TUGAS AKHIR – KS 141501

ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN APLIKASI INSTANT *MESSENGER* (LINE, FACEBOOK, DAN TELEGRAM) PADA SISTEM OPERASI WINDOWS 10.

LIVE FORENSICS ANALYSIS FOR COMPARING INSTANT *MESSENGER APPLICATIONS (LINE, FACEBOOK, AND TELEGRAM) ON WINDOWS 10 OPERATING SYSTEM.*

TAYOMI DWI LARASATI
NRP 5213 100 099

Dosen Pembimbing
Bekti Cahyo Hidayanto, S.Si., M.Kom.

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

TUGAS AKHIR – KS141501

ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN APLIKASI INSTANT *MESSENGER* (LINE, FACEBOOK, DAN TELEGRAM) PADA SISTEM OPERASI

Tayomi Dwi Larasati
5213 100 099

Dosen Pembimbing
Bekti Cahyo Hidayanto, S.Si., M.Kom.

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

TUGAS AKHIR – KS141501

LIVE FORENSICS ANALYSIS FOR COMPARING INSTANT *MESSENGER APPLICATIONS (LINE, FACEBOOK, AND TELEGRAM) ON WINDOWS 10 OPERATING SYSTEM.*

Tayomi Dwi Larasati
5213 100 099

Supervisor
Bekti Cahyo Hidayanto, S.Si., M.Kom.

INFORMATION SYSTEMS DEPARTMENT
Faculty of Information Technology
Institut Teknologi Sepuluh Nopember
Surabaya 2017

LEMBAR PENGESAHAN

ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN APLIKASI INSTANT *MESSENGER* (LINE, FACEBOOK, DAN TELEGRAM) PADA SISTEM OPERASI WINDOWS 10.

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

Tayomi Dwi Larasati
5213 100 099

Surabaya, Juli 2017

KEPALA
DEPARTEMEN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M.Kom.
NIP 196503101991021001

LEMBAR PERSETUJUAN

ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN APLIKASI INSTANT *MESSENGER* (LINE, FACEBOOK, DAN TELEGRAM) PADA SISTEM OPERASI WINDOWS 10.

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

Tayomi Dwi Larasati
5213 100 099

Disetujui Tim Penguji: Tanggal Ujian: 17 Juli 2017
Periode Wisuda: September 2017

Bekti Cahyo Hidayanto, S.Si., M.Kom. **(Pembimbing I)**

Dr. Ir. Aris Tjahyanto, M.Kom., PhD. **(Penguji I)**

Faizal Mahananto, S.Kom, M.Eng., PhD. **(Penguji II)**

ANALISIS *LIVE FORENSICS* UNTUK PERBANDINGAN APLIKASI INSTANT *MESSENGER* (LINE, FACEBOOK, DAN TELEGRAM) PADA SISTEM OPERASI WINDOWS 10.

Nama Mahasiswa : Tayomi Dwi Larasati
NRP : 5213100099
Departemen : Sistem Informasi FTIF-ITS
Pembimbing 1 : Bekti Cahyo Hidayanto, S.Si., M.Kom.

ABSTRAK

Salah satu teknik dalam digital forensik, yaitu *live forensics* yang digunakan untuk menangani kejahatan komputer dan mendapatkan bukti-bukti yang ditinggalkan pada RAM. Tingkat keamanan suatu aplikasi dapat dianalisa menggunakan *live forensics*. Pada penggunaan teknik live forensic, diperlukan dumping atau menggandakan data yang ada untuk dipindahkan dan dianalisa nantinya. Analisa dilakukan untuk aplikasi Instant *Messenger* seperti Line *Messenger*, Facebook *Messenger* dan Telegram *Messenger* yang beroperasi pada platform sistem operasi windows 10.

Dalam penelitian ini dilakukan pengujian skenario dan eksperimen yang sering terjadi pada kasus kejahatan yang melibatkan aplikasi instant *messenger* seperti penggunaan percakapan biasa hingga penghapusan pesan atau percakapan. Data yang dihasilkan dari skenario dan pengujian ini nantinya akan diproses mnggunakan aplikasi forensika digital untuk dianalisa dan diteliti. Tools dumpIt dan Belkasoft RamCapturer yang digunakan untuk pengambilan data digital, Tools winhex dan Belkasoft Evidence Center yang digunakan untuk menganalisa data digital.

Hasil penelitian yang dilakukan yaitu Aplikasi Instant *Messenger* seperti LINE *Messenger*, Facebook *Messenger* dan

Telegram *Messenger* memiliki karakteristik masing-masing sehingga data yang didapatkan juga berbeda bergantung bagaimana struktur data yang disusun pada aplikasi.

Perbandingan data aplikasi yang dinilai dari data primer percakapan dan media yang dianalisa menggunakan 2 tools yaitu winhex dan belkasoft menghasilkan aplikasi Facebook Messenger sebesar 76% dan 5%, aplikasi LINE messenger sebesar 100% dan 10% dan aplikasi Telegram Messenger sebesar 0% dan 0%.

Dengan jumlah object yang dilakukan pada saat pelaksanaan skenario dan eksperimen, persentase jumlah object yang dikirim dengan jumlah object yang terdeteksi menggunakan tools winhex dan Belkasoft pada Facebook Messenger sebesar 60,95% dan 6,67%, untuk LINE Messenger sebesar 100% dan 33,33%. Dan untuk aplikasi Telegram Messenger sebesar 0% dan 0%.

Kata kunci : *Live forensics*, *Line Messenger*, *Facebook Messenger*, *Telegram Messenger*.

LIVE FORENSICS ANALYSIS FOR COMPARING INSTANT *MESSENGER APPLICATIONS (LINE, FACEBOOK, AND TELEGRAM) ON WINDOWS 10 OPERATING SYSTEM.*

Student Name : Tayomi Dwi Larasati
NRP : 5213100099
Department : Sistem Informasi FTIF-ITS
First Supervisor : Bekti Cahyo Hidayanto, S.Si., M.Kom.

ABSTRACT

One technique in digital forensics, namely live forensics is used to handle with computer crimes and obtain evidence left on the RAM. An application's security level can be analyzed using live forensics. On the use of live forensic techniques, required dumping or duplicate existing data to be transferred and analyzed later. Analyze are performed for Instant Messenger applications such as Line Messenger, Facebook Messenger and Telegram Messenger operating on Windows operating system platform 10.

In this research, scenario testing and experiments is often conducted in cases of crime involving instant messenger applications such as the use of ordinary conversation to deleting messages or conversations. The data generated from these scenarios and tests will be processed using digital forensics applications to be analyzed and researched. The dumpIt and Belkasoft RamCapturer tools used for digital data retrieval, the Winhex Tools and the Belkasoft Evidence Center are used to analyze digital data.

The results of the research are Instant Messenger Applications such as LINE Messenger, Facebook Messenger and Telegram Messenger have their own characteristics so that the data obtained also to differ depending on how the data structures are arranged in the application.

Comparison of the data application is assessed from the primary data conversations and media were analyzed using 2 tools that WinHex and belkasoft produce Messenger Facebook application by 76% and 5%, the applications LINE messenger by 100% and 10% and the application Telegram Messenger of 0% and 0% .

With the number of objects performed during the scenario and experiment implementation, the percentage of the number of objects sent with the number of objects detected using winhex and Belkasoft tools on Facebook Messenger of 60.95% and 6.67%, for LINE Messenger apps of 100% and 33, 33%. And for Telegram Messenger apps of 0% and 0%.

Keywords: *Live forensics, Line Messenger, Facebook Messenger, Telegram Messenger.*

KATA PENGANTAR

Syukur Alhamdulillah terucap atas segala petunjuk, pertolongan, rahmat dan kekuatan yang diberikan oleh Allah SWT kepada penulis sehingga dapat menyelesaikan buku tugas akhir dengan judul:

ANALISIS *LIVE FORENSICS* UNTUK PERBANDINGAN APLIKASI INSTANT *MESSENGER* (LINE, FACEBOOK, DAN TELEGRAM) PADA SISTEM OPERASI WINDOWS 10.

Pada kesempatan ini, penulis ingin menyampaikan terima kasih kepada semua pihak yang telah memberikan dukungan, bimbingan, arahan, bantuan, dan semangat dalam menyelesaikan tugas akhir ini, yaitu:

- Orang tua dan keluarga yang senantiasa mendoakan dan memberikan semangat dan menjadi sumber motivasi, dan orang-orang tercinta yang selalu mendorong untuk menyelesaikan tugas akhir tepat waktu.
- Bapak Bekti Cahyo Hidayanto, S.Si., M.Kom. selaku dosen pembimbing yang yang telah meluangkan waktu untuk membimbing, mengarahkan dan mendukung dalam penyelesaian tugas akhir.
- Ibu Mahendrawati E. R S.T., M.SC., PH.D selaku dosen wali yang senantiasa memberikan pengarahan selama penulis menempuh masa perkuliahan dan pengerjaan tugas akhir.
- Untuk teman-teman Lab IKTI, BELTRANIS, dan teman-teman lain yang telah memberikan waktu untuk berdiskusi dan saling memberikan semangat dalam menyelesaikan tugas akhir.

Penyusunan tugas akhir ini masih jauh dari sempurna, untuk itu penulis menerima kritik dan saran yang membangun untuk perbaikan di masa mendatang. Semoga tugas akhir ini dapat

menjadi salah satu acuan bagi penelitian-penelitian yang serupa dan bermanfaat bagi pembaca.

Surabaya, 21 Juni 2017

Penulis

DAFTAR ISI

“Halaman ini sengaja dikosongkan”

DAFTAR GAMBAR

“Halaman ini sengaja dikosongkan”

DAFTAR TABEL

BAB I
PENDAHULUAN

Pada bab ini, akan dijelaskan mengenai latar belakang masalah, perumusan masalah, batasan masalah, tujuan tugas akhir, dan manfaat tugas akhir, serta relevansi penelitian tugas akhir dengan bidang keilmuan Sistem Informasi.

1.1 Latar Belakang

Kejahatan dunia maya setiap tahunnya mengalami peningkatan yang sangat pesat [1] [2], hal ini dikarenakan semakin berkembangnya teknologi komputer yang berdampak pada kehidupan manusia. Banyak orang yang memanfaatkan teknologi komputer sebagai media untuk melakukan tindak kejahatan yang bertentangan dengan hukum. Salah satu tindak kejahatan yang marak terjadi adalah penggunaan data seseorang oleh pihak lain yang tidak bertanggung jawab. Hal ini dikarenakan masih banyaknya cara untuk mendapatkan data orang lain dengan mudah, salah satu caranya adalah dengan memanfaatkan data yang tertinggal dari aktifitas penggunaan sebuah aplikasi pada random access memory (RAM).

Pada aktifitas penggunaan sebuah aplikasi pasti terdapat data dan informasi yang terdapat pada random access memory (RAM). Random Access Memory merupakan suatu memori tempat penyimpanan data sementara, ketika saat komputer dijalankan dan dapat diakses secara acak (random) [3]. Karena itu terdapat suatu teknik untuk mendapatkan data dan informasi yang ditinggalkan agar dapat menjadi sebuah bukti digital. Untuk mendapatkan bukti digital tersebut maka perlu dilakukan sebuah teknik dari digital forensik.

Digital forensik adalah ilmu yang mempelajari tentang bagaimana cara untuk menangani berbagai kejahatan yang melibatkan teknologi komputer [4]. Ada

beberapa teknik didalam digital forensik salah satunya adalah *live forensics* yang digunakan untuk menangani kejahatan komputer yang menggunakan pendekatan terhadap sistem komputer yang sedang bekerja dan terhubung pada jaringan komputer. Tools yang biasanya digunakan untuk *live forensics* memiliki berbagai jenis, bisa berupa case, hex dan editor. Tools yang digunakan juga memiliki kelebihan dan kekurangannya masing-masing dikarenakan mengikuti bagaimana kasus yang terjadi, Tools yang free/trial dan tools yang berbayar sama-sama tidak dapat menjamin persentase keberhasilan untuk mendapatkan bukti digital [5].

Pada era ini, terdapat banyak aplikasi yang digunakan, terutama aplikasi chatting atau yang sering disebut dengan instant *messenger*. Aplikasi instant *messenger* (IM) merupakan aplikasi yang sering digunakan oleh user komputer [5]. menurut wearesocial.com pada bulan januari 2016 jumlah penduduk dunia mencapai 7.395 juta jiwa. 2.307 juta atau sekitar 31% diantaranya adalah pengguna active sosial media [6]. jumlah ini meningkat 10% dari tahun sebelumnya tahun 2015, dan diprediksi akan meningkat terus setiap tahunnya. Masih dengan sumber yang sama [5], jumlah pengguna sosial media berbasis *messenger* terbesar di indonesia adalah bbm sebesar 19%, whatsapp *messenger* 14%, facebook *messenger* 13%, LINE *messenger* 12%, dan wechat 8%.

Untuk menjalankan sebuah computer dibutuhkan sebuah system operasi. Sistem Operasi yang popular saat ini adalah sytem operasi windows yang digunakan oleh 87% dari seluruh penggunaan system operasi [7]. Windows 10 merupakan windows versi terbaru dari system operasi windows dan merupakan system operasi dengan pengguna terbanyak kedua setelah windows 7 dan kemungkinan akan menyaingi windows 7 karena mengingat usia windows 7 yang sudah cukup berumur.

Dengan adanya permasalahan yang telah dijabarkan sebelumnya, penulis berinisiatif untuk melakukan penelitian mengenai tingkat keamanan dari aktifitas penggunaan instant *messenger* (IM) pada sistem operasi windows 10 menggunakan metode *live forensics* yang nantinya akan dijadikan bukti digital.

1.2. Perumusan Masalah

Permasalahan yang dihadapi dalam penelitian ini adalah sebagai berikut:

1. Apa saja karakteristik bukti digital yang didapat dari aktivitas penggunaan aplikasi Instant *Messenger* (Facebook, LINE dan Telegram)?
2. Bagaimana cara mengimplementasikan teknik live forensics dari aktivitas penggunaan aplikasi Instant *Messenger* (Facebook, LINE dan Telegram)?
3. Bagaimana perbandingan bukti digital yang didapatkan oleh ke-3 aplikasi instant *messenger* tersebut?
4. Implikasi apa yang akan terjadi dari hasil live forensics pada masing-masing aplikasi Instant *Messenger* (LINE, Facebook dan Telegram) dilihat dari faktor keamanan pada sisi examiner dan pelaku kejahatan?

1.3. Batasan Masalah

Batasan pemasalahan dalam tugas akhir ini adalah:

1. Penelitian implementasi live forensics dilakukan pada sebuah komputer personal yang memiliki sistem operasi windows 10 yang terhubung dengan jaringan internet.
2. Aplikasi Instant *messenger* yang digunakan adalah versi terbaru desktop yaitu :
   - LINE *Messenger* : versi 5.1.1.1422
   - Facebook *Messenger* : versi v2.1.4623
   - Telegram *Messenger* : versi 1.1.7

3. Penelitian menggunakan skenario percakapan dan eksperimen penggunaan aplikasi. Skenario percakapan disesuaikan dengan percakapan yang biasa terjadi pada kondisi kejahatan. Untuk eksperimen penggunaan aplikasi menitikberatkan pada penggunaan aplikasi seperti penggunaan biasa dan penghapusan pesan dan/atau percakapan.
4. Karakteristik yang dimaksud pada penelitian ini adalah bukti digital apa saja yang didapatkan dari aktifitas penggunaan aplikasi LINE *Messenger*, Facebook *Messenger* dan Telegram *Messenger*.
5. Pada penelitian ini menggunakan tools yang tidak berbayar yaitu DumpIt dan Belkasoft RamCapturer untuk pengambilan data digital, Winhex dan Belkasoft Evidence Center untuk analisa data digital.

1.4. Tujuan

Tujuan dari pengerjaan tugas akhir ini adalah:

1. Mengimplementasikan teknik live forensics untuk menginvestigasi bukti digital dari aktivitas penggunaan aplikasi LINE *Messenger*, Facebook *Messenger* dan Telegram *Messenger*.
2. Mengetahui karakteristik bukti digital dari aktivitas penggunaan aplikasi LINE *Messenger*, Facebook *Messenger* dan Telegram *Messenger*.
3. Mengetahui perbandingan bukti digital yang didapatkan dari ke-3 aplikasi instant *messenger* tersebut.

1.5. Manfaat

Manfaat yang diberikan dengan adanya tugas akhir ini adalah sebagai berikut:

1. Memberikan gambaran untuk mengimplementasikan teknik live forensics dalam menginvestigasi bukti

digital dari aktivitas penggunaan aplikasi LINE *Messenger*, Facebook *Messenger* dan Telegram *Messenger*.

2. Memberikan informasi tentang tingkat keamanan pada penggunaan aplikasi LINE *Messenger*, Facebook *Messenger* dan Telegram *Messenger*
3. Menjadi referensi untuk kalangan akademisi dalam pengembangan penelitian terkait forensika digital di Indonesia

1.6. Relevansi

Hasil dari penelitian tugas akhir ini difokuskan terhadap pengembangan data yang ada pada aplikasi instant *messenger*. Penelitian ini mengambil cakupan mata kuliah Sistem Operasi, Keamanan Aset dan Informasi dan mata kuliah Forensika Digital. Selain itu, penelitian tugas akhir ini juga termasuk dalam topik yang ada pada Laboratorium Infrastruktur dan Keamanan Teknologi Informasi di Departemen Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember, Surabaya.

“Halaman ini sengaja dikosongkan”

BAB II
TINJAUAN PUSTAKA

Sebelum melakukan penelitian tugas akhir, penulis melakukan tinjauan pustaka terhadap tulisan dari beberapa penelitian sebelumnya yang sesuai dengan tema yang diambil. Dan dibawah ini merupakan rincian hasil yang didapatkan :

2.1. Studi Sebelumnya

Pada tabel 2.1 merupakan daftar penelitian yang telah dilakukan sebelummya terkait Forensika Digital di bidang aplikasi instant *messenger*:

Tabel 2.1 Daftar Penelitian Sebelumnya

No	Judul Penelitian	Metode Yang digunakan	Kesimpulan
1.	Live Digital Forensics: Windows XP vs Windows 7. (Fenu Gianni, 2013) [8]	Penggunaan metode *live forensics* untuk perbandingan keamanan antara windows xp dan windows 7 menggunakan studi kasus skype, google talk dan internet explorer.	Hasil dari penelitian ini adalah tidak menemukan perbedaan yang signifikan antara keamanan windows xp dan windows 7 menggunakan metode *live forensics*, akan tetapi terdapat hasil bahwa penggunaan web browser Internet Explorer untuk Facebook pada windows XP tidak memiliki keamanan yang cukup dikarenakan

No	Judul Penelitian	Metode Yang digunakan	Kesimpulan
			username dan password dapat terlihat tanpa di enkripsi terlebih dahulu, berbeda dengan windows 7 yang tidak dapat menampilkan informasi yang diujikan sebelumnya.
2.	Analisis kinerja metode *live forensics* untuk investigasi random access memory pada sistem proprietary. (Rusydi Umar, 2014) [9]	Penelitian menggunakan metode *live forensics* pada sistem operasi proprietary untuk menganalisa data volatile pada sistem yang berjalan pada RAM agar dapat mengetahui log aktivitas dari pengguna.	Hasil dari penelitian ini dilakukan untuk dapat merekomendasikan tools yang sesuai dengan kasus dan berjalan pada sistem operasi proprietary, dengan adanya pertimbangan kinerja dari tools akan dihitung akurasi, waktu, penggunaan memori serta jumlah langkahnya dan merekomendasikan kepada investigator tools yang sesuai dengan kasus yang terjadi.

No	Judul Penelitian	Metode Yang digunakan	Kesimpulan
3.	Analisis *live forensics* untuk perbandingan kemananan email pada sistem operasi proprietary. (Muhammad Nur Faiz, 2016) [7]	Menganalisa perbandingan keamanan email (gmail, yahoo dan outlook pada beberapa browser (google chrome, mozilla Firefox dan Microsoft Edge pada penggunaan sistem operasi windows 10 menggunakan teknik *live forensics*.	Hasil yang didapatkan dari analisa menggunakan WinHex pada akun email yang telah ditentukan yaitu Gmail sebagai penyedia email no 2 di dunia saat ini sangatlah dibutuhkan keamanan yang tinggi dan jika dibandingkan dengan Outlook dan Yahoo, gmail merupakan email terbaik saat ini dengan dukungan keamanan yang tinggi pada mode browser private.
4.	Teknik *Live forensics* Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi	Penggunaan metode *live forensics* untuk mengetahui karakteristik dan bukti digital pada aktivitas zeus malware, penelitian ini	Hasil yang didapatkan pada penelitian ini yaitu adanya data artefak dari aktifitas zeus malware yang dapat dijadikan acuan dalam pembuatan kerangka investigasi untuk mendukung

No	Judul Penelitian	Metode Yang digunakan	Kesimpulan
	Malware Forensics. (Aan Kurniawan, 2014) [10]	digunakan untuk menganalisa image memory dengan memanfaatkan jaringan komputer sebagai media pengiriman data.	malware forensics. Adanya tools volatility yang digunakan untuk penelitian ini digunakan untuk menganalisa image memory dan bukan tools yang digunakan untuk menganalisa zeus malware.
5.	Security Analysis Testing For Secure Instant Messaging In Android With Study Case: Telegram (Chandra. Kurniawan & Rhee, 2016) [11]	Menganalisa *instant messaging appications vulnerabilities*: Telegram dengan 3 metode tes yaitu *static analysis, dynamic analysis* dan *inspection of safe operation* pada resiko yang didefinisikan sebagai V1-V7 yaitu server, *developer*, ISP, *government*,	Hasil yang didapatkan dari analisis penilitian ini yaitu melalui *dynamic analysis,* menunjukkan telegram menyediakan proteksi data-on-transit yang aman untuk percakapan di layer *network* tapi kurang sekuritasnya pada penyimpanan data lokal dan *cache*. Potensi vulnerabilitas juga dapat ditemukan pada penerapan beberapa kriptografi yang

No	Judul Penelitian	Metode Yang digunakan	Kesimpulan
		adversary, *cryptanalysis* dan *attacker*.	kurang bagus pada enkripsi pesan dan mekanisme dekripsi dengan menampilkan analisis statistic pada *source code* Telegram.
6.	Digital Forensic Analysis of Telegram *Messenger* on Android Devices. (Satrya, daely & Nugroho, 2016) [12]	Menganalisa data pada Telegram sehingga bisa dijadikan bukti dalam penyelidikan *cybercrime* dengan menunjukkan nama *file*, lokasi dan isi. Penelitian ini menggunakan 5 skenario *post-mortem investigation* yaitu aplikasi dan aktivitas *user*, informasi dari kontak, informasi ertukaran pesan, *sharing*, dan *deleted*	Hasil yang didapatkan dari penelitian ini adalah berdasarkan dari *post-mortem* 5 skenario yang dilakukan pada Telegram 3.4.2 di system operasi android menunjukkan bahwa telegram dapat digunakan untuk bukti digital pada kasus *cybercrime*. Paada beberapa scenario juga menunjukkan interpretasi dari adanya database kontak dan pesan, baik teks maupun multimedia.

No	Judul Penelitian	Metode Yang digunakan	Kesimpulan
		communicatio n.	
7	Analisa Forensik Whatsapp dan LINE *Messenger* pada Smartphone Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia. (Syukur Ikhsani, 2016) [13]	Forensika digital yang dilakukan pada mobile forensics pada aplikasi Whatsapp *Messenger* dan Line *Messenger* untuk mendapatkan bukti digital yang akan menjadi barang bukti yang kuat dan valid di Indonesia melalui beberapa skenario dan eksperimen yang telah ditentukan.	Hasil yang didapatkan dari penelitian ini yaitu melalui forensika digital atau mobile forensics dari skenario dan eksperimen yang dijalankan menunjukkan bahwa didapatkan data utama berupa database berisikan kontak dan percakapan dan artefak file penyusun aplikasi dan data pendukung aplikasi berupa database cadangan dan file-file terkait media seperti gambar, video, dan suara. Dan aplikasi WhatsApp menjadi rujukan dalam forensika digital di Indonesia, sedangkan untuk LINE *Messenger* menjadi aplikasi

No	Judul Penelitian	Metode Yang digunakan	Kesimpulan
			yang lebih aman karena sulit untuk dilakukan proses analisa forensika digital

Dari beberapa studi yang dipelajari pada Tabel 2.1 sebelumnya, maka penulis memutuskan untuk melakukan pengembangan dan modifikasi penelitian pada tugas akhir ini dari studi ke tiga dari Muhammad Nur Faiz yang berjudul "Analisis *live forensics* untuk perbandingan kemananan email pada sistem operasi propriatery". Pengembangan dilakukan dengan menggunakan objek aplikasi Instant *Messenger* yaitu LINE *Messenger*, Facebook *Messenger* dan Telegram *Messenger* untuk dapat dianalisa dan diperbandingkan. Modifikasi dilakukan dengan mengubah objek penelitian dan menggunakan aplikasi yang berbeda dari studi tersebut.

2.2. Dasar Teori

Bagian ini akan menjelaskan mengenai konsep atau teori yang berkaitan dengan tugas akhir.

2.2.1. Forensika Digital

Forensika digital atau forensika komputer adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi, nirkabel dan perangkat penyimpanan sedemikian.

Sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum [4]. Di dalam perkembangannya ilmu forensika digital sudah mengalami perkembangan, karena ilmu ini termasuk

baru dalam bidang teknologi informasi. Oleh karena termasuk kedalam ilmu baru, belum banyak ahli forensika digital yang ada di Indonesia.

