Jurnal Teknik Elektro Vol. 10 No. 1
Januari - Juni 2018

P-ISSN 1411 - 0059
E-ISSN 2549 - 1571

Identifikasi Bukti Digital WhatsApp pada Sistem Operasi *Proprietary* Menggunakan *Live Forensics*

Imam Riadi[1], Sunardi[2], dan Muhamad Ermansyah Rauli[3]

[1]*Program Studi Sistem Informasi Universitas Ahmad Dahlan*

[2]*Program Studi Teknik Elektro Universitas Ahmad Dahlan*

[3]*Program Studi Magister Teknik Informatika Universitas Ahmad Dahlan*

Jalan Prof. Dr. Soepomo S.H, Janturan, Yogyakarta, 55164, Indonesia

imam.riadi@is.uad.ac.id[1], sunardi@mti.uad.ac.id[2], muhamad1707048006@webmail.uad.ac.id[3]

Abstract— Rapid development of computer technology is also accompanied with increasing of cybercrime. One of the most common crimes is fraud case in the online shop. This crime abuses Whatapps, one of the most popular Instant Messenger (IM) applications. WhatsApp is one of the IM applications that can be used on computers, especially on windows 8.1 operating system. All applications running on the computer leave data and information on Random Access Memory (RAM). The data and information that exist in RAM can be obtained using digital forensic technique called Live Forensics. Live forensics can be used when the computer is running and connected to the network. This research aims to find digital evidence related to online shop fraud case. The digital evidence can be obtained using one of the forensic tools FTK Imager. FTK Imager can retrieve and analyze data and information on RAM. The results obtained in this research is the content of WhatsApp conversations that can be used as digital evidence to reveal a fraud in the online shop.

Keywords— WhatsApp, live forensics, digital evidence

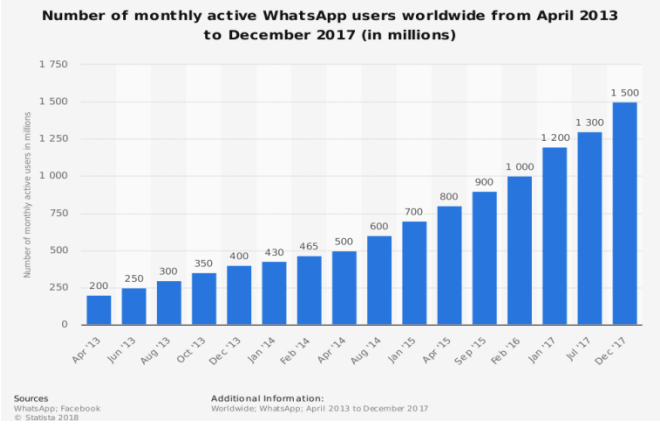
Abstrak— Perkembangan teknologi komputer semakin pesat, hal ini berbanding lurus dengan meningkatnya tindak kejahatan dunia maya. Salah satu tindak kejahatan yang sering terjadi adalah kasus penipuan *online shop*. Kejahatan ini memanfaatkan salah satu aplikasi *Instant Messenger* (IM) yang sangat populer yaitu aplikasi WhatsApp. WhatsApp merupakan salah satu aplikasi IM yang bisa digunakan pada komputer, khususnya pada komputer sistem operasi windows 8.1. Semua aplikasi yang dijalankan pada komputer meninggalkan data dan informasi pada *Random Access Memory* (RAM). Data dan informasi yang ada pada RAM dapat diperoleh menggunakan teknik forensik digital yaitu *Live Forensics*. *Live forensics* dapat digunakan pada saat komputer sedang berjalan dan terhubung jaringan internet. Penelitian ini bertujuan untuk menemukan bukti digital terkait kasus penipuan *online shop*. Bukti digital tersebut dapat diperoleh menggunakan salah satu *tools* forensik yaitu FTK Imager. FTK Imager dapat mengambil dan menganalisis data dan informasi pada RAM. Hasil yang didapat pada penelitian ini berupa isi percakapan WhatsApp yang dapat menjadi bukti digital dalam mengungkap tindak kejahatan penipuan *online shop* yang terjadi.

