

## **Investigasi Aplikasi *Facebook messenger* Pada Smartphone Berbasis iOS Menggunakan Metode DFRWS**

**Muhammad Syahrizal Darwis<sup>\*1</sup>, Erick Irawadi Alwi<sup>2</sup>, Huzain Azis<sup>3</sup>**

<sup>1, 3</sup>Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Muslim Indonesia Makassar Indonesia, <sup>2</sup>Program Studi Sistem Informasi Fakultas Ilmu Komputer Universitas Muslim Indonesia Makassar Indonesia

E-mail: <sup>\*1</sup>[muhammadsyahrizal3@gmail.com](mailto:muhammadsyahrizal3@gmail.com), <sup>2</sup>[erick.alwi@umi.ac.id](mailto:erick.alwi@umi.ac.id), <sup>3</sup>[huzain.azis@umi.ac.id](mailto:huzain.azis@umi.ac.id)

### **Abstrak**

*Meningkatnya jumlah pengguna aplikasi Facebook messenger tentunya membawa dampak positif dan negatif. Kejahatan umum seperti perdagangan narkoba, terorisme, perencanaan pembunuhan dan kejahatan lainnya yang menggunakan facebook messenger sebagai media komunikasi. Kejahatan tersebut tentunya akan meninggalkan jejak yang dapat dijadikan sebagai barang bukti digital. Penelitian ini bertujuan untuk melakukan analisis terhadap smartphone berbasis iOS dan mengkaji bukti digital pada aplikasi Facebook messenger. Metode yang digunakan adalah workshop penelitian forensik digital dalam menginvestigasi perangkat smartphone dengan mencari bukti berupa percakapan digital melalui pesan teks. Hasil penyidikan yang dilakukan berupa informasi untuk membuktikan bahwa pelaku merupakan pelaku tindak pidana, informasi tersebut kemudian disajikan dalam bentuk laporan forensik yang akan digunakan selama persidangan.*

**Kata Kunci**—Facebook; Messenger; iOS; Bukti Digital; DFRWS

### **Abstract**

*The increase in the number of Facebook messenger application users certainly has positive and negative impacts. Common crimes such as drug trafficking, terrorism, murder planning and other crimes that use facebook messenger as a medium of communication. The crime will certainly leave a trail that can be used as digital evidence. This study aims to conduct an analysis on an iOS-based smartphone and examine digital evidence on the Facebook messenger application. The method used is a digital forensics research workshop in investigating smartphone devices by looking for evidence in the form of digital conversations via text messages. The results of the investigation carried out in the form of information to prove that the perpetrator is a criminal, the information is then presented in the form of a forensic report that will be used during the trial.*

**Keywords**—Facebook; Messenger; iOS; Digital Evidence; DFRWS

### **1. PENDAHULUAN**

Kemajuan teknologi komunikasi yang begitu pesat merambah ke semua lapisan dan telah merubah gaya hidup masyarakat. Munculnya *smartphone* menjadi tanda perkembangan teknologi, objek yang sangat cerdas dapat digunakan untuk keperluan karena dapat menyimpan berbagai macam dokumen ataupun data pribadi. *Smartphone* dilengkapi berbagai macam aplikasi untuk keperluan telepon, SMS (*short message service*), *chat*, *e-mail*, media sosial dan aplikasi-aplikasi lainnya [1]. Jumlah pengguna aplikasi pesan instan berkembang pesat setiap tahunnya. Aplikasi pesan instan saat ini telah menggantikan *short message service* (SMS) sebagai aplikasi jarak jauh karena mudah diakses dan murah. Popularitas aplikasi pesan instan telah menyebabkan munculnya berbagai aplikasi perpesanan instan yang menawarkan fitur dan

kualitas yang berbeda, salah satu fiturnya adalah keamanan data terbaik untuk melindungi privasi penggunanya [2].

