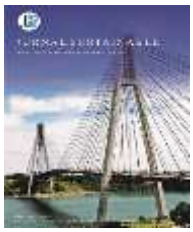


Jurnal Sustainable: Jurnal Hasil Penelitian dan Industri Terapan
Vol. 08, No. 01, hal. 38- 47, Mei 2019
Jurnal Sustainable: Jurnal Hasil Penelitian dan Industri Terapan
ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

Simulasi Analisis Bukti Digital Aplikasi Skype Berbasis Android menggunakan NIST SP 800-101 R1

Irfan Fathur Rohman[1], Nur Widiyasono[2], Rohmat Gunawan[3]
[1,2,3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Siliwangi
[1,2,3]Jl. Siliwangi No 24, Kota Tasikmalaya 46115
[*]Corresponding Author: irfanfr95@gmail.com

Abstract—The use of the Skype application continues to increase, potentially adding criminal activity based on instant messaging. Data security features in skype applications designed to protect user privacy, can be misused by perpetrators to hide digital evidence from criminal activity. This study aims to analyze the digital evidence of skype applications on android-based smartphones. The analysis process is carried out on digital evidence from 14 simulation scenarios using application features that have the potential to be misused into crime. Data acquisition techniques use the physical imaging method to get full smartphone memory access. Experimental results in the study show that, after scenario 1 - 9, digital evidence can still be found and equipped with supporting data stored in the Skype application database After scenario 10, blocked contact information is still found, and scenario 11 is still found digital evidence stored in the Skype application database. Scenario 12-13 is an activity that can eliminate digital evidence. Message history information and call history deleted on the Skype application have a small chance to be restored. While scenario 14, still leaves media files such as: videos, voice messages, pictures, archives *.PDF and message history and call history not found.

Keywords—android, forensic, mobile, skype

Intisari—Penggunaan aplikasi skype yang terus mengalami peningkatan, berpotensi menambah aktivitas kriminal berbasis *instant messaging*. Fitur keamanan data pada aplikasi skype yang dirancang untuk melindungi privasi pengguna, dapat disalahgunakan oleh pelaku untuk menyembunyikan bukti digital dari aktivitas kriminal. Penelitian ini bertujuan untuk melakukan analisis bukti digital aplikasi skype pada *smartphone* berbasis android. Proses analisis dilakukan pada bukti digital dari 14 skenario simulasi penggunaan fitur aplikasi yang berpotensi untuk disalahgunakan menjadi tindakan kriminal. Teknik akuisisi data menggunakan metode *physical imaging* untuk mendapatkan akses memori *smartphone* secara penuh. Hasil percobaan pada penelitian menunjukan bahwa, setelah dilakukan skenario 1 - 9, bukti digital masih dapat ditemukan dan dilengkapi dengan data-data pendukung yang tersimpan pada *database* aplikasi skype. Setelah dilakukan skenario 10, informasi kontak yang diblokir masih ditemukan, serta skenario 11 masih ditemukan bukti digital yang tersimpan pada *database* aplikasi Skype. Skenario 12-13 merupakan aktivitas yang dapat menghilangkan bukti digital. Informasi riwayat pesan dan riwayat panggilan yang dihapus pada aplikasi skype memiliki peluang yang kecil untuk dipulihkan. Sedangkan skenario 14, masih meninggalkan berkas media seperti: video, pesan suara, gambar, arsip *.PDF serta riwayat pesan dan riwayat panggilan tidak ditemukan.

Kata kunci— android, forensik, mobile, skype

I. PENDAHULUAN

Aplikasi Skype merupakan salah satu program untuk berkomunikasi dengan teknologi *Peer to Peer* (P2P) yang dapat digunakan untuk berkomunikasi berbasiskan internet [1]. Aplikasi skype dirancang dengan fitur keamanan data untuk melindungi privasi pengguna. Fitur Keamanan yang baik dapat memberikan dampak positif bagi pengguna, namun dapat disalahgunakan oleh orang yang tidak bertanggungjawab untuk menutupi aktivitasnya saat melakukan tindakan kriminal [2]. Aplikasi skype merupakan 1 dari 13 aplikasi instan messenger android populer di Indonesia [3].