Kata kunci— WhatsApp, *live forensics*, bukti digital

I. PENDAHULUAN

Perkembangan teknologi komputer setiap tahunnya semakin pesat. Perkembangan ini berdampak pada peningkatan kejahatan dunia maya [1]. Para penjahat dunia maya memanfaatkan teknologi komputer sebagai media melakukan kegiatan yang bertentangan dengan hukum [2]. Salah satu tindak kejahatan yang sering terjadi adalah kasus penipuan *online shop*. Hal ini bisa dilakukan dengan memanfaatkan aplikasi *instant messenger* (IM) berbasis desktop sebagai media komunikasi dengan korban.

IM merupakan salah satu aplikasi yang sering digunakan untuk berkomunikasi menggantikan peran *Short Message Services* (SMS) [1]. WhatsApp merupakan salah satu aplikasi IM yang sangat populer dan bisa digunakan pada perangkat seluler dan komputer [3]. WhatsApp memiliki banyak fitur seperti telepon, *group chat*, pengiriman pesan, *video call*, pengiriman file, dan pesan suara. Menurut data Statista, hingga bulan desember 2017 jumlah pengguna aktif WhatsApp diseluruh dunia sebanyak 1,5 miliar [4]. Jumlah tersebut mengalami peningkatan dibandingkan jumlah pengguna WhatsApp pada bulan januari 2017 sebanyak 1,2 miliar [4]. Banyaknya pengguna memungkinkan WhatsApp dijadikan sebagai media komunikasi untuk melakukan tindak kejahatan. Gambar 1 menunjukkan statistik pengguna WhatsApp dari bulan April 2013 sampai dengan Desember 2017 [4].



Gambar 1. Statistik pengguna WhatsApp

Penggunaan aplikasi pada komputer meninggalkan data dan informasi pada *Random Access Memory* (RAM). RAM merupakan memori tempat penyimpanan sementara ketika komputer sedang dijalankan [5]. Penanganan data dan informasi pada RAM harus dilakukan dengan hati-hati karena data dan informasi tersebut bisa hilang jika sistem mati [6]. Data dan informasi yang terdapat pada RAM yang berpotensi menjadi bukti digital bisa didapat [7]. Upaya untuk mendapatkan bukti digital terkait kasus kejahatan yang terjadi dikenal sebagai forensik digital [8].

Forensik digital merupakan ilmu yang digunakan untuk kepentingan bukti hukum, yang dalam hal ini adalah membuktikan kejahatan komputer secara ilmiah untuk bisa didapatkan bukti digital yang valid [9]. Bukti tersebut didapakan melalui teknik *live forensics* yang digunakan untuk menangani kejahatan komputer yang menggunakan pendekatan ketika komputer sedang berjalan dan terhubung jaringan internet [10]. *Live forensics* bergantung pada saat komputer sedang berjalan, karena membutuhkan data dan informasi yang ada pada RAM [11]. Proses pengambilan data dan informasi tersebut harus secepatnya dilakukan setelah barang bukti ditemukan [12]. Teknik ini juga menjamin integritas data tanpa harus menghilangkan bukti digital yang potensial [13].

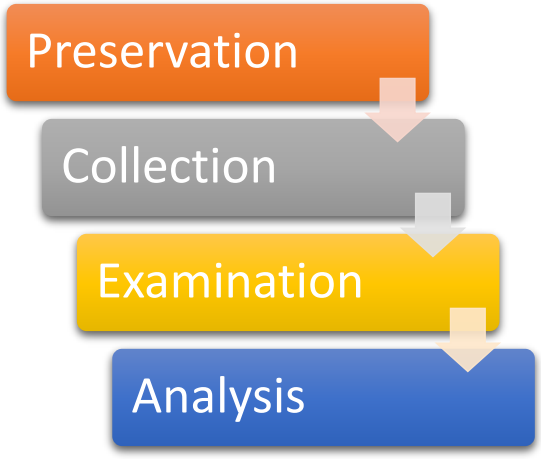
Komputer dijalankan membutuhkan sistem operasi. Sistem operasi terbagi menjadi dua yakni sistem operasi *open source* dan sistem operasi *proprietary* [13]. Penelitian ini menggunakan sistem operasi *proprietary* windows 8.1. Windows 8.1 merupakan windows versi terbaru dari versi 8 yang rilis pada tanggal 18 Oktober 2013 [14].