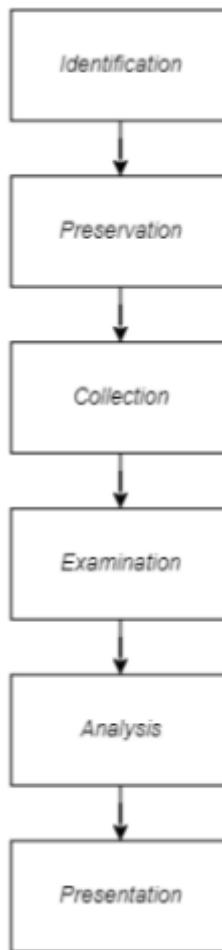
Peningkatan jumlah pengguna aplikasi *facebook messenger* tentu memiliki dampak positif dan negatif. Salah satu dampak negatifnya adalah tindakan kejahatan seperti perdagangan narkoba, terorisme, perencanaan pembunuhan dan kejahatan lainnya yang menggunakan *facebook messenger* sebagai media komunikasi. Kejahatan tersebut tentunya akan meninggalkan jejak yang dapat dijadikan sebagai barang bukti digital [3].

Metode yang digunakan untuk melakukan pemeriksaan bukti digital pada barang bukti pada perangkat *mobile* dalam konteks hukum adalah *mobile forensic*. Mengekstrak bukti digital berarti memulihkan, mengumpulkan, dan menganalisis data yang disimpan di dalam memori perangkat *mobile* [2]. Forensik digital memiliki beberapa jenis yang dikategorikan oleh perangkat atau media yang diinvestigasi, salah satunya yang digunakan pada penelitian ini adalah *mobile forensics*. Peran *mobile forensics* untuk mendapatkan bukti digital yang digunakan dalam mengungkapkan kasus kriminal dengan menganalisa isi dari ponsel. *Mobile forensics* merupakan ilmu berbasis digital forensik atau komputer forensik. Forensik digital adalah ilmu yang mempelajari tentang rekonstruksi kasus kriminal atau membantu untuk mengantisipasi tindakan yang terbukti melanggar prosedur yang telah ditentukan [4].

Studi mengenai pemeriksaan bukti digital pada *smartphone* telah banyak dilakukan oleh peneliti. Diantaranya adalah penelitian pada aplikasi *facebook messenger* yang terinstal pada *smartphone* berbasis *android* yang menggunakan metode NIJ dengan bantuan beberapa *tool* dengan hasil yang didapatkan. Bukti digital yang diperoleh adalah melakukan rekonstruksi terkait percakapan dan berhasil merecovery 2 akun, 11 chat dan 26 gambar [1]. Oleh karena itu, dibutuhkan tahapan untuk mendapatkan bukti valid dalam melakukan investigasi barang bukti digital pada *smartphone* berbasis *iOS* dengan prosedur pemeriksaan digital forensik. Pihak berwenang dapat menggunakan data data dalam aplikasi *facebook messenger* sebagai barang bukti. Metode forensik diperlukan untuk memastikan keberhasilan proses pengambilan data-data tersebut.

## 2. METODE PENELITIAN

Penelitian ini menggunakan metode digital forensik *Digital Forensic Research Workshop* (DFRWS) dalam memperoleh barang bukti dan merekam informasi yang dibutuhkan untuk kemudian dikumpulkan menggunakan data mekanisme terpusat [7]. Investigasi forensik digunakan untuk mengetahui bukti digital dan alat bukti menggunakan alat yang berbeda dan merupakan proses yang sulit dan kompleks. Tujuan digital forensik adalah untuk mempertahankan dokumentasi dan mengetahui siapa yang bertanggung jawab sehingga dapat digunakan sebagai bukti di pengadilan. Metode *Digital Forensics Research Workshop* (DFRWS) mempunyai beberapa tahapan yaitu seperti pada Gambar 1 [9].



Gambar 1. Tahapan DFRWS

#### 2.1. *Identification (Identifikasi)*

Tahap awal yang dilakukan pada penelitian ini adalah melakukan perancangan kebutuhan yang diperlukan untuk membantu proses penyelidikan dalam pencarian barang bukti digital dengan proses identifikasi.

#### 2.2. *Preservation (Pemeliharaan)*

Pada tahap ini merupakan tahap pemeliharaan yang diperlukan untuk menjaga bahwa barang bukti digital masih terjaga keasliannya. Barang bukti tidak dilakukan perubahan atau disabotase.