Kejahatan digital yang dapat dilakukan dengan cara memanfaatkan aplikasi skype sebagai media komunikasi diantaranya: terorisme, pornografi, dan peredaran narkoba, disamping itu aplikasi skype juga dapat digunakan dengan memanfaatkan celah keamanan data pada aplikasi untuk melindungi pada saat melakukan aksi kriminal [4]. Salah satu cara untuk mendapatkan bukti dari suatu aktivitas kriminal berbasis teknologi komputer yaitu dengan forensik digital. Forensik digital merupakan bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum, kejahatan sehingga diperoleh bukti-bukti digital yang dapat menjerat pelaku kejahatan [5]. Proses forensik digital dilakukan untuk mencari bukti digital yang dapat diakui dan dijadikan bukti yang sah di ranah hukum.

Berbagai analisis forensik digital untuk menemukan bukti dari suatu aktivitas kriminal berbasis instant messaging pernah dilakukan dalam penelitian sebelumnya, diantaranya: analisi forensik digital pada aplikasi whatsapp [6], [7], [8], [9], analisis dan perbandingan bukti forensik facebook dan twitter pada smartphone android [10], analisis dan perbandingan bukti digital aplikasi instant messenger (whatsapp, telegram, line, imo) pada android [11], purwarupa forensik BBM di telepon seluler android menggunakan IGN-SDK [12].

Penelitian ini bertujuan untuk melakukan investigasi bukti digital melalui simulasi dari beberapa skenario yang mencakup pemakaian fitur aplikasi skype yang sering digunakan, serta skenario yang dapat menghilangkan bukti digital. Beberapa skenario mengacu kepada penelitian [11], serta ditambahkan skenario baru. Bukti digital dan perubahan yang disebabkan oleh aktivitas yang dilakukan pada skenario tersebut dianalisis dan ditampilkan ke dalam bentuk tabel. Proses analisis dilakukan untuk mengetahui karakteristik bukti digital dari aplikasi skype yang diteliti.

II. METODOLOGI

A. Pembuatan Skenario Untuk Simulasi

Skenario dibuat untuk merekontruksi aksi relevan yang mungkin dilakukan oleh pelaku tindakan kriminal dan digunakan untuk menyembunyikan jejak aktivitasnya. Pembuatan skenario dilakukan berdasarkan hasil analisis fungsionalitas aplikasi serta referensi terkait. Proses analisis fungsional merupakan proses pembuatan daftar fitur aplikasi yang memiliki potensi untuk digunakan sebagai alat bantu tindakan kriminal. Skenario mencakup fitur-fitur aplikasi *Skype* yang berpotensi digunakan untuk tindakan kriminal dan aksi yang bisa dilakukan pengguna untuk menyembunyikan jejak dari tindakan kriminal, yaitu:

1. Kirim dan terima pesan satu kontak.
2. Kirim dan terima pesan group.
3. Kirim nomor kontak.
4. Kirim dan terima pesan lokasi melalui *Google Maps*.
5. Mengirim pesan dengan fitur "*private chat"*.
6. Melakukan *voice call.*
7. Melakukan *video call*.
8. Kirim dan terima *file* dokumen.
9. Kirim dan terima pesan gambar, video, dan suara.
10. Blok kontak.
11. Hapus kontak.
12. Hapus riwayat pesan.
13. Hapus riwayat panggilan.
14. *Uninstall* aplikasi.

Skenario simulasi yang tela dibuat selanjutnya akan diterapkan pada aplikasi Skype yang telah disiapkan. Setelah setiap skenario dijalankan, akan diteliti fitur-fitur pada aplikasi yang terkait dengan skenario, sehingga diketahui bukti digital yang masih ditinggalkan dari penggunaan fitur tersebut serta

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

karakteristiknya. Beberapa dari skenario merupakan aktivitas yang dapat merubah dan menghilangkan bukti digital.

B. Implementasi Skenario Pada Aplikasi Skype

Tahap kedua dari penelitian ini adalah implementasi skenario yang telah disiapkan sebelumnya pada aplikasi Skype. Implementasi dilakukan untuk mengetahui teknis aktivitas yang terjadi berdasarkan skenario yang telah dirancang untuk menjalankan fitur-fitur pada aplikasi Skype, sehingga dapat diketahui bukti-bukti digital yang dapat ditemukan untuk dilakukan analisis selanjutnya.

C. Proses Forensik

Proses forensik dilakukan menggunakan metode *National Institute of Standard and Technology* (NIST) 800-101 R1 [13]. Tahapannya terdiri dari:

1) *Preservation:* merupakan proses mengamankan *smartphone* yang akan diinvestigasi supaya data tidak berubah.