Penelitian ini bertujuan untuk menemukan bukti digital tindak kejahatan kasus penipuan *online shop* yang terjadi pada aplikasi WhatsApp berbasis dekstop menggunakan teknik *live forensics*.

II. METODOLOGI

A. Metode

Metode pada penelitian ini menggunakan metode yang yang dijelaskan oleh Ravneet Kaur dan Amandeep Kaur dalam jurnal ilmiahnya yang mengacu pada proses investigasi tindak kejahatan [15]. Metode tersebut terdiri dari beberapa tahapan, seperti ditunjukkan pada Gambar 2 [15].



Gambar 2. Tahapan penelitian

- *Preservation*
  Menjaga keutuhan dan pengamanan barang bukti yang telah ditemukan agar tidak hilang atau berubah.
- *Collection*
  Mengumpulkan barang bukti yang terkait dengan tindak kejahatan pelaku untuk membantu proses investigasi.
- *Examination*
  Memproses bukti yang telah dikumpulkan sehingga ditemukan bukti-bukti yang terkait tindak kejahatan pelaku. Hasil dari tahap ini dapat berupa teks, video, gambar atau pesan suara.
- *Analysis*
  Menganalisis hasil dari proses *examination* yang telah dilakukan, sehingga dapat mengidentifikasi konten atau file yang dapat dijadikan barang bukti pada kasus penipuan *online shop*.

Alat dan bahan dibutuhkan pada penelitian ini untuk mendapatkan bukti digital terkait kasus penipuan *online shop*. Alat dan bahan yang digunakan adalah laptop ASUS tipe X453S dengan sistem operasi Windows 8.1 yang telah terpasang aplikasi IM WhatsApp berbasis dekstop versi 0.2.8691 dan *smartphone* Samsung Galaxy S5 yang telah terpasang aplikasi WhatsApp. *Tools* forensik yang digunakan untuk mengambil, menggandakan, dan analisis bukti digital adalah FTK Imager.

B. Rancangan Simulasi

Penelitian ini membutuhkan simulasi untuk mendapatkan bukti digital. Simulasi yang dibuat lengkap dari aktivitas yang dijalankan pada aplikasi WhatsApp. Tujuan simulasi ini adalah agar menjadi pedoman untuk informasi yang akan diidentifikasi sebagai sebuah penipuan. Simulasinya sebagai berikut:

- Membuat akun WhatsApp tersangka.
- Membuat akun WhatsApp korban.
- Korban melakukan *chatting* untuk negosiasi kepada tersangka.
- Korban mengirimkan gambar pada tersangka.
- Tersangka melakukan penipuan terhadap tersangka.
- Menghapus pesan percakapan dari akun tersangka.

Pesan percakapan yang dihapus dari WhatsApp akan diungkap dari laptop tersangka menggunakan *tools* forensik. Gambar 3 menunjukkan simulasi yang akan dijalankan.

Gambar 3. Simulasi kasus penipuan *online shop*

III. Hasil dan Pembahasan

Penelitian ini dilakukan dengan menggunakan sebuah laptop Sistem Operasi Windows 8.1 64 Bit yang sudah terpasang aplikasi IM WhatsApp berbasis dekstop versi 0.2.8691. Pada kasus ini, penyidik menemukan barang bukti sebuah laptop dalam kondisi hidup yang digunakan oleh tersangka. Laptop dibiarkan dalam kondisi menyala dan tidak dilakukan *resfresh* (penyegaran) untuk menghindari kehilangan bukti digital.

