SMARTICS Journal, Vol.6 No.2 20xx. p62-69
ISSN online: 2476-9754, ISSN print: 2623-0429
DOI : https://doi.org/10.21067/smartics.v6i2.4703

Analisis Forensik Untuk Mendeteksi Pesan yang Disembunyikan pada *Short Message Service* Menggunakan Aplikasi Berlisensi *Open Source*

Ike Yunia Pasa[a], Dedy Hariyadi[b,*]
[a]Universitas Muhammdiyah Purworejo
[b]Universitas Jenderal Achmad Yani Yogyakarta
[*]correspondence email : dedy@unjaya.ac.id

Abstract*—Anti Forensic Techniques aim to complicate the process of investigating a crime. Hiding an SMS message with the aim or support of a crime can be categorized as an Anti Forensic technique. On smartphones with the MIUI operating system, it is equipped with features to block an SMS message and even hide an SMS message. The existence of a feature to hide SMS messages will complicate the investigation process if this feature uses to support crime. This research proposes a forensic analysis method to detect hidden SMS messages using open-source software. Differences in the process of retrieving digital evidence will affect the results of forensic analysis. So in this research to compare the results of the analysis of two digital forensic software to detect hidden messages.

Index Terms — MIUI, SMS, Digital Forensics, Anti Forensics, Open Source

Abstrak*—Teknik Anti Forensik bertujuan untuk menyulitkan proses investigasi suatu tindak kejahatan. Menyembunyikan suatu pesan SMS dengan tujuan atau mendukung tindak kejahatan dapat dikategorikan sebagai teknik Anti Forensik. Pada ponsel cerdas bersistem operasi MIUI telah dilengkapi fitur untuk memblok suatu pesan SMS bahkan menyembunyikan suatu pesan SMS. Adanya fitur menyembunyikan pesan SMS akan menyulitkan proses investigasi jika fitur tersebut digunakan untuk mendukung tindak kejahatan. Pada penelitian ini diusulkan metode analisis forensik untuk mendeteksi pesan SMS yang disembunyikan menggunakan perangkat lunak berlisensi Open Source. Perbedaan proses pengambilan barang bukti digital akan mempengaruhi hasil analisis forensik. Maka pada penelitian ini membandingkan hasil analisis dua perangkat lunak forensik digital untuk mendeteksi pesan tersembunyi.

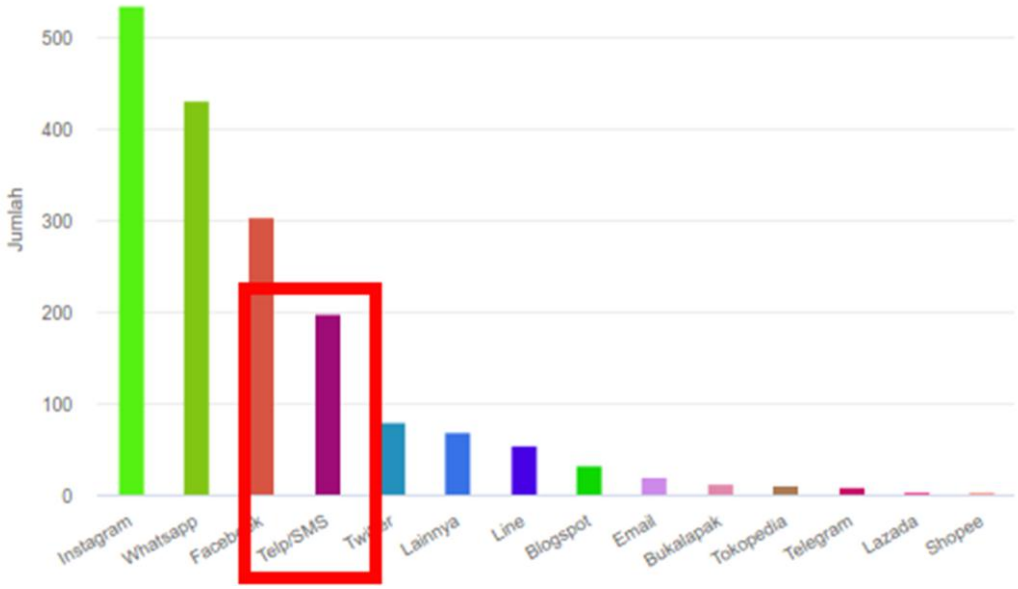
Kata Kunci — MIUI, SMS, Forensik Digital, Anti Forensik, Open Source

I. PENDAHULUAN

Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri pada tahun 2019 menerima laporan tindak kejahatan siber sebanyak 4.586 aduan. Dari 4.586 aduan yang melaporkan melalui portal patrolisiber.id sebanyak 1.443 aduan. *Short Message Service* (SMS) pernah menjadi layanan pesan yang populer, sehingga menjadi lahan bisnis yang menjanjikan [1]. Hal ini juga menjadi peluang kejahatan, berdasarkan aduan yang masuk berdasarkan platform, *Short Message Service* (SMS) atau telepon masih cukup tinggi sekitar 198 aduan seperti tampak pada Gambar 1.