Dengan adanya perkembangan teknologi yang semakin pesat, maka semakin banyak pula penyalahgunaannya. Penyalahgunaan ini yang saat ini sering terseret kedalam meja hijau karena adanya Undang-Undang No 11 Tahun 2008 mengenai Transaksi Elektronik. Ketika sudah masuk kedalam meja hijau, maka bukti digital/bukti elektronik tidak dapat terhindarkan. Hal tersebut memaksa lembaga atau badan hukum untuk menggunakan jasa-jasa dari orang ahli komputer umum atau ahli komputer dengan spesialisasi pada bidang tertentu seperti *programming, networking, security*, *hacking, web develompment* atau bidang ilmu lain yang berkaitan dengan forensika digital/forensika komputer. Namun mereka tidak memahami dasar-dasar yang digunakan untuk melakukan forensika digital dikarenakan ilmu yang digunakan hanya sebatas pada teknis, sementara forensika digital tidak hanya bicara tentang teknis, tapi juga prosedur yang harus dipatuhui untuk membuktikan barang bukti yang sudah didapatkan.

Hasil dari pekerjaan seseorang yang bukan ahli di bidang forensika digital bisa jadi ditolak di persidangan karena seseorang tersebut karena tidak memiliki ilmu yang mumpuni untuk melakukan forensika digital dan tidak diakui atau belum mengantongi sertifikasi di bidang forensika digital.

2.2.2. Bukti Digital

Pada penyelidikan yang dilakukan, pasti terdapat bukti yang disimpan, baik bukti informasi atau data, Menurut [14] bukti digital dapat didefinisikan sebagai informasi elektronik yang dikumpulkan pada saat

melakukan investigasi pada sebuah kasus, yang melibatkan perangkat-perangkat digital seperti email, transaksi perbankan online, foto, web histori maupun audio dan video.

Barang bukti digital dalam komputer forensik secara garis besar terbagi menjadi 3 jenis [15], yaitu:

a) Data Aktif, yaitu data yang terlihat mudah karena digunakan untuk berbagai kepentingan yang berkaitan erat dengan kegiatan yang dilakukan, misalnya program, file gambar atau dokumen teks.
b) Data Arsip, yaitu data yang telah disimpan untuk keperluan backup misalnya dokumen file yang di digitalisasi untuk disimpan dalam format TIFF dengan tujuan menjaga kualitas dokumen.
c) Data Laten, yaitu data ambitient atau data yang tidak dapat dilihat langsung karena tersimpan pada lokasi yang tidak umum dan dalam format yang tidak umum pula, contohnya seperti database log atau internet log. Data laten juga disebut sebagai resudial data yang artinya adalah data sisa atau data sementara.

2.2.3. *Live forensics*

Live forensic yaitu suatu teknik analisis dimana menyangkut data yang berjalan pada sistem atau data volatile yang umumnya tersimpan pada Random Access Memory (RAM) atau transit pada jaringan [9]. Teknik *live forensics* memerlukan kecermatan dan ketelitian, dikarenakan data volatile pada RAM dapat hilang jika sistem mati, dan adanya kemungkinan tertimpanya data penting yang ada pada RAM oleh aplikasi yang lainnya.

Karena itu diperlukan metode *live forensics* yang dapat menjamin integritas dan keaslian data volatile tanpa menghilangkan data yang berpotensial menjadi barang bukti.

Live forensics pada dasarnya memiliki kesamaan pada teknik forensik tradisonal dalam hal metode yang dipakai yaitu identifikasi, penyimpanan, analisis, dan presentasi, hanya saja *live forensics* merupakan respon dari kekurangan teknik forensik tradisonal yang tidak bisa mendapatkan informasi dari data dan informasi yang hanya ada ketika sistem sedang berjalan misalnya aktifitas memory, network proses, swap file, running system proses, dan informasi dari file sistem. Pada metode *Live forensics* bertujuan untuk penanganan insiden lebih cepat, integritas data lebih terjamin, teknik enkripsi lebih memungkinkan bisa dibuka dan kapasitas memori yang lebih rendah bila dibandingkan dengan metode forensik tradisional.

Banyak tools untuk digunakan *live forensics* untuk analisis data baik tools yang berbayar atau tidak berbayar (free). Tools yang dibandingan pada metode *live forensics* yaitu dari kemampuan penggunaan memory, waktu, jumlah langkah dan akurasi paling baik dalam melakukan live forensic.

2.2.4. Memory Forensik

Memory forensik merupakan sebuah proses dalam upaya mendapatkan informasi dan data yang terdapat dalam memory pada sebuah sistem yang sedang berjalan dan akan hilang ketika sistem tersebut dimatikan. Beberapa informasi yang berada pada memory dan dapat digunakan untuk keperluan digital forensik [10] adalah sebagai berikut :

- Konfigurasi dari software dan hardware
- Windows registry dan even logs
- File yang sedang running.
- Malware.
- URLs, IP address, dan network sockets
- Informasi dari pengguna
- Encryption keys
- Process dan threads

Performa forensik memori memiliki potensi untuk memberikan kontribusi yang signifikan untuk penyelidikan forensik dimana data tersebut tersedia untuk menangkap dan analisis [16].

Memori forensik ini sangat berharga karena mengatasi beberapa keterbatasan analisis forensik tradisional, selain untuk mengatasi masalah yang teknologi baru seperti enkripsi dapat menyebabkan selama pemeriksaan died-box. Sebagai teknologi terus berkembang, forensik memori akan menjadi semakin penting agar dapat secara efektif mengumpulkan bukti yang diperlukan [16].

Keterbatasan lain dikenakan oleh ketidakmampuan disk fisik untuk mengungkapkan informasi tentang proses yang berjalan di memori, yang menyangkal wawasan penyidik bagaimana aplikasi sedang digunakan pada sistem pada saat serangan itu.

Hal ini juga mungkin untuk menduga untuk menyembunyikan data dalam memori, atau untuk penyerang remote yang telah dikompromikan sistem untuk alat, data, dan artefak lainnya daripada di drive sistem yang ada.

2.2.5. Tahapan Forensik

Secara umum ada empat tahapan yang harus dilakukan dalam mengelola bukti pada forensika digital, yaitu pengumpulan, pemeliharaan, analisa, dan presentasi. Dalam tugas akhir ini, penulis menggunakan

metode penelitian dari Ellick M. Chan yang menggunakan metodologi penelitian The U.S. National Institute of Justice (NIJ) dirumuskan pada tahapan-tahapan forensika digital ke dalam langkah-langkah berikut ini :

1. Identification
2. Collection
3. Examination
4. Analysis
5. Reporting

Metode tahapan digital forensics ini, diawali dengan identifikasi apakah hal tersebut merupakan suatu tindak kejahatan atau tidak, langkah selanjutnya yaitu collection atau disebut mengumpulkan barang bukti termasuk imaging. langkah selanjutnya yaitu examination adalah proses dimana hasil imaging diuji kebenaranya, apakah sama persis dengan data yang pertama kali imaging, kemudian langkah analisis yaitu langkah untuk mengetahui keseluruhan apa yang telah diperbuat oleh pengguna, hal apa saja yang dikatakan menyimpang dan langkah terakhir yaitu reporting atau laporan yaitu melaporkan dan menjelaskan apa yang telah dianalisis kemudian dipaparkan barang bukti yang telah ditemukan dan didokumentasikan secara rinci.

Dari 5 langkah ini nantinya akan diolah menjadi metodologi penelitian yang akan diterangkan pada bagian selanjutnya.

2.2.6. Random Access Memory (RAM)

Random Access Memory atau yang sering disebut RAM, sebuah tipe penyimpanan komputer yang isinya dapat diakses dalam waktu yang tetap tidak memperdulikan letak data tersebut dalam memori [17]. RAM berperan penting dalam dilakukannya memori forensik dikarenakan forensik memori melibatkan penangkapan dan analisis memori volatile seperti RAM.

Ada banyak data yang tersedia dalam memori volatile. Pada proses RAM, informasi tentang file yang terbuka dan menangani registry, jaringan informasi, password dan kunci kriptografi, konten tidak terenkripsi yang dienkripsi (dan dengan demikian tidak tersedia) pada disk, data yang disembunyikan, dan worm dan rootkit ditulis untuk menjalankan hanya dalam memori semua berpotensi tersimpan di sana. Bagian ini akan pergi ke detail tentang apa jenis informasi dapat diperoleh kembali melalui forensik memori [16].

2.2.7. Aplikasi Instant *Messenger*

2.2.7.1. Facebook *Messenger*

Facebook *Messenger* adalah aplikasi pengirim pesan instan gratis yang dapat digunakan pada berbagai platform seperti telepon cerdas, tablet, dan komputer. Facebook *Messenger* memiliki layanan dan perangkat lunak yang menyediakan teks dan suara pada komunikasinya. Terintegrasi dengan Facebook berbasis web obrolan fitur dan dibangun diatas MQTT protokol [18].

Facebook *Messenger* memungkinkan pengguna Facebook chatting dengan teman-teman baik di ponsel dan di situs utama. Beberapa fitur yang dikeluarkan oleh Facebook *Messenger* sudah memiliki keamanan yang dilakukan, salah satunya enkripsi end-to-end sebagai fitur opsional untuk pengguna Facebook *Messenger*. Ini tersedia dalam mode opsional yang disebut "Percakapan Rahasia" dan menggunakan Protokol Signal. Untuk membuktikan fitur yang telah ada pada Facebook *Messenger* ini maka perlu dilakukan uji coba keamanannya.

2.2.7.2 LINE *Messenger*

LINE *Messenger* adalah sebuah aplikasi pengirim pesan instan gratis yang dapat digunakan pada berbagai

platform seperti telepon cerdas, tablet, dan komputer. LINE difungsikan dengan menggunakan jaringan internet sehingga pengguna dapat melakukan aktivitas seperti mengirim pesan teks, mengirim gambar, video, pesan suara, dan lain lain [19].

LINE *Messenger* dapat digunakan pada berbagai platform pada penelitian ini menggunakan aplikasi LINE *Messenger* Dekstop untuk Microsoft Windows. LINE menggunakan nomor telepon sebagai ID dan dapat membuat ID pengguna untuk memudahkan orang mengundang dalam group atau percakapan. Terdapat beberapa fitur dari LINE *Messenger* yaitu dapat menyembunyikan nomor telepon untuk melindungi privasi. Adanya fitur *Blocked List* pada tab *privacy setting*, dan juga menyedikan fitur keamanan password untuk menghindari orang lain membuka dan melihat isi percakapan. Untuk membuktikan fitur yang telah ada pada LINE *Messenger* ini maka perlu dilakukan uji coba keamanan

2.2.7.3 Telegram *Messenger*

Telegram *messenger* adalah aplikasi pesan chatting multiplatform yang memungkinkan pengguna untuk mengirimkan pesan chatting rahasia yang dienkripsi end-to-end sebagai keamanan tambahan [20]. Fitur pada Telegram salah satunya dapat berbagi lebih dari sekedar gambar dan video, tapi Telegram juga dapat mentransfer dokumen atau mengirim lokasi saat ini ke kontak telegram yang lain dengan mudah.

Telegram *Messenger* mempunyai user interface yang baik dan mempunyai berbagai fitur. Telegram *Messenger* adalah aplikasi berbasis cloud, yang berarti memindahkan percakapan antara smartphone, tablet, web dan desktop. Untuk membuktikan fitur yang telah ada pada Telegram *Messenger* ini maka perlu dilakukan

uji coba keamanan untuk fitur percakapan yang telah dijalankan sebelumnya.

2.2.8. Tools Analisa

2.2.8.1. Winhex

Winhex adalah aplikasi/software yang dibuat oleh perusahaan X-Ways Software Technology yang berupa editor hexadesimal. Editor Hexadesimal ini bisa digunakan untuk kegiatan forensik baik forensik tradisional maupun live forensics, data recovery, keamanan IT, dan proses data dalam tingkat yang lebih rendah. winhex mendukung RAM editor dan menyediakan akses kepada physical RAM. winhex juga mampu mengkonversi antara biner, hex ASCII, Intel hex, dan Motorola S. winhex mendukung file dengan ukuran diatas 4GB. [21]

2.2.8.2. Belkasoft Evidence Center

Belkasoft Evidence Center adalah aplikasi / toolkit untuk memudahkan penyidik untuk mencari, menganalisis, menyimpan dan berbagi bukti digital ditemukan di dalam komputer dan perangkat mobile. Toolkit ini akan cepat mengekstrak bukti digital dari berbagai sumber dengan menganalisis hard drive, drive gambar, memori sampah, iOS, Blackberry dan backup Android, UFED, JTAG dan pembuangan chip off. Belkasoft Evidence Center otomatis akan menganalisis sumber data dan lay out artefak yang paling penting bagi penyidik untuk mempermudah meninjau, mengkaji lebih dekat, atau menambah laporan. [22]

Berikut ini merupakan keunggulan dari Belkasoft Evidence Center diantaranya yaitu

a) Mampu digunakan untuk memeriksa perangkat komputer dan mobile

b) Mampu menemukan lebih dari 700 jenis artefak
c) Mendukung penuh SQLite
d) Mendukung live forensic
e) Bisa digunakan pada page file, hibernation file, dan konten RAM

2.2.8.3. FTK Imager

FTK Imager atau kependekan dari "Forensic Toolkit Imager" merupakan sebuah aplikasi stand-alone untuk disk imaging yang dibuat oleh perusahaan AccessData. Beberapa fitur umum dari FTK ini adalah pembuatan image, melakukan analisis registry, mendeskripsi file, mengidentifikasikan adanya pesan dalam suatu citra (steganografi). [24]

2.2.8.4. Registry Recon

Registry Recon merupakan aplikasi forensik Registry yang terdegradasi untuk menganalisis Registry diakses dari Microsoft Windows. Registry Recon tidak hanya untuk melihat registri. Metode baru yang kuat untuk mengurai data yang Registry, daripada mengandalkan Microsoft API, sehingga Registry yang telah ada pada sistem Windows dari waktu ke waktu dapat dipulihkan kembali. Registry Recon menyediakan akses ke volume besar data registri yang telah dihapus secara efektif, apakah penghapusan yang terjadi akibat aktivitas sistem jinak atau penyalahgunaan jabatan oleh pengguna jadwal Anda sekarang dapat menyertakan data Registry yang aktif, didukung di restore point atau salinan volume shadow. Dengan harga $599 sementara Registry Recon menampilkan data Registry yang unik secara default, akses tanpa batas ke semua contoh kunci Registry tertentu dan nilai-nilai yang tersedia (dengan jalan penuh dan offset sektor) sehingga temuan dapat dikonfirmasi secara efisien. [25]

2.2.8.5. EnCase

Encase Forensic adalah sebuah platform investigasi handal yang mengumpulkan data digital, melakukan analisis, melaporkan temuan dan menyimpannya dalam bentuk yang sesuai secara forensik dan dapat diterima di pengadilan. Tidak hanya dapat membaca data-data yang sudah terhapus, encase juga dapat memberitahukan sistem-sistem yang belum di patch, menerima masukkan dari intrusion detection system untuk menyelidiki keanehan jaringan yang terjadi, merespon sebuah insiden keamanan, memonitoring pengaksesan sebuah file penting. [26]

2.2.8.6. Perbandingan Tools analisa

Pada penjelasan dari berbagai tools yang dijelaskan yaitu tools winhex, belkasoft evidence center, FTK Imager, Registry Recon dan EnCase, maka pada pada tabel 2.2 akan menjelaskan perbandingan dari tools yang nantinya akan menjadi pertimbangan untuk digunakan.

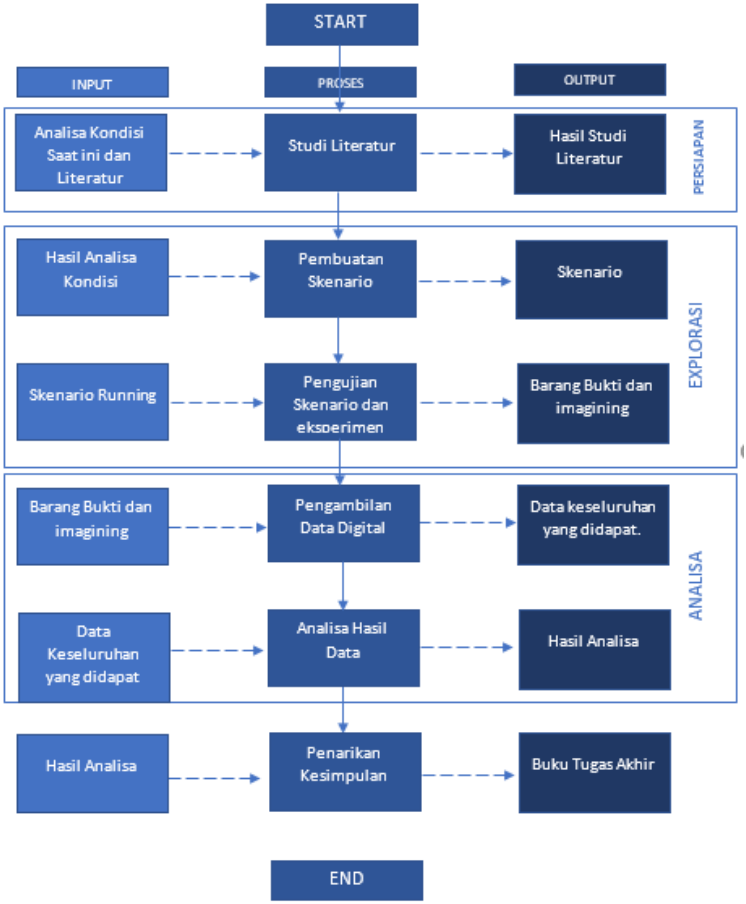
Pada tabel 2.2 menjelaskan perbandingan 5 tools yang nantinya akan digunakan untuk penelitian tugas akhir ini, dimulai dari melihat, menimbang dan mengambil keputusan untuk menggunakan tools winhex dan belkasoft evidence center dikarenakan tools yang telah mendukung untuk digunakan pada live forensics dan memiliki fitur yang sama dan memiliki keunggulan yaitu free/trial, dikarenakan sulit kemungkinannya penelitian tugas akhir ini menggunakan tools yang berbayar.

Tabel 2.2 Perbandingan Tools

Tools	Winhex	FTK Imager	Encase	Registry Recon	Belkasoft
Perusahaan	X-ways	AccessData	Encase®	Arsenal Recon	Belkasoft
Fitur	Mendukung Live Forensics	Tidak Mendukung Live Forensics	Tidak Mendukung Live Forensics	Mendukung Live Forensics	Mendukung Live Forensics
	RAM Editor, Menyediakan akses ke RAM fisik dan memori virtual lain	Disk Imaging, melalui hardisk	Disk Imaging, melalui hardisk	RAM Editor, Menyediakan akses ke RAM fisik dan memori virtual lain	RAM Editor, Menyediakan akses ke RAM fisik dan memori virtual lain
	256 bit enkripsi AES, checksum, CRC32, Hash (MD5, SHA-1)	256 bit enkripsi AES, checksum, CRC32, Hash (MD5, SHA-1)	256 bit enkripsi AES, checksum, CRC32, Hash (MD5, SHA-1)	256 bit enkripsi AES, checksum, CRC32, Hash (MD5, SHA-1)	256 bit enkripsi AES, checksum, CRC32, Hash (MD5, SHA-1)
	Konversi ASCII Hex	Konversi ASCII Hex	Konversi ASCII Hex	Konversi ASCII Hex	Konversi ASCII Hex
	analisis registry, mendeskripsi file	analisis registry, mendeskripsi file	analisis registry, mendeskripsi file	analisis registry, mendeskripsi file	analisis registry, mendeskripsi file
	UI dan penggunaan lebih mudah	UI dan penggunaan lebih mudah	UI dan penggunaan cukup rumit	UI dan penggunaan cukup rumit	UI dan penggunaan lebih mudah
	Proses pembacaan data cepat	Proses pembacaan data cepat	Proses pembacaan data cepat	Proses pembacaan data cepat	Proses pembacaan data cepat
	Trial/Berbayar	Trial/Berbayar	Berbayar $995	Berbayar $399	Trial/Berbayar

BAB III
METODOLOGI PENELITIAN

Bagian ini akan menjelaskan bagaimana runtutan pengerjaan tugas akhir yang akan disertakan detail penjelasan untuk masing-masing tahapan.



Gambar 3.1 Metodologi Penelitian

Berdasarkan pada Gambar 3.1 diagram alur metodologi penelitian, berikut merupakan penjelasan dari setiap prosesnya.

3.1. Studi Literatur

Tahapan ini merupakan awal dari penelitian tugas akhir. Pada tahapan ini, penulis menggali dan menganalisa informasi terkait penelitan yang diambil, khususnya mengenai perangkat lunak serta model pengujian yang sesuai untuk studi kasus. Selain itu, penulis harus memahami dan memastikan bahwa setiap perangkat dan konsep yang ingin diajukan dalam penelitian ini sudah memenuhi kebutuhan dan dukungan terhadap luaran yang diharapkan.

Pada tahap studi literatur ini diharapkan menjadi jembatan awal untuk memulai membuat model pengujian dan kerangka analisa bagi tahapan-tahapan selanjutnya.

3.2. Pembuatan Skenario

Pembuatan skenario dan ekperimen berguna untuk mendapatkan barang bukti sebagai langkah menuju tahap analisa. Penelitian ini menggunakan kondisi yang biasanya terjadi di kehidupan sehari-hari dalam melakukan kejahatan atau transaksi yang dicurigai. Hasil pengujian akan berimplikasi pada penelusuran dan pengembangan barang bukti. Skenario dan eksperimen yang akan dijalankan pada penelitian ini yaitu skenario percakapan dan eksperimen penggunaan aplikasi. Berikut merupakan deskripsi dari eksperimen yang akan dijalankan pada penelitian kali ini :

a. Eksperimen 1 : Aplikasi dijalankan dengan biasa. Pembicaraan meliputi percakapan antar pengguna dan pertukaran media (picture, video, dan audio)
b. Eksperimen 2 : Aplikasi dijalankan dengan biasa namun dengan adanya penghapusan beberapa pesan/percakapan melalui layanan aplikasi

3.3. Pengujian Skenario dan Eksperimen

Pada tahapan ini penulis akan menguji skenario dan eksperimen untuk mendapatkan data digital. Lama pengujian skenario tidak dibatasi. Hal ini dilakukan agar mempermudah dalam pengambilan dan menganalisa data digital yang akan dilakukan pada proses selanjutnya.

Eksperimen akan dijalankan sesuai dengan kondisi yang ada pada lingkungan yang sebenarnya. Metode dalam menguji eksperimen adalah dengan menggunakan aplikasi yang telah ada dan terpasang di laptop penulis.

3.4. Pengambilan Data Digital

Pada tahap ini kita akan mengambil data digital yang telah diujikan melalui skenario dan eksperimen yang telah ditentukan sebelumnya. Pada tahap pengambilan data digital membutuhkan tools yaitu dumpIt dan Belkasoft RamCapturer. Pengambilan data melalui tools yang telah ditentukan akan mendapatkan hasil keseluruhan data-data yang berjalan pada Random Access Memory (RAM) dan nantinya dilakukan tahap selanjutnya.

3.5. Analisa Data Digital

Setelah data berhasil didapatkan, maka akan dianalisa menggunakan aplikasi dan literatur pendukung untuk mencapai tujuan dari penelitian. Sebagai pengujian standar, maka penulis menggunakan aplikasi forensika digital yang sudah banyak digunakan dan tersedia secara gratis, yaitu WinHex dan Belkasoft Evidence Center .

Hasil analisa yang diharapkan ada 3 macam, yaitu struktur penyimpanan data, macam-macam data yang didapatkan, dan tingkat keamanan dari kedua aplikasi instant *messenger* tersebut. Struktur penyimpanan data akan memperlihatkan bagaimana tingkat kompleksitas dan penjelasan terhadap data yang dapat dianalisa oleh para

examiner. Struktur penyimpanan ini juga dapat dilakukan untuk mengecek kembali apakah data yang didapatkan pada tools sesuai dengan kondisi pada aplikasi tersebut.

Struktur pesan dilakukan untuk mengetahui bagaimana pesan percakapan tersebut terbentuk, terdiri dari tipe data apa saja yang nantinya apakah dapat dibandingkan dengan ke-3 aplikasi yang telah ditentukan sebelumnya. Pada tingkat keamanan akan mempertimbangkan kelengkapan struktur dan analisa data yang didapatkan pada skenario dan eksperimen dari ketiga aplikasi instant *messenger*. Semakin lengkap data yang dapat dianalisa maka dianggap menjadi aplikasi dengan rujukan terbaik bagi para penegak hukum untuk mendapatkan bukti digital. Semakin sedikit data yang dapat dianalisa maka dianggap menjadi aplikasi dengan tingkat keamanan terbaik bagi pengguna.