A. Pengumpulan Barang Bukti

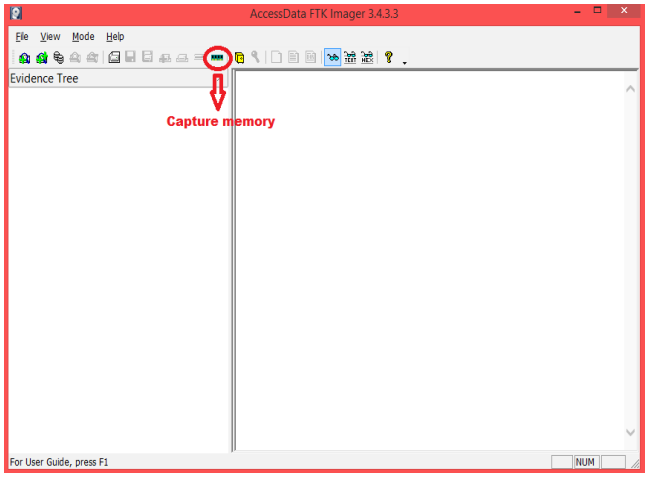
Pada tahap ini, penyidik mengumpulkan barang bukti yang digunakan tersangka untuk melakukan tindak kejahatan penipuan *online shop*. Barang bukti tersebut akan digunakan penyidik untuk menemukan bukti digital terkait tindak kejahatan penipuan yang telah dilakukan tersangka. Tahap ini bertujuan untuk membantu proses investigasi yang akan dilakukan pada tahap selanjutnya. Barang bukti yang ditemukan adalah sebuah laptop ASUS tipe X453S sistem operasi windows 8.1 yang telah terpasang aplikasi WhatsApp. Aplikasi WhatsApp tersebut masih dalam kondisi dijalankan dan tidak ditutup.

B. Pemrosesan Bukti Digital

Pada tahap ini, pemrosesan bukti digital yang terdapat pada RAM dengan aplikasi WhatsApp masih dalam kondisi dijalankan menggunakan teknik *live forensics*.

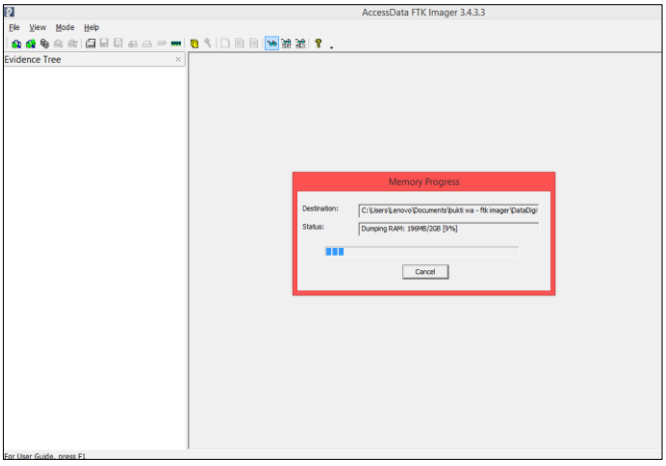
1) Pengambilan Bukti Digital

Penggunaan teknik *live forensics* dilakukan untuk mendapatkan bukti digital percakapan WhatsApp yang terdapat pada RAM. *Tools live forensics* yang digunakan pada penelitian ini adalah FTK Imager karena memiliki fitur *Capture Memory* yang mendukung teknik *live forensics*. Fitur ini dapat mengambil data dan informasi yang terdapat pada RAM, termasuk data percakapan WhatsApp. Gambar 4 menunjukkan fitur *Capture Memory* yang ada pada *tools* FTK Imager.



Gambar 4. Fitur FTK Imager

FTK Imager mengambil semua data dan informasi dari aplikasi yang sedang berjalan pada laptop termasuk data percakapan WhatsApp yang telah dihapus. Gambar 5 menunjukkan sebuah *screenshot* proses pengambilan data pada RAM.

