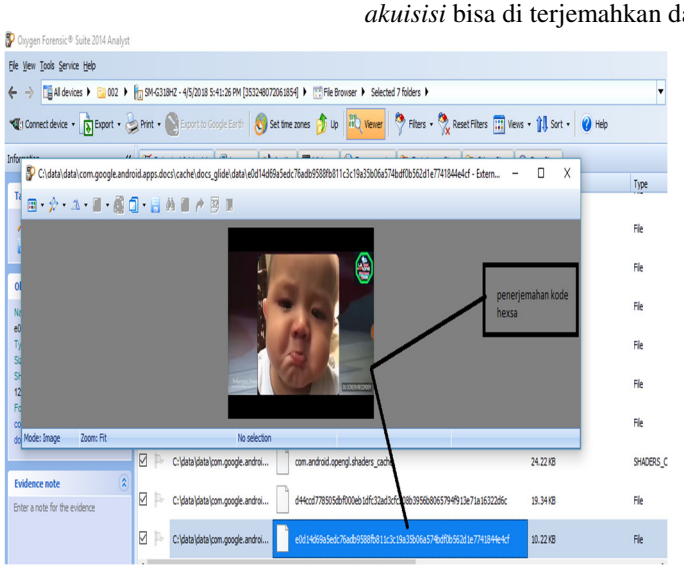
Gambar 4 akun email Google Drive yang di hapus

Data - data dari media penyimpanan *cloud* seperti google drive yang ada di android setelah di lakukan ekstraksi atau akuisisi dapat diketahui jenis-jenis data yang ada dan informasi data yang terhapus juga tersedia dapat dilihat pada gambar 5.



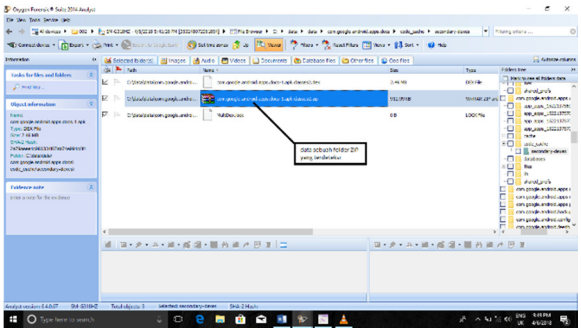
Gambar 5 ekstensi data dari media storage *Google Drive*

Gambar 6 menunjukkan kode hexsa dari proses *akuisisi* bisa di terjemahkan dalam bentuk gambar.



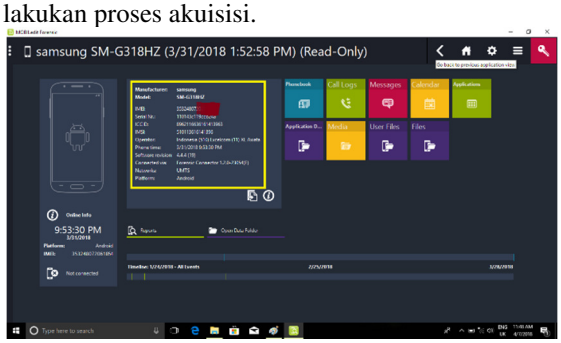
Gambar 6 gambar yang bisa di buka dari kode hexsa

Gambar 7 juga menunjukkan bahwa di temukan sebuah file Zip dalam media penyimpanan Google Drive.



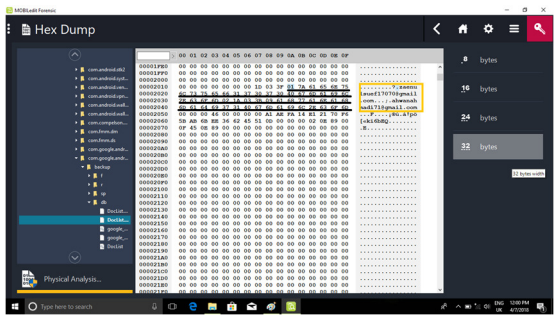
Gambar 7 file zip yang di temukan dalam proses analisis media Google Drive di android

Sebagai perbandingan peneliti juga menggunakan tool forensik lainnya yaitu *MOBILedit Forensics*. Dapat di lihat pada gambar 8, smartphone *Samsung Galaxy V Plus* yang sudah terkoneksi dengan tool *MOBILedit Forensics* kemudian di lakukan proses akuisisi.