#### 2.3. *Collection (Pengumpulan)*

Pada tahap ini, peneliti melakukan proses pengumpulan dan mengidentifikasi bagian yang dibutuhkan untuk melakukan identifikasi dari sumber data berdasarkan barang bukti digital.

#### 2.4. *Examination (Pemeriksaan)*

Pada tahap ini, peneliti melakukan proses *filtering* pada salah satu bagian yang berasal dari sumber data, tetapi tetap menjaga keaslian dari isi data tersebut dikarenakan sifat dari

keaslian data sangat penting oleh karena itu *filtering* data dilakukan hanya dari sisi perubahan bentuk pada data dengan tetap menjaga keaslian data.

### 2.5. Analysis (Analisis)

Pada tahap ini, peneliti melakukan proses penelitian untuk dapat mengetahui dimana, oleh siapa dan bagaimana data dari sebuah kasus tersebut dapat diperoleh.

### 2.6. Presentation (Presentasi)

Pada tahap ini, peneliti melakukan tahapan presentasi dilakukan dengan menampilkan informasi yang diperoleh dari tahap analisis sebelumnya, kemudian dilakukan pendataan data hasil dari analisis yang diperoleh meliputi pelaporan tindakan yang sudah dilakukan. Penjelasan mengenai metode dan tools yang diterapkan untuk menentukan tindakan yang dibutuhkan serta memberikan saran dan masukan untuk perbaikan sebuah kebijakan atau hasil yang diperoleh.

## 3. HASIL DAN PEMBAHASAN

Digital forensik adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemui pada perangkat digital. Proses digital forensik adalah mengidentifikasi, memelihara, menganalisa dan mempergunakan bukti digital menurut hukum yang berlaku [2].

Mobile Forensic adalah ilmu yang melakukan proses pemulihan bukti digital dari perangkat seluler menggunakan cara yang sesuai dengan kondisi dan metode forensik. Penggunaan ponsel seperti *smartphone* dengan berbagai macam tipe dan sistem operasi untuk kejahatan sudah semakin tinggi jumlahnya, tetapi dengan adanya forensik untuk perangkat mobile dapat membantu mengatasi kasus kejahatan yang berhubungan dengan perangkat ponsel khususnya *smartphone* [5].

Facebook merilis aplikasi pesan instan untuk mobile agar sejajar atau bersaing dengan layanan yang sama seperti blackberry messenger, kakao talk, whatsapp dan line. Pasar yang terus maju pesat untuk aplikasi pesan instan membuat pendapatan tradisional operator selular menurun. Facebook messenger merupakan aplikasi pesan instan yang dapat mengirimkan teks, gambar, video dan pesan suara. Aplikasi ini ada untuk *smartphone* berbasis android, iOS, blackberry dan windows. Aplikasi *facebook messenger* digunakan untuk mempermudah pengguna facebook dalam pengiriman pesan antar sesama pengguna facebook [6].

Digital Forensics Research Workshop (DFRWS) adalah kerangkakerja ilmiah dengan dasar yang terbukti untuk proses forensik yang mencakup pemeliharaan bukti digital yang diperoleh dari sumber digital dari tempat perkara atau alat dilakukannya kejadian cybercrime dengan tujuan untuk memfasilitasi atau melanjutkan rekonstruksi peristiwa yang melanggar hukum teknologi informasi, atau membantu untuk mengantisipasi tindakan yang merusak keaslian barang bukti sehingga membuat barang bukti yang telah didapatkan menjadi tidak sah di mata hukum dan terbukti mengganggu untuk operasi yang direncanakan dalam prosesinvestigasi [7]. Metode DFRWS membantu dalam mendapatkan barang bukti dan mekanisme terpusat untuk merekam informasi yang dikumpulkan. Tahapan metode DFRWS yaitu identifikasi, reservasi, pengumpulan, pengujian, analisis dan presentasi [8].

### 3.1. Identification

Metode *Digital Forensics Research Workshop* (DFRWS) merupakan salah satu metode yang memiliki tahapan cukup lengkap dalam menjalakan proses forensik dan banyak digunakan oleh penyidik dalam mengumpulkan barang bukti. Proses mendapatkan barang bukti pada *smartphone* berbasis iOS menggunakan *software* forensik *Mobiledit Forensic Express* dan *FTK Imager*. Informasi tentang *hardware* dan *software* yang digunakan dijelaskan pada Tabel 1.