SMS dapat dikategorikan sebagai dokumen elektronik menurut Undang-undang No. 19 Tahun 2016 tentang perubahan Undang-undang Informasi dan Transaksi Elektronik. Jika SMS dimanfaatkan pada tindak kejahatan maka dapat dijadikan sebagai alat bukti yang sah di pengadilan [2] [3]. Pada penelitian sebelumnya bahwa analisis barang bukti digital berupa SMS tidak hanya berbasiskan tangkapan layar atau hasil cetak pesan SMS [4]. Pesan SMS dapat dianalisis menggunakan algoritma *Machine Learning*. Analisis yang dilakukan oleh Zaid Romegar Mair dalam menganalisis SPAM pada SMS pengambilan barang bukti digital menggunakan perangkat lunak AFLogical OSE yang berlisensi Open Source [5].

Produsen ponsel cerdas dari Tiongkok, Xiaomi memiliki sistem operasi yang berbasis Android yang disebut MIUI [6]. Pada sistem operasi tersebut memiliki beberapa fitur yang tidak tersedia pada sistem operasi Android pada umumnya, yaitu *SMS Hide*. Fitur *SMS Hide* merupakan fitur dari MIUI yang berfungsi untuk menyembunyikan pesan SMS.



Gambar 1. Aduan pada Patrolisiber.id Berdasarkan Platform

Dalam menganalisis forensik suatu tindak kejahatan dengan barang bukti digital harus memperhatikan proses pengambilan barang bukti digital. Kementerian Perdagangan Amerika Serikat menerbitkan sebuah standar pengambilan barang bukti digital pada ponsel, yaitu NIST SP 800-101. Pada standar NIST SP 800-101 pengambilan barang bukti digital pada ponsel cerdas dapat menggunakan teknik *Logical Extraction*, yaitu teknik penyalinan berkas digital sebagai barang bukti digital yang memperhatikan integritas data [7]. Zaid Romegar Mair yang menggunakan AFLogical OSE juga mengimplementasikan *Logical Extraction* dalam proses pengambilan barang bukti [8]. Pada penelitian ini melakukan analisis *pre-process* teks yang terdapat pada SMS menggunakan aplikasi forensik digital berlisensi *Open Source* seperti AFLogical OSE dan Andriller untuk mendeteksi pesan yang tersembunyi. Sebelumnya Andriller berlisensi tertutup, saat ini telah mengubah lisensinya menjadi *Open Source*, yaitu *MIT License [9]*.

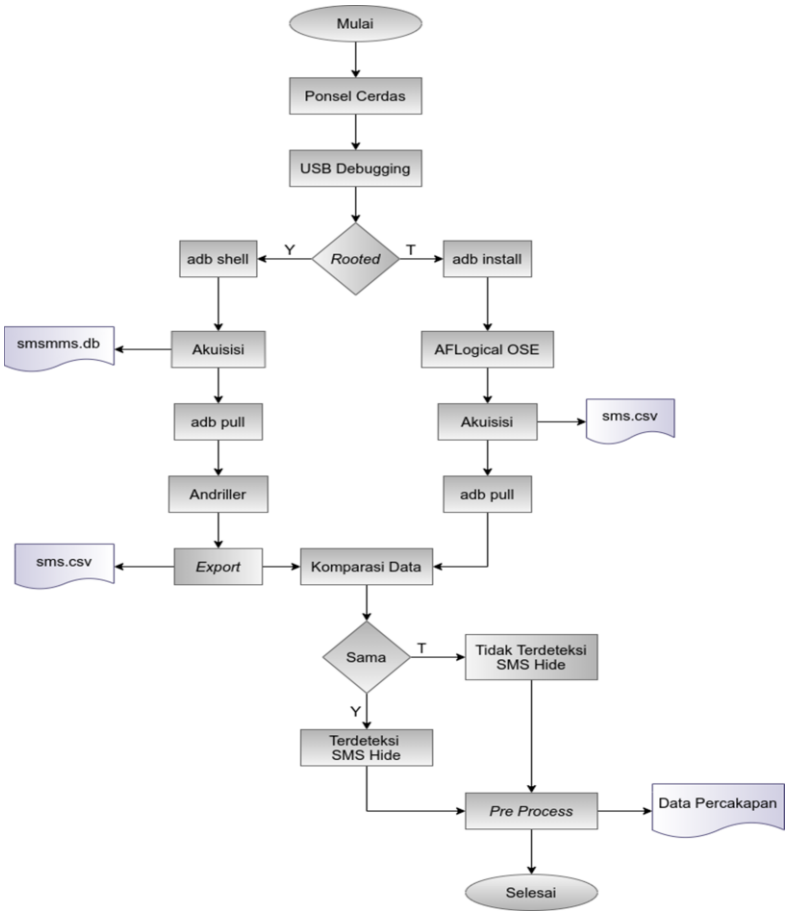
II. METODOLOGI PENELITIAN

Pada penelitian ini menggunakan standarisasi yang dikeluarkan oleh Kementerian Perdagangan Amerika Serikat yaitu NIST SP 800-101 tentang petunjuk analisis forensik digital pada perangkat gemerak (mobile devices). Pada NIST SP 800-101 terdapat prosedur teknik mengamankan barang bukti digital yang menjadi acuan Aparat Penegak Hukum atau pihak swasta. Adapun teknik yang digunakan untuk mengambil barang bukti digital diantaranya: *Manual Extraction, Logical Extraction, Hex Dumping/JTAG, Chip-Off*, dan *Micro Read* [7].