Pada tabel 3.1 merupakan contoh struktur penyimpanan data pada aplikasi LINE *Messenger*:

Tabel 3.1 Contoh Struktur Penyimpanan LINE Messnger

Konten	Direktori	File
Database Kontak	/LINE/data/db/AutoSuggest	LINE.db (SQLite v.3)
Database obrolan	/LINE/data/bgChat	Msgstore.db (SQLite v.3)

Pada tabel 3.2 merupakan contoh struktur penyimpanan data aplikasi Telegram *Messenger*:

Tabel 3.2 Contoh Struktur Penyimpanan Telegram

Konten	Direktori	File
Database Kontak	/AppData/Roaming/Telegram Dekstop/ tdata	telegram.db (SQLite v.3)

Konten	Direktori	File
Database obrolan	/AppData/Roaming/Telegram Dekstop/ tdata	Msgstore.db (SQLite v.3)

Pada tabel 3.3 merupakan contoh struktur penyimpanan data aplikasi Facebook *Messenger* sebagai berikut :

Tabel 3.3 Contoh Struktur Penyimpanan Facebook

Konten	Direktori	File
Database Kontak	/WinUAPEntry/Resources/Assets/Apps/*Messenger*	*messenger*.db (SQLite v.3)
Database obrolan	/WinUAPEntry/Resources/Assets/Apps/*Messenger*	Msgstore.db (SQLite v.3)

3.6. Penyusunan Laporan Tugas Akhir

Tahapan terakhir adalah pembuatan laporan tugas akhir sebagai bentuk dokumentasi atas terlaksananya penelitian tugas akhir ini. Di dalam laporan tersebut mencakup:

a. Bab I Pendahuluan
   Pada bab ini dijelaskan mengenai latar belakang, rumusan dan batasan masalah, tujuan dan manfaat pengerjaan tugas akhir ini.

b. Bab II Tinjauan Pustaka
   Dijelaskan mengenai teori – teori yang menunjang permasalahan yang dibahas pada penelitian tugas akhir ini

c. Bab III Metodologi
   Pada bab ini dijelaskan mengenai tahapan – tahapan apa saja yang harus dilakukan dalam pengerjaan penelitian tugas akhir

d. Bab IV Perancangan

Bab yang berisi tentang perancangan yang akan dilakukan dalam penyelesaian permasalahan yang dibahas pada pengerjaan tugas akhir ini

e. Bab V Implementasi

- Bab yang berisi tentang implementasi dilakukan dalam penyelesaian permasalahan yang dibahas pada pengerjaan tugas akhir ini

f. Bab VI Analisis dan Pembahasan
Bab yang berisi tentang analisa dan pembahasan yang dilakukan dalam penyelesaian permasalahan yang dibahas pada pengerjaan tugas akhir ini

g. Bab VII Kesimpulan dan Saran
Berisi tentang kesimpulan dan saran yang ditujukan untuk kelengkapan penyempurnaan tugas akhir ini.

BAB IV
PERANCANGAN

Pada bab ini akan dijelaskan terkait perancangan yang dilakukan untuk mendapatkan hasil analisa yang baik dalam proses penelitian live forensik pada aplikasi instant *messenger*. Perancangan pada penelitian ini menitik beratkan pada teknis, dimulai dari proses pembuatan skenario hingga analisa data. Pada proses pembuatan skenario, penulis mempertimbangkan kondisi yang sering atau mungkin terjadi pada kasus hukum di kehidupan sebenarnya. Proses pelaksanaan eksperimen, penulis mempertimbangkan kemungkinan yang terjadi pada kegiatan berbagi pesan pada aplikasi yang digunakan sehingga harus memunculkan eksperimen dari semua kemungkinan yang ada. Setelah eksperimen dilakukan, maka proses pengambilan data harus mempertimbangkan kesamaan proses pada setiap aplikasi yang digunakan dan kesesuaian dengan tujuan penelitian yang ada. Setelah didapatkan hasil dari eksperimen, maka analisa data dilakukan dengan menyeluruh dan teliti sehingga memunculkan hasil analisa yang sempurna atau mendekati kebenaran menggunakan aplikasi forensika digital yang telah disepakati sebelumnya.

4.1. Pembuatan Skenario Percakapan

Dalam membuat penelitian terkait analisa live forensik terhadap aplikasi instant *messenger*, penulis membutuhkan kesamaan kuantitas dan kualitas percakapan untuk dibandingkan antar aplikasi. Oleh karena itu, dibutuhkan sebuah skenario percakapan untuk digunakan dalam penelitian ini. Skenario ini selain harus dibuat dengan mempertimbangkan kemungkinan kasus yang melibatkan aplikasi instant *messenger*, juga yang harus menyediakan berbagai media yang dilampirkan agar dapat dipersandingkan kemampuan setiap aplikasi instant *messenger* yang terlibat dalam penelitian ini.

Dalam penelitian ini, penulis membuat skenario sederhana dan mencakup semua kebutuhan dalam penelitian ini. Penulis mengambil sebuah kasus tentang kejahatan terkait penipuan online shopping yang dilakukan pada aplikasi *messenger* yang nantinya akan dijadikan barang bukti bahwa kejadian tersebut benar adanya. Pada skenario yang digunakan, barang bukti yang digunakan tersangka adalah personal pc (laptop) yang masih menyala/aktif dan nantinya akan dilakukan dump pada RAM. Dalam skenario yang digunakan terdapat beberapa file yang dilampirkan, seperti gambar/foto, emoji/sticker, pesan suara, dan juga video.

Untuk skenario percakapan yang dilakukan pada penelitian ini terdapat dalam **LAMPIRAN A.**

4.2. Pelaksanaan Eksperimen

Berdasarkan skenario yang telah dibuat dan ditentukan dalam penelitian ini, maka semua hal yang akan digunakan dalam setiap pelaksanaan eksperimen harus dipersiapkan dengan teliti dan benar. Dalam penelitian ini, ada 2 macam eksperimen yang telah ditentukan sebelumnya, yaitu

1. Eksperimen 1 yaitu penggunaan biasa
   Pada eksperimen pertama merupakan pelaksanaan sesuai skenario percakapan tanpa ada modifikasi apapun. Eksperimen dijalankan sesuai lingkungan yang ada dan dijalankan pada tiga aplikasi yang berbeda sesuai dengan rancangan yang telah dibuat sebelumnya.
2. Eksperimen 2 yaitu penghapusan percakapan
   Pada eksperimen kedua merupakan pelaksanaan skenario percakapan dengan melakukan modifikasi terhadap keberlansungan data, yaitu penghapusan beberapa pesan/percakapan setelah skenario percakapan utama telah selesai.

Diharapkan eksperimen yang akan dilakukan berjalan dengan baik dan lancar sehingga dapat dilakukan analisa yang akurat dan dapat dipertanggungjawabkan hasilnya.

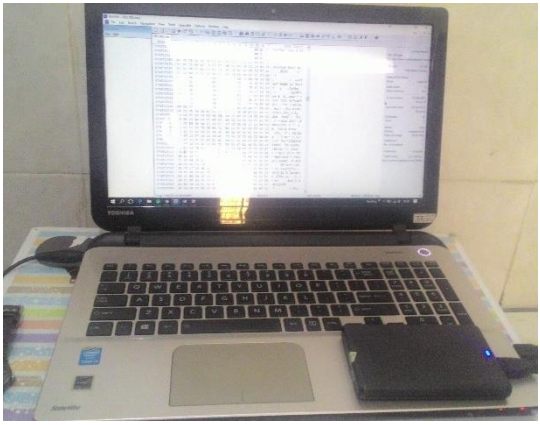
4.2.1. Perangkat dan Kelengkapannya

Ada beberapa jenis perangkat yang harus dipersiapkan dalam pelaksanaan eksperimen ini, seperti perangkat fisik dan perangkat lunak aplikasi instant *messenger*. Untuk perangkat fisik, penulis mempersiapkan 1 buah telepon genggam dan satu buah personal komputer (PC)/Laptop, yaitu sebagai berikut :

a. Perangkat Telephone genggam dengan merk Asus Zenfone 5 yang digunakan korban untuk skenario dan eksperimen.

Gambar 4.1. Perangkat Asus Zenfone 5

b. Perangkat Personal Computer (PC) dengan merk Toshiba yang digunakan tersangka untuk skenario dan eksperimen yang nantinya dijadikan bukti digital dan untuk dilakukannya analisa pada penelitian ini.



Gambar 4.2. Perangkat Laptop dan tools WinHex

Untuk perangkat fisik, penulis juga harus menentukan aktor beserta perangkatnya agar memberikan kepastian dan kesepahaman dalam melakukan eksperimen nantinya.

Selain perangkat fisik, penulis juga harus mempersiapkan perangkat lunak yang menjadi pembahasan utama dalam penelitian ini yang juga telah diatur dalam batasan masalah, yaitu aplikasi instant *messenger*. Aplikasi instant *messenger* yang digunakan harus sesuai dengan batasan masalah dan tidak boleh diperbaharui untuk menjaga keberlansungan dan keseimbangan dalam penelitian nantinya. Berdasarkan batasan masalah, aplikasi instant *messenger* yang harus dipasang adalah sebagai berikut :

- LINE *Messenger* : versi 5.1.1.1422
- Facebook *Messenger* : versi v2.1.4623
- Telegram *Messenger* : versi 1.1.7

4.2.2. Kebutuhan Data Pendukung

Selain kebutuhan terkait perangkat, berdasarkan skenario yang telah ditentukan sebelumnya maka penulis diharapkan telah mempersiapkan data-data

untuk mendukung setiap eksperimen yang akan dilakukan. Berikut merupakan data-data yang harus dipersiapkan untuk setiap eksperimen yang akan dijalankan dalam penelitian ini :

1. 2 akun e-mail yang aktif, yaitu :
   a. olshopguccies@gmail.com
   b. tayomidwi@outlook.com
2. Kontak korban yang digunakan yang ada pada perangkat tersangka, yaitu “Kurnia Ayu” dengan nomor telephone 08998631291
3. Perangkat pendukung berupa :
   a. Pada gambar yang digunakan terkait skenario yang telah ditentukan, pada Gambar 4.3 dengan nama file Screenshot_2017-06-16-15-37-53.jpg dan Gambar 4.4 dengan nama file IMG_20170616_173413_302.jpg :

Gambar 4.3 Gambar Perangkat pendukung skenario

Gambar 4.4. Gambar Perangkat pendukung skenario

b. Potongan tampilan video terkait skenario
Pada gambar 4.5 merupakan cuplikan video pada skenario yang telah ditentukan untuk mendukung berjalannya skenario sesuai dengan kondisi nyata.

Gambar 4.5 Cuplikan Video Skenario

c. Bukti transfer terkait skenario, dengan nama file IMG_20170616_174106_556.jpg:

Gambar 4.6 Bukti Transfer Skenario

d. Pesan suara selama 7 detik yang menggambarkan skenario dengan nama file voice_175 atau xxxx.mp4. Dan isi skenario pesan suara adalah :

"Halo sist, bagaimana barang saya? Sudah dikirim kah? Terimakasih."

4.2.3. Kondisi Pelaksanaan yang Diharapkan

Kondisi pelaksanaan yang diharapkan adalah situasi yang mirip dengan realita, dengan mempertimbangkan kondisi yang dapat membedakan antara perangkat korban (HP) dan tersangka (PC), serta dengan mempertimbangkan tingkat aktivitas disetiap perangkat yang digunakan.

4.3. Pengambilan Data Digital

Pada tahap ini, peneliti mengambil data dari setiap eksperimen yang telah dijalankan pada Random Access Memory (RAM). Data yang akan diambil adalah data terkait skenario yang dijalankan pada aplikasi instant *messenger* yang telah ditentukan, yaitu terdiri dari folder data dan sistem yang berada pada perangkat tersangka.

Dengan perbedaan aplikasi yang dijalankan, maka proses ini akan mempertimbangkan kondisi perangkat dan aplikasi dengan kebutuhan sistem atau aplikasi untuk melakukan akuisisi data dari eksperimen yang telah dijalankan.

Pada tahap pengambilan data digital membutuhkan tools yaitu dumpIt dan Belkasoft RamCapturer. Pengambilan data ini membutuhkan waktu yang cukup lama dikarenakan pelaksanaan skenario dan eksperimen dilakukan secara langsung dan dilaksanakan sesuai dengan kondisi nyata.

Pengambilan data melalui tools yang telah ditentukan akan mendapatkan hasil keseluruhan data-data yang berjalan pada Random Access Memory (RAM) dan nantinya dilakukan tahap selanjutnya yaitu analisa data digital untuk memilah dan memilih data yang terkait skenario dan eksperimen untuk dapat dijadikan bukti digital.

4.4. Analisa Data

Pada proses analisa data dilakukan pasca pengambilan data (dump). Analisa data dilakukan mengikuti tujuan penelitian dengan menggunakan aplikasi forensika digital yang telah disepakati sebelumnya. Tools yang digunakan untuk analisa data yaitu Winhex dan Belkasoft Evidence Center.

Proses analisa data dimulai dari penelusuran secara singkat hingga mendalam terhadap hasil yang didapatkan dari proses pengambilan data. Proses penelusuran ini dilakukan untuk memeriksa dan mengetahui sejauh mana data yang dibuat oleh aplikasi instant *messenger* dapat diambil oleh proses pengambilan data pada RAM. Selain itu, proses penelusuran ini menjadi kunci untuk proses analisa selanjutnya. Luaran dari proses penelusuran ini adalah struktur data dari skenario yang telah ditentukan pada aplikasi instant *messenger* yaitu LINE *Messenger*, Facebook *Messenger* dan Telegram *Messenger*.

Struktur yang diharapkan yaitu struktur pesan yang berisikan artefak-artefak penyusun data pada setiap aplikasi yang nantinya akan dilakukan proses selanjutnya yaitu membaca data-data yang telah didapatkan. Proses pembacaan ini dilakukan untuk mencoba mencari tahu artefak-artefak apa saja yang dapat dihasilkan dari proses pengambilan data pada RAM. Proses ini mungkin akan melibatkan pembukaan kode enkripsi, pembacaan kasus dari skenario, dan hal lain yang dilakukan untuk mencaritahu data yang ada. Proses analisa ini akan menghasilkan macam-macam luaran data yang didapatkan dari ketiga aplikasi instant *messenger* tersebut.

Macam-macam luaran yang diharapkan dibagi menjadi 2 bagian yaitu struktur data pesan dan media. Dari struktur data yang didapatkan dibagi menjadi 2 bagian yaitu struktur data primer percakapan dan struktur data pendukung percakapan, data primer percakapan terdiri dari 5 hal yang bersifat penting seperti userId, senderId, chatId, text dan time dikarenakan akan menjadi barang bukti digital yang akan dapat mengungkapkan kasus pada skenario dan eksperimen, untuk data pendukung percakapan terdiri dari struktur pesan yang dihasilkan pada setiap aplikasi. Untuk media sendiri dibagi menjadi 4 hal yaitu picture, audio, video dan sticker.

Setelah proses pembacaan selesai dilakukan, maka proses analisa selanjutnya yaitu proses perbandingan. Proses perbandingan ini dilakukan untuk membandingkan hasil-hasil yang didapatkan dari proses sebelumnya diantara aplikasi instant *messenger* yang menjadi objek penelitian. Analisa ini akan memberikan luaran yaitu perbandingan data aplikasi untuk bukti digital yang didapatkan dari ketiga aplikasi instant *messenger* tersebut menggunakan tools yang telah ditentukan.

Analisa dilanjutkan dengan membandingkan hasil dari kedua eksperimen yang dilakukan. Hal ini akan memberikan hasil analisa untuk analisa faktor-faktor yang mempengaruhi keberhasilan mendapatkan bukti digital dari kedua aplikasi instant *messenger* tersebut. Pada proses ini, penulis akan menitikberatkan pada perbedaan eksperimen yang dilakukan.

Setelah proses penelusuran, pembacaan, dan perbandingan terhadap aplikasi dan eksperimen, maka proses terakhir dalam analisa adalah penilaian. Proses penilaian disini merajuk pada hasil sebelumnya sehingga diharapkan adanya luaran berupa aplikasi mana yang menjadi aplikasi instant *messenger* yang memiliki sekuritas tertinggi atau mudah untuk dilakukan forensika digital pada ketiga aplikasi instant *messenger* pada penelitian ini.

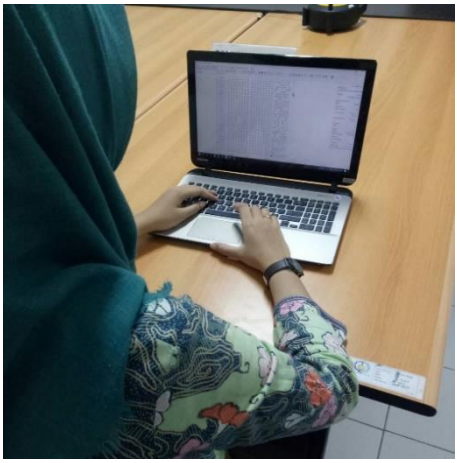
BAB V
IMPLEMENTASI

Bab implementasi ini akan menjelaskan terkait pelaksanaan dari penelitian yang dilakukan dengan menggunakan metode dan tools yang telah dirancang pada bab sebelumnya. Tahap implementasi yaitu proses pelaksanaan skenario dan eksperimen dan pengambilan data digital, Pada proses ini akan menghasilkan luaran data digital yang menjadi masukan pada bab selanjutnya, yaitu hasil dan pembahasan.

5.1. Pelaksanaan Skenario dan Eksperimen

Pelaksanaan Skenario dan eksperimen dilaksanakan mengikuti rancangan skenario yang telah dibuat dengan implementasi penanganan aplikasi yang berbeda untuk setiap eksperimen. Setiap pelaksanaan eksperimen lansung diikuti dengan proses pengambilan digital sehingga proses ini dilakukan secara bersamaan.

Gambar 5.1 Proses Eksperimen Menggunakan Zenfone 5



Gambar 5.2 Proses Eksperimen Menggunakan Laptop

Aktor pada skenario ini dibagi menjadi dua, yaitu tersangka dan korban. Pembagian perangkat dan pengguna dijelaskan pada tabel 5.1 berikut :

Tabel 5.1 Pembagian Perangkat

Aktor	Perangkat	Nomor Telepon	Email
Tersangka	Laptop Toshiba	081230243100	olshopguccies@gmail.com
Korban	Asus Zenfone 5	08998631291	tayomidwi@outlook.com

Berikut merupakan detail terkait pelaksanaan eksperimen yang telah dilakukan :

5.1.1. Eksperimen 1

Eksperimen pertama merupakan pelaksanaan sesuai skenario percakapan tanpa ada modifikasi apapun. Eksperimen dijalankan sesuai lingkungan yang

ada dan dijalankan pada tiga perangkat berbeda sesuai dengan rancangan yang telah dibuat.

5.1.2. Eksperimen 2

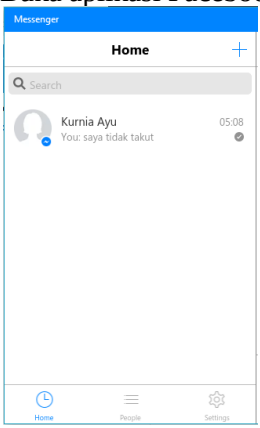
Eksperimen kedua merupakan pelaksanaan skenario percakapan dengan melakukan modifikasi terhadap keberlansungan data, yaitu penghapusan percakapan/pesan percakapan setelah skenario percakapan selesai.

Berikut merupakan contoh penghapusan percakapan pada LINE *Messenger,* Facebook *Messenger* dan Telegram *Messenger* :

5.1.2.1. Facebook *Messenger*

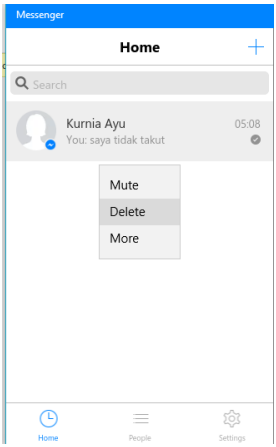
A. Penghapusan Percakapan
Berikut ini langkah untuk menghapus percakapan :

1. Buka aplikasi Facebook *Messenger*.



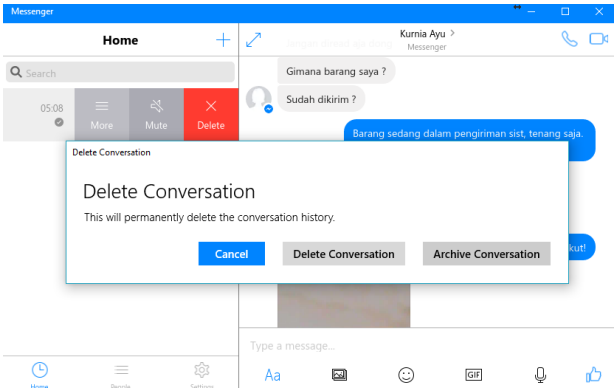
Gambar 5.3 Tampilan Awal Facebook *messenger*

2. Pilih percakapan yang ingin dihapus. Klik kanan pada percakapan yang ingin dihapus hingga muncul pilihan seperti berikut :



Gambar 5.4 Pilihan Penghapusan Percakapan

3. Pilih Delete Chat, lalu pilih Delete Coversation. Maka percakapan akan terhapus.

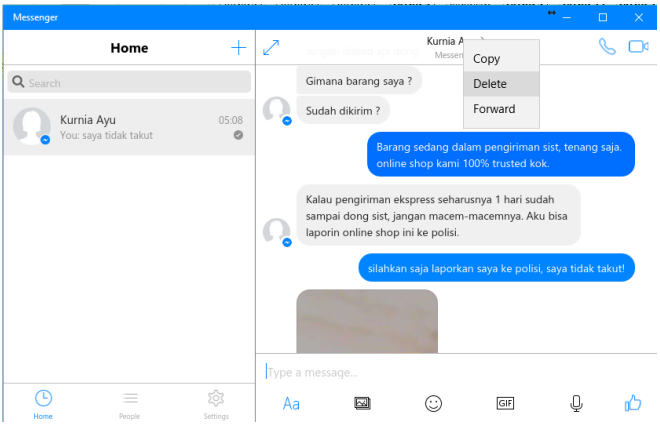


Gambar 5.5 Konfirmasi Penghapusan Percakapan

B. Penghapusan Pesan Percakapan

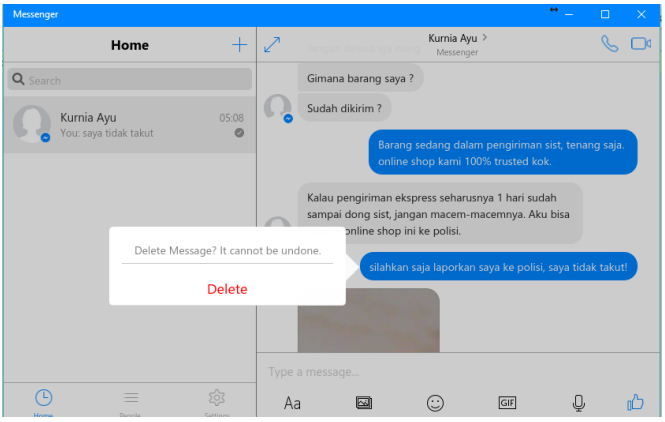
Berikut ini langkah untuk menghapus pesan percakapan:

1. Pilih pesan percakapan yang ingin dihapus. Klik kanan pada pesan percakapan yang ingin dihapus dan pilih delete hingga muncul pilihan konfirmasi :



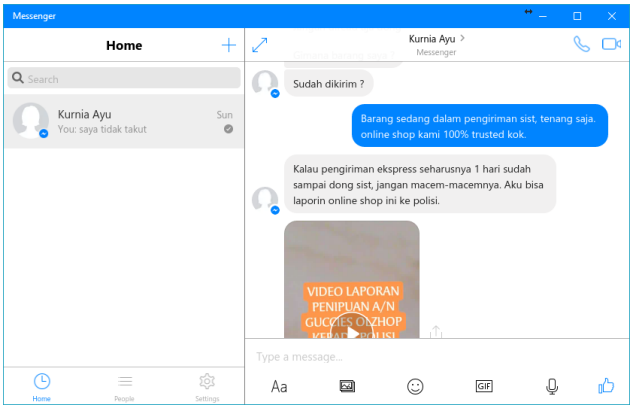
Gambar 5.6 Penghapusan percakapan

2. Lalu klik delete untuk konfirmasi bahwa pesan percakapan tersebut akan dihapus, maka pesan akan langsung terhapus.



Gambar 5.7 Penghapusan Pesan Percakapan

3. Setelah pesan percakapan dihapus maka tampilan akan menjadi seperti berikut ini :



Gambar 5.8 Hasil Penghapusan pesan percakapan

5.1.2.2. LINE *Messenger*

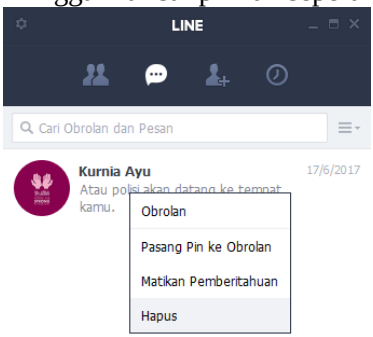
A. Penghapusan Percakapan

Berikut ini langkah untuk menghapus percakapan:

1. Buka aplikasi LINE *Messenger*.

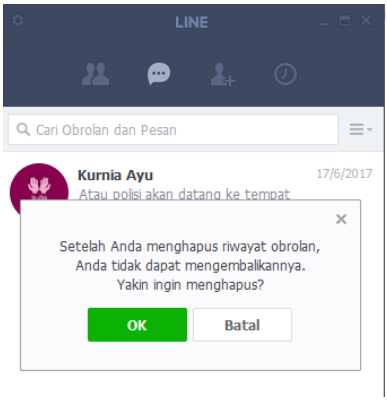
Gambar 5.9 Tampilan Awal LINE *Messenger*

2. Pilih percakapan yang ingin dihapus. Klik kanan pada percakapan yang ingin dihapus hingga muncul pilihan seperti berikut :



Gambar 5.10 Pilihan Penggunaan Percakapan

3. Pilih Hapus, lalu konfirmasi dengan cara klik OK. Maka percakapan akan terhapus.



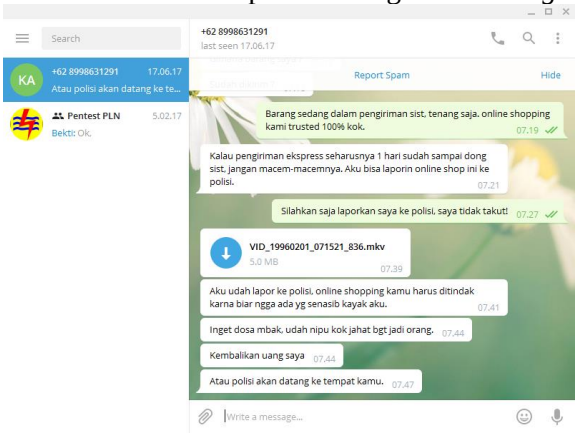
Gambar 5.11 Konfirmasi Penghapusan Percakapan

5.1.2.3. Telegram *Messenger*

A. Penghapusan Percakapan

Berikut ini langkah untuk menghapus percakapan:

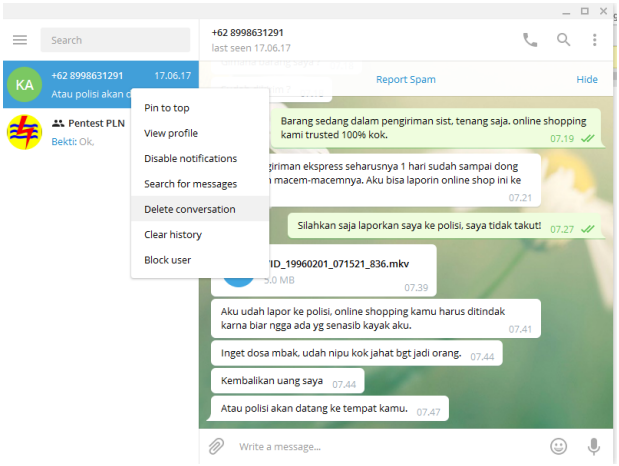
1. Buka aplikasi Telegram *Messenger*.