2) *Collection*: proses akuisisi data yang dilakukan menggunakan metode *physical acquisition*. Langkah-langkah yang digunakan untuk akuisisi *physical image smartphone* diantaranya:

a) *Smartphone* sudah dalam keadaan *rooted* agar dapat menggunakan perintah DD (*Data Dump*).

b) Hubungkan *smartphone* dengan laptop menggunakan kabel USB dan pastikan *smartphone* telah mengizinkan USB *Debugging* seperti pada Gambar 1.

c) Buat *folder* untuk menyimpan **"adb.exe"** dan **"netcat.exe"** di laptop.

d) Simpan **"adb.exe"** dan **"netcat.exe"** ke dalam *folder* yang sudah dibuat.

e) *Download* dan *Install* aplikasi *Busybox* di *smartphone*.

f) Buka *command prompt* pada direktori yang terdapat **"adb.exe"**, lalu gunakan perintah **"adb –d shell"** untuk membuka *session* agar dapat berkomunikasi dengan *smartphone*.

Gambar 1. USB *Debugging*

g) Gunakan perintah **"su"** untuk mendapatkan hak akses *root* ke *smartphone* yang diinvestigasi.

h) Gunakan *data dump* untuk melakukan *imaging*, dengan perintah **"dd if=/dev/block/mmcblk0 | busybox nc –l –p 8888"**. Perintah tersebut untuk mengirim data dari partisi **"mmcblk0"** menggunakan *Netcat* yang terdapat di aplikasi *Busybox* dan sudah dilakukan instalasi di *smartphone* melalui *port* 8888.

i) Buka *command prompt* pada *folder* yang terdapat **nc.exe** dengan menggunakan perintah **"nc.exe 127.0.0.1 8888 > android.dd"**. Perintah tersebut dilakukan untuk menerima data yang masuk melalui **"port 8888"** via *Netcat* dan disimpan dengan nama **"android.dd".**

3) *Examination:* proses pemeriksaan terhadap *physical image smartphone* menggunakan aplikasi FTK Imager dan diberi *Hash Message Digest* 5 (MD5) untuk menjaga integritas data.

4) *Analysis:* Data bukti digital yang ditemukan pada tahap *examination* dianalisis untuk membuat kesimpulan dari bukti digital. *Databases* aplikasi skype yang relevan akan dibuka dan dianalisis menggunakan aplikasi *DB Browser for SQLite*.

5) *Reporting:* Investigator melaporkan hasil investigasi beserta bukti digital yang ditemukan. Pelaporan dalam penelitian meliputi penyajian artefak digital yang telah disimpulkan dari tahap analisis.

D. Spesifikasi software dan hardware yang digunakan

Spesifikasi *software* yang digunakan dalam percobaan pada penelitian ini ditampilkan pada Tabel 1.

Tabel 1. Spesifikasi software yang digunakan

Software	**Kegunaan**
Kingroot	Aplikasi untuk root *smartphone*
Skype versi 8.15.0.417	Aplikasi yang akan diinvestigasi
Android Debug Bridge (ADB)	Baris perintah untuk berkomunikasi dengan *smartphone Android*.
Netcat (NC)	Aplikasi yang menyediakan koneksi TCP untuk mengirimkan *physical image smartphone* ke laptop
Busybox	Utilitas yang menyediakan NC pada *smartphone*
Ftk Imager	Aplikasi untuk mengakses *file image smartphone* dan memberikan *hash* untuk menjaga integritas data
DB Browser Sqlite	Aplikasi untuk mengakses *databases*

Spesifikasi *hardware* yang digunakan dalam percobaan pada penelitian ini ditampilkan pada Tabel 2.

Tabel 2. Spesifikasi *hardware* yang digunakan

Hardware	**Kegunaan**
Laptop CQ42	Komputer untuk proses investigasi
Lenovo a2010	*Smartphone* yang diinvestigasi
Xiaomi Redmi 5 Plus	*Smartphone* untuk membantu proses skenario simulasi
Kabel USB	Penghubung laptop dan komputer pada tahap akuisisi data

III. HASIL DAN PEMBAHASAN

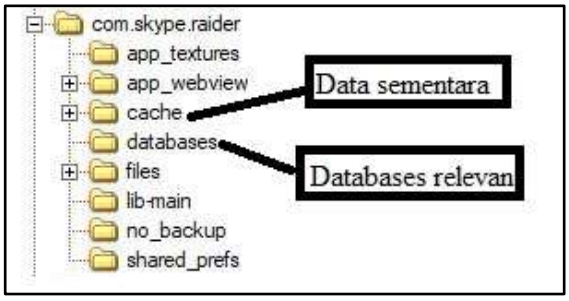
A. Analisis Aplikasi Skype

Aplikasi Skype menyimpan berbagai data yang digunakan ketika dijalankan. Data-data tersebut tersimpan dalam *folder* khusus seperti terlihat pada tabel 3.