Tabel 1. Alat Penelitian

No.	Alat Penelitian	Deskripsi
1	Laptop	Asus Tuf Gaming FX505DT, Windows 11 64 Bit
2	Smartphone	iPhone 6, Versi iOS 12.5.5
3	Kabel USB	Konektor dari Hp ke Laptop
4	Facebook messenger	Aplikasi sosial media
5	Mobileedit Forensic Express	Aplikasi berbasis windows yang dapat digunakan untuk memperoleh bukti digital pada smartphone
6	FTK Imager	Aplikasi berbasis windows yang dapat digunakan untuk menganalisis hasil dari bukti digital pada smartphone

Tahapan pertama yang dilakukan adalah proses identifikasi untuk dijadikan bahan acuan pada pencarian barang bukti berdasarkan kasus yang telah terjadi sebelumnya. Barang bukti yang akan diidentifikasi adalah sebuah *smartphone* dengan spesifikasi lebih detail dapat dilihat pada Tabel 2 seperti berikut :

Tabel 2. Spesifikasi *Smartphone*

Spesifikasi	Type
Nama	Amie Iphone 6
Versi Perangkat Lunak	12.5.5
Nama Model	iPhone 6
Nomor Model	MG632LL/A
Nomor Seri	C7JNVSFNG5MG
Kapasitas	64 GB
IMEI	35 698606 091631 9
ICCID	8962115939431125073
MEID	35698606091631

### 3.2. *Preservation*

Tahap *preservation* adalah tahap pemeliharaan barang bukti digital dan memastikan keadaan barang bukti asli. Proses penjagaan integritas dilakukan untuk menjaga barang bukti itu asli dan tidak rusak. Tahap yang dilakukan adalah melakukan isolasi perangkat *smartphone* dari

komunikasi data masuk dan keluar. Teknik isolasi perlu dilakukan untuk menghindari hal-hal yang dapat merusak barang bukti digital atau mempengaruhi integritas data didalamnya. Kegiatan isolasi barang bukti yang dilakukan adalah merubah status perangkat kedalam mode pesawat seperti pada Gambar 2.

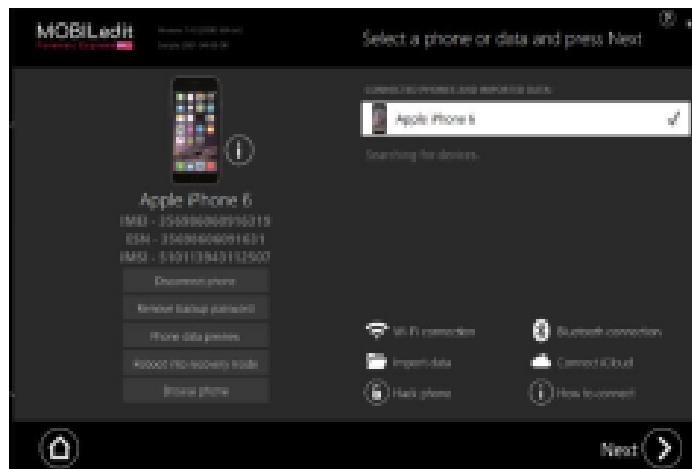


Gambar 2. Isolasi *Smartphone* dengan Mode Pesawat

Proses isolasi diperlukan untuk mengurangi kemungkinan data pada *smartphone* berubah. Bisa disebabkan oleh penambahan atau pengurangan data dari luar yang menyebabkan barang bukti hilang atau rusak saat dilakukan proses forensik pencarian barang bukti.

### 3.3. Collection

Tahap *collection* barang bukti digital pada *smartphone* memiliki resiko yang tinggi, dikarenakan jika terjadi kesalahan fatal, data dan bukti digital yang ada pada *smartphone* dapat hilang atau *corrupted* sehingga tidak data tidak terbaca. Kemampuan *tool MOBILedit Forensic Express* adalah dapat membuat sebuah *backup* sistem (*itunes*) dan *collection* data pada *smartphone* kemudian mengekstraksinya seperti pada Gambar 3. Hasil dari proses *backup* data ini berupa dokumen *image* dari *smartphone* dengan ekstensi *.img* dengan ukuran dokumen yang bervariasi tergantung banyaknya data yang disimpan pada *smartphone* tersebut.