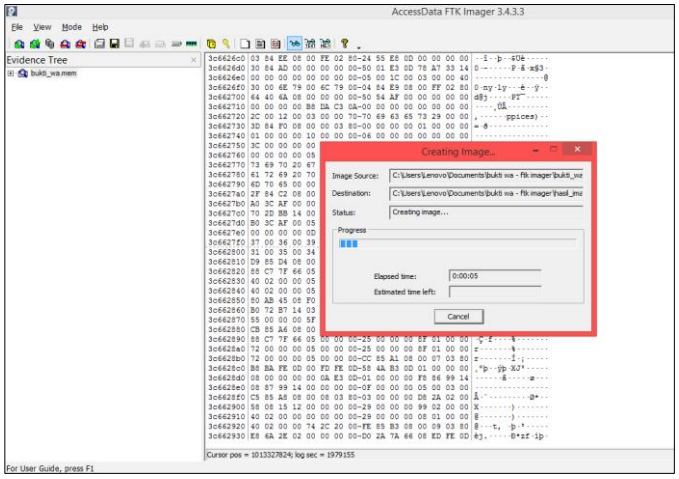


Gambar 5. Proses pengambilan data

Lamanya proses pengambilan bukti digital pada RAM tergantung besarnya kapasitas RAM. Semakin besar kapasitasnya maka semakin lama proses pengambilan bukti digitalnya, begitu juga sebaliknya. Hasil dari proses pengambilan bukti digital berupa file berekstensi .mem. Jenis file ini dapat dibuka dan dianalisis menggunakan *tools* yang mendukung ekstensi file tersebut, salah satunya adalah FTK Imager.

2) Penggandaan Bukti Digital *(Imaging)*

Proses *imaging* bertujuan untuk menghindari kerusakan pada barang bukti digital asli pada saat proses analisis dilakukan. Bukti digital dari proses *imaging* harus sama dengan bukti digital asli, karena sedikit perbedaan akan berdampak pada hasil analisis. Gambar 6 menunjukkan sebuah *screenshot* proses *imaging* bukti digital.



Gambar 6. Proses *imaging*

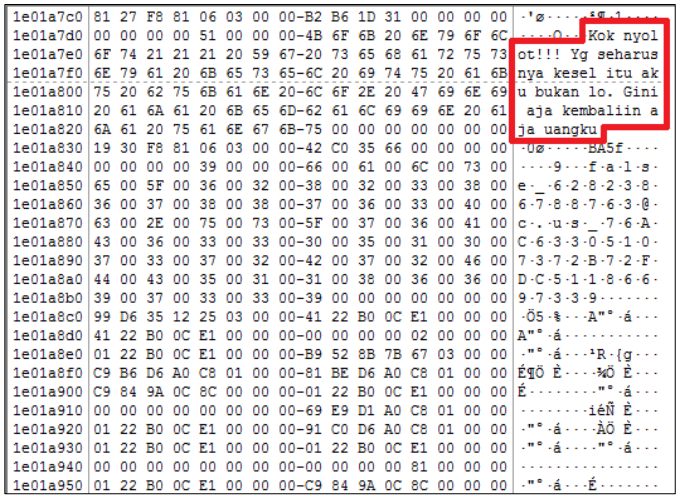
Proses analisis yang dilakukan pada tahap selanjutnya menggunakan bukti digital hasil *imaging*. Bukti digital yang asli atau bukti digital dari proses pengambilan bukti digital akan disimpan untuk mengantisipasi kesalahan saat proses analisis dilakukan.

C. Analisis

Pada tahap ini, dilakukan analisis dari hasil pengambilan data menggunakan *tools* FTK Imager.

1) Analisis Data Digital

Berdasarkan dari hasil pengambilan data RAM yang telah dilakukan, penyidik menemukan rekaman data percakapan yang terjadi pada WhatsApp. Data percakapan WhatsApp yang ditemukan berupa teks percakapan, seperti ditunjukkan pada Gambar 7. Gambar 7 menunjukkan salah satu data percakapan yang terjadi pada WhatsApp. Data percakapan yang didapat hanya memiliki satu tipe data. Tipe data tersebut hanya berupa teks percakapan, seperti ditunjukkan pada Tabel I.



Gambar 7. Data digital

TABEL I. STRUKTUR PERCAKAPAN

Tipe Data	Keterangan
Kok nyolot!!! Yg seharusnya kesel itu aku bukan lo. Gini aja kembaliin aja uangku	Isi percakapan

Tabel I menunjukkan tipe data yang didapat pada data percakapan WhatsApp. Pada data percakapan tersebut tidak ada nomor telepon pengirim, nomor telepon penerima, dan waktu percakapan, hanya berupa teks percakapan. Pada percakapan yang telah disimulasikan, terdapat 2 file gambar. Saat proses analisis dilakukan, satu file gambar hanya berupa nama file dan satu file gambar lainnya tidak ditemukan.