Pada teknik *logical extraction* ponsel cerdas harus memenuhi beberapa persyaratan diantaranya: ponsel dalam kondisi menyala, dan mode *USB Debugging* sudah aktif [10]. Perangkat lunak yang digunakan untuk mengamankan barang bukti digital memiliki lisensi *Open Source*. Adapun perangkat lunak yang digunakan adalah AFLogical OSE dan Andriller. Persamaan AFLogical OSE dan Andriller adalah memerlukan akses ke sistem konsol sistem operasi melalui *Android Debug Bridge* (ADB), sedangkan perbedaannya AFLogical OSE tidak memerlukan akses root hanya perlu menginstall aplikasi AFLogical OSE pada ponsel, Andriller memerlukan data dari hasil akses ke sistem konsol dan hak akses root. AFLogical OSE merupakan perangkat lunak yang digunakan pada proses pengamanan barang bukti digital berbasis agen [9].

Pada proses pengamanan barang bukti digital menggunakan AFLogical OSE menghasilkan barang bukti digital berupa SMS.csv. Sedangkan pada proses yang menggunakan perangkat lunak Andriller

terlebih dahulu terhubung ke ponsel cerdas menggunakan ADB untuk mengamankan barang bukti berupa mmssms.db [11]. Selanjutnya berkas mmssms.db diolah menggunakan Andriller yang menghasilkan luaran berupa berkas yang dapat disesuaikan dengan kebutuhan, misal berfomat CSV atau XLS untuk memudahkan pengolahan/analisis lebih lanjut. Adapun alur penelitian ini dapat dilihat pada
Gambar 2.



Gambar 2. Alur Penelitian

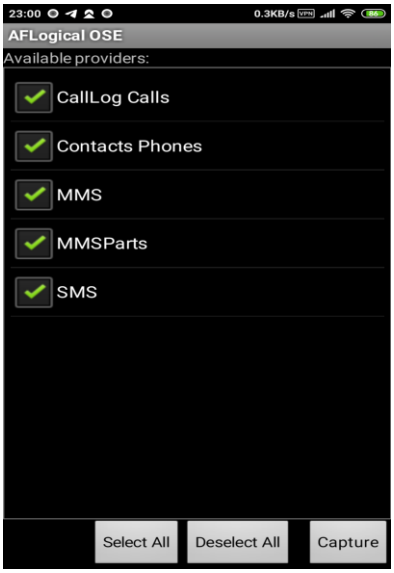
III. HASIL DAN PEMBAHASAN

Percobaan pada penelitian ini menggunakan ponsel cerdas dengan sistem operasi MIUI yang mendapatkan kiriman pesan SMS. Adapun pesan SMS yang diterima berisi teks *"Tes sms hidden"*. Sesuai dengan alur penelitian pada
Gambar 2 maka proses analisis terbagi menjadi 3 tahapan, yaitu: tahapan forensik menggunakan aplikasi AFLogical OSE, tahapan forensik menggunakan Andriller, dan komparasi data.

A. AFLogical OSE

Aplikasi AFLogical OSE merupakan aplikasi forensik berlisensi *Open Source* ini bertujuan untuk melakukan pengamanan barang bukti digital berupa *Call Logs*, *Contacts Phones*, MMS, dan SMS [12]. Aplikasi AFLogical OSE juga dapat digolongkan aplikasi forensik yang berbasis agen, jadi untuk menggunakannya harus melakukan pemasangan aplikasi pada ponsel cerdas [9]. Sebelum melakukan proses pemasangan aplikasi AFLogical OSE, ponsel cerdas sebaiknya dalam kondisi menyala, *mode USB Debugging* menyala, dan diizinkan melakukan pemasangan aplikasi melalui USB.

Setelah aplikasi AFLogical sudah terpasang maka menjalankan aplikasi tersebut melalui ponsel cerdas. Secara umum Gambar 3 menunjukan tampilan AFLogical OSE saat pertama kalinya. Pada penelitian ini yang dipilih hanya MMS, MMSParts, dan SMS. Berkas yang diamankan berupa SMS.csv yang tersimpan pada *internal memory* ponsel cerdas. Maka proses pengambilan barang bukti tersebut menggunakan ADB.