Gambar 3. *Backup* dan *Collection* Data

### 3.4. Examination

Proses *examination* atau *filtering* barang bukti dilakukan sesuai dengan kebutuhan investigator dalam menganalisis barang bukti digital. Tahap ini akan membatasi dalam melakukan penyelidikan barang bukti agar tidak melebihi dari *case* yang telah diinvestigasi, karena dalam hal investigasi forensik investigator hanya diperbolehkan menganalisis sesuai perkara yang telah diajukan. Dalam penelitian ini, hanya *case message* yang akan diekstraksi seperti Gambar 4.



Gambar 4. *Filtering*

Hasil dari ekstraksi yang telah dilakukan akan tampil dalam bentuk *full report* bentuk format.pdf. Tampilan *file* data hasil ekstraksi seperti yang ditunjukkan pada Gambar 5.

Name	Date modified	Type	Size
analysis_file	1/26/2022 12:25 AM	File folder	
apple_device	1/26/2022 8:51 PM	File folder	
phone_file	1/26/2022 9:40 PM	File folder	
log_all.txt	1/21/2022 12:29 AM	Text Document	39,656 KB
log_short.txt	1/21/2022 12:29 AM	Text Document	2 KB
report_config.txt	1/26/2022 8:51 PM	CFG File	5 KB

Gambar 5. Hasil Ekstraksi Data

### 3.5. Analysis

Tahap analisis merupakan tahap untuk melihat hasil dari tahap pemeriksaan secara detail untuk mendapatkan bukti digital. Tahap ini membatasi proses pencarian pada bagian tertentu dari hasil yang didapat pada tahap pemeriksaan. Pembatasan ini dapat berupa hal-hal yang berhubungan dengan data atau aplikasi tertentu. Penelitian ini membatasi pencarian bukti digital pada hasil yang didapat dari aplikasi *facebook messenger*. Hasil yang telah ditemukan kemudian dilakukan analisis menggunakan *tool FTK Imager* seperti Gambar 6.

00de90	41 4F 5A 48 79 34 36 39-35 33 31 98 39 30 30 31	NOBy46952189001
00dea0	36 34 34 34 30 37 39 39-32 E1 6D 62 69 4C 20 E3	644467992ambil t
00deb0	61 72 61 6E 67 E6 79 E1-20 29 73 69 61 62 75 26	kepungnya (habu)
00dec0	20 70 73 74 5B 06 17 DF-48 C0 80 02 02 03 01 81	pub - 101P-----
00ded0	EC 8C 41 D2 02 81 12 02-3E 05 05 51 33 13 05 01 1 A0	-----0 03 ...

Gambar 6. Kode Hexa Teks Percakapan

Hasil dari analisa, didapatkan data berupa bukti percakapan antara pelaku dan korban. Gambar 13 adalah salah satu isi dari sekian percakapan. Gambar tersebut merupakan kode hexa teks percakapan dari hasil akuisisi pada aplikasi *MOBILEedit Forensic Express*. Isi dalam percakapan tersebut menyatakan “ambil barangnya (shabu) put” yang dimana percakapan tersebut sesuai yang ada pada *smartphone* yang diamankan.



Gambar 7. Tampilan Hasil Gambar

Pada Gambar 7 adalah gambar yang ada pada isi percakapan. Didalam kode hexa setelah diterjemahkan mendapatkan hasil teks percakapan antar pelaku dan korban.

### 3.6. Presentation

Tahap presentation merupakan hasil analisis yang telah dilakukan, berikut hasil dari *tools forensik* yang telah ditemukan pada Tabel 3.