Tabel 3. Lokasi bukti digital aplikasi Skype

Bukti Digital	**Lokasi**
Riwayat pesan	data/data/com.skype.raider/databases/ live:caf993801f8a35.db
Riwayat Panggilan	data/data/com.skype.raider/databases/ live:caf993801f8a35.db
Kontak	data/data/com.skype.raider/databases/ live:caf993801f8a35.db

Dari tabel 3 diketahui bahwa lokasi bukti digital aplikasi skype tersimpan di lokasi **`data/data/com.skype.raider/databases/.`** Selain folder **`databases`**, pada lokasi **`data/data/com.skype.raider/`** juga terdapat folder lainnya yang dapat digunakan untuk mencari data pada proses investigasi. Secara umum struktur direktori **`data/data/.com.skype.raider`** ditampilkan pada Gambar 2.



Gambar 2. Struktur direktori com.skype.raider

Direktori **`com.skype.raider`** hanya dapat ditemukan pada *smartphone* yang telah melalui proses *rooting*. Direktori ini meyimpan data yang digunakan oleh skype pada direktori *databases*. Skype memiliki satu *databases* relevan untuk proses investigasi yaitu **`live:caf993801f8a35.db`**. Skype menyimpan data sementara pada direktori *cache* yang mungkin bisa membantu pada proses investigasi.

B. Implementasi Hasil Skenario

Skenario 1: Skenario kirim dan terima pesan dengan teman satu kontak. Aktivitas ini dilakukan dengan mengrim pesan **"Kirim obat bius ke rumah yah"** yang dikirim oleh *user*

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

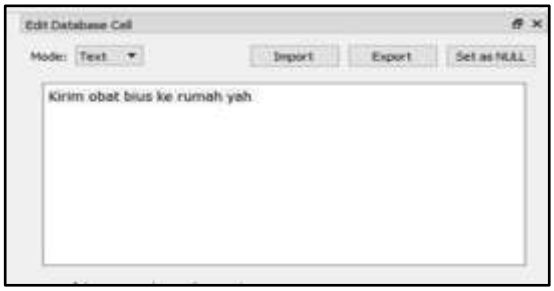
dengan nama "Yayah" seperti ditampilkan pada gambar 3.

Gambar 3. Tampilan pesan awal yang dikirim ke satu kontak

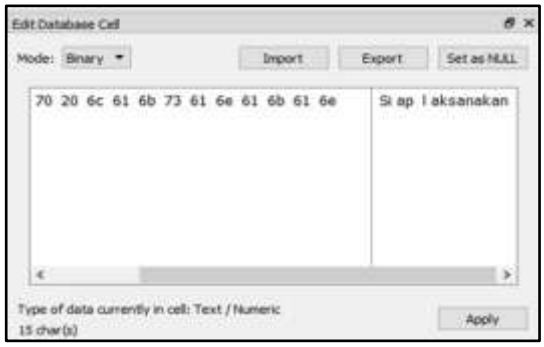
Setelah pesan diterima, kemudian dibalas oleh teman satu kontak yang isi pesannya **"Siap laksanakan"** ditampilkan pada gambar 4.

Gambar 4. Tampilan pesan balasan dalam satu kontak

Setelah skenario 1 dilakukan, kemudian *smartphone* yang terlibat pada saat skenario dihubungkan dengan laptop. DB Browser Sqlite digunakan untuk mengkases data yang tersimpan pada *database* aplikasi Skype. Bukti digital setelah skenario 1 dilakukan ditampilkan pada gambar 5 dan gambar 6.



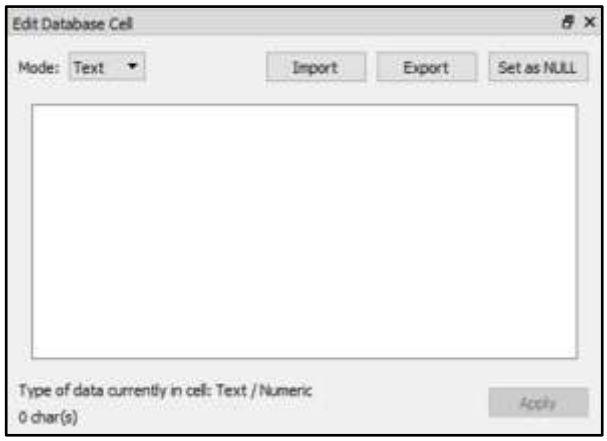
Gambar 5. Bukti digital pesan yang diterima dengan tipe data teks



Gambar 6. Bukti digital pesan yang diterima dengan tipe data *binary*

Gambar 5 dan gambar 6 menunjukan bahwa setelah dilakukan skenario 1, informasi pesan awal yang dikirim dan pesan balasan yang dilakukan terhadap satu kontak masih tersimpan dalam *database* dan dapat diakses.