Gambar 5.12 Tampilan Awal Telegram *messenger*

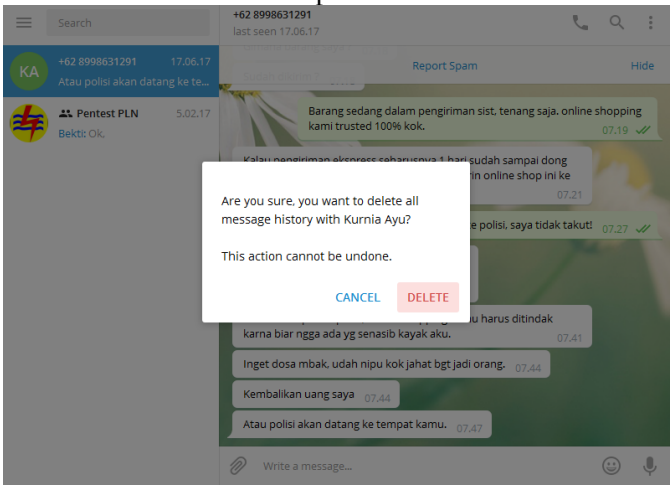
2. Pilih percakapan yang ingin dihapus. Klik kanan pada percakapan yang ingin

dihapus hingga muncul pilihan seperti berikut :



Gambar 5.13 Pilihan Penghapusan Percakapan

3. Pilih Delete Conversation, lalu konfirmasi dengan cara klik Delete. Maka percakapan akan terhapus.

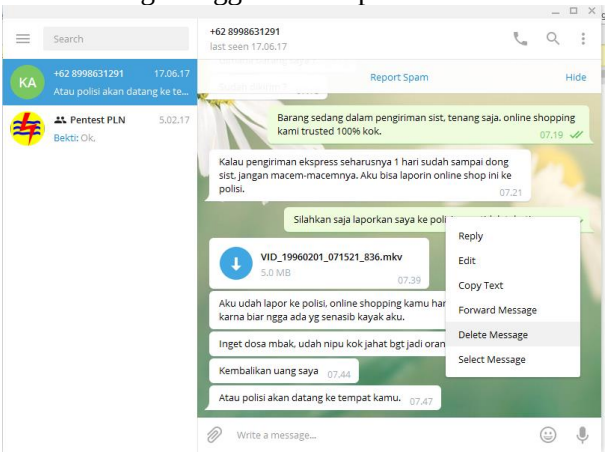


Gambar 5.14 Konfirmasi penghapusan percakapan

B. Penghapusan Pesan Percakapan

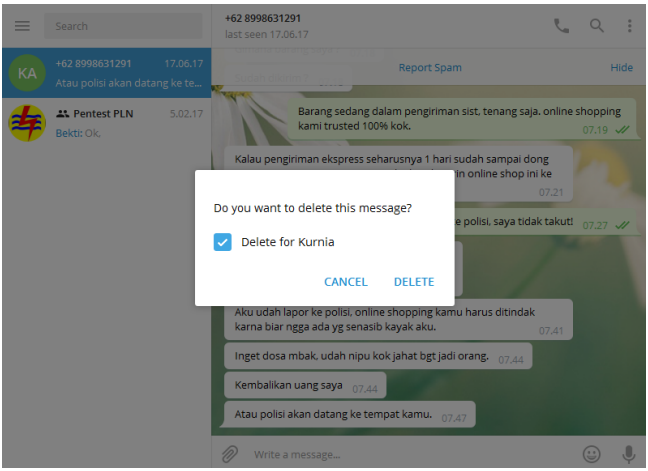
Berikut ini langkah untuk menghapus pesan percakapan:

1. Pilih pesan percakapan yang ingin dihapus. Klik kanan pada pesan percakapan yang ingin dihapus dan pilih delete message hingga muncul pilihan konfirmasi :



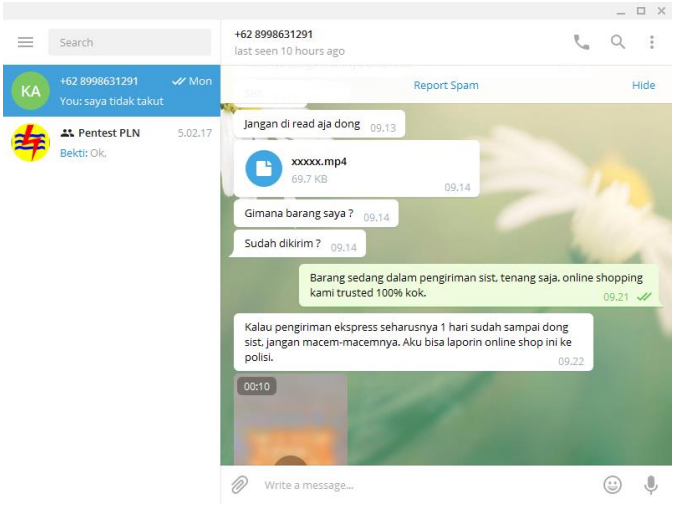
Gambar 5.15 Penghapusan pesan percakapan

2. Lalu klik delete untuk konfirmasi bahwa pesan percakapan tersebut akan dihapus, maka pesan akan langsung terhapus.



Gambar 5.16 Konfirmasi penghapusan percakapan

3. Setelah pesan percakapan dihapus maka tampilan akan menjadi seperti berikut ini :



Gambar 5.17 Tampilan Akhir Penghapusan

5.2. Pengambilan Data Digital

Pada tahap ini, kita mengambil data dari setiap eksperimen yang telah dijalankan. Data yang diambil adalah data terkait aplikasi instant *messenger* yang dijalankan dalam penelitian ini, yang terdiri dari folder data dan sistem yang berada pada Personal Computer (PC) Tersangka.

Dengan perbedaan aplikasi yang dijalankan, maka proses ini mempertimbangkan kondisi perangkat dan aplikasi dengan kebutuhan sistem atau aplikasi untuk melakukan akuisisi data dari eksperimen yang telah dijalankan. Pengambilan Data digital ini dilakukan menggunakan tools DumpIt dan Belkasoft RamCapturer.

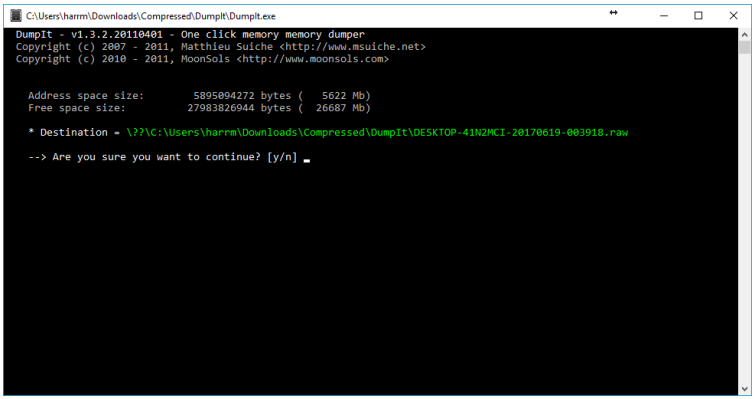
Berikut ini merupakan langkah-langkah yang dilakukan pada saat pengambilan bukti data digital :

5.2.1. DumpIt

Pada aplikasi DumpIt melakukan dump pada *random access memory* (RAM) yang telah dijalankan dari setiap aplikasi instant *messenger* sesuai dengan eksperimen yang dijalankan dan akan dianalisa dengan aplikasi WinHex.

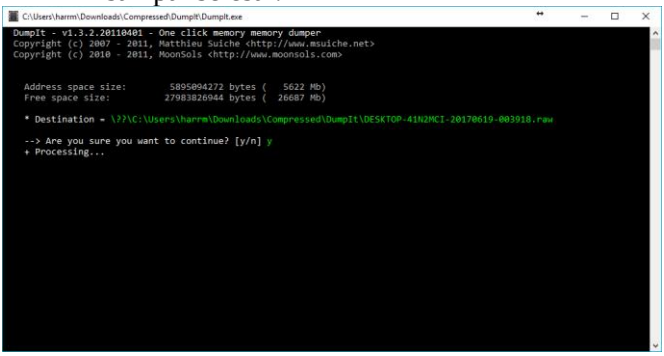
Berikut ini adalah penggunaan dumpIt dalam melakukan dump pada RAM:

1. Buka aplikasi dumpIt.exe
2. Lalu akan muncul konfirmasi bahwa aplikasi dumpIt akan dijalankan.



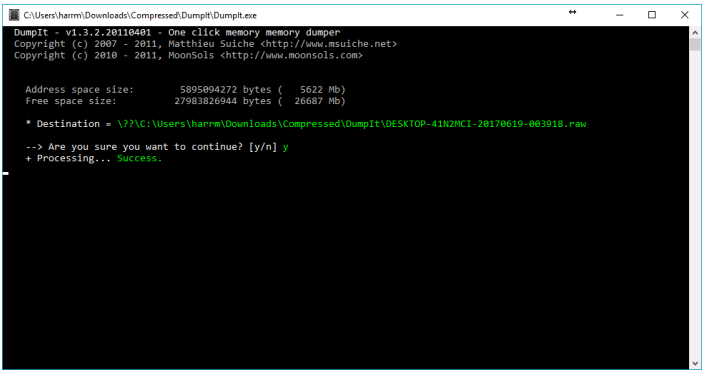
Gambar 5.18 Pengambilan data pada Aplikasi DumpIt

3. Selanjutnya ketik y atau yes untuk dapat menjalankan aplikasi dumpIt dan menunggu proses sampai selesai.



Gambar 5.19 Proses awal pada Aplikasi DumpIt

4. Setelah proses selesai maka akan ada pemberitahuan success, bahwa proses dump ini telah berhasil dengan destination yang telah ditentukan sebelumnya.



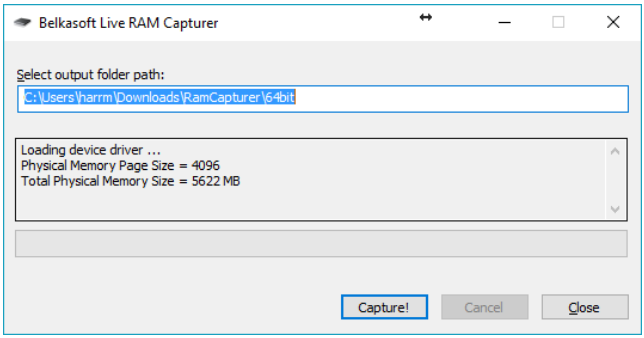
Gambar 5.20 Proses akhir pada Aplikasi DumpIt

5.2.2. Belkasoft RamCapturer

Pada aplikasi Belkasoft RamCapturer ini melakukan dump pada *random access memory* (RAM) yang telah dijalankan dari setiap aplikasi instant *messenger* sesuai dengan eksperimen yang dijalankan dan akan dianalisa dengan aplikasi bawaan dari Belkasoft Evidence Center.

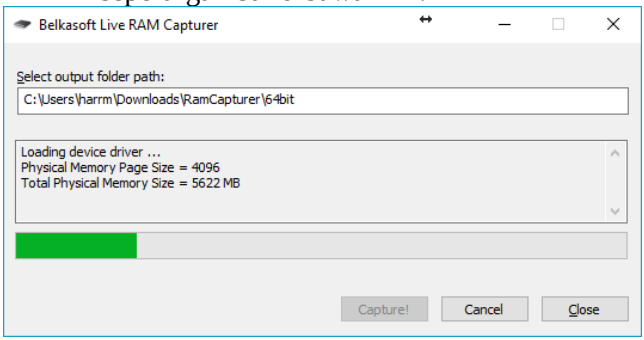
Berikut ini adalah penggunaan RamCapturer dalam melakukan dump pada RAM:

1. Buka aplikasi Belkasoft RamCapturer.exe
2. Pilih Folder yang digunakan untuk menyimpan hasil capture dari RamCapturer. Lalu klik Capture! untuk memulai prosesnya.



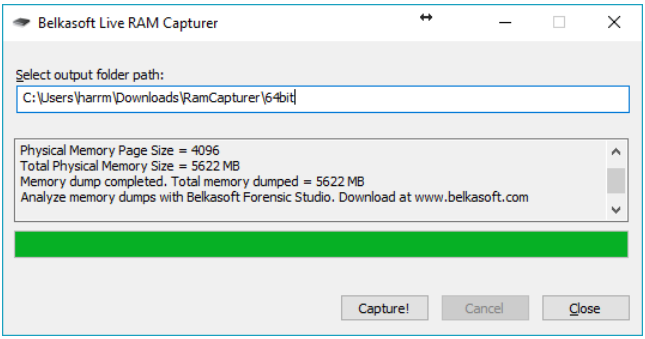
Gambar 5.21 Pemilihan folder data pada RamCapturer

3. Maka Ramcapturer akan melakukan proses dump seperti gambar dibawah ini:



Gambar 5.22 Proses pengambilan data pada RamCapturer

4. Setelah proses capture RAM selesai maka akan muncul pemberitahuan bahwa proses tersebut telah dilaksanakan.



Gambar 5.23 Proses akhir pada Aplikasi RamCapturer

5.3. Analisa Data Digital

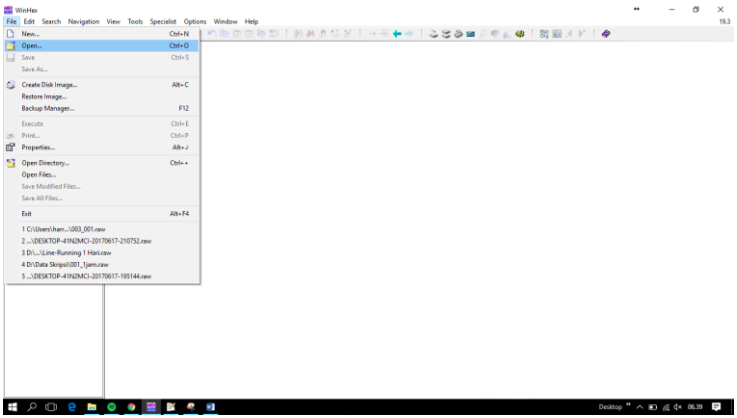
Setelah data digital dapat diambil, selanjutnya dilaksanakan dengan melakukan analisa awal menggunakan aplikasi terkait. Dalam penelitian ini, penulis menggunakan beberapa aplikasi forensik digital seperti WinHex dan Belkasoft Evidence Center untuk menganalisa dan membuka beberapa file terkati aplikasi instant *messenger* yang menjadi objek penelitian kali ini.

5.3.1. WinHex

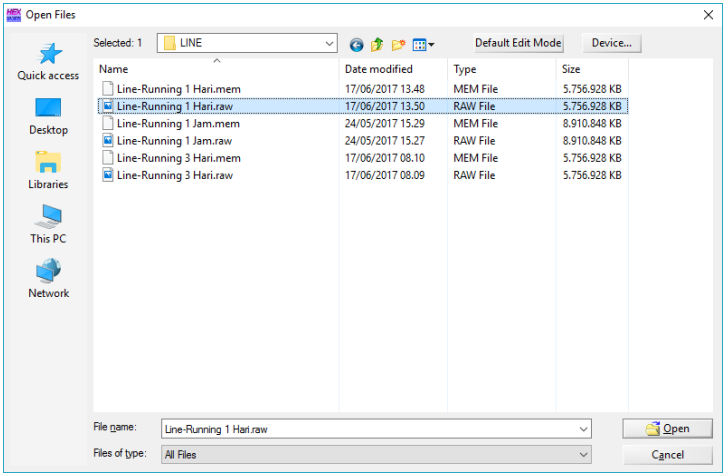
WinHex merupakan aplikasi editor hexadesimal yang digunakan untuk menganalisa data dari physical RAM. WinHex yang nantinya akan mengeluarkan atau mendapatkan beberapa barang bukti digital dari hasil analisa yang dilakukan.

Berikut merupakan langkah untuk menganalisa data menggunakan aplikasi WinHex:

- Buka aplikasi WinHex
- Tambahkan hasil dari proses DumpIt yang nantinya akan dianalisa. Proses analisa memakan waktu cukup lama dikarenakan menganalisa hasil dari 4gb RAM yang digunakan.



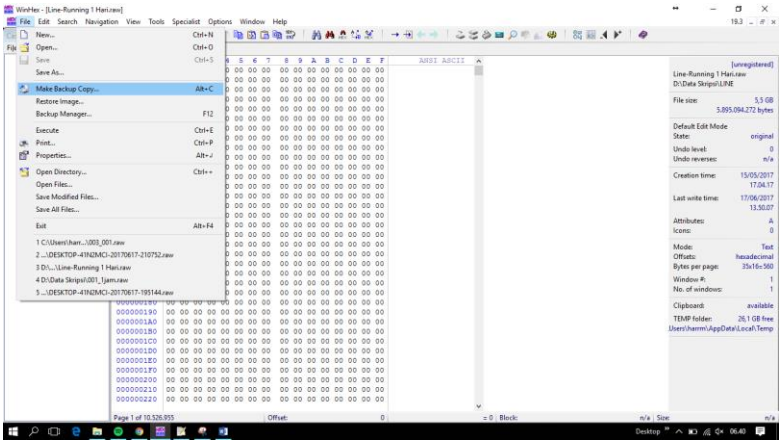
Gambar 5.24 Tampilan Open file pada WinHex



Gambar 5.25 Memilih file yang dianalisa dengan WinHex

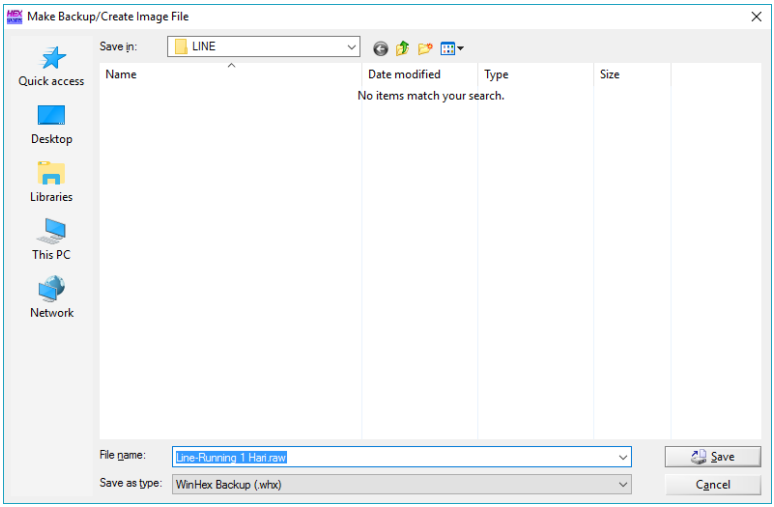
Untuk kebutuhan analisa yang lebih mendalam ataupun untuk membuka file di langsung dengan aplikasi, maka disarankan untuk melakukan membuat file cloning yaitu membuat backup copy data agar apabila terjadi kesalahan pada saat analisa, data yang digunakan tidak merusak file aslinya. Berikut merupakan fitur Make backup Copy :

a. Pilih file yang ingin dianalisa lebih lanjut, lalu klik Files dan pilih fitur Make Backup Copy.



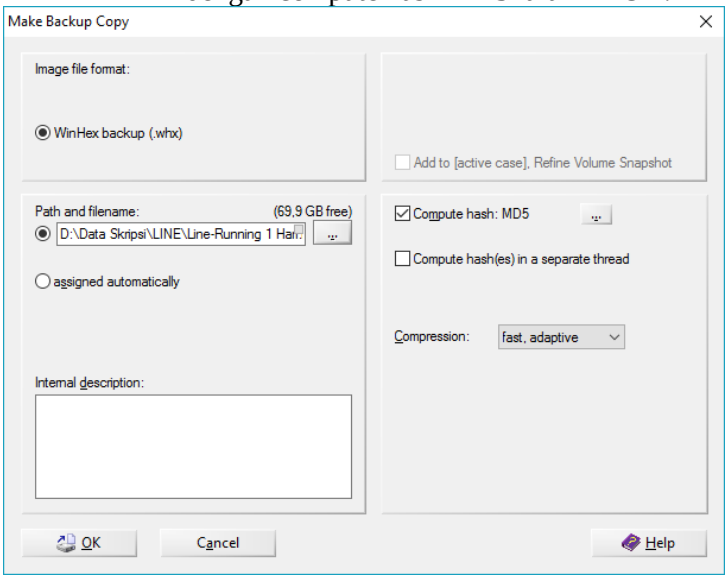
Gambar 5.26 Memilih opsi Make Backup Copy

b. Pilih folder untuk destinasi file yang akan dibuat backup copy.



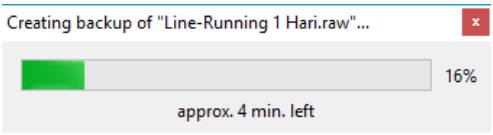
Gambar 5.27 Memilih destinasi file.

c. Lalu pilih image file format WinHex Backup dengan compute hash MD5 lalu klik OK.



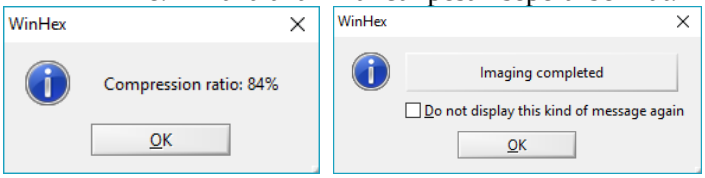
Gambar 5.28 Image file format

d. Tunggu hingga proses Backup Copy selesai.



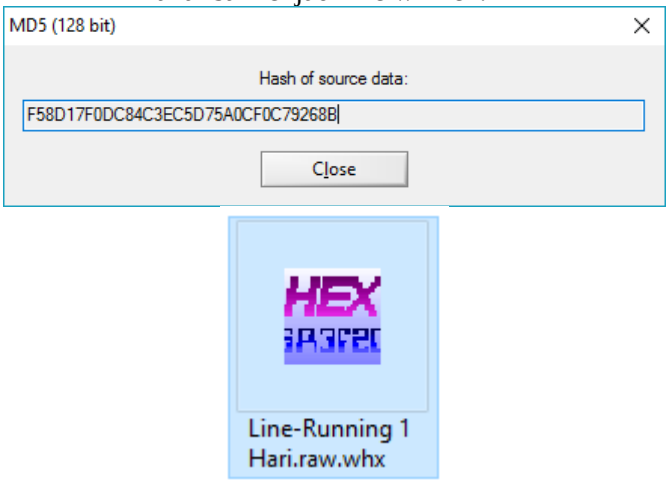
Gambar 5.29 Proses Backup Copy

e. Maka akan muncul pesan seperti berikut.



Gambar 5.30 Pesan proses Backup copy berhasil

f. Menggunakan Hash of source data yang nantinya akan digunakan untuk membuka file analisa menjadi file winhex.



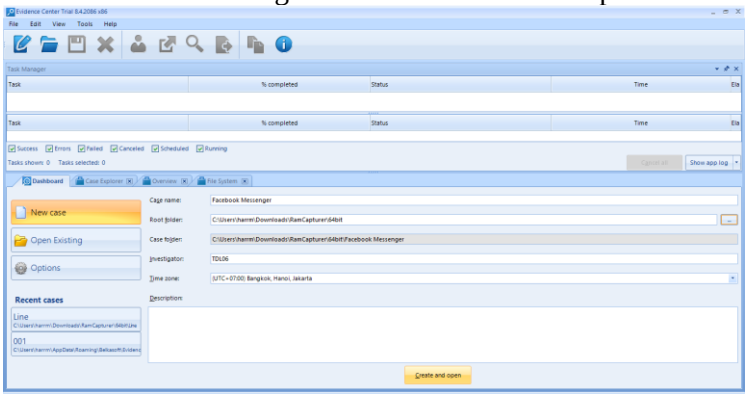
Gambar 5.31 Hash dan hasil Backup Copy

5.3.2. Belkasoft Evidence Center

Belkasoft Evidence Center merupakan aplikasi untuk membuka dan membaca isi data dari RAM, Aplikasi yang nantinya akan mengeluarkan atau mendapatkan beberapa barang bukti digital dari hasil analisa yang dilakukan.

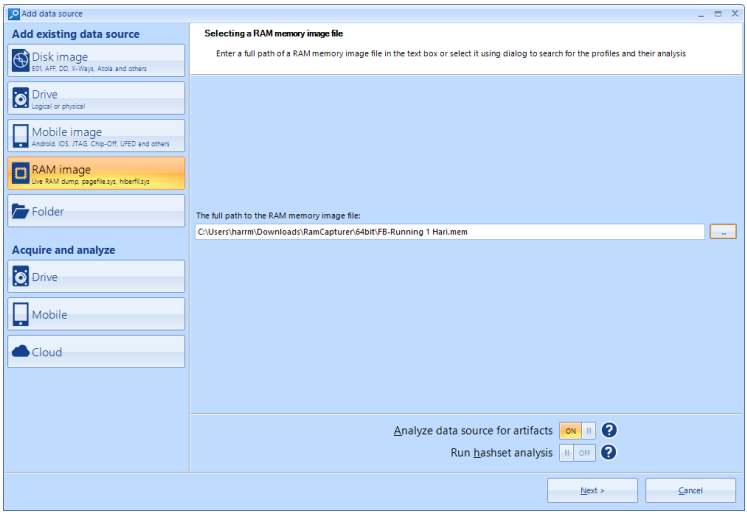
Berikut merupakan langkah untuk menganalisa data menggunakan aplikasi Belkasoft Evidence Center.