No.	Bukti Digital	Mobileedit Forensic Express
1	Teks Percakapan	Ya
2	Gambar	Ya
3	Profil	Tidak
4	Waktu Percakapan	Tidak

Pada tahap ini telah melakukan skenario yaitu data pesan dihapus dan tidak dihapus, pada saat ketika data pesan dihapus, tidak ada satupun data yang didapat dan pada waktu tidak dihapus, dapat menampilkan berupa teks percakapan dan gambar pada saat menggunakan *tools Mobileedit Forensic Express*.

---

#### 4. KESIMPULAN DAN SARAN

Berdasarkan hasil dari proses penelitian mengenai analisis bukti digital aplikasi *facebook* yang berjalan pada *smartphone* berbasis *iOS* memberikan beberapa kesimpulan sebagai berikut: 1) Dalam penelitian ini telah melakukan skenario penelitian yang dilakukan adalah menggunakan *smartphone* iPhone 6 versi *iOS* 12.5.5, melakukan proses instalasi aplikasi *Facebook messenger*, pembuatan pesan, melakukan investigasi menggunakan *tool* forensik yaitu *Mobileedit forensic* dan *FTK Imager*. 2) Bedasarkan bukti digital yang didapatkan pada 2 *tools* forensik dapat disimpulkan bahwa hasil akuisisi dan analisis data menggunakan *tool* *Mobileedit Forensic* dan *FTK Imager* pada *smartphone* berbasis *ios* tersebut akan dilaporkan sebagai barang bukti. Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan metode DFRWS (*Digital Forensic Research Workshop*) dengan tahapan *identification*, *preservation*, *collection*, *examination*, *analysis* dan *presentation*. Hasil yang telah didapatkan adalah teks percakapan dan gambar yang tidak terhapus. Hasil penelitian menunjukan bahwa pelaku melakukan tindak kejahatan menggunakan *smartphone* sebagai media komunikasi untuk melakukan transaksi narkoba.

Adapun saran sebagai pengembangan penelitian ini lebih lanjut adalah untuk penelitian selanjutnya yaitu dapat menemukan *file* yang telah dihapus menggunakan *tools* forensik yang lainnya dengan menggunakan metode yang berbeda untuk dapat menemukan *file* terhapus pada *smartphone* berbasis *iOS* dengan versi *iOS* yang terbaru.

#### DAFTAR PUSTAKA

- [1] S. Madiyanto, H. Mubarok, N. Widiyasono, T. Informatika Fakultas Teknik Universitas Siliwangi Tasikmalaya Jl Siliwangi No, and K. Tasikmalaya, “PROSES INVESTIGASI MOBILE FORENSIK PADA SMARTPHONE BERBASIS IOS INVESTIGATION PROCESS MOBILE FORENSICS ON SMARTPHONE IOS BASED,” 2017.
- [2] M. S. Asyaky, N. Widiyasono, and R. Gunawan, “Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android,” *J. Penelit. Tek. Inform.*, vol. 3, no. 1, 2018.
- [3] A. Yudhana, I. Riadi, and I. Anshori, “Analisis Bukti Digital *Facebook messenger* Menggunakan Metode Nist,” *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.
- [4] I. Riadi, “Analisis Forensik *Smartphone* Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express,” [Online]. Available: <http://openjournal.unpam.ac.id/index.php/informatika89>.
- [5] I. Riadi and A. Dahlan, “Analisis Forensik Recovery pada *Smartphone* Android Menggunakan Metode National Institute Of Justice (NIJ),” *JURTI*, vol. 3, no. 1, 2019, [Online]. Available: [www.Belkasoft.com](http://www.Belkasoft.com)
- [6] S. R. Ardingintias and H. , Sunardi, “Investigasi Digital Pada *Facebook messenger*,” pp. 19–26, 2018. [7] S. Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti, I. Riadi, and P. Widiandana, “Terakreditasi SINTA Peringkat 2 Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics Research Workshop,” *Masa Berlaku Mulai*, vol. 1, no. 3, pp. 730–735, 2017.

- [7] A. Yudhana, I. Riadi, and I. Zuhriyanto, “Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS),” *J. TECHNO*, vol. 20, no. 2, pp. 125–130, 2019.
- [8] I. Zuhriyanto, A. Yudhana, and I. Riadi, “Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop,” *J. Resti*, vol. 1, no. 3, pp. 829–836, 2017.