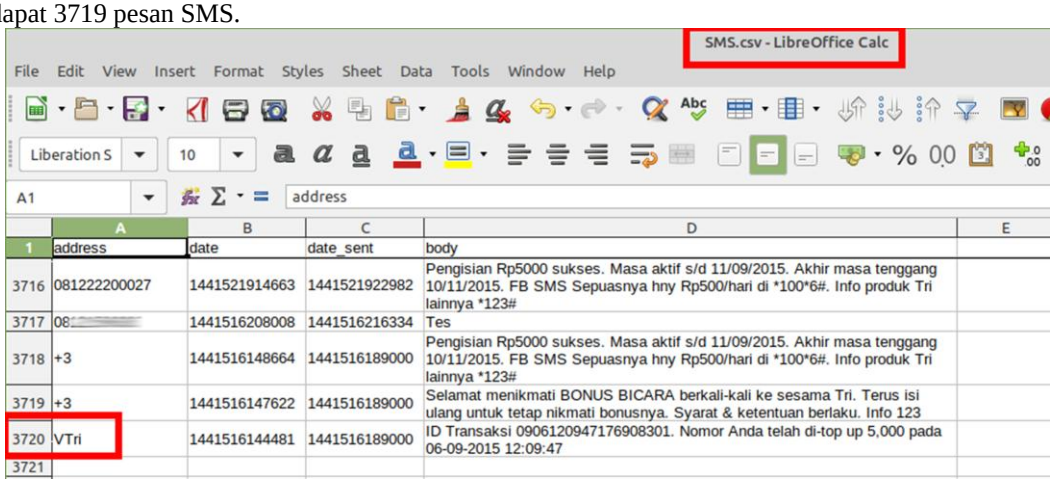
Gambar 3. Tampilan AFLogical OSE

Berkas SMS.csv yang berhasil diamankan atau diakuisisi memiliki nama kolom diantaranya, _id, thread_id, address, person, date, date_sent, protocol, read, status, type, reply_path_present, subject, body, service_center, locked, error_code, seen, timed, deleted, sync_state, marker, source, bind_id, mx_status, mx_id, mx_id_v2, out_time, account, sim_id, block_type, advanced_seen, b2c_ttl, b2c_numbers, fake_cell_type, url_risky_type, creator, dan favorite_date. Pada penelitian ini kolom yang digunakan adalah address, date, date_sent, dan body. Kolom *address* merupakan identitas pengirim pesan yang berupa nomor panjang, nomor pendek atau *masking*. Kolom *date* merupakan tanggal diterima pesan SMS. Kolom date_sent merupakan tanggal pengiriman pesan SMS, jika berisi 0 artinya pesan yang dikirim. Baik kolom *date* atau *date_sent* menggunakan format *unix timestamp*, maka perlu dikonversi menjadi *human date*. Kolom *body* merupakan isi pesan SMS. Tabel 1 merupakan cuplikan data yang berhasil diakuisisi menggunakan AFLogical OSE dan telah disesuaikan dengan kebutuhan.

TABEL 1. CUPLIKAN TABEL SMS.CSV

address	*date*	*date_sent*	*body*
LinkAja	1597713295360	1597713294000	Kode Verifikasi Anda adalah XXXX. RAHASIAKAN kode verifikasi Anda. Abaikan Jika Anda tidak meminta kode verifikasi ini.
LinkAja	1597712892687	1597712892000	Kode Verifikasi Anda adalah XXXX. RAHASIAKAN kode verifikasi Anda. Abaikan Jika Anda tidak meminta kode verifikasi ini.
LinkAja	1597712773843	1597712773000	Kode Verifikasi Anda adalah XXXX. RAHASIAKAN kode verifikasi Anda. Abaikan Jika Anda tidak meminta kode verifikasi ini.
+6285283283019	1597678782264	0	Kalah cepet!!! Sudah laku.
+6282311334870	1596957382063	0	Waduuuh ibu kemana.... Kami kangen.
+6285298971054	1596831593567	1596831593000	AYO GABUNG PROGRAM INVESTASI 600 GET 7jt 1jt GET 15jt 1,5jt GET 32jt 2jt GET 40jt 4jt GET 80jt 5jt GET 95jt Info klik : bit.ly/investasititipdana
3355	1596101103711	1596101103000	<DEBIT Rp. X.XXX,00 pada rek. 1 TB xxxxxx tgl. 30/07/2020,jam 16:26:57- Jika transaksi tidak Anda kenal,hub mandiri call 14000.

Berdasarkan proses pengamanan barang bukti digital menggunakan AFLogical OSE didapatkan pesan SMS sebanyak 3719. Hal ini terlihat pada Gambar 4 yang menunjukan baris terakhir dari berkas SMS.csv, yaitu 3720 baris termasuk nama kolom. Maka setelah jumlah baris dikurangi baris kolom maka terdapat 3719 pesan SMS.