Setelah skenario 1 dilakukan dan pencarian bukti digital hasil dari skenario tersebut dilakukan, tahap berikutnya dilakukan penghapusan terhadap pesan yang telah dikirimkan pada skenario 1. Hasil penghapusan pesan setelah skenario 1 dapat dilihat pada gambar 7.

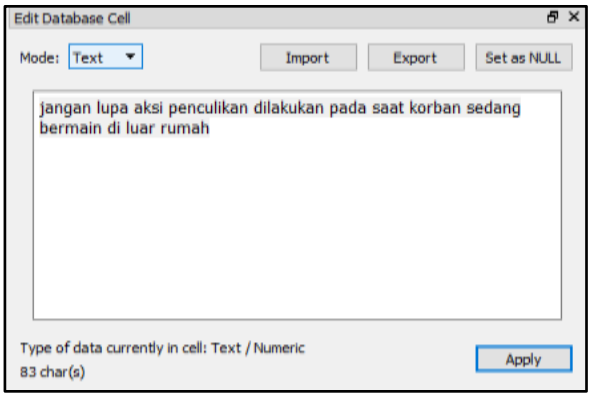


Gambar 7. Hasil penghapusan jejak digital skenario 1

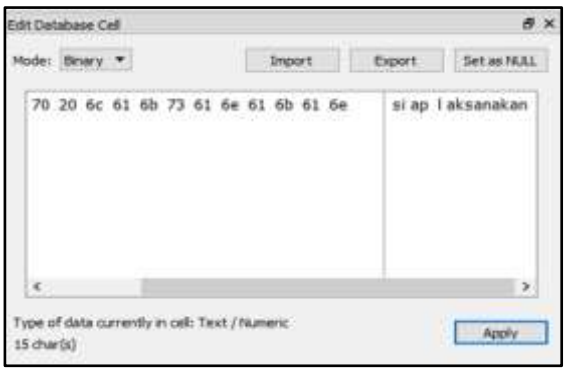
Gambar 7 menunjukan, bahwa setelah skenario 1 dikerjakan dan dilakukan penghapusan terhadap pesan yang dikirim, maka informasi jejak digital tidak dapat diakses lagi.

Selanjutnya aktivitas penghapusan jejak digital ini dilakukan setelah setiap skenario dikerjakan untuk memastikan bahwa tidak terdapat jejak digital dari skenario sebelumnya yang berpotensi mempengaruhi informasi jejak digital skenario berikutnya yang akan dijalankan.

Skenario 2: Mengirim dan menerima pesan dalam *group*. Skenario ini dilakukan pada salah satu *group* yang dibuat dalam aplikasi Skype dengan nama **"residivis"**. *Group* tersebut seolah-olah dibuat untuk mendukung rencana aksi penculikan. Sebuah pesan berisi **"Jangan lupa aksi penculikan dilakukan pada saat korban sedang bermain di luar rumah"** dikirim melalui *smartphone* yang diinvestigasi, lalu dibalas oleh anggota group lainnya dengan isi pesan **"Siap laksanakan"**. Bukti digital dari aktivitas tersebut dapat dilihat pada gambar 8 dan gambar 9.



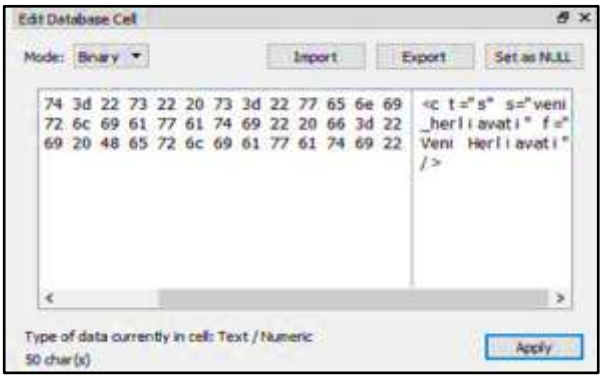
Gambar 8. Bukti digital kirim pesan kepada group