1. Membuat New Case untuk mempermudah dalam menganalisa kembali. Berikut cara membuat Case baru.
   a. Klik new case, isikan nama case sesuai dengan aplikasi yang akan dianalisa, pilih file destinasi untuk menyimpan case, isikan nama investigator dan klik Create dan Open.



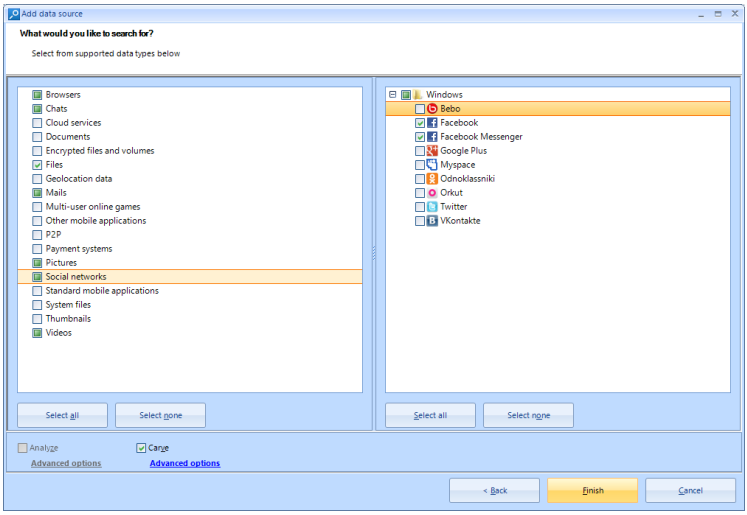
Gambar 5.32 Membuat New Case

2. Pilih fitur RAM Image pada add existing data source dan pilih file yang akan dianalisa lalu klik next.



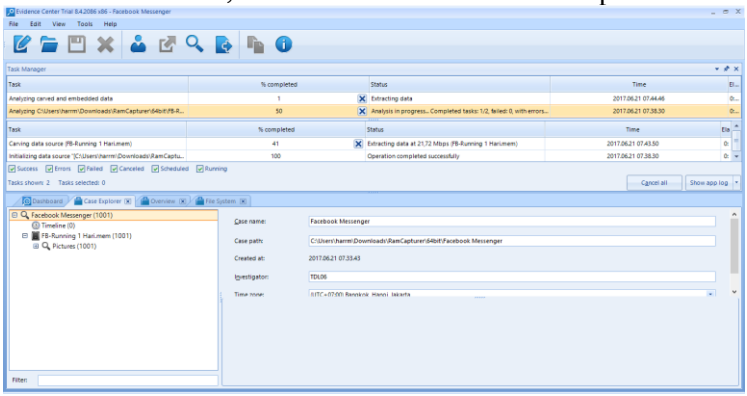
Gambar 5.33 Menentukan File Destinasi

3. Pilih Browser, Chats, Mails, Pictures, Social networks dan videos untuk menganalisa studi kasus sesuai dengan instant *messenger* yang diujikan, lalu klik finish.



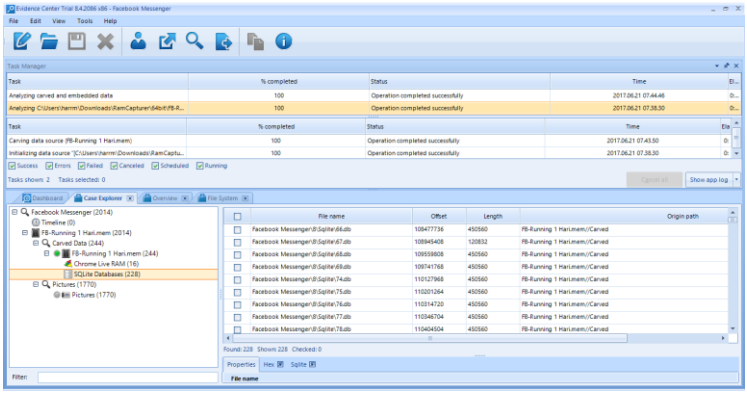
Gambar 5.34 Pemilihan Fitur Analisa

Tunggu proses analisa dan extracting data sampai selesai, ini akan memakan waktu cukup lama.



Gambar 5.35 Proses Analisa dan Extracting Data

Setelah proses selesai maka akan menampilkan hasil dari proses analisa dan extracting data sesuai dengan apa yang kita cari.



Gambar 5.36 Finishing Proses Analisa dan Extracting Data

5.4. Analisa Bukti Digital

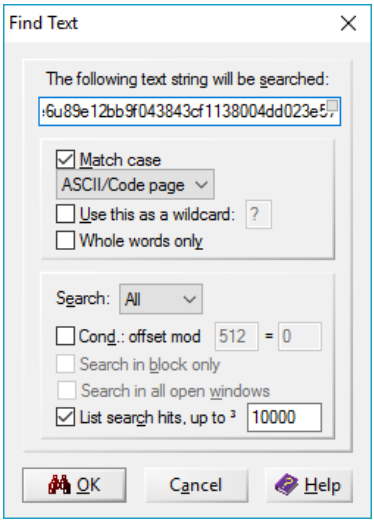
Setelah analisa data digital dilakukan, maka selanjutnya melakukan analisa bukti digital. Dalam penelitian ini, penulis menggunakan beberapa aplikasi forensik digital yaitu WinHex dan Belkasoft Evidence Center untuk menganalisa bukti digital dan membuka beberapa file terkait aplikasi instant *messenger* yang menjadi objek penelitian kali ini.

5.4.1. WinHex

Pada aplikasi winhex, dalam mengidentifikasi bukti digital untuk data primer percakapan, data pendukung dan media dibutuhkan spesifikasi yang dilakukan untuk menemukan bukti digital tersebut. Berikut ini merupakan langkah menemukan bukti digital menggunakan aplikasi winhex :

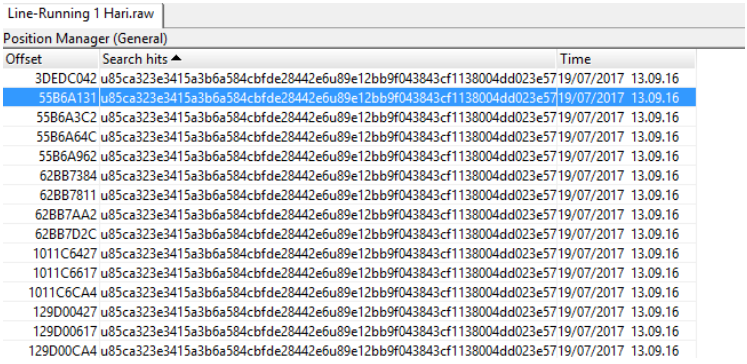
Pada data primer dan media untuk menganalisa barang bukti yang didapatkan pada winhex, maka masukkan userid dan senderid secara berurutan, lalu lakukan search seperti gambar 5.37, yang nantinya akan ditemukan semua yang berhubungan dengan userid dan

senderid, baik itu akan menemukan bentuk text, picture, audio, video dan sticker.



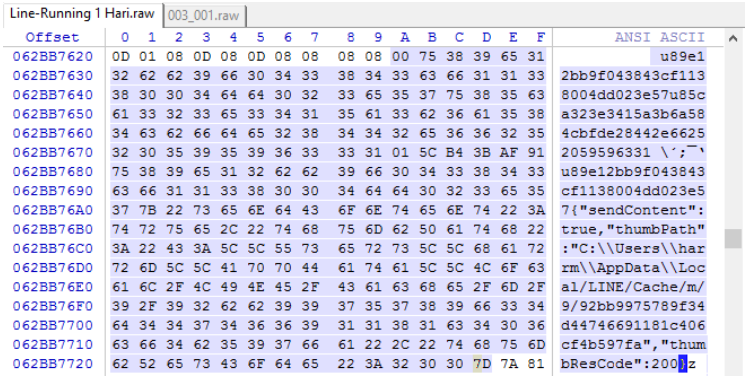
Gambar 5.37 Search box untuk userid dan senderid

Berikut ini merupakan hasil search yang nantinya akan dianalisa apakah termasuk bukti digital atau tidak.



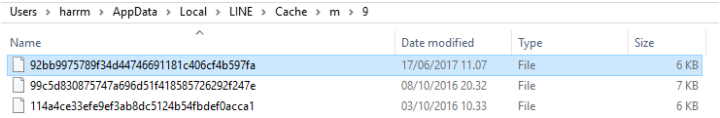
Gambar 5.38 Hasil Search pada winhex

Hasil search pada gambar 5.38, maka dilakukan sortir untuk mengetahui tipe data pada percakapan. Pada gambar 5.39 akan menunjukkan hasil salah satu media yaitu picture.



Gambar 5.39 Hasil winhex picture LINE Messenger

Setelah didapatkan path pada winhex, maka selanjutnya mengecek apakah data tersebut benar tidaknya sesuai dengan kasus. Pada gambar 5.40 berikut ini adalah contoh cache penyimpanan data media picture.



Gambar 5.40 *Cache* Penyimpanan Data

5.5. Hambatan dan Rintangan

Dalam implementasi ini, terdapat beberapa hambatan dan rintangan dalam melakukan eksperimen dan pengambilan data. Dalam melakukan eksperimen, penulis harus berhati-hati agar aplikasi tidak diperbaharui secara otomatis, baik untuk aplikasi instant *messenger* itu sendiri maupun sistem perangkat. Untuk aplikasi, penulis harus menjaga versi yang dipasang dikarenakan agar tidak mempengaruhi dalam analisa dan pengambilan keputusan dalam proses penelitian ini.

Penggunaan Skenario pada eksperimen sangat menentukan hasil akhir, karena penulis sempat menggunakan skenario yang dilakukan lebih dari 3 hari (penggunaan seperti pada skenario yang ditentukan sebelumnya) dan tidak mendapatkan bukti-bukti yang dibutuhkan pada saat proses analisa. Penggunaan tools yang tepat juga mempengaruhi jalannya proses dumping dan proses analisa data digital. Di sisi lain, pengambilan data digital juga harus dilakukan secara teliti. Hal ini dikarenakan penulis sempat terkecoh ketika menggunakan aplikasi tambahan untuk melakukan ekstraksi data yang sempat menemukan folder Facebook *messenger* dan LINE *Messenger* secara mudah, namun ternyata belum menyeluruh atau tidak terdeteksi. Hal ini mempengaruhi proses analisa selanjutnya dikarenakan pada filedi aplikasi telegram *messenger* dikenakan proses enkripsi dan hanya terdapat file media saja. Selain itu untuk folder LINE dan Facebook hanya berisi artefak-artefak yang tidak terlalu banyak dan tidak bisa dibaca.

“Halaman ini sengaja dikosongkan”

BAB VI
HASIL DAN ANALISA

Pada bab ini akan menjelaskan hasil yang didapatkan dari pelaksanaan skenario dan eksperimen yang telah dilakukan dan pembahasan analisa terhadap permasalahan yang ingin dijawab dalam penelitian ini.

Pada pembahasan terdapat empat macam analisa yang akan dibahas yaitu penelusuran sktruktur data, pembacaan jenis dan isi data, perbandingan hasil dan data yang didapatkan, dan diakhiri dengan penilaian dari sekuritas terbaik pada aplikasi instant *messenger*.

6.1 Ketersediaan Data Digital

Bagian ini akan menjelaskan tentang data digital yang tersedia pasca proses pengambilan data digital dari perangkat berbeda dengan menggunakan metode manual dan aplikasi tambahan. Berikut merupakan hasil ketersediaan data digital yang diambil pada setiap eksperimen yang dilakukan

6.1.1. Hasil Data Eksperimen 1

Eksperimen pertama dilakukan dengan menggunakan kondisi normal. Tabel 6.1 berikut merupakan hasil eksperimen pertama yang berhasil didapatkan pada proses pengambilan data digital :

Tabel 6.1 Hasil Data Eksperimen 1

Tools/ Perangkat	**Facebook *Messenger***	**LINE *Messenger***	**Telegram *Messenger***
Winhex	Data yang didapatkan Lengkap	Data yang didapatkan Lengkap	Data yang didapatkan Tidak Lengkap

Tools/ Perangkat	Facebook *Messenger*	LINE *Messenger*	Telegram *Messenger*
Belkasoft Evidence	Hanya data Media	Hanya data Media	Hanya data Media

Penjelasan

Pada Tabel 6.1 merupakan Eksperimen pertama yang berupa aktivitas penggunaan aplikasi dengan kondisi normal, tanpa ada modifikasi penggunaan maupun penanganan terhadap aplikasi. Oleh karena itu, penulis mendapatkan semua file yang dibutuhkan dengan lengkap yaitu data struktur pesan, pesan percakapan, data-data yang didapatkan seperti media, khususnya pada pengambilan data digital melalui tools winhex. Pada tools belkasoft evidence hanya mendapatkan data media seperti picture, video dan audio.

6.1.2. Hasil Data Eksperimen 2

Eksperimen kedua dilakukan dengan menggunakan kondisi penghapusan percakapan. Tabel 6.2 berikut merupakan hasil eksperimen kedua yang berhasil didapatkan pada proses pengambilan data digital :

Tabel 6.2 Hasil Data Eksperimen 2

Tools/ Perangkat	Facebook *Messenger*	LINE *Messenger*	Telegram *Messenger*
Winhex	Data yang didapatkan Lengkap	Data yang didapatkan Lengkap	Data yang didapatkan Tidak Lengkap
Belkasoft Evidence	Hanya data media	Hanya data media	Hanya data media

Penjelasan

Pada Tabel 6.2 merupakan Eksperimen kedua yang berupa aktivitas penggunaan aplikasi dengan modifikasi terhadap isi aplikasi, yaitu penghapusan pesan/percakapan yang melibatkan skenario percakapan. Penghapusan pesan/percakapan tidak memberikan efek kepada data aplikasi sehingga jumlah data yang dapat diambil tidak jauh berbeda dengan eksperimen pertama. Dengan tools winhex, penulis mendapatkan semua file yang dibutuhkan dengan lengkap yaitu data struktur pesan, pesan percakapan, data-data yang didapatkan seperti media picture, video, audio dan sticker. Akan tetapi, karena adanya proses penghapusan percakapan beberapa data percakapan ganda ditemukan. Sama seperti eksperimen 1, pada tools belkasoft evidence hanya mendapatkan data pendukung seperti media picture, video dan audio.

6.2 Analisa Data Digital

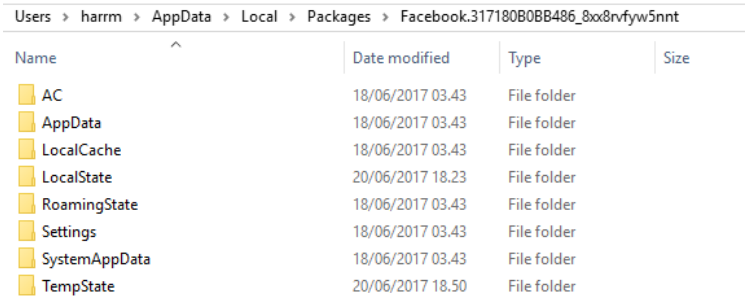
Bagian ini menjelaskan tentang struktur dari data digital yang telah didapatkan pada proses pengambilan data digital.

6.2.1 Lokasi Data pada Perangkat

Bagian ini akan menjelaskan lokasi data aplikasi yang terdapat pada perangkat Personal Computer (PC). Berikut merupakan penjelasan pada masing-masing aplikasi:

6.2.1.1 Lokasi Folder Facebook *Messenger*:

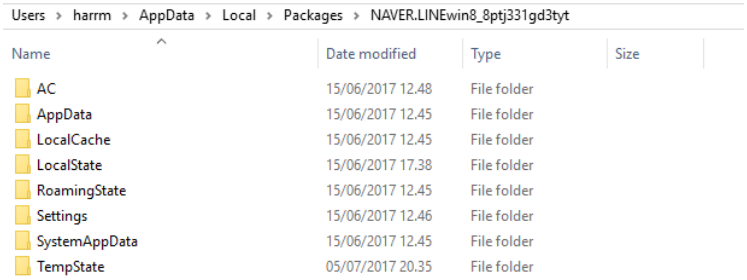
Pada aplikasi Facebook *Messenger* terdapat folder-folder yang terekam pada folder aplikasi, pada gambar 6.1 menggambarkan folder-folder yang terdapat pada aplikasi. Pada penelitian yang dilakukan hanya menggunakan folder LocalSlate untuk melihat data-data yang dibutuhkan untuk penelitian.



Gambar 6.1 Lokasi Folder Facebook *Messenger*

6.2.1.2 Lokasi Folder LINE *Messenger*:

Pada aplikasi LINE *Messenger* terdapat folder-folder yang terekam pada folder aplikasi, pada gambar 6.2 menggambarkan folder-folder yang terdapat pada aplikasi. Pada penelitian yang dilakukan hanya menggunakan folder LocalSlate untuk melihat data-data yang dibutuhkan untuk penelitian.

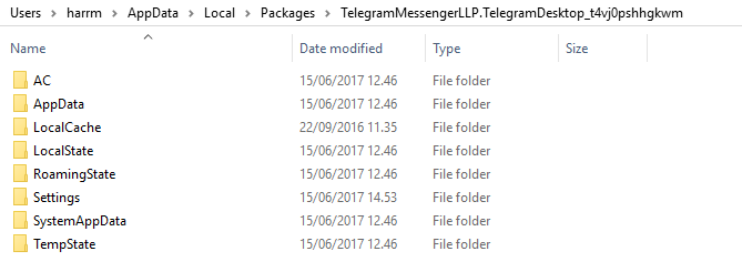


Gambar 6.2 Lokasi Folder LINE *Messenger*

6.2.1.3 Lokasi Folder Telegram *Messenger*:

Pada aplikasi Telegram *Messenger* terdapat folder-folder yang terekam pada folder aplikasi, pada gambar 6.3 menggambarkan folder-folder yang terdapat pada aplikasi. Pada penelitian yang

dilakukan hanya menggunakan folder LocalSlate untuk melihat data-data yang dibutuhkan untuk penelitian.



Gambar 6.3 Lokasi Folder Telegram *Messenger*

6.2.2 Struktur Pesan

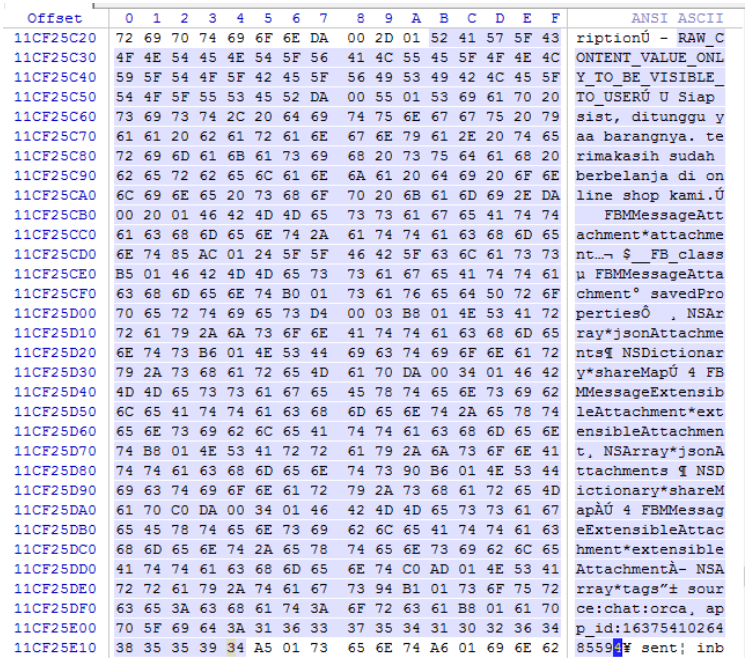
Pada penelitian ini, struktur pesan merupakan data-data yang didapatkan dari pengerjaan sebelumnya yang nantinya akan dianalisa apakah terdapat bukti digital yang dibutuhkan atau tidak. Struktur pesan yang dihasilkan dari setiap aplikasi berbeda, berikut ini penjelasan struktur pesan dari setiap aplikasi:

6.2.2.1 Struktur Pesan Facebook *Messenger*:

Pada Struktur Pesan aplikasi Facebook *Messenger* terdiri dari struktur dan tipe data yang berbeda, terdiri dari pengambilan sample dari text, picture, video, audio dan sticker untuk mendapatkan bukti digital. Berikut ini penjelasan dari setiap sample yang ada:

Text

Pada Facebook *Messenger*, melalui tools winhex mendapatkan bukti digital Text dalam bentuk hexadecimal pada gambar 6.4 yang menjelaskan bagaimana struktur pesan facebook *messenger* yang terdapat pada gambar 6.5.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
11CF25C20	72	69	70	74	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	riptionÚ - RAW_C
11CF25C30	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	ONTENT_VALUE_ONL
11CF25C40	59	5F	54	4F	5F	42	45	5F	56	49	53	49	42	4C	45	5F	Y_TO_BE_VISIBLE_
11CF25C50	54	4F	5F	55	53	45	52	DA	00	55	01	53	69	61	70	20	TO_USERÚ U Siap
11CF25C60	73	69	73	74	2C	20	64	69	74	75	6E	67	67	75	20	79	sist, ditunggu y
11CF25C70	61	61	20	62	61	72	61	6E	67	6E	79	61	2E	20	74	65	aa barangnya. te
11CF25C80	72	69	6D	61	6B	61	73	69	68	20	73	75	64	61	68	20	rimakasih sudah
11CF25C90	62	65	72	62	65	6C	61	6E	6A	61	20	64	69	20	6F	6E	berbelanja di on
11CF25CA0	6C	69	6E	65	20	73	68	6F	70	20	6B	61	6D	69	2E	DA	line shop kami.Ú
11CF25CB0	00	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	FBMMessageAtt
11CF25CC0	61	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	65	achment*attachme
11CF25CD0	6E	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	nt…¬ $__FB_class
11CF25CE0	B5	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	µ FBMMessageAtta
11CF25CF0	63	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	6F	chment° savedPro
11CF25D00	70	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	72	pertiesÔ ¸ NSAr
11CF25D10	72	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	ray*jsonAttachme
11CF25D20	6E	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	nts¶ NSDictionar
11CF25D30	79	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	42	y*shareMapÚ 4 FB
11CF25D40	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	MMessageExtensib
11CF25D50	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	leAttachment*ext
11CF25D60	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	ensibleAttachmen
11CF25D70	74	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	t¸ NSArray*jsonA
11CF25D80	74	74	61	63	68	6D	65	6E	74	73	90	B6	01	4E	53	44	ttachments ¶ NSD
11CF25D90	69	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	ictionary*shareM
11CF25DA0	61	70	C0	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	apÀÚ 4 FBMMessag
11CF25DB0	65	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	eExtensibleAttac
11CF25DC0	68	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	hment*extensible
11CF25DD0	41	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	41	AttachmentÀ- NSA
11CF25DE0	72	72	61	79	2A	74	61	67	73	94	B1	01	73	6F	75	72	rray*tags”± sour
11CF25DF0	63	65	3A	63	68	61	74	3A	6F	72	63	61	B8	01	61	70	ce:chat:orca¸ ap
11CF25E00	70	5F	69	64	3A	31	36	33	37	35	34	31	30	32	36	34	p_id:16375410264
11CF25E10	38	35	35	39	34	A5	01	73	65	6E	74	A6	01	69	6E	62	85594¥ sent¦ inb

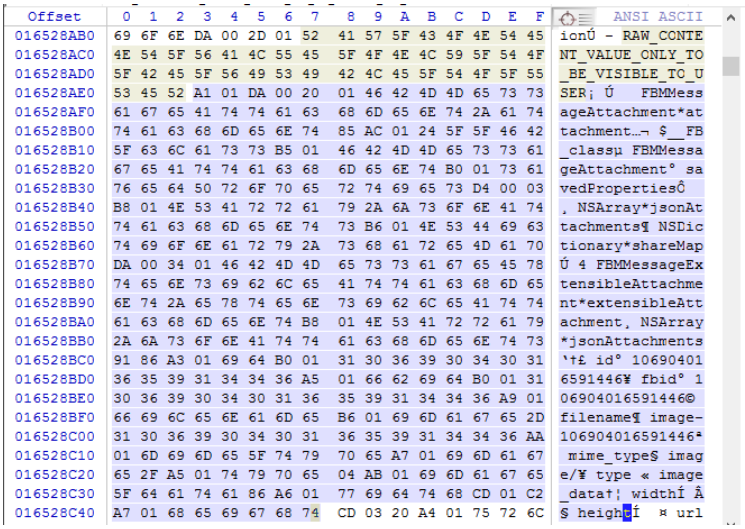
Gambar 6.4 Hasil winhex Text Facebook *Messenger*

Gambar 6.5 Struktur Pesan Text Facebook *Messenger*

Struktur pesan Text pada Facebook *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe pada struktur pesan akan dijelaskan pada analisa data percakapan.