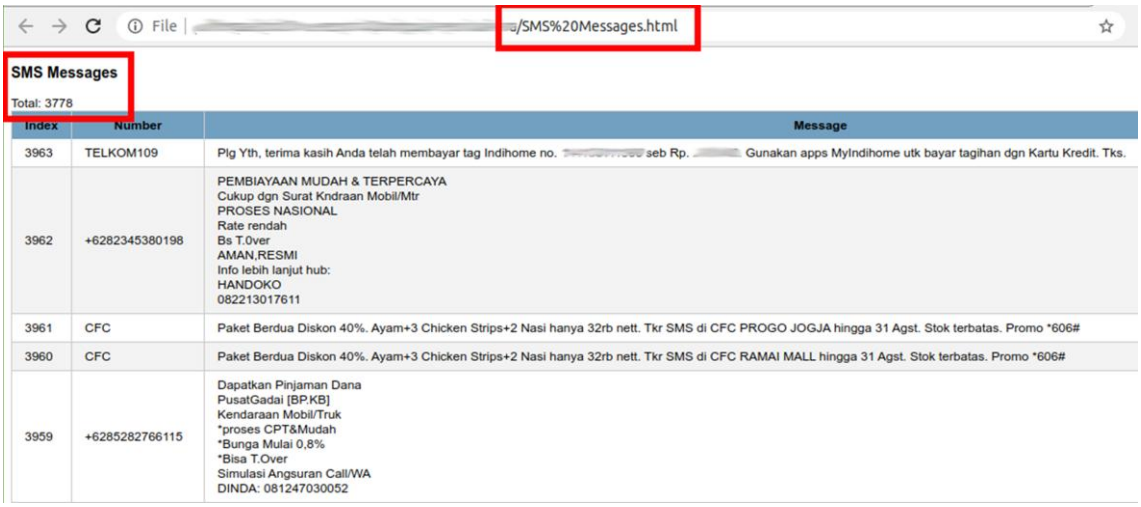


	A	B	C	D	E
1	address	date	date_sent	body	
3716	081222200027	1441521914663	1441521922982	Pengisian Rp5000 sukses. Masa aktif s/d 11/09/2015. Akhir masa tenggang 10/11/2015. FB SMS Sepuasnya hny Rp500/hari di *100*6#. Info produk Tri lainnya *123#	
3717	08[redacted]	1441516208008	1441516216334	Tes	
3718	+3	1441516148664	1441516189000	Pengisian Rp5000 sukses. Masa aktif s/d 11/09/2015. Akhir masa tenggang 10/11/2015. FB SMS Sepuasnya hny Rp500/hari di *100*6#. Info produk Tri lainnya *123#	
3719	+3	1441516147622	1441516189000	Selamat menikmati BONUS BICARA berkali-kali ke sesama Tri. Terus isi ulang untuk tetap nikmati bonusnya. Syarat & ketentuan berlaku. Info 123	
3720	VTri	1441516144481	1441516189000	ID Transaksi 0906120947176908301. Nomor Anda telah di-top up 5,000 pada 06-09-2015 12:09:47	
3721					

Gambar 4. Baris Terakhir Berkas SMS.csv

B. Andriller

Andriller merupakan aplikasi yang berfungsi untuk melakukan *decode* barang bukti digital dari ponsel cerdas awal mulanya berlisensi tertutup [13]. Namun, pada akhir tahun 2019 lisensi berganti menjadi lisensinya yang selaras dengan lisensi *Open Source* yang diunggah kodenya di Github. Pada penelitian ini Andriller digunakan untuk melakukan *decode* pesan SMS dari ponsel cerdas Android. Barang bukti yang di-*decode* oleh Andriller adalah berkas mmssms.db.



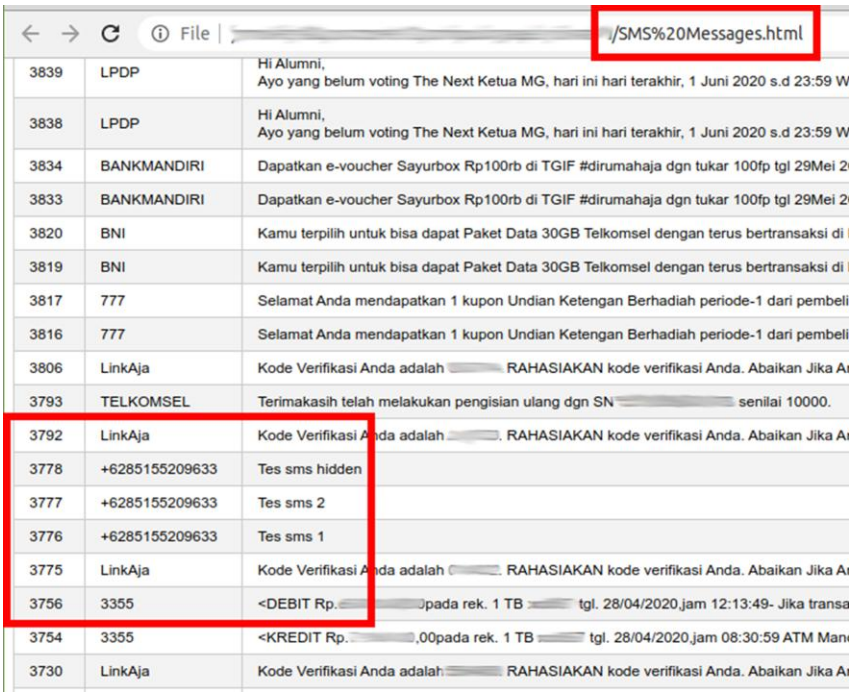
Index	Number	Message
3963	TELKOM109	Plg Yth, terima kasih Anda telah membayar tag Indihome no. [redacted] seb Rp. [redacted] Gunakan apps MyIndihome utk bayar tagihan dgn Kartu Kredit. Tks.
3962	+6282345380198	PEMBIAYAAN MUDAH & TERPERCAYA Cukup dgn Surat Kndraan Mobil/Mtr PROSES NASIONAL Rate rendah Bs T.0ver AMAN,RESMI Info lebih lanjut hub: HANDOKO 082213017611
3961	CFC	Paket Berdua Diskon 40%. Ayam+3 Chicken Strips+2 Nasi hanya 32rb nett. Tkr SMS di CFC PROGO JOGJA hingga 31 Agst. Stok terbatas. Promo *606#
3960	CFC	Paket Berdua Diskon 40%. Ayam+3 Chicken Strips+2 Nasi hanya 32rb nett. Tkr SMS di CFC RAMAI MALL hingga 31 Agst. Stok terbatas. Promo *606#
3959	+6285282766115	Dapatkan Pinjaman Dana PusatGadai [BP,KB] Kendaraan Mobil/Truk *proses CPT&Mudah *Bunga Mulai 0,8% *Bisa T.Over Simulasi Angsuran Call/WA DINDA: 081247030052