Gambar 9. Bukti digital pesan balasan anggota group

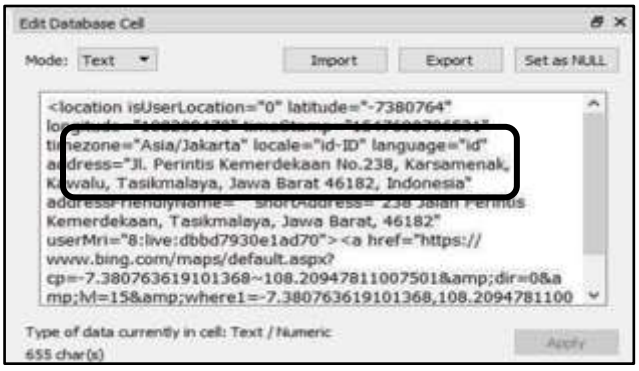
Gambar 8 dan gambar 9 menunjukan, bahwa setelah skenario 2 dilakukan, informasi pesan awal yang dikirim dan pesan balasan yang dilakukan dalam group tersebut masih tersimpan dalam *database* dan dapat diakses

Skenario 3: Mengirim nomor kontak. Aktivitas ini dilakukan dengan mengirim nomor kontak dengan nama **"Veni Herliawati"**. Setelah skenario ini dilakukan, data yang ditemukan dan dapat dipersepsi langsung hanya nama kontak yang dikirim melalui *smartphone* yang diinvestigasi. Bukti digital dapat dilihat pada Gambar 10.



Gambar 10. Bukti digital kirim kontak

Skenario 4: Mengirim dan menerima *geo-location.* Aktivitas ini dilakukan dengan cara mengirim peta lokasi (geo-location) yang diambil dari *Google Maps* dikirim melalui *smartphone* yang diinvestigasi. Bukti digital dapat dilihat pada Gambar 11 dan Gambar 12.



Gambar 11. Bukti digital kirim pesan lokasi

Dari gambar 11 dapat diketahui bahwa setelah skenario 4 dijalankan, masih meninggalkan bukti digital yang dapat diakses.

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

Gambar 12. Bukti digital pesan lokasi yang diterima

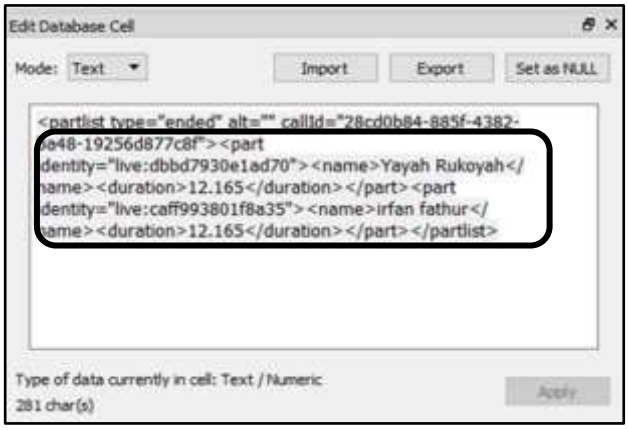
Gambar 12 menampilkan informasi jejak digital berupa identitas lokasi *geo-location* berupa teks alamat lokasi masih dapat diakses.

Skenario 5: Skenario mengirim pesan dengan fitur *private chat.* Aktivitas ini dilakukan dengan mengirim pesan **"Kirim obat bius ke rumah yah"** menggunakan fitur enkripsi *end-to-end* dari *smartphone* yang diinvestigasi. Bukti digital dari pesan yang dikirim dengan menggunakan fitur *private chat* dapat dilihat pada Gambar 13.

Gambar 13. Bukti digital pesan *private chat*

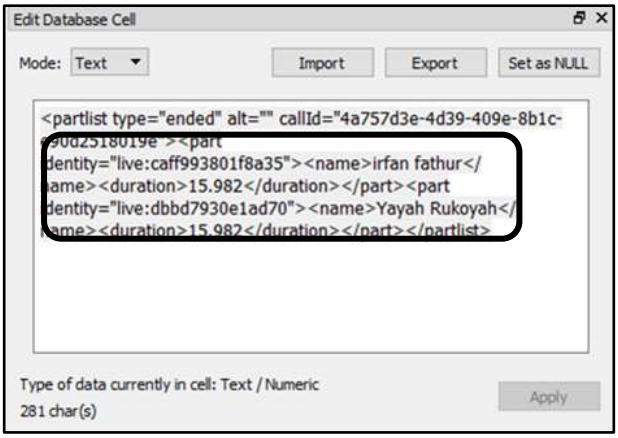
Gambar 13 menunjukan, bahwa setelah dilakukan skenario 5, informasi pesan yang dikirim dengan menggunakan fitur *private chat* masih tersimpan dalam *database* dan dapat diakses.