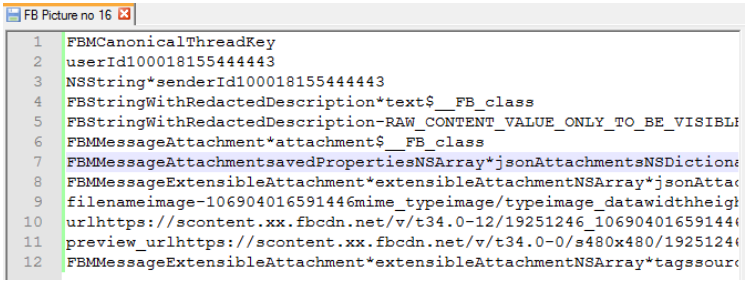
Picture

Pada Facebook *Messenger*, melalui tools winhex mendapatkan bukti digital Picture dalam bentuk hexadecimal pada gambar 6.6 yang menjelaskan bagaimana struktur pesan facebook *messenger* yang terdapat pada gambar 6.7.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
016528AB0	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	4F	4E	54	45	ionÚ - RAW_CONTE
016528AC0	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	NT_VALUE_ONLY_TO
016528AD0	5F	42	45	5F	56	49	53	49	42	4C	45	5F	54	4F	5F	55	_BE_VISIBLE_TO_U
016528AE0	53	45	52	A1	01	DA	00	20	01	46	42	4D	4D	65	73	73	SER¡ Ú FBMMess
016528AF0	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	74	ageAttachment*at
016528B00	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	42	tachment…¬ $__FB
016528B10	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	61	_classµ FBMMessa
016528B20	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	61	geAttachment° sa
016528B30	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	00	03	vedPropertiesÔ
016528B40	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	¸ NSArray*jsonAt
016528B50	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	63	tachments¶ NSDic
016528B60	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	70	tionary*shareMap
016528B70	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	45	78	Ú 4 FBMMessageEx
016528B80	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	tensibleAttachme
016528B90	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	74	nt*extensibleAtt
016528BA0	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	79	achment¸ NSArray
016528BB0	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	73	*jsonAttachments
016528BC0	91	86	A3	01	69	64	B0	01	31	30	36	39	30	34	30	31	‘†£ id° 10690401
016528BD0	36	35	39	31	34	34	36	A5	01	66	62	69	64	B0	01	31	6591446¥ fbid° 1
016528BE0	30	36	39	30	34	30	31	36	35	39	31	34	34	36	A9	01	069040165914469©
016528BF0	66	69	6C	65	6E	61	6D	65	B6	01	69	6D	61	67	65	2D	filename¶ image-
016528C00	31	30	36	39	30	34	30	31	36	35	39	31	34	34	36	AA	1069040165914468
016528C10	01	6D	69	6D	65	5F	74	79	70	65	A7	01	69	6D	61	67	mime_type§ imag
016528C20	65	2F	A5	01	74	79	70	65	04	AB	01	69	6D	61	67	65	e/¥ type « image
016528C30	5F	64	61	74	61	86	A6	01	77	69	64	74	68	CD	01	C2	_data† widthÍ Â
016528C40	A7	01	68	65	69	67	68	74	CD	03	20	A4	01	75	72	6C	§ heightÍ ¤ url

Gambar 6.6 Hasil Winhex Picture Facebook *Messenger*



FB Picture no 16

```
1  FBMCanonicalThreadKey
2  userId100018155444443
3  NSString*senderId100018155444443
4  FBStringWithRedactedDescription*text$__FB_class
5  FBStringWithRedactedDescription-RAW_CONTENT_VALUE_ONLY_TO_BE_VISIBL
6  FBMMessageAttachment*attachment$__FB_class
7  FBMMessageAttachmentsavedPropertiesNSArray*jsonAttachmentsNSDictiona
8  FBMMessageExtensibleAttachment*extensibleAttachmentNSArray*jsonAtta
9  filenameimage-106904016591446mime_typeimage/typeimage_datawidthheigh
10 urlhttps://scontent.xx.fbcdn.net/v/t34.0-12/19251246_106904016591446
11 preview_urlhttps://scontent.xx.fbcdn.net/v/t34.0-0/s480x480/1925124
12 FBMMessageExtensibleAttachment*extensibleAttachmentNSArray*tagssourc
```

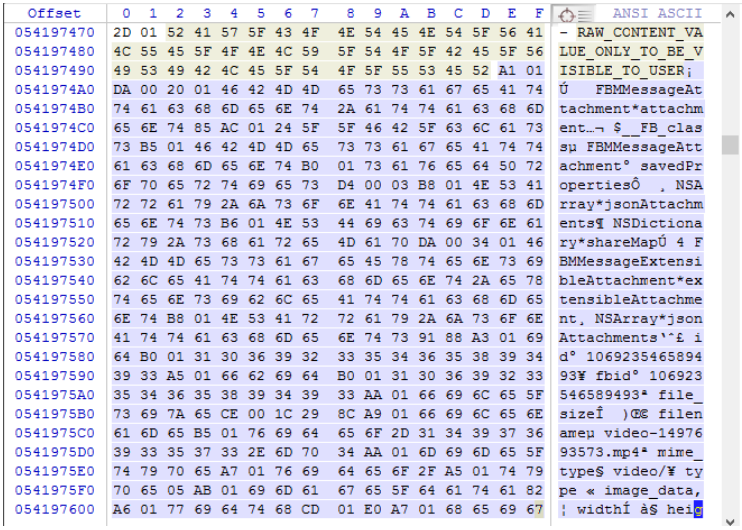
Gambar 6.7 Struktur Pesan Picture Facebook *Messenger*

Struktur pesan Picture pada Facebook *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe

pada struktur pesan akan dijelaskan pada analisa data percakapan.

Video

Pada Facebook *Messenger*, melalui tools winhex mendapatkan bukti digital Video dalam bentuk hexadecimal pada gambar 6.8 yang menjelaskan bagaimana struktur pesan facebook *messenger* yang terdapat pada gambar 6.9.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
054197470	2D	01	52	41	57	5F	43	4F	4E	54	45	4E	54	5F	56	41	- RAW_CONTENT_VA
054197480	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	5F	42	45	5F	56	LUE_ONLY_TO_BE_V
054197490	49	53	49	42	4C	45	5F	54	4F	5F	55	53	45	52	A1	01	ISIBLE_TO_USER¡
0541974A0	DA	00	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	Ú FBMMessageAt
0541974B0	74	61	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	tachment*attachm
0541974C0	65	6E	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	ent…¬ $__FB_clas
0541974D0	73	B5	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	sµ FBMMessageAtt
0541974E0	61	63	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	achment° savedPr
0541974F0	6F	70	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	opertiesÔ ¸ NSA
054197500	72	72	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	rray*jsonAttachm
054197510	65	6E	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	ents¶ NSDictiona
054197520	72	79	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	ry*shareMapÚ 4 F
054197530	42	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	BMMessageExtensi
054197540	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	bleAttachment*ex
054197550	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	tensibleAttachme
054197560	6E	74	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	nt¸ NSArray*json
054197570	41	74	74	61	63	68	6D	65	6E	74	73	91	88	A3	01	69	Attachments‘^£ i
054197580	64	B0	01	31	30	36	39	32	33	35	34	36	35	38	39	34	d° 1069235465894
054197590	39	33	A5	01	66	62	69	64	B0	01	31	30	36	39	32	33	93¥ fbid° 106923
0541975A0	35	34	36	35	38	39	34	39	33	AA	01	66	69	6C	65	5F	546589493ª file_
0541975B0	73	69	7A	65	CE	00	1C	29	8C	A9	01	66	69	6C	65	6E	sizeÎ)Œ© filen
0541975C0	61	6D	65	B5	01	76	69	64	65	6F	2D	31	34	39	37	36	ameµ video-14976
0541975D0	39	33	35	37	33	2E	6D	70	34	AA	01	6D	69	6D	65	5F	93573.mp4ª mime_
0541975E0	74	79	70	65	A7	01	76	69	64	65	6F	2F	A5	01	74	79	type§ video/¥ ty
0541975F0	70	65	05	AB	01	69	6D	61	67	65	5F	64	61	74	61	82	pe « image_data,
054197600	A6	01	77	69	64	74	68	CD	01	E0	A7	01	68	65	69	67	¦ widthÍ à§ heig

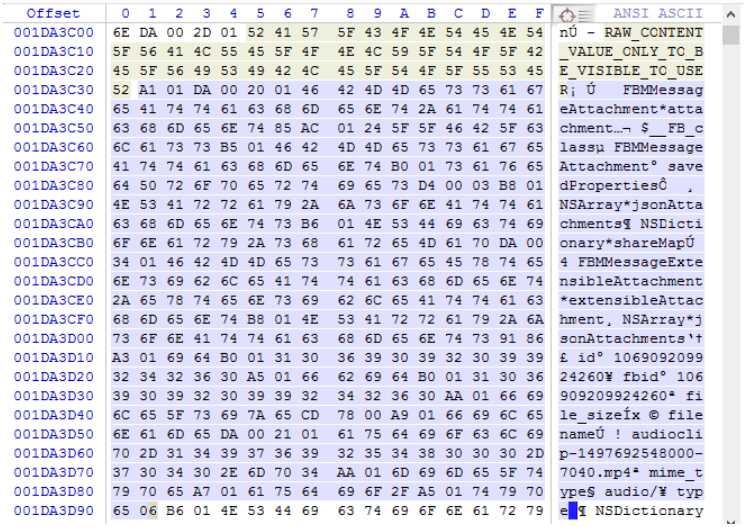
Gambar 6.8 Hasil Winhex Video Facebook *Messenger*

Gambar 6.9 Struktur Pesan Video Facebook *Messenger*

Struktur pesan Video pada Facebook *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe pada struktur pesan akan dijelaskan pada analisa data percakapan.

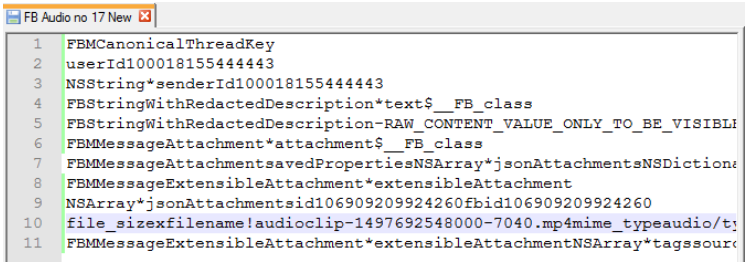
Audio

Pada Facebook *Messenger*, melalui tools winhex mendapatkan bukti digital Audio dalam bentuk hexadecimal pada gambar 6.10 yang menjelaskan bagaimana struktur pesan facebook *messenger* yang terdapat pada gambar 6.11.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
001DA3C00	6E	DA	00	2D	01	52	41	57	5F	43	4F	4E	54	45	4E	54	nÚ - RAW_CONTENT
001DA3C10	5F	56	41	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	5F	42	_VALUE_ONLY_TO_B
001DA3C20	45	5F	56	49	53	49	42	4C	45	5F	54	4F	5F	55	53	45	E_VISIBLE_TO_USE
001DA3C30	52	A1	01	DA	00	20	01	46	42	4D	4D	65	73	73	61	67	R¡ Ú FBMMessag
001DA3C40	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	74	74	61	eAttachment*atta
001DA3C50	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	42	5F	63	chment…¬ $__FB_c
001DA3C60	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	61	67	65	lassµ FBMMessage
001DA3C70	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	61	76	65	Attachment° save
001DA3C80	64	50	72	6F	70	65	72	74	69	65	73	D4	00	03	B8	01	dPropertiesÔ ¸
001DA3C90	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	74	61	NSArray*jsonAtta
001DA3CA0	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	63	74	69	chments¶ NSDicti
001DA3CB0	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	70	DA	00	onary*shareMapÚ
001DA3CC0	34	01	46	42	4D	4D	65	73	73	61	67	65	45	78	74	65	4 FBMMessageExte
001DA3CD0	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	nsibleAttachment
001DA3CE0	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	*extensibleAttac
001DA3CF0	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	79	2A	6A	hment¸ NSArray*j
001DA3D00	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	73	91	86	sonAttachments‘†
001DA3D10	A3	01	69	64	B0	01	31	30	36	39	30	39	32	30	39	39	£ id° 1069092099
001DA3D20	32	34	32	36	30	A5	01	66	62	69	64	B0	01	31	30	36	24260¥ fbid° 106
001DA3D30	39	30	39	32	30	39	39	32	34	32	36	30	AA	01	66	69	909209924260ª fi
001DA3D40	6C	65	5F	73	69	7A	65	CD	78	00	A9	01	66	69	6C	65	le_sizeÍx © file
001DA3D50	6E	61	6D	65	DA	00	21	01	61	75	64	69	6F	63	6C	69	nameÚ ! audiocli
001DA3D60	70	2D	31	34	39	37	36	39	32	35	34	38	30	30	30	2D	p-1497692548000-
001DA3D70	37	30	34	30	2E	6D	70	34	AA	01	6D	69	6D	65	5F	74	7040.mp4ª mime_t
001DA3D80	79	70	65	A7	01	61	75	64	69	6F	2F	A5	01	74	79	70	ype§ audio/¥ typ
001DA3D90	65	06	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	e¶ NSDictionary

Gambar 6.10 Hasil Winhex Audio Facebook *Messenger*



FB Audio no 17 New

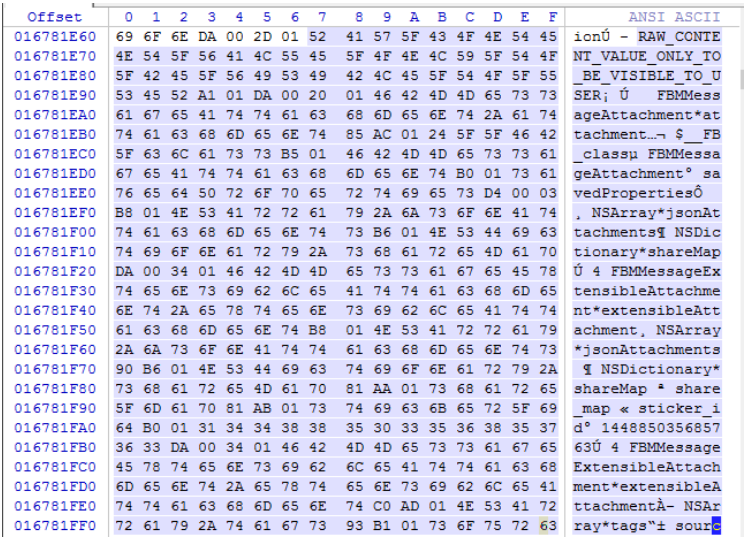
```
1  FBMCanonicalThreadKey
2  userId100018155444443
3  NSString*senderId100018155444443
4  FBStringWithRedactedDescription*text$__FB_class
5  FBStringWithRedactedDescription-RAW_CONTENT_VALUE_ONLY_TO_BE_VISIBLE
6  FBMMessageAttachment*attachment$__FB_class
7  FBMMessageAttachmentsavedPropertiesNSArray*jsonAttachmentsNSDictiona
8  FBMMessageExtensibleAttachment*extensibleAttachment
9  NSArray*jsonAttachmentsid106909209924260fbid106909209924260
10 file_sizexfilename!audioclip-1497692548000-7040.mp4mime_typeaudio/ty
11 FBMMessageExtensibleAttachment*extensibleAttachmentNSArray*tagssourc
```

Gambar 6.11 Struktur Pesan Audio Facebook *Messenger*

Struktur pesan Audio pada Facebook *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe pada struktur pesan akan dijelaskan pada analisa data percakapan.

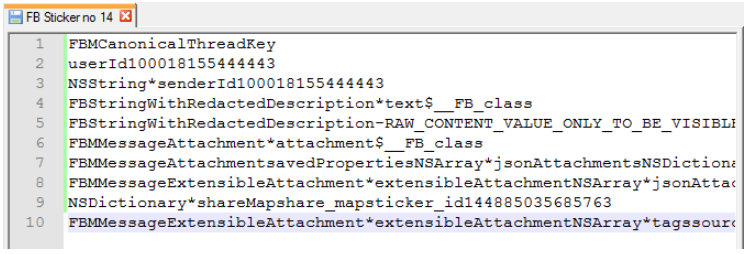
Sticker

Pada Facebook *Messenger*, melalui tools winhex mendapatkan bukti digital Sticker dalam bentuk hexadecimal pada gambar 6.12 yang menjelaskan bagaimana struktur pesan facebook *messenger* yang terdapat pada gambar 6.13.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
016781E60	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	4F	4E	54	45	ionÚ - RAW_CONTE
016781E70	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	NT_VALUE_ONLY_TO
016781E80	5F	42	45	5F	56	49	53	49	42	4C	45	5F	54	4F	5F	55	_BE_VISIBLE_TO_U
016781E90	53	45	52	A1	01	DA	00	20	01	46	42	4D	4D	65	73	73	SER¡ Ú FBMMess
016781EA0	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	74	ageAttachment*at
016781EB0	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	42	tachment…¬ $__FB
016781EC0	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	61	_classµ FBMMessa
016781ED0	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	61	geAttachment° sa
016781EE0	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	00	03	vedPropertiesÔ
016781EF0	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	¸ NSArray*jsonAt
016781F00	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	63	tachments¶ NSDic
016781F10	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	70	tionary*shareMap
016781F20	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	45	78	Ú 4 FBMMessageEx
016781F30	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	tensibleAttachme
016781F40	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	74	nt*extensibleAtt
016781F50	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	79	achment¸ NSArray
016781F60	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	73	*jsonAttachments
016781F70	90	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	2A	¶ NSDictionary*
016781F80	73	68	61	72	65	4D	61	70	81	AA	01	73	68	61	72	65	shareMap ª share
016781F90	5F	6D	61	70	81	AB	01	73	74	69	63	6B	65	72	5F	69	_map « sticker_i
016781FA0	64	B0	01	31	34	34	38	38	35	30	33	35	36	38	35	37	d° 1448850356857
016781FB0	36	33	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	63Ú 4 FBMMessage
016781FC0	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	ExtensibleAttach
016781FD0	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	ment*extensibleA
016781FE0	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	41	72	ttachmentÀ- NSAr
016781FF0	72	61	79	2A	74	61	67	73	93	B1	01	73	6F	75	72	63	ray*tags"± sourc

Gambar 6.12 Hasil Winhex Sticker Facebook *Messenger*



FB Sticker no 14

```
1  FBMCanonicalThreadKey
2  userId100018155444443
3  NSString*senderId100018155444443
4  FBStringWithRedactedDescription*text$__FB_class
5  FBStringWithRedactedDescription-RAW_CONTENT_VALUE_ONLY_TO_BE_VISIBLI
6  FBMMessageAttachment*attachment$__FB_class
7  FBMMessageAttachmentsavedPropertiesNSArray*jsonAttachmentsNSDictiona
8  FBMMessageExtensibleAttachment*extensibleAttachmentNSArray*jsonAtta
9  NSDictionary*shareMapshare_mapsticker_id144885035685763
10 FBMMessageExtensibleAttachment*extensibleAttachmentNSArray*tagssourc
```

Gambar 6.13 Struktur Pesan Sticker Facebook *Messenger*

Struktur pesan Sticker pada Facebook *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe pada struktur pesan akan dijelaskan pada analisa data percakapan.

6.2.2.2 Struktur Pesan LINE *Messenger*:

Pada Struktur Pesan aplikasi LINE *Messenger* terdiri dari struktur dan tipe data yang berbeda, terdiri dari pengambilan sample dari text, picture, video, audio dan sticker untuk mendapatkan bukti digital. Berikut ini penjelasan dari setiap sample yang ada:

Text

Pada LINE *Messenger*, melalui tools winhex mendapatkan bukti digital Text dalam bentuk hexadecimal pada gambar 6.14 yang menjelaskan bagaimana struktur pesan LINE *messenger* yang terdapat pada gambar 6.15.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
092A870B0	30	34	64	64	30	32	33	65	35	37	7B	22	66	72	6F	6D	04dd023e57{"from
092A870C0	22	3A	22	75	38	35	63	61	33	32	33	65	33	34	31	35	":"u85ca323e3415
092A870D0	61	33	62	36	61	35	38	34	63	62	66	64	65	32	38	34	a3b6a584cbfde284
092A870E0	34	32	65	36	22	2C	22	74	6F	22	3A	22	75	38	39	65	42e6","to":"u89e
092A870F0	31	32	62	62	39	66	30	34	33	38	34	33	63	66	31	31	12bb9f043843cf11
092A87100	33	38	30	30	34	64	64	30	32	33	65	35	37	22	2C	22	38004dd023e57","
092A87110	74	6F	54	79	70	65	22	3A	30	2C	22	69	64	22	3A	22	toType":0,"id":"
092A87120	36	32	35	32	31	39	37	32	35	31	34	31	30	22	2C	22	6252197251410","
092A87130	63	72	65	61	74	65	64	54	69	6D	65	22	3A	31	34	39	createdTime":149
092A87140	37	36	37	34	35	31	32	30	37	39	2C	22	64	65	6C	69	7674512079,"deli
092A87150	76	65	72	65	64	54	69	6D	65	22	3A	30	2C	22	74	65	veredTime":0,"te
092A87160	78	74	22	3A	22	53	69	61	70	20	73	69	73	74	2C	20	xt":"Siap sist,
092A87170	64	69	74	75	6E	67	67	75	20	79	61	61	20	62	61	72	ditunggu yaa bar
092A87180	61	6E	67	6E	79	61	2E	20	54	65	72	69	6D	61	6B	61	angnya. Terimaka
092A87190	73	69	68	20	73	75	64	61	68	20	62	65	72	62	65	6C	sih sudah berbel
092A871A0	61	6E	6A	61	20	64	69	20	6F	6E	6C	69	6E	65	20	73	anja di online s
092A871B0	68	6F	70	70	69	6E	67	20	6B	61	6D	69	2E	22	2C	22	hopping kami.","
092A871C0	68	61	73	43	6F	6E	74	65	6E	74	22	3A	66	61	6C	73	hasContent":fals
092A871D0	65	2C	22	63	6F	6E	74	65	6E	74	54	79	70	65	22	3A	e,"contentType":
092A871E0	30	2C	22	63	6F	6E	74	65	6E	74	4D	65	74	61	64	61	0,"contentMetada
092A871F0	74	61	22	3A	7B	7D	2C	22	73	65	73	73	69	6F	6E	49	ta":{},"sessionI
092A87200	64	22	3A	30	2C	22	6C	6F	63	61	74	69	6F	6E	22	3A	d":0,"location":
092A87210	7B	7D	2C	22	63	68	75	6E	6B	73	22	3A	5B	5D	2C	22	{},"chunks":[],"
092A87220	74	79	70	65	22	3A	31	2C	22	73	74	61	74	75	73	22	type":1,"status"
092A87230	3A	32	2C	22	63	68	61	74	49	64	22	3A	22	75	38	39	:2,"chatId":"u89
092A87240	65	31	32	62	62	39	66	30	34	33	38	34	33	63	66	31	e12bb9f043843cf1
092A87250	31	33	38	30	30	34	64	64	30	32	33	65	35	37	22	2C	138004dd023e57",

Gambar 6.14 Hasil Winhex Text LINE *Messenger*

Line Text no 15


```
{
"from":"u85ca323e3415a3b6a584cbfde28442e6",
"to":"u89e12bb9f043843cf1138004dd023e57",
"toType":0,
"id":"6252197251410",
"createdTime":1497674512079,
"deliveredTime":0,
"text":"Siap sist, ditunggu yaa barangnya.
Terimakasih sudah berbelanja di online shopping kami.",
"hasContent":false,
"contentType":0,
"contentMetadata":{},
"sessionId":0,
"location":{},
"chunks":[],
"type":1,
"status":2,
"chatId":"u89e12bb9f043843cf1138004dd023e57",
"readCount":0,
"reqSeqV2":5,
"reqSeq":0,
"contentInfo":{},
"eventInfo":{},
"rev":126,
"errorCode":0,
"urlPreview":{},
"hasUrlPreview":false,
"syncToken":"",
"fromType":0
}
```


Gambar 6.15 Struktur Pesan Text LINE *Messenger*

Struktur pesan Text pada LINE *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe pada struktur pesan akan dijelaskan pada analisa data percakapan.