Gambar 5. Hasil *Decode* Andriller

Berkas mmssmsdb disalin ke komputer menggunakan ADB selanjutnya di-*decode* menggunakan Andriller. Hasil dari *decode* Andriller berupa berkas berformat HTML yang dibuka menggunakan peramban web seperti pada Gambar 5. Hasil *decode* menjadi sebuah laporan yang terdiri dari lima kolom, yaitu *Index, Number, Message, Time*, dan *Type*. Kolom *Index* merupakan nomor urut atau ID pesan SMS. Kolom *Number* merupakan identitas pengirim pesan yang berupa nomor panjang, nomor pendek atau *masking*. Kolom *Message* merupakan isi pesan SMS. Kolom *Time* merupakan waktu pengiriman atau menerima pesan SMS. Waktu telah menggunakan format *human date*. Kolom *Type* merupakan tipe pesan berupa *inbox* atau *sent*. Selanjutnya pesan SMS tersebut di-*export* ke berkas CSV seperti hasil *capture* dari AFLogical OSE. Berdasarkan Gambar 5 menunjukan bahwa pesan SMS hasil dari *decode* Andriller sebanyak 3778 pesan SMS baik pesan yang terkirim maupun pesan yang diterima.

C. Komparasi Data

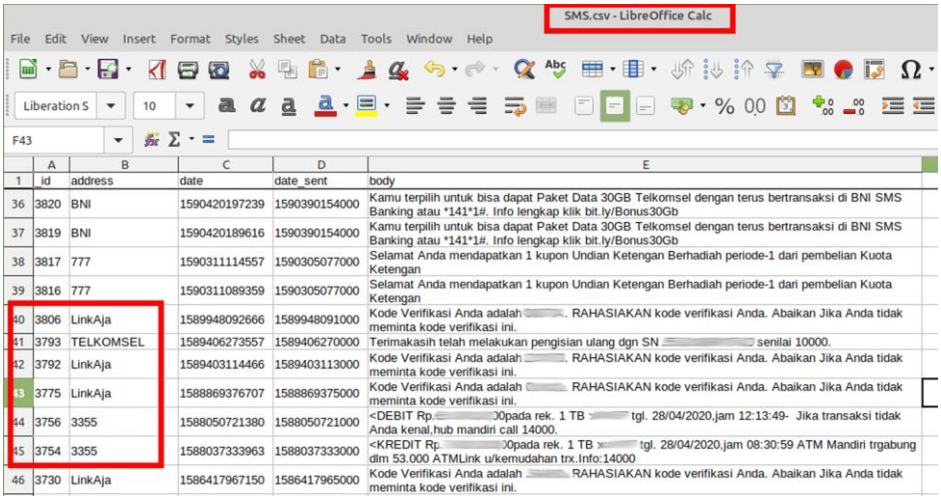
Baik AFLogical OSE dan Andriller hasil akhirnya berupa format CSV yang dapat diolah menggunakan aplikasi *Spreadsheet* seperti LibreOffice Calc atau MS Excel [14]. Kedua berkas CSV hasil dari *decode* AFLogical OSE dan Andriller dibandingkan jumlah baris yang ter-*decode*. Berdasarkan hasil perbandingan terdapat perbedaannya jumlah pesan SMS secara keseluruhan baik pesan terkirim dan pesan yang masuk seperti ditunjukan pada Gambar 4 dan Gambar 5. Menggunakan AFLogical OSE jumlah keseluruhan pesan SMS sejumlah 3719 pesan sedangkan Andriller sejumlah 3778. Terdapat selisih pesan SMS yang terkirim maupun diterima sejumlah 59 pesan SMS.