2) Analisis Bukti Digital

Pada bagian ini, analisis data digital telah selesai dilakukan. Berdasarkan hasil analisis data digital, teks percakapan yang telah ditemukan akan dibandingkan dengan teks percakapan WhatsApp yang ada pada *smartphone* korban, seperti ditunjukkan pada Tabel II. Tabel II menunjukkan hasil perbandingan percakapan WhatsApp yang terjadi pada laptop tersangka dengan *smartphone* korban. Berdasarkan hasil perbandingan tersebut dapat disimpulkan teks percakapannya sama, sehingga penyidik dapat menjadikan data percakapan tersebut sebagai bukti digital kasus penipuan *online shop*.

Penelitian ini berhasil mendapatkan bukti digital terkait kasus tindak kejahatan penipuan *online shop*. Bukti digital yang didapat berupa data percakapan WhatsApp antara tersangka dan korban. Data percakapan tersebut berupa teks percakapan. Tidak ada nomor telepon pengirim, nomor telepon penerima, dan waktu percakapan. Dua file gambar yang ada pada percakapan juga ditemukan tidak lengkap, satu file gambar hanya berupa nama file saja dan satu file gambar lainnya tidak ditemukan. Ketidaklengkapan bukti digital yang didapat kemungkinan disebabkan *tools* yang digunakan pada saat proses pengambilan dan analisis bukti digital. Kecocokan *tools live forensics* dengan aplikasi IM yang digunakan sangat mempengaruhi kelengkapan bukti digital yang didapat. Semakin lengkap bukti digital maka semakin cepat penyidik mengungkap kasus tindak kejahatan penipuan *online shop*.

Penelitian ini juga dapat dilakukan pada simulasi kasus kejahatan lainnya yang mendukung teknik *live forensics*. Kerumitan dalam mencari, mendapatkan, dan menganalisis bukti digital yang ada saat aplikasi sedang dijalankan pada laptop membutuhkan pengetahuan, kemampuan, dan pengalaman yang banyak. Hal ini juga sangat membutuhkan *tools* forensik yang mendukung untuk mendapatkan bukti digital yang berkualitas. Penelitian ini dapat menjadi langkah pertama untuk mengatasi kasus kejahatan yang rumit dan dapat membantu penelitian selanjutnya, khususnya pada lingkup forensik digital.

TABEL II. PERBANDINGAN PERCAKAPAN

Offset	Isi Percakapan	Kesimpulan
5998c190	File gambar: Screenshot_2018-03-28-09-51.PNG	Hanya nama filenya saja
0c006150	Masih ready gan?	Sama dan terbukti
39177f30	Ready gan, ukuran berapa gan?	Sama dan terbukti
4dcdfcc0	Ukuran 41 gan. Btw boleh tau detail sizenya gak?	Sama dan terbukti
70f2eb50	Ukuran 41 : panjang 26.5 cm	Sama dan terbukti
0632ca40	Harganya berapa ya gan?	Sama dan terbukti
1918e770	IDR : 140.000	Sama dan terbukti
1918ee30	Sip gan... langsungku order	Sama dan terbukti
24acb640	Nomor rekening : 5424-01-021098-53-6. A/n Muhamad Ermansyah Rauli	Sama dan terbukti
44e4d700	Kirimin alamat lengkapnya gan	Sama dan terbukti
463f75a0	Nama : Rauli Anugerah Pratama Alamat : Jln. Kusumanegara semaki gede RT 5 RW 16 No 16 Umbulharjo, Yogyakarta	Sama dan terbukti
-	File gambar : IMG-20180328-WA0001.JPEG	Tidak ditemukan
0a5446d0	Udahku transfer gan. Berapa hari paketnya nyampe gan?	Sama dan terbukti
22218960	2-3 hari gan. Ditunggu aja gan, terima kasih	Sama dan terbukti
2d77b2f0	Paketnya kok belum nyampe gan? Udah seminggu lho. Minta resinya dong	Sama dan terbukti
222b90d0	Udah aku kirim gan. Resinya hilang gan	Sama dan terbukti
23966cc0	Serius gan, ini udah seminggu. Masak hilang resinya, atau jangan2 kamu nipu aku	Sama dan terbukti
3fee31a0	Beneran gan udah aku kirim, gak percaya bgt sih	Sama dan terbukti
50befe80	Kok nyolot!!! Yang seharusnya kesel itu aku bukan lo. Gini aja kembaliin aja uangku	Sama dan terbukti
61924940	Enak aja lo	Sama dan terbukti
6dfbc3d0	Gue laporin polisi seriusan	Sama dan terbukti
6eed8910	Ya terserah	Sama dan terbukti