Picture

Pada LINE *Messenger*, melalui tools winhex mendapatkan bukti digital Picture dalam bentuk hexadecimal pada gambar 6.16 yang menjelaskan bagaimana struktur pesan facebook *messenger* yang terdapat pada gambar 6.17.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
055B6A130	00	75	38	35	63	61	33	32	33	65	33	34	31	35	61	33	u85ca323e3415a3
055B6A140	62	36	61	35	38	34	63	62	66	64	65	32	38	34	34	32	b6a584cbfde28442
055B6A150	65	36	75	38	39	65	31	32	62	62	39	66	30	34	33	38	e6u89e12bb9f0438
055B6A160	34	33	63	66	31	31	33	38	30	30	34	64	64	30	32	33	43cf1138004dd023
055B6A170	65	35	37	36	32	35	32	30	32	35	37	30	36	32	35	32	e576252025706252
055B6A180	01	5C	B4	33	E4	FC	7B	22	4F	42	53	5F	43	4F	4E	54	\´3äü{"OBS_CONT
055B6A190	45	4E	54	5F	49	4E	46	4F	22	3A	22	7B	5C	22	63	61	ENT_INFO":"{\"ca
055B6A1A0	74	65	67	6F	72	79	5C	22	3A	5C	22	6F	72	69	67	69	tegory\":\"origi
055B6A1B0	6E	61	6C	5C	22	2C	5C	22	65	78	74	65	6E	73	69	6F	nal\",\"extensio
055B6A1C0	6E	5C	22	3A	5C	22	4A	50	45	47	5C	22	2C	5C	22	61	n\":\"JPEG\",\"a
055B6A1D0	6E	69	6D	61	74	65	64	5C	22	3A	66	61	6C	73	65	2C	nimated\":false,
055B6A1E0	5C	22	77	69	64	74	68	5C	22	3A	31	38	33	36	2C	5C	\"width\":1836,\
055B6A1F0	22	68	65	69	67	68	74	5C	22	3A	33	32	36	34	2C	5C	"height\":3264,\
055B6A200	22	66	69	6C	65	53	69	7A	65	5C	22	3A	37	38	33	34	"fileSize\":7834
055B6A210	32	39	7D	22	7D	02	75	38	39	65	31	32	62	62	39	66	29}"} u89e12bb9f
055B6A220	30	34	33	38	34	33	63	66	31	31	33	38	30	30	34	64	043843cf1138004d
055B6A230	64	30	32	33	65	35	37	04	7B	22	63	61	74	65	67	6F	d023e57 {"catego
055B6A240	72	79	22	3A	74	72	75	65	2C	22	66	69	6C	65	4E	61	ry":true,"fileNa
055B6A250	6D	65	22	3A	22	49	4D	47	5F	32	30	31	37	30	36	31	me":"IMG_2017061
055B6A260	36	5F	31	37	33	34	31	33	5F	33	30	32	2E	6A	70	67	6_173413_302.jpg
055B6A270	22	2C	22	70	61	74	68	22	3A	22	43	3A	5C	5C	55	73	","path":"C:\\Us
055B6A280	65	72	73	5C	5C	68	61	72	72	6D	5C	5C	41	70	70	44	ers\\harrm\\AppD
055B6A290	61	74	61	5C	5C	4C	6F	63	61	6C	5C	5C	4C	49	4E	45	ata\\Local\\LINE
055B6A2A0	5C	5C	43	61	63	68	65	5C	5C	74	6D	70	2F	66	36	34	\\Cache\\tmp/f64
055B6A2B0	38	63	62	61	32	2D	39	36	63	63	2D	34	36	33	37	2D	8cba2-96cc-4637-
055B6A2C0	62	31	31	63	2D	32	33	32	31	35	65	37	38	39	63	37	b11c-23215e789c7
055B6A2D0	30	2E	6A	70	67	22	2C	22	72	65	71	49	64	22	3A	22	0.jpg","reqId":"
055B6A2E0	6C	64	66	32	34	64	32	31	64	2D	30	64	38	31	2D	34	ldf24d21d-0d81-4
055B6A2F0	62	37	33	2D	39	32	33	34	2D	33	34	34	33	39	39	61	b73-9234-344399a
055B6A300	62	32	32	36	33	22	2C	22	73	65	6E	64	43	6F	6E	74	b2263","sendCont
055B6A310	65	6E	74	22	3A	74	72	75	65	2C	22	73	69	7A	65	22	ent":true,"size"
055B6A320	3A	37	38	33	34	32	39	2C	22	74	68	75	6D	62	50	61	:783429,"thumbPa
055B6A330	74	68	22	3A	22	43	3A	5C	5C	55	73	65	72	73	5C	5C	th":"C:\\Users\\
055B6A340	68	61	72	72	6D	5C	5C	41	70	70	44	61	74	61	5C	5C	harrm\\AppData\\
055B6A350	4C	6F	63	61	6C	2F	4C	49	4E	45	2F	43	61	63	68	65	Local/LINE/Cache

Gambar 6.16 Hasil Winhex Picture LINE *Messenger*

Line Picture no 10

```
u85ca323e3415a3b6a584cbfde28442e6
u89e12bb9f043843cf1138004dd023e57
6252025706252
{"OBS_CONTENT_INFO":"{\"category\":\"original\",
\"extension\":\"JPEG\",
\"animated\":false,
\"width\":1836,\"height\":3264,
\"fileSize\":783429}"}
u89e12bb9f043843cf1138004dd023e57
{
"category":true,
"fileName":"IMG_20170616_173413_302.jpg",
"path":"C:\\Users\\harrm\\AppData\\Local\\LINE\\Cache\\tmp/f648cba2-96cc-4637-b11c-23215e
"reqId":"ldf24d21d-0d81-4b73-9234-344399ab2263",
"sendContent":true,
"size":783429,
"thumbPath":"C:\\Users\\harrm\\AppData\\Local/LINE/Cache/m/b/bdceacf62cab92438e076a3bb777
"thumbResCode":200
}
```

Gambar 6.17 Struktur Pesan Picture LINE *Messenger*

Struktur pesan Picture pada LINE *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe pada struktur pesan akan dijelaskan pada analisa data percakapan

Video

Pada LINE *Messenger*, melalui tools winhex mendapatkan bukti digital Video dalam bentuk hexadecimal pada gambar 6.18 yang menjelaskan bagaimana struktur pesan facebook *messenger* yang terdapat pada gambar 6.19.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
129D002C0	02	08	0D	08	0D	08	08	08	08	00	75	38	39	65	31	32	u89e12
129D002D0	62	62	39	66	30	34	33	38	34	33	63	66	31	31	33	38	bb9f043843cf1138
129D002E0	30	30	34	64	64	30	32	33	65	35	37	75	38	35	63	61	004dd023e57u85ca
129D002F0	33	32	33	65	33	34	31	35	61	33	62	36	61	35	38	34	323e3415a3b6a584
129D00300	63	62	66	64	65	32	38	34	34	32	65	36	36	32	35	32	cbfde28442e66252
129D00310	36	33	34	39	31	33	38	38	36	01	5C	B4	C6	14	18	02	634913886 \´Æ
129D00320	7B	22	44	55	52	41	54	49	4F	4E	22	3A	22	39	33	35	{"DURATION":"935
129D00330	35	22	2C	22	4F	42	53	5F	50	4F	50	22	3A	22	62	22	5","OBS_POP":"b"
129D00340	2C	22	53	52	43	5F	53	56	43	5F	43	4F	44	45	22	3A	,"SRC_SVC_CODE":
129D00350	22	74	61	6C	6B	22	7D	75	38	39	65	31	32	62	62	39	"talk"}u89e12bb9
129D00360	66	30	34	33	38	34	33	63	66	31	31	33	38	30	30	34	f043843cf1138004
129D00370	64	64	30	32	33	65	35	37	7B	22	73	65	6E	64	43	6F	dd023e57{"sendCo
129D00380	6E	74	65	6E	74	22	3A	74	72	75	65	2C	22	74	68	75	ntent":true,"thu
129D00390	6D	62	52	65	73	43	6F	64	65	22	3A	32	30	30	2C	22	mbResCode":200,"
129D003A0	74	68	75	6D	62	50	61	74	68	22	3A	22	43	3A	5C	5C	thumbPath":"C:\\
129D003B0	55	73	65	72	73	5C	5C	68	61	72	72	6D	5C	5C	41	70	Users\\harrm\\Ap
129D003C0	70	44	61	74	61	5C	5C	4C	6F	63	61	6C	2F	4C	49	4E	pData\\Local/LIN
129D003D0	45	2F	43	61	63	68	65	2F	6D	2F	34	2F	35	30	34	66	E/Cache/m/4/504f
129D003E0	61	38	65	66	61	33	66	39	37	39	34	37	61	31	38	66	a8efa3f97947a18f
129D003F0	62	33	63	32	61	31	36	32	32	34	34	33	39	61	62	65	b3c2a16224439abe
129D00400	62	31	65	22	7D	00	95	81	4D	18	1D	4F	4F	08	27	05	b1e"} • M OO '

Gambar 6.18 Hasil Winhex Video LINE *Messenger*

Line Video no 25

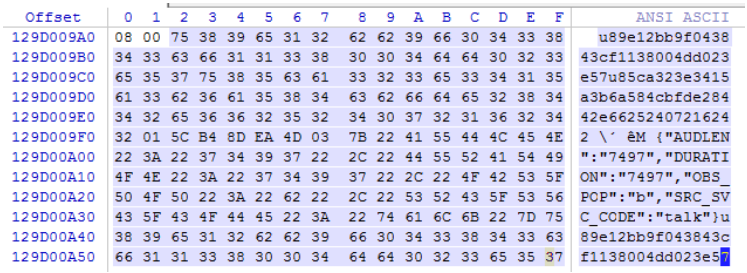
```
u89e12bb9f043843cf1138004dd023e57
u85ca323e3415a3b6a584cbfde28442e6
6252634913886
{
"DURATION":"9355",
"OBS_POP":"b",
"SRC_SVC_CODE":"talk"
}
u89e12bb9f043843cf1138004dd023e57
{
"sendContent":true,
"thumbResCode":200,
"thumbPath":"C:\\Users\\harrm\\AppData\\Local/LINE/Cache/m/4/504fa8efa3f97947a18fb3c2a16224
}
```

Gambar 6.19 Struktur Pesan Video LINE *Messenger*

Struktur pesan Video pada LINE *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe pada struktur pesan akan dijelaskan pada analisa data percakapan

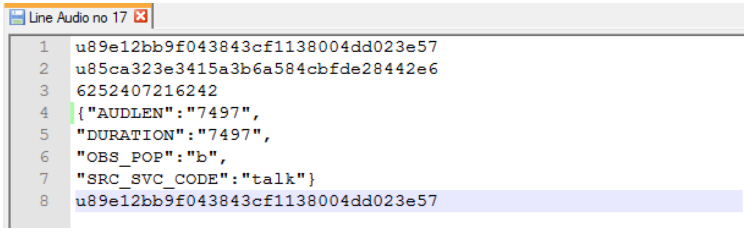
Audio

Pada LINE *Messenger*, melalui tools winhex mendapatkan bukti digital Audio dalam bentuk hexadecimal pada gambar 6.20 yang menjelaskan bagaimana struktur pesan facebook *messenger* yang terdapat pada gambar 6.21.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
129D009A0	08	00	75	38	39	65	31	32	62	62	39	66	30	34	33	38	u89e12bb9f0438
129D009B0	34	33	63	66	31	31	33	38	30	30	34	64	64	30	32	33	43cf1138004dd023
129D009C0	65	35	37	75	38	35	63	61	33	32	33	65	33	34	31	35	e57u85ca323e3415
129D009D0	61	33	62	36	61	35	38	34	63	62	66	64	65	32	38	34	a3b6a584cbfde284
129D009E0	34	32	65	36	36	32	35	32	34	30	37	32	31	36	32	34	42e6625240721624
129D009F0	32	01	5C	B4	8D	EA	4D	03	7B	22	41	55	44	4C	45	4E	2 \´ êM {"AUDLEN
129D00A00	22	3A	22	37	34	39	37	22	2C	22	44	55	52	41	54	49	":"7497","DURATI
129D00A10	4F	4E	22	3A	22	37	34	39	37	22	2C	22	4F	42	53	5F	ON":"7497","OBS_
129D00A20	50	4F	50	22	3A	22	62	22	2C	22	53	52	43	5F	53	56	POP":"b","SRC_SV
129D00A30	43	5F	43	4F	44	45	22	3A	22	74	61	6C	6B	22	7D	75	C_CODE":"talk"}u
129D00A40	38	39	65	31	32	62	62	39	66	30	34	33	38	34	33	63	89e12bb9f043843c
129D00A50	66	31	31	33	38	30	30	34	64	64	30	32	33	65	35	37	f1138004dd023e57

Gambar 6.20 Hasil Winhex Audio LINE *Messenger*



Line Audio no 17

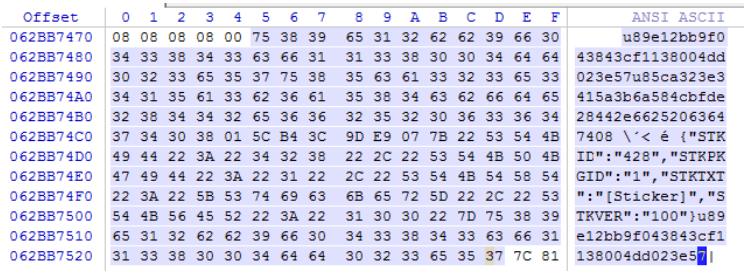
```
1  u89e12bb9f043843cf1138004dd023e57
2  u85ca323e3415a3b6a584cbfde28442e6
3  6252407216242
4  {"AUDLEN":"7497",
5  "DURATION":"7497",
6  "OBS_POP":"b",
7  "SRC_SVC_CODE":"talk"}
8  u89e12bb9f043843cf1138004dd023e57
```

Gambar 6.21 Struktur Pesan Audio LINE *Messenger*

Struktur pesan Audio pada LINE *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe pada struktur pesan akan dijelaskan pada analisa data percakapan

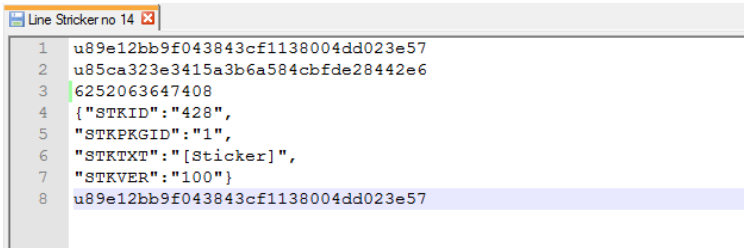
Sticker

Pada LINE *Messenger*, melalui tools winhex mendapatkan bukti digital Text dalam bentuk hexadecimal pada gambar 6.22 yang menjelaskan bagaimana struktur pesan facebook *messenger* yang terdapat pada gambar 6.23.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
062BB7470	08	08	08	08	00	75	38	39	65	31	32	62	62	39	66	30	u89e12bb9f0
062BB7480	34	33	38	34	33	63	66	31	31	33	38	30	30	34	64	64	43843cf1138004dd
062BB7490	30	32	33	65	35	37	75	38	35	63	61	33	32	33	65	33	023e57u85ca323e3
062BB74A0	34	31	35	61	33	62	36	61	35	38	34	63	62	66	64	65	415a3b6a584cbfde
062BB74B0	32	38	34	34	32	65	36	36	32	35	32	30	36	33	36	34	28442e6625206364
062BB74C0	37	34	30	38	01	5C	B4	3C	9D	E9	07	7B	22	53	54	4B	7408 \´< é {"STK
062BB74D0	49	44	22	3A	22	34	32	38	22	2C	22	53	54	4B	50	4B	ID":"428","STKPK
062BB74E0	47	49	44	22	3A	22	31	22	2C	22	53	54	4B	54	58	54	GID":"1","STKTXT
062BB74F0	22	3A	22	5B	53	74	69	63	6B	65	72	5D	22	2C	22	53	":"[Sticker]","S
062BB7500	54	4B	56	45	52	22	3A	22	31	30	30	22	7D	75	38	39	TKVER":"100"}u89
062BB7510	65	31	32	62	62	39	66	30	34	33	38	34	33	63	66	31	e12bb9f043843cf1
062BB7520	31	33	38	30	30	34	64	64	30	32	33	65	35	37	7C	81	138004dd023e57|

Gambar 6.22 Hasil Winhex Sticker LINE *Messenger*



Gambar 6.23 Struktur Pesan Sticker LINE *Messenger*

Struktur pesan Sticker pada LINE *messenger* sendiri memiliki karakteristik dan tipe data yang unik, penjelasan tipe pada struktur pesan akan dijelaskan pada analisa data percakapan

6.2.2.3 Struktur Pesan Telegram *Messenger*:

Untuk studi kasus telegram *messenger* penulis tidak mendapatkan sesuatu pada Struktur pesan yang berkaitan dengan skenario yang telah dijalankan.

6.3 Analisa Bukti Digital

Pada bagian ini, hasil analisa struktur dan isi folder serta aplikasi menjadi jawaban untuk mengungkap sebuah kasus kejahatan sesuai skenario percakapan yang telah dibuat pada bagian perancangan dan dilaksanakan pada bagian implementasi. Analisa barang bukti digital meliputi pengumpulan data digital penting dan pembacaan bukti digital.

6.3.1 Analisa Data Percakapan

Pada penelitian ini, data percakapan merupakan data-data yang didapatkan dari pengerjaan sebelumnya yaitu struktur pesan. Data percakapan dari struktur pesan yang dihasilkan dari setiap aplikasi berbeda.

6.3.1.1 Data Primer

Data Primer merupakan data percakapan dari struktur pesan yang dianggap penting dikarenakan pada penyeledikan dan pembuktian barang bukti harus mengandung bukti digital yang konkrit yang nantinya akan dijadikan bukti dalam hukum. Berikut ini adalah data-data primer dari setiap aplikasi:

6.3.1.1.1 Facebook Messenger

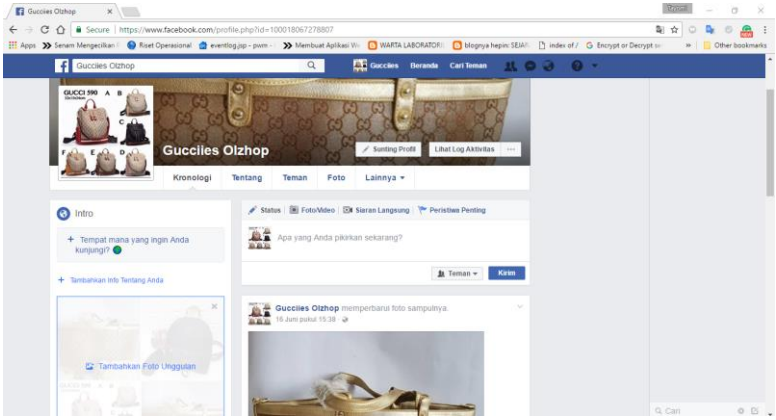
Pada tabel 6.3 menjelaskan bahwa tipe data dari aplikasi Facebook *messenger* memiliki 3 data yang dapat dijadikan bukti digital, yaitu userId, senderId dan text.

Tabel 6.3 Data Primer Facebook *Messenger*

Tipe Data	Keterangan
userId100018155444443	identitas percakapan yang sekaligus menunjukan identitas lawan bicara
senderId100018067278807	identitas pengirim pesan
chatId	Tidak ditemukan
Siap sist, ditunggu yaa barangnya. terimakasih sudah berbelanja di online shop kami.	teks percakapan yang dikirim
createdTime	Tidak ditemukan

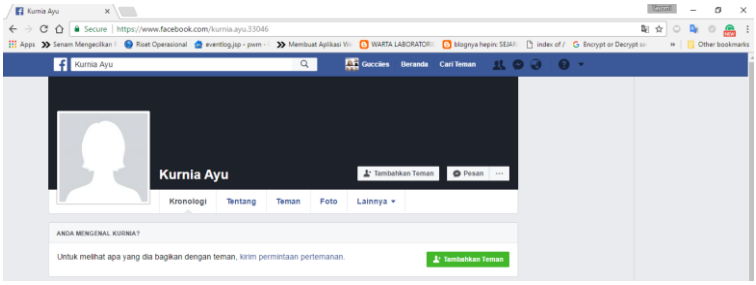
Tipe data pada facebook messenger memiliki karakter unix yang terdiri dari tipe data integer dan tidak dilakukan hashing atau enkripsi. Setelah mendapatkan userId dan senderId, maka dilanjutkan dengan mengecek userId dan dihubungkan langsung dengan facebook yaitu facebook.com/userId maka akan muncul seperti gambar berikut ini:

Untuk userId : 100018067278807 merupakan userId dari tersangka yang dapat dilihat pada gambar 6.24.



Gambar 6.24 UserId Facebook *Messenger* Tersangka

Untuk userId : 100018155444443 merupakan userId dari korban yang dapat dilihat pada gambar 6.25.



Gambar 6.25 UserId Facebook *Messenger* Korban

Setelah dilakukan pengecekan dari data primer tersebut maka didisimpulkan pada Tabel 6.4:

Tabel 6.4 Data Percakapan Facebook *Messenger*

ID	Alamat Facebook	Peran
100018067278807	https://www.facebook.com/Gucciies-Olzhop	Tersangka
100018155444443	https://www.facebook.com/kurnia.ayu.33046	Korban

6.3.1.1.2 LINE Messenger

Pada tabel 6.4 menjelaskan bahwa tipe data dari aplikasi LINE *messenger* memiliki 5 data yang dapat dijadikan bukti digital, yaitu from/userId, to/senderId, chatId, text dan time.

Tabel 6.5 Data Primer LINE *Messenger*

Tipe Data	Keterangan
from:"u85ca323e3415a3b6a584cbfde28442e6",	identitas pengirim pesan
to:"u89e12bb9f043843cf1138004dd023e57",	identitas penerima pesan
chatId:"u89e12bb9f043843cf1138004dd023e57",	id percakapan, jika percakapan bersifat unicast maka id percakapan sama dengan id dari lawan bicaranya.
text:"Siap sist, ditunggu yaa barangnya. Terimakasih sudah	isi dari pesan yang dikirim

berbelanja di online shopping kami.",	
createdTime:1497674512079,	waktu saat pesan dibuat. Berbentuk unix hex

Tipe data pada LINE messenger memiliki karakter unix yang terdiri dari tipe data MD5 dan tidak dilakukan hashing atau enkripsi.

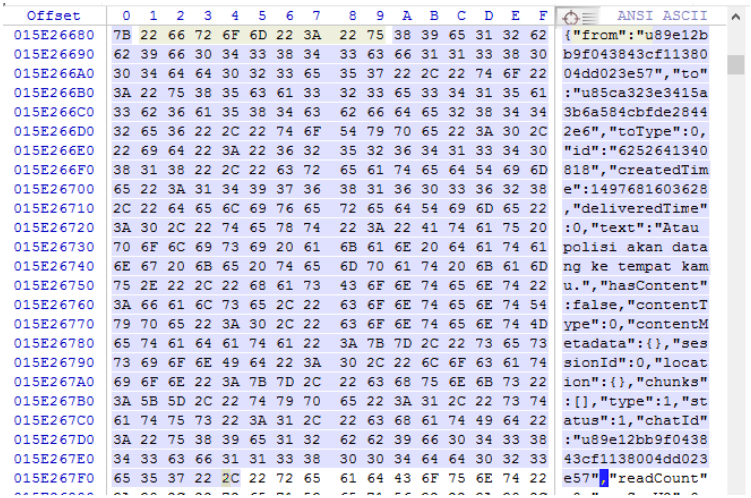
Setelah mendapatkan userId dan senderId, maka dapat disimpulkan dengan tabel 6.6.

Tabel 6.6 Data Percakapan LINE *Messenger*

Id	Peran
u85ca323e3415a3b6a584cbfde28443e6	Tersangka
u89e12b9f043843cf1138004dd023e57	Korban

Pada LINE *Messenger* mendapatkan createdTime yang berbentuk unix hex, maka akan dilakukan pengecekan apakah waktu yang ditampilkan sama dengan skenario yang dijalankan:

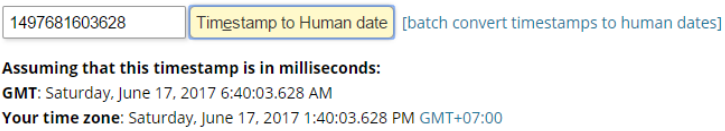
Berikut ini Penggalan percakapan dari korban kepada tersangka



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
015E26680	7B	22	66	72	6F	6D	22	3A	22	75	38	39	65	31	32	62	{"from":"u89e12b
015E26690	62	39	66	30	34	33	38	34	33	63	66	31	31	33	38	30	b9f043843cf11380
015E266A0	30	34	64	64	30	32	33	65	35	37	22	2C	22	74	6F	22	04dd023e57","to"
015E266B0	3A	22	75	38	35	63	61	33	32	33	65	33	34	31	35	61	:"u85ca323e3415a
015E266C0	33	62	36	61	35	38	34	63	62	66	64	65	32	38	34	34	3b6a584cbfde2844
015E266D0	32	65	36	22	2C	22	74	6F	54	79	70	65	22	3A	30	2C	2e6","toType":0,
015E266E0	22	69	64	22	3A	22	36	32	35	32	36	34	31	33	34	30	"id":"6252641340
015E266F0	38	31	38	22	2C	22	63	72	65	61	74	65	64	54	69	6D	818","createdTim
015E26700	65	22	3A	31	34	39	37	36	38	31	36	30	33	36	32	38	e":1497681603628
015E26710	2C	22	64	65	6C	69	76	65	72	65	64	54	69	6D	65	22	,"deliveredTime"
015E26720	3A	30	2C	22	74	65	78	74	22	3A	22	41	74	61	75	20	:0,"text":"Atau
015E26730	70	6F	6C	69	73	69	20	61	6B	61	6E	20	64	61	74	61	polisi akan data
015E26740	6E	67	20	6B	65	20	74	65	6D	70	61	74	20	6B	61	6D	ng ke tempat kam
015E26750	75	2E	22	2C	22	68	61	73	43	6F	6E	74	65	6E	74	22	u.","hasContent"
015E26760	3A	66	61	6C	73	65	2C	22	63	6F	6E	74	65	6E	74	54	:false,"contentT
015E26770	79	70	65	22	3A	30	2C	22	63	6F	6E	74	65	6E	74	4D	ype":0,"contentM
015E26780	65	74	61	64	61	74	61	22	3A	7B	7D	2C	22	73	65	73	etadata":{},"ses
015E26790	73	69	6F	6E	49	64	22	3A	30	2C	22	6C	6F	63	61	74	sionId":0,"locat
015E267A0	69	6F	6E	22	3A	7B	7D	2C	22	63	68	75	6E	6B	73	22	ion":{},"chunks"
015E267B0	3A	5B	5D	2C	22	74	79	70	65	22	3A	31	2C	22	73	74	:[],"type":1,"st
015E267C0	61	74	75	73	22	3A	31	2C	22	63	68	61	74	49	64	22	atus":1,"chatId"
015E267D0	3A	22	75	38	39	65	31	32	62	62	39	66	30	34	33	38	:"u89e12bb9f0438
015E267E0	34	33	63	66	31	31	33	38	30	30	34	64	64	30	32	33	43cf1138004dd023
015E267F0	65	35	37	22	2C	22	72	65	61	64	43	6F	75	6E	74	22	e57","readCount"

Gambar 6.26 Penggalan Percakapan LINE *Messenger*

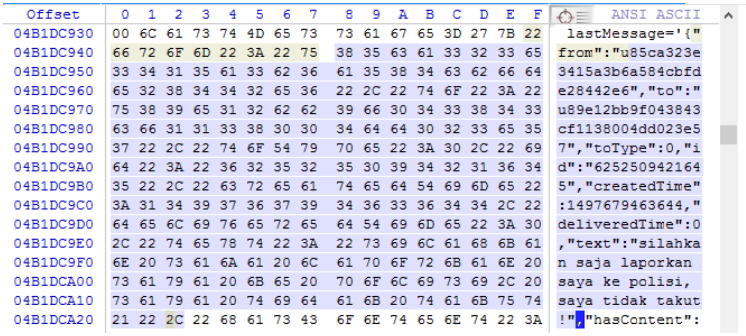
Menggunakan EpochConverter atau https://www.epochconverter.com untuk unix Timestamp conversation tools yang akan mengubah data berbentuk hexadesimal ke timestamp untuk human date yang ditujukkan pada gambar 6.27



Gambar 6.27 Timestamp Percakapan LINE *Messenger*

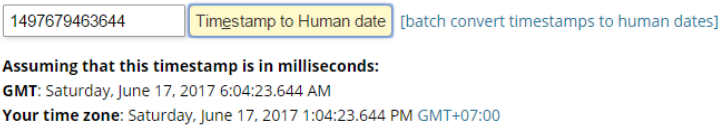
Dari penggalan percakapan yang didapatkan dan diubah menjadi human date maka percakapan tersebut terjadi pada 17 Juni 2017 dengan waktu 06.40 AM.