Gambar 6. Andriller: Penelusuran Pesan SMS

Perbedaan ini disebabkan oleh beberapa faktor diantaranya penerapan *SMS Blocker* dan *SMS Hide* yang merupakan fitur dari MIUI. Kedua fitur tersebut secara *default* tidak aktif, sehingga perlu diaktifkan oleh pengguna ponsel cerdas. Pada penelitian ini pengguna ponsel cerdas telah mengaktifkan fitur *SMS Blocker* dan *SMS Hide*. Khusus pada *SMS Hide* telah dilakukan ujicoba pengiriman pesan dengan isi, *"Tes sms hidden"*. Berdasarkan hal tersebut untuk melakukan komparasi data menggunakan teknik membandingkan jumlah pesan SMS yang masuk dan kata kunci dari pesan yang disembunyikan. Aplikasi yang digunakan untuk melakukan komparasi data bisa menggunakan aplikasi apa pun, pada penelitian ini menggunakannya aplikasi *Spreadsheet* yang lebih mudah melihat pesan per baris dalam bentuk tabel.

Pada Gambar 6 menunjukan terdapat pesan yang berisi *"Tes sms hidden"* dengan nomor urut pesan 3778. Selain itu nomor urut pesan juga terlihat urut dari 3775, 3776, 3777, 3778, dan seterusnya. Berbeda pada Gambar 7 terjadi lompatan nomor urut dari 3775 ke 3792. Hal ini menandakan adanya sebuah pesan yang dialihkan dengan cara diblok, disembunyikan atau dihapus.



	A	B	C	D	E
1	_id	address	date	date_sent	body
36	3820	BNI	1590420197239	1590390154000	Kamu terpilih untuk bisa dapat Paket Data 30GB Telkomsel dengan terus bertransaksi di BNI SMS Banking atau *141*1#. Info lengkap klik bit.ly/Bonus30Gb
37	3819	BNI	1590420189616	1590390154000	Kamu terpilih untuk bisa dapat Paket Data 30GB Telkomsel dengan terus bertransaksi di BNI SMS Banking atau *141*1#. Info lengkap klik bit.ly/Bonus30Gb
38	3817	777	1590311114557	1590305077000	Selamat Anda mendapatkan 1 kupon Undian Ketengan Berhadiah periode-1 dari pembelian Kuota Ketengan
39	3816	777	1590311089359	1590305077000	Selamat Anda mendapatkan 1 kupon Undian Ketengan Berhadiah periode-1 dari pembelian Kuota Ketengan
40	3806	LinkAja	1589948092666	1589948091000	Kode Verifikasi Anda adalah [redacted]. RAHASIAKAN kode verifikasi Anda. Abaikan Jika Anda tidak meminta kode verifikasi ini.
41	3793	TELKOMSEL	1589406273557	1589406270000	Terimakasih telah melakukan pengisian ulang dgn SN [redacted] senilai 10000.
42	3792	LinkAja	1589403114466	1589403113000	Kode Verifikasi Anda adalah [redacted]. RAHASIAKAN kode verifikasi Anda. Abaikan Jika Anda tidak meminta kode verifikasi ini.
43	3775	LinkAja	1588869376707	1588869375000	Kode Verifikasi Anda adalah [redacted] RAHASIAKAN kode verifikasi Anda. Abaikan Jika Anda tidak meminta kode verifikasi ini.
44	3756	3355	1588050721380	1588050721000	<DEBIT Rp.[redacted]0pada rek. 1 TB [redacted] tgl. 28/04/2020,jam 12:13:49- Jika transaksi tidak Anda kenal,hub mandiri call 14000.
45	3754	3355	1588037333963	1588037333000	<KREDIT Rp: [redacted]0pada rek. 1 TB [redacted] tgl. 28/04/2020,jam 08:30:59 ATM Mandiri trgabung dlm 53.000 ATMLink u/kemudahan trx.Info:14000
46	3730	LinkAja	1586417967150	1586417965000	Kode Verifikasi Anda adalah [redacted] RAHASIAKAN kode verifikasi Anda. Abaikan Jika Anda tidak meminta kode verifikasi ini.

Gambar 7. AFLogical OSE: Penelusuran Pesan SMS

IV. KESIMPULAN

Menurut peneliti dari The MITRE Corporation, anti forensik merupakan metode untuk menghalangi proses forensik sehingga menyulitkan analis forensik dalam menganalisis barang bukti elektronik dan/atau digital. Adapun usaha untuk melakukan anti forensik diantaranya, menghancurkan barang bukti, menyembunyikan barang bukti, merekayasa barang bukti, memalsukan barang bukti, dan mengelabui sistem deteksi perangkat forensik [15]. Sehubungan ada usaha untuk menyembunyikan suatu pesan SMS melalui fitur SMS Hide pada MIUI maka dapat dikategorikan melakukan teknik anti forensik jika pesan tersebut digunakan untuk tindak kejahatan.