IV. PENUTUP

Teknik *live forensics* dapat diterapkan pada proses pengambilan bukti digital dari aplikasi IM WhatsApp berbasis *dekstop* pada sistem operasi windows 8 menggunakan *tools* forensik FTK Imager. Bukti digital yang diperoleh berupa teks percakapan WhatsApp yang terjadi antara tersangka dan korban yang dapat dijadikan bukti digital terkait kasus tindak kejahatan penipuan *online shop* yang terjadi.

Beberapa saran untuk penelitian selanjutnya adalah terdapat beberapa macam metode forensik digital, aplikasi IM berbasis dekstop, dan sistem operasi komputer yang bisa dikombinasikan menjadi topik penelitian yang kemungkinan besar mendukung teknik *live forensics* dan mendapatkan hasil penelitian yang berbeda dan lebih akurat. Penggunaan *tools live forensics* dalam proses pengambilan dan analisis bukti digital dapat juga dikombinasikan dengan *tools* lainnya, agar memperoleh bukti digital yang berkualitas sehingga dapat membantu para penyidik dalam mengungkap sebuah tindak kejahatan yang terjadi.

REFERENSI

[1] N. Anwar dan I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI)*, vol. 3, pp. 1–10, Juni 2017.

[2] S. Ikhsani dan B. C. Hidayanto, "Analisa Forensik Whatsapp dan LINE Messenger Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia," *Jurnal Teknik ITS*, vol. 5, pp. A728–A736, 2016.

[3] G. M. Zamroni, R. Umar, dan I. Riadi, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," *Jurnal Ilmu Komputer (ILKOM)*, vol. 2, pp. 102–105, Desember 2016.

[4] Statista (2017) Number of monthly active WhatsApp users worldwide from April 2013 to December 2017 (in millions)," *www.statista.com*, 2017. [Online]. Available: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/.

[5] H. K. Mann dan G. S. Chhabra, "Volatile Memory Forensics: A Legal Perspective," *Int. J. Comput. Appl.*, vol. 155, pp. 975–8887, 2016.

[6] D. S. Yudhistira, I. Riadi, dan Y. Prayudi, "Live Forensics Analysis Method For Random Access Memory On Laptop Devices," vol. 16, pp. 188–192, 2018.

[7] H. Bintoro, N. D. Cahyani, dan E. Ariyanto, "Analisis Kinerja Metode *Live Forensics* Untuk Investigasi *Random Access Memory* pada Sistem Operasi Microsoft Windows XP," Tugas Akhir, Universutas Telkom, Indonesia, 2012.

[8] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Evaluation of integrated digital forensics investigation framework for the investigation of smartphones using soft system methodology," *Int. J. Electr. Comput. Eng.*, vol. 7, pp. 2806–2817, 2017.

[9] I. Riadi, R. Umar, dan A. Firdonsyah, "Identification Of Digital Evidence On Android ' s," vol. 15, no. 5, pp. 3–8, 2017.

[10] M. N. Faiz, R. Umar, dan A. Yudhana, "Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary," *J. Ilm. Ilk.*, vol. 8, pp. 242–247, 2016.

[11] M. I. Mazdadi, I. Riadi, dan A. Luthfi, "Live Forensics on RouterOS using API Services to Investigate Network Attacks," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, pp. 406–410, 2017.

[12] T. Rochmadi, I. Riadi, dan Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," *Int. J. Comput. Apl.*, vol. 164, pp. 31–37, 2017.

[13] R. Umar, A. Yudhana, dan M. N. Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," *Prosiding Konferensi Nasional ke-4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM)* ISBN: 978-602-19568-1-6, pp 201-211, 2016.

[14] C. E. Suharyanto, "Analisis Komparatif Sistem Keamanan Windows 7 Dan Windows 8," *JIF (Jurnal Ilm. Inform.*, vol. 4, pp. 1–16, 2016.

[15] R. Kaur dan K. Amandeep, "Digital Forensics," *Int. J. Comput. Appl.*, vol. 50, pp. 5–9, 2012.