Skenario 6: Melakukan *Voice call.* Aktivitas ini dilakukan cara melakukan panggilan suara pada *smartphone* yang diinvestigasi. Setelah dilakukan skenario ini bukti digital yang masih tersimpan dan dapat diakses berupa *id*, nama, dan durasi waktu ketika *voice call* berlangsung. Bukti digital dari skenario 6 dapat dilihat pada Gambar 14.



Gambar 14. Bukti digital *voice call*

Skenario 7: Melakukan *Video call.* Aktivitas ini dilakukan cara melakukan *video call* pada *smartphone* yang diinvestigasi. Setelah dilakukan skenario ini bukti digital yang masih tersimpan dan dapat diakses berupa *id*, nama, dan durasi waktu ketika *video call* berlangsung. Bukti digital dari skenario 7 dapat dilihat pada Gambar 15.



Gambar 15. Bukti digital *video call*

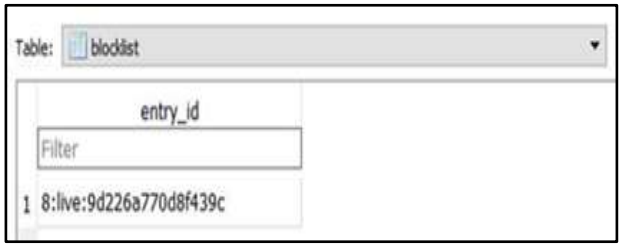
Skenario 8: Kirim dan terima *file* dokumen. Aktivitas ini dilakukan dengan mengirim berkas *.pdf. Setelah skenario 8 dikerjakan, langkah berikutnya melakukan investigasi pada *smartphone* pengirim dan penerima. Tampilan aplikasi Skype ketika proses pengiriman berkas *.pdf dapat dilihat pada gambar 16.

Gambar 16. Tampilan kirim berkas dokumen (*.pdf)

Pada gambar 16 terlihat arsip **pengesahan.pdf** dengan ukuran 28 KB dikirimkan menggunakan aplikasi skype oleh *user id* **"Yayah".** Jejak informasi digital dari berkas yang dikirim tersimpan pada direktori **"storage/emulated/0/Download".**

Skenario 9: Kirim dan terima pesan gambar, video dan suara. Setelah dilakukan skenario ini, semua berkas media yang diterima dan dikirimkan ditemukan pada direktori **"storage/emulated/0/Download".**

Skenario 10: Blok kontak. Skenario ini dilakukan dengan memblokir salah satu kontak yang ada. Kontak yang diblokir bernama **"Rian",** bukti digital dapat dilihat pada Gambar 17.

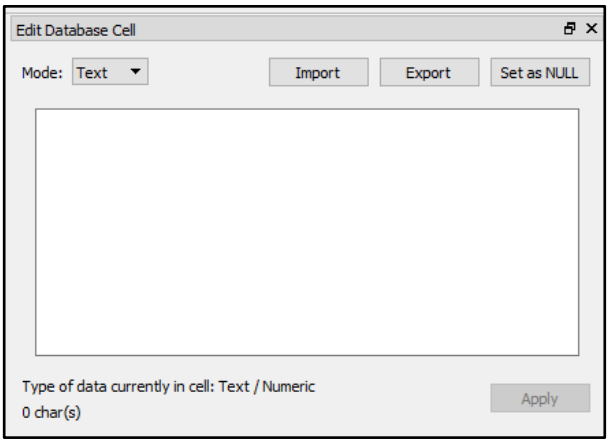


Gambar 17. Bukti digital blokir kontak

Skenario 11: Hapus kontak. Aktivitas pada skenario ini dilakukan dengan kontak dengan **"Gunawan Puji"**. Bukti digital setelah skenario ini dilakukan dapat dilihat pada Gambar 18.

Gambar 18. Bukti digital hapus kontak

Skenario 12: Hapus riwayat pesan. Skenario ini dilakukan dengan menghapus riwayat pesan yang telah dikirimkan. Hasil penghapusan riwayat pesan dapat dilihat pada gambar 19.



Gambar 19. Hasil Penghapusan Riwayat Pesan

Skenario 13: Hapus riwayat panggilan. Skenario ini dilakukan dengan menghapus riwayat panggilan yang telah dilakukan. Hasil penghapusan riwayat panggilan ditampilkan pada gambar 20.