Untuk mengantisipasi pengguna ponsel cerdas bersistem operasi Android dalam hal ini MIUI yang memanfaatkan fitur *SMS Blocker* dan *SMS Hide* sebaiknya dalam melakukan analisis percakapan pada barang bukti digital SMS menggunakan sumber dari berkas *mmssms.db*. Semua percakapan pada SMS tercatat pada barang bukti digital *mmssms.db*. Untuk menganalisis barang bukti digital pada ponsel cerdas berupa pesan SMS dapat menggunakan aplikasi berlisensi *Open Source* dalam hal ini AFLogical OSE, Andriller, dan LibreOffice Calc. Pada penelitian ini proses pengamanan barang bukti digital menggunakan metode *logical acquisition* yang masih memiliki kelemahan yaitu tidak dapat mendeteksi sebuah pesan SMS yang telah dihapus. Untuk melakukan penelitian lebih lanjut yang bertujuan mendeteksi pesan SMS yang terhapus dapat melakukan pengamanan barang bukti digital secara *physical acquisition*.

REFERENSI

[1] J. Brown, B. Shipman, dan R. Vetter, "SMS: The Short Message Service," *Computer*, vol. 40, no. 12, hal. 106–110, Des 2007.

[2] V. G. Larenda, M. Unik, dan H. Mukhtar, "Analisis SMS Forensik Smartphone sebagai Rujukan Menghadirkan Barang Bukti yang Sah di Pengadilan," 2016.

[3] S. Kurniawan, "Perancangan Prosedur Operasional Standar Penanganan Alat Bukti Digital: Studi Kasus Kementerian Komunikasi dan Informatika," Universitas Indonesia, 2014.

[4] F. G. Hikmatyar, "Analisis Forensik Digital pada Smartphone Android untuk Penanganan Kasus Cybercrime," Universitas Islam Negeri Sunan Kalijaga, 2017.

[5] Z. R. Mair, "Aplikasi untuk Identifikasi Short Message Service (SMS) SPAM Berbasis Android," Universitas Gadjah Mada, 2013.

[6] I. Y. Pasa dan D. Hariyadi, "Identifikasi Barang Bukti Percakapan Aplikasi Dual Apps Whatsapp Pada Ponsel Xiaomi Menggunakan Metode NIST Mobile Forensics," *J. INTEK Univ. Muhammadiyah Purworejo*, vol. 1, hal. 1–7, 2018, [Daring]. Tersedia pada: http://ejournal.umpwr.ac.id/index.php/intek/article/view/4815/4641.

[7] R. Ayers, S. Brothers, dan W. Jansen, "NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics," Gaithersburg, MD, Mei 2014. doi: http://dx.doi.org/10.6028/NIST.SP.800-101r1.

[8] Z. R. Mair dan A. Ashari, "Aplikasi untuk Identifikasi Short Message Service (SMS) Spam Berbasis Android," *Berk. MIPA*, vol. 24, no. 4, 2014.

[9] M. P. Aji, D. Hariyadi, dan T. Rochmadi, "Logical Acquisition in the Forensic Investigation Process of Android Smartphones based on Agent using Open Source Software," in *IOP Conference Series: Materials Science and Engineering*, Mar 2020, vol. 771, hal. 012024, doi: 10.1088/1757-899X/771/1/012024.

[10] D. Hariyadi dan A. A. Huda, "Laron: Aplikasi Akuisisi Berbasis SNI 27037:2014 pada Ponsel Android," *Indonesia Security Conference 2015*. Cirebon, hal. 1–10, 2015, doi: 10.13140/RG.2.1.3819.9520.

[11] M. Unik dan V. G. Larenda, "Analisis Investigasi Android Forensik Short Message Service (SMS) Pada Smartphone," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 3, no. 1, hal. 10, 2019, doi: 10.35145/joisie.v3i1.414.

[12] S. C. Sathe dan N. M. Dongre, "Data acquisition techniques in mobile forensics," 2018, doi: 10.1109/ICISC.2018.8399079.

[13] I. Riadi dan A. Firdonsyah, "Forensic Analysis of Android-based Instant Messaging Application," in *2018 12th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, Okt 2018, vol. 4, hal. 1–6, doi: 10.1109/TSSA.2018.8708798.

[14] D. Hariyadi dan E. T. Irawan, "Purwarupa Forensik BBM di Telepon Seluler Android Menggunakan IGN-SDK," *Indonesia Security Conference 2014*. Yogyakarta, hal. 2–8, 2014, doi: 10.13140/RG.2.1.2771.3764.

[15] J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," in *Digital Investigation*, 2013, vol. 10, no. SUPPL., doi: 10.1016/j.diin.2013.06.002.

Ike Yunia Pasa, Meraih gelar sarjana teknik (S.T) dari Universitas Ahmad Dahlan pada tahun 2006. Kemudian meraih gelar Master (M.Kom) dari Universitas Islam Indonesia pada tahun 2017. Saat ini Penulis menjadi dosen program studi Teknologi Informasi di Universitas Muhammadiyah Purworejo.

Dedy Hariyadi, Meraih gelar sarjana teknik (S.T) dari Universitas Pembangunan Nasional Veteran Yogyakarta pada tahun 2004. Kemudian meraih gelar Master (M.Kom) dari Universitas Islam Indonesia pada tahun 2016. Saat ini Penulis menjadi dosen program studi Teknologi Informasi di Universitas Jenderal Achmad Yani Yogyakarta.