Gambar 8 tampilan MOBILedit Forensic

Gambar 9 menunjukkan file dari media Google Drive, ketika di*akuisisi* menunjukkan kode-kode hexsa yang di mana kode hexsa tersebut menunjukkan sebuah *account email* dari pengguna Google Drive.



Gambar 9 menunjukkan *account email* yang bisa di temukan

Dari hasil penelitian yang di lakukan maka didapatkan perbandingan hasil dari kedua buah *tool* forensik dengan data sebagai berikut.

Tabel 1. perbandingan hasil analisis dari dua tool yang berbeda

Tool	Account	Ekstensi file	Gambar yang bisa di munculkan	Folder zip yang terdeteksi
Oxygen Forensics	Yes	Yes	Yes	yes
Mobile Edit Forensik	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.

KESIMPULAN DAN SARAN

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

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

REFERENSI

[1] S. Sahiruddin, Imam Riadi, "Analisis Forensik Recovery Dengan Keamanan Fingerprint."

[2] G. M. Zamroni, R. Umar, and I. Riadi, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," Annu. Res. Semin., vol. 2, no. 1, pp. 102–105, 2016.

[3] A. Firdonsyah, I. Riadi, and Sunardi, "Analisis Forensik Bukti Digital Blackberry Messenger Pada Android," Semin. Nas. Click Karawang, pp. 25–29, 2016.

[4] B. Martini and K. K. R. Choo, "Cloud storage forensics: OwnCloud as a case study," Digit. Investig., vol. 10, no. 4, pp. 287–299, 2013.

[5] V. Roussev and S. McCulley, "Forensic analysis of cloud-native artifacts," Digit. Investig., vol. 16, pp. S104–S113, 2016.

[6] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services," Digit. Investig., vol. 9, no. 2, pp. 81–95, 2016.

[7] D. Rathod, "G o o g l e D r i v e F o r e n s i c s," pp. 136–140.

[8] C. Long and Z. Qing, "Forensic Analysis to China's Cloud Storage Services," Int. J. Mach. Learn. Comput., vol. 5, no. 6, pp. 467–470, 2015.

[9] M. N. Faiz, R. Umar, A. Yudhana, and U. A. Dahlan, "Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary," J. Ilm. Ilk., vol. 8, no. 3, pp. 242–247, 2016.

[10] J. T. Informatika, F. T. Industri, and U. I. Indonesia, "Usb Analisys Tool Untuk Investigasi Forensika Digital Fietyata Yudha."

[11] H. Chung, J. Park, S. Lee, and C. Kang, "Digital forensic investigation of cloud storage services," Digit. Investig., vol. 9, no. 2, pp. 81–95, 2012.

[12] R. Umar, A. Yudhana, and M. N. Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," pp. 207–211.

[13] I. A. Vassil Roussev, "Forensic Acquisition of Cloud Drives Forensic Acquisition of Cloud Drives ∗," no. January 2016, 2017.

[14] A. A. Anton Yudhana , Rusydi Umar, "Akuisisi dan analisis google drive pada smartphone android," 2017.

[15] Y. Prayudi, B. Sugiantoro, M. T. Informatika, F. T. Industri, and U. I. Indonesia, "Abstrak."

Esley

[16] R. A. Putra, A. Fadlil, and I. Riadi, "Forensik Mobile Pada Smartwach Berbasis Android," *Jurti*, vol. 1, no. 1. pp. 41–47, 2017.

[17] M. Nur Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," JISKa, vol. 1, no. 3, pp. 108–114, 2017