ISSN 2615-6334 (Online)
ISSN 2087-5347 (Print)

Gambar 20. Hasil Penghapusan Riwayat Panggilan

Pada gambar 20 ditampilkan, bahwa setelah skenario 13 dilakukan, data riwayat panggilan tidak ditemukan di *database*.

Tabel 7. Hasil investigasi bukti digital pada Skype

No.	Aplikasi skype		
	Skenario	**Bukti digital ditemukan**	**Bukti digital tidak ditemukan**
1.	Kirim dan terima pesan satu kontak	✓	-
2.	Kirim dan terima pesan group	✓	-
3.	Kirim nomor kontak	✓	-
4.	Kirim dan terima pesan lokasi	✓	-
5.	Menggunakan fitur private chat	✓	-
6.	Melakukan *voice call*	✓	-
7.	Melakukan *video call*	✓	-
8.	Kirim dan terima file document.pdf	✓	-
9.	Kirim dan terima pesan gambar, video, dan suara	✓	-
10.	Block kontak	✓	-
11.	Hapus kontak	✓	-
12.	Hapus histori pesan	-	✓
13.	Hapus histori panggilan	-	✓
14.	*Uninstal* aplikasi	-	✓

Skenario 14: *Uninstall* aplikasi. Skenario ini dilakukan dengan cara *uninstall* aplikasi Skype. Aktivitas ini menghapus aplikasi Skype sehingga tidak dapat digunakan lagi. Setelah skenario ini dilakukan, informasi digital yang ditinggalkan berupa data berkas media seperti: video, pesan suara, gambar dan berkas *.pdf. Sedangkan riwayat pesan dan riwayat panggilan tidak ditemukan.

Hasil investigasi bukti digital pada Skype ditunjukkan pada Tabel 7.

IV. KESIMPULAN

Hasil percobaan pada penelitian menunjukan bahwa, setelah dilakukan skenario 1-9, bukti digital masih dapat ditemukan dan dilengkapi dengan data-data pendukung yang tersimpan pada *database* aplikasi Skype. Setelah dilakukan skenario 10, informasi kontak yang diblokir masih ditemukan, serta skenario 11 (hapus kontak) masih ditemukan bukti digital yang terdapat pada *database* aplikasi Skype.

Skenario 12-13 merupakan aktivitas yang dapat menghilangkan bukti digital. Informasi riwayat pesan dan riwayat panggilan yang dihapus pada aplikasi Skype memiliki peluang yang kecil untuk dapat dipulihkan. Sedangkan skenario 14, setelah dilakukan masih meninggalkan berkas media seperti video, pesan suara, gambar, arsip *.pdf serta riwayat pesan dan riwayat panggilan tidak ditemukan.

REFERENSI

[1] R. J. Daswani, Neil, "An Experimental Study of the Skype Peer-to-Peer VoIP System," 2015.

[2] Tahiri, *Mastering Mobile Forensics*. Birmingham: Packet Publishing, 2016.

[3] A. Mushanif, "Top 13 Apalikasi Chat Terbaik Yang Banyak Digunakan," *Yatekno*, 2017. .

[4] M. Dargahi, Tooska; Dehghantanhab, Ali; Contic, "Forensics Analysis of Android Mobile VoIP Apps," no. 1–24, 2017.

[5] M. N. Al-Azhar, *Digital Forensic : Panduan Praktis Investigasi Komputer*. Jakarta: SalembaInfotek, 2012.

[6] I. Y. Pasa and 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, no. November, pp. 1–7, 2018.

[7] Y. N. Kunang and A. Khristian, "Implementation of forensic procedures for whatsapp applications on android phones," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 59–68, 2016.

[8] 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, 2018.

[9] I. Riadi and E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *Sci. J. Informatics UNNES*, vol. 10, no. 1, pp. 18–22, 2018.

[10] 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.

[11] M. S. Asyaky, "Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android," vol. 3, no. October, 2019.

[12] D. Hariyadi and E. T. Irawan, "Purwarupa Forensik BBM di Telepon Seluler Android Menggunakan IGN-SDK," *Indones. Secur. Conf. 2014*, no. November, pp. 2–8, 2014.

[13] W. J. Ayers Rick, Sam Brother, "Guidelines on Mobile Device (NIST Special Publication 800-101 Revision 1)," http://dx.doi.org/10.6028/NIST.SP. 800-101r, 2014.