Berikut Penggalan percakapan dari tersangka kepada korban



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
04B1DC930	00	6C	61	73	74	4D	65	73	73	61	67	65	3D	27	7B	22	lastMessage='{"
04B1DC940	66	72	6F	6D	22	3A	22	75	38	35	63	61	33	32	33	65	from":"u85ca323e
04B1DC950	33	34	31	35	61	33	62	36	61	35	38	34	63	62	66	64	3415a3b6a584cbfd
04B1DC960	65	32	38	34	34	32	65	36	22	2C	22	74	6F	22	3A	22	e28442e6","to":"
04B1DC970	75	38	39	65	31	32	62	62	39	66	30	34	33	38	34	33	u89e12bb9f043843
04B1DC980	63	66	31	31	33	38	30	30	34	64	64	30	32	33	65	35	cf1138004dd023e5
04B1DC990	37	22	2C	22	74	6F	54	79	70	65	22	3A	30	2C	22	69	7","toType":0,"i
04B1DC9A0	64	22	3A	22	36	32	35	32	35	30	39	34	32	31	36	34	d":"625250942164
04B1DC9B0	35	22	2C	22	63	72	65	61	74	65	64	54	69	6D	65	22	5","createdTime"
04B1DC9C0	3A	31	34	39	37	36	37	39	34	36	33	36	34	34	2C	22	:1497679463644,"
04B1DC9D0	64	65	6C	69	76	65	72	65	64	54	69	6D	65	22	3A	30	deliveredTime":0
04B1DC9E0	2C	22	74	65	78	74	22	3A	22	73	69	6C	61	68	6B	61	,"text":"silahka
04B1DC9F0	6E	20	73	61	6A	61	20	6C	61	70	6F	72	6B	61	6E	20	n saja laporkan
04B1DCA00	73	61	79	61	20	6B	65	20	70	6F	6C	69	73	69	2C	20	saya ke polisi,
04B1DCA10	73	61	79	61	20	74	69	64	61	6B	20	74	61	6B	75	74	saya tidak takut
04B1DCA20	21	22	2C	22	68	61	73	43	6F	6E	74	65	6E	74	22	3A	!","hasContent":

Gambar 6.28 Penggalan Percakapan LINE *Messenger*



Gambar 6.29 Timestamp Percakapan LINE *Messenger*

Dari penggalan percakapan yang didapatkan dan diubah menjadi human date maka percakapan tersebut terjadi pada 17 Juni 2017 dengan waktu 06:04:23 AM.

6.3.1.1.3 Telegram Messenger

Untuk studi kasus Aplikasi Telegram *messenger* penulis tidak mendapatkan sesuatu pada Data percakapan dari struktur pesan yang berkaitan dengan skenario yang telah dijalankan.

6.3.1.2 Data Pendukung

Data pendukung merupakan data-data yang mendukung adanya barang bukti digital yang dihasilkan dari aplikasi sesuai dengan skenario dan eksperimen.

6.3.1.2.1 Facebook Messenger

Pada Facebook messenger akan menjelaskan data pendukung yaitu text, picture, audio, video dan sticker. Berikut ini penjelasan data pendukung dari setiap kategori :

Text

Pada tabel 6.7 akan menjelaskan 6 tipe data dari struktur pesan text pada Facebook *Messenger* yaitu sebagai berikut:

Tabel 6.7 Tipe Data Text Facebook *Messenger*

Tipe Object	Keterangan
FBStringWithRedactedDescription *text$__FB_class	Deskripsi Kelas FB berupa text
FBStringWithRedactedDescription -RAW_CONTENT_VALUE_ONLY_ TO_BE_VISIBLE_TO_USER	Deskripsi konten dapat dilihat oleh user
FBMMessageAttachment* attachment$__FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMMessageExtensibleAttachment* extensibleAttachmentNSArray *jsonAttachmentsNSDictionary* shareMap4	Deskripsi Ekstensi Attachment
FBMMessageExtensibleAttachment *extensibleAttachmentNSArray *tagssource:chat:orcaapp_id:1637541026485594	Deksripsi ekstensi Attachment dengan tagsource

Picture

Pada tabel 6.8 akan menjelaskan 9 tipe data dari struktur pesan picture pada Facebook *Messenger* yaitu sebagai berikut

Tabel 6.8 Tipe Data Picture Facebook *Messenger*

Tipe Object	Keterangan
FBMMessageAttachment* attachment$__FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMMessageExtensibleAttachment *extensibleAttachmentNSArray *jsonAttachmentsid106904016591446fbid106904016591446	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
filenameimage-106904016591446	Nama file gambar yang dikirim
mime_tipeimage/tipeimage_datawidthheight	Deskripsi data mime tipe image
urlhttps://scontent.xx.fbcdn.net/v/t34.0-12/19251246_106904016591446_1240998779_n.jpg?oh=086f8004d88b69359a3c80c27b093d7d&oe=594745DB	url file gambar yang dikirim
preview_urlhttps://scontent.xx.fbcdn.net/v/t34.00/s480x480/19251246_106904016591446_1240998779_n.jpg?oh=9df2fda172c7ce7fc8e5f7a61f3be3f1&oe=59471518	url file thumbnail gambar yang dikirim

render_as_stickerimage_tipe NSDictionary*shareMap4	mengubah image menjadi stiker image
FBMMessageExtensibleAttachment* extensibleAttachmentNSArray*tags source: chat:orcaapp_id:256002347743983	Deksripsi ekstensi Attachment dengan tagsource

Video

Pada tabel 6.9 akan menjelaskan 9 tipe data dari struktur pesan video pada Facebook *Messenger* yaitu sebagai berikut

Tabel 6.9 Tipe Data Video Facebook *Messenger*

Tipe Object	Keterangan
FBMMessageAttachment* attachment$__FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMMessageExtensibleAttachment* extensibleAttachmentNSArray*jsonA ttachmentsid106923546589493fbid1 06923546589493file_size)	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
filenamevideo-1497693573.mp4	nama file video yang dikirim
mime_tipevideo/tipeimage_datawid thheight	Deskripsi data mime tipe video dengan image
video_dataurlhttps://video.xx.fbcdn. net/v/t42.3356-2/19288123_106923563256158_838 4727728976297984_n.mp4/video-1497693573.mp4?vabr=1640572&o	url file video yang dikirim

h=3cdf37d84b7fdf57d738b7644d2328e6&oe=59476C95&dl=1	
preview_urlhttps://scontent.xx.fbcdn.net/v/t15.3394-10/p480x480/19213436_106923566589491_2549496340707016704_n.jpg?oh=1820b9983dded4df401dd22ea542f0a2&oe=59E74E9A	url file video gambar yang dikirim
video_tipelength NSDictionary*shareMap4	Panjang tipe video
FBMMessageExtensibleAttachment* extensibleAttachmentNSArray*tagssource:chat:orcaapp_id:2560023477439983	Deksripsi ekstensi Attachment dengan tagsource

Audio

Pada tabel 6.10 akan menjelaskan 7 tipe data dari struktur pesan audio pada Facebook *Messenger* yaitu sebagai berikut

Tabel 6.10 Tipe Data Audio Facebook *Messenger*

Tipe Object	Keterangan
FBMMessageAttachment* attachment$__FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMMessageExtensibleAttachment* extensibleAttachmentNSArray*jsonAttachments	Deskripsi Ekstensi Attachment dengan id attachment dan id fb

NSArray*jsonAttachmentsid106909209924260fbid106909209924260	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
file_sizexfilename!audioclip-1497692548000-7040.mp4	nama file audio yang dikirim
mime_tipeaudio/tipeNSDictionary*shareMap4	Deskripsi data mime tipe audio
FBMMessageExtensibleAttachment*extensibleAttachmentNSArray*tagssource:chat:orcaapp_id:2560023477439983	Deksripsi ekstensi Attachment dengan tagsource

Sticker

Pada tabel 6.11 akan menjelaskan 5 tipe data dari struktur pesan sticker pada Facebook *Messenger* yaitu sebagai berikut

Tabel 6.11 Tipe Data Sticker Facebook *Messenger*

Tipe Object	Keterangan
FBMMessageAttachment*attachment$__FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMMessageAttachmentsavedPropertiesNSArray*jsonAttachmentsNSDictionary*shareMap4	Deskripsi Attachment Properties
FBMMessageExtensibleAttachment*extensibleAttachmentNSArray*jsonAttachments	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
NSDictionary*shareMapshare_mapsticker_id144885035685763	identitas stiker yang dikirim
FBMMessageExtensibleAttachment*extensibleAttachmentNSArray*tagssource:chat:orcaapp_id:2560023477439983	Deksripsi ekstensi Attachment dengan tagsource

6.3.1.2.2 LINE Messenger

Pada LINE messenger akan menjelaskan data pendukung yaitu text, picture, audio, video dan sticker. Berikut ini penjelasan data pendukung dari setiap kategori :

Text

Pada tabel 6.12 akan menjelaskan 25 tipe data dari struktur pesan text pada LINE *Messenger* yaitu sebagai berikut

Tabel 6.12 Tipe Data Text LINE *Messenger*

Tipe Object	Keterangan
toTipe:0,	jenis pesan. 0 untuk unicast dan 1 untuk multicast
id:"6252197251410",	identitas pesan yang bersangkutan
deliveredTime:0,	waktu saat pesan diterima
hasContent:false,	Tidak Diketahui
contentTipe:0,	Tipe konten
contentMetadata:{},	Metadata konten
sessionId:0,	ID dari session yang digunakan.
location:{},	Keterangan lokasi
chunks:[],	mendeskripsikan urutan pesan jika pesan terlalu besar dan dipecah menjadi beberapa pesan kecil.
tipe:1,	Tidak Diketahui
status:2,	status dari pesan tersebut. 0 untuk mengirim 1 untuk terkirim 2 untuk terbaca
chatId:"u89e12bb9f043 843cf1138004dd023e57",	id percakapan, jika percakapan bersifat unicast maka id

	percakapan sama dengan id dari lawan bicaranya.
readCount:0,	jumlah dari user yang telah membaca pesan tersebut.
reqSeqV2:5,	Tidak Diketahui
reqSeq:0,	Tidak Diketahui
contentInfo:{},	Informasi konten
eventInfo:{},	Informasi event
rev:126,	Tidak Diketahui
errorCode:0,	menampilkan kode kesalahan jika terjadi kesalahan
urlPreview:{},	berisi url yang terdapat pada pesan tersebut
hasUrlPreview:false,	mengindikasikan pesan terdapet url atau tidak
syncToken:"",	Tidak Diketahui
fromTipe:0	Tidak Diketahui

Picture

Pada tabel 6.13 akan menjelaskan 7 tipe data dari struktur pesan picture pada LINE *Messenger* yaitu sebagai berikut

Tabel 6.13 Tipe Data Picture LINE *Messenger*

Tipe Object	Keterangan
u89e12bb9f043843cf1138004dd023e57	identitas pengirim pesan
u85ca323e3415a3b6a584cbfde28442e6	identitas penerima pesan
6251971991394	identitas pesan

89e12bb9f043843cf1138004dd02 3e57	identitas percakapan
{"sendContent":true,	informasi pengiriman konten
thumbPath:"C:\\Users\\harrm\ \AppData\\Local/LINE/*Cache*/m/8/ f194ff32c2e09701b6 76c8aaab8518f41aaac2a",	lokasi file thumbnail
thumbResCode:200}	ukuran gambar thumbnail

Video

Pada tabel 6.14 akan menjelaskan 10 tipe data dari struktur pesan video pada LINE *Messenger* yaitu sebagai berikut

Tabel 6.14 Tipe Data Video LINE *Messenger*

Tipe Object	Keterangan
u89e12bb9f043843cf1138004dd02 3e57	identitas pengirim pesan
u85ca323e3415a3b6a584cbfde284 42e6	Identitas penerima pesan
6252634913886	identitas pesan
{DURATION:"9355",	Durasi Video
OBS_POP:"b",	Durasi Audio
SRC_SVC_CODE:"talk"}	Tidak Diketahui
sendContent:true,	informasi pengiriman konten
thumbResCode:200,	ukuran file thumbnail

thumbPath:"C:\\Users\\harrm\\ AppData\\Local/LINE/*Cache*/m/4/ 504fa8efa3f97947a18fb3c2a1622 4439abeb1e"}	lokasi gambar thumbnail
u89e12bb9f043843cf1138004dd02 3e57	identitas percakapan

Audio

Pada tabel 6.15 akan menjelaskan 8 tipe data dari struktur pesan audio pada LINE *Messenger* yaitu sebagai berikut

Tabel 6.15 Tipe Data Audio LINE *Messenger*

Tipe Object	Keterangan
u89e12bb9f043843cf1138004dd02 3e57	identitas pengirim pesan
u85ca323e3415a3b6a584cbfde284 42e6	Identitas penerima pesan
6252407216242	identitas pesan
{"AUDLEN":"7497",	Panjang Audio
DURATION:"7497",	Durasi Audio
OBS_POP:"b",	Tidak diketahui
SRC_SVC_CODE:"talk"}	Tidak diketahui
u89e12bb9f043843cf1138004dd02 3e57	identitas percakapan

Sticker

Pada tabel 6.16 akan menjelaskan 8 tipe data dari struktur pesan sticker pada LINE *Messenger* yaitu sebagai berikut

Tabel 6.16 Tipe Data Sticker LINE *Messenger*

Tipe Object	Keterangan
u89e12bb9f043843cf1138004dd023e57	identitas pengirim pesan
u85ca323e3415a3b6a584cbfde28442e6	Identitas penerima pesan
6252063647408	identitas pesan stiker
{"STKID":"428",	identitas stiker yang di-attach
STKPKGID:"1",	identitas dari paket stiker
STKTXT:"[Sticker]",	teks dari stiker yang dikirim
STKVER:"100"}	versi dari stiker yang dikirim
u89e12bb9f043843cf1138004dd023e57	identitas percakapan

6.3.1.2.3 Telegram Messenger

Untuk studi kasus Aplikasi Telegram *messenger* penulis tidak mendapatkan sesuatu pada Data pendukung data percakapan dari struktur pesan yang berkaitan dengan skenario yang telah dijalankan.

Setelah menganalisa bukti digital pendukung, maka dihasilkan perbandingan tipe data pendukung pada tabel 6.17.

Tabel 6.17 Perbandingan Tipe Data Pendukung

Tipe Data / Aplikasi	FACEBOOK	LINE	TELEGRAM
Text	Langsung menampilkan text	text:"..."	Tidak diketahui
	Terdapat Class untuk Text	Tidak terdapat Class untuk Text	Tidak diketahui
	Tidak terdapat chatId	Terdapat chatId	Tidak diketahui
Picture	Terdapat Class untuk Attachment	tidak terdapat Class untuk Attachment	Tidak diketahui
	Terdapat id attachment	Tidak terdapat id attachment	Tidak diketahui
	Terdapat deksripsi nama file gambar	tidak terdapat deksripsi nama file gambar	Tidak diketahui
	url file gambar dan preview url thumbnail	tidak terdapat url file gambar dan preview url thumbnail	Tidak diketahui
	tidak terdapat ukuran gambar thumbnail	terdapat ukuran gambar thumbnail	Tidak diketahui
	Tidak terdapat lokasi file thumbnail	Terdapat lokasi file thumbnail	Tidak diketahui
Video	Terdapat Class untuk Attachment	tidak terdapat Class untuk Attachment	Tidak diketahui
	Terdapat id attachment	Tidak terdapat id attachment	Tidak diketahui
	Terdapat deksripsi nama file video	tidak terdapat deksripsi nama file video	Tidak diketahui
	url file videodan preview url thumbnail	tidak terdapat url file video dan preview url thumbnail	Tidak diketahui
	tidak terdapat ukuran file thumbnail	terdapat ukuran file thumbnail	Tidak diketahui
	Tidak terdapat lokasi file thumbnail	Terdapat lokasi file thumbnail	Tidak diketahui
	Tidak terdapat durasi video	Terdapat durasi video	Tidak diketahui
Audio	Terdapat Class untuk Attachment	tidak terdapat Class untuk Attachment	Tidak diketahui
	Terdapat id attachment	Tidak terdapat id attachment	Tidak diketahui
	Terdapat deksripsi nama file audio	tidak terdapat deksripsi nama file audio	Tidak diketahui
	tidak terdapat ukuran file thumbnail	terdapat ukuran file thumbnail	Tidak diketahui
	Tidak terdapat lokasi file thumbnail	Terdapat lokasi file thumbnail	Tidak diketahui
	Tidak terdapat durasi video	Terdapat durasi video	Tidak diketahui
Sticker	Terdapat Class untuk Attachment	tidak terdapat Class untuk Attachment	Tidak diketahui
	Terdapat id sticker	Terdapat id sticker	Tidak diketahui
	Tidak terdapat keterangan id stiker, versi stiker dan teks stiker	Terdapat keterangan id stiker, versi stiker dan teks stiker	Tidak diketahui

6.3.2 Analisa Media

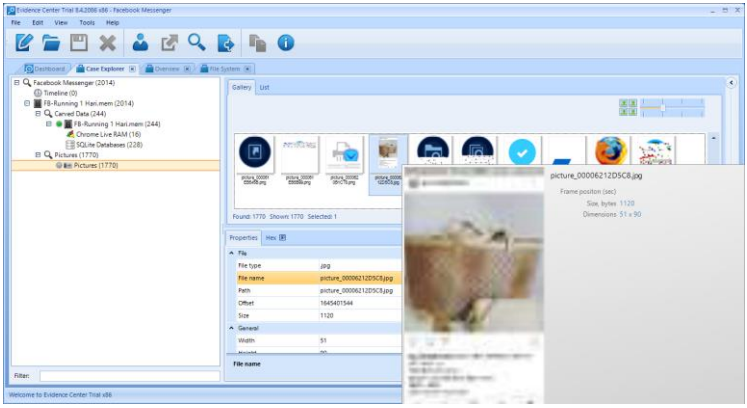
Analisa media dilakukan pada tools Belkasoft Evidence Center. Data yang nantinya akan dianalisa dan disesuaikan dengan skenario yang telah dijalankan, maka akan dihasilkan bukti digital. Berikut ini penjelasan data-data dari media yang dihasilkan pada setiap aplikasi:

6.3.2.1 Facebook *Messenger*

Pada Facebook *Messenger* didapatkan beberapa data media yaitu picture yang sesuai dengan skenario dan eksperimen yang telah dijalankan:

Picture

Pada tools Belkasoft Evidence Center hanya didapatkan data-data picture pada Facebook *messenger*. Pada gambar 6.30 menggambarkan hasil yang didapatkan yaitu gambar dengan nama file picture_00006212D5C8.jpg dan Pada gambar 6.31 perbandingan dengan nama file pada saat skenario dijalan kan dengan nama file Screenshot_2017-06-16-15-37-53.jpg.



Gambar 6.30 Media Picture Facebook *Messenger*

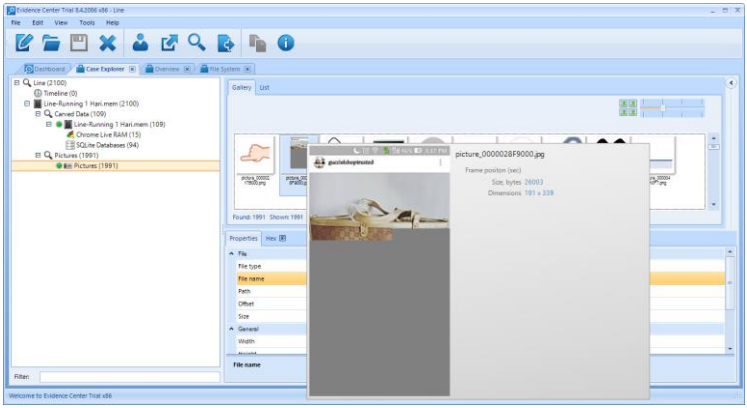
Gambar 6.31 Media Picture Skenario Facebook *Messenger*

6.3.2.2 LINE *Messenger*

Pada LINE *Messenger* didapatkan beberapa data media yaitu Picture dan Sticker yang sesuai dengan skenario dan eksperimen yang telah dijalankan.

Picture

Pada tools Belkasoft Evidence Center hanya didapatkan data-data picture pada LINE *messenger*. Pada gambar 6.32 menggambarkan hasil yang didapatkan yaitu gambar dengan nama file picture_0000028F9000.jpg dan pada gambar 6.33 perbandingan dengan nama file pada saat skenario dijalan kan dengan nama file Screenshot_2017-06-16-15-37-53.jpg



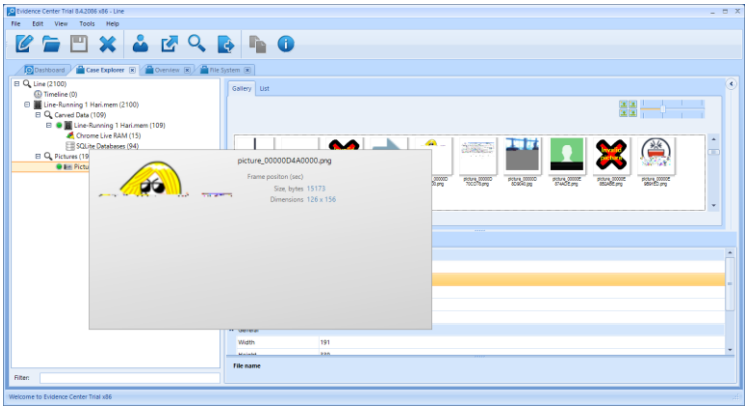
Gambar 6.32 Media Picture LINE *Messenger*

Gambar 6.33 Media Picture Skenario Line *Messenger*

Sticker

Pada tools Belkasoft Evidence Center hanya didapatkan data-data Sticker pada LINE *messenger*. Pada gambar 6.32

menggambarkan hasil yang didapatkan yaitu sticker dengan nama file picture_00000D4A0000.png.



Gambar 6.34 Media Sticker LINE *Messenger*

6.3.2.3 Telegram *Messenger*

Berikut ini adalah Analisa Media dari percakapan yang dilakukan dengan menganalisa hasil dari winhex.

Untuk studi kasus telegram *messenger* penulis tidak mendapatkan data-data media yang berkaitan dengan skenario yang telah dijalankan.

6.4 Analisa Percakapan Aplikasi

Dalam analisa percakapan, pertama adalah melakukan pembuktian terbalik dengan menyamakan percakapan yang terjadi pada aplikasi dengan skenario percakapan yang telah dibuat sebelumnya. Hal ini dilakukan untuk kondisi bukti hanya berasal dari salah satu pihak saja (bukti dari tersangka atau korban).

Jika bukti berasal dari dua belah pihak (tersangka dan korban), maka percakapan akan dianalisa menggunakan kunci percakapan. Untuk membantu dalam melakukan analisa kita menggunakan fitur filter untuk menyaring data yang

dibutuhkan. Filter digunakan untuk menyaring data yang sesuai dengan skenario percakapan yang telah disebutkan di bagian sebelumnya.

Berikut merupakan analisa dari percakapan, baik dari Facebook *Messenger*, LINE *Messenger* maupun Telegram *Messenger*:

6.4.1 Facebook *Messenger*

Bagian ini membahas tentang analisa percakapan dari aplikasi Facebook *messenger*. Pada aplikasi Facebook *messenger*, penulis menganalisa hasil dump dari tools DumpIt dan Belkasoft RamCapturer, dimana hasilnya akan dianalisa dengan WinHex dan Belkasoft Evidence Center.

Untuk menganalisa aktivitas percakapan, maka penulis menggunakan kata kunci yang terdapat pada skenario. Berikut merupakan hasil analisa untuk membandingkan aktivitas percakapan pada aplikasi dengan skenario percakapan yang telah dibuat:

Tabel 6.18 Tabel Percakapan Facebook dan skenario

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
-	-	-	Hai sist, mau tanya. Gucci silvi totebag 189# A34 available ?	Tidak Sesuai dan Tidak Terbukti
-	-	-	Send Picture	Tidak Sesuai dan Tidak Terbukti
-	-	-	Availabe sist, mau pesan warna apa ?	Tidak Sesuai dan Tidak Terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
-	-	-	Aku mau yang gold sist 2 ya	Tidak Sesuai dan Tidak Terbukti
-	-	-	Send Emoji	Tidak Sesuai dan Tidak Terbukti
-	-	-	Send Sticker	Tidak Sesuai dan Tidak Terbukti
-	-	-	Isi ini dulu sist: Format Pembelian Nama: Alamat: No. HP: Pesan:	Tidak Sesuai dan Tidak Terbukti
-	-	-	Format Pembelian : Nama: Kurnia Ayu Alamat: jl. Kertajaya Indah Blok X No. 001 No.hp: 085424631524 Pesan: Gucci Silvi Totebag	Tidak Sesuai dan Tidak Terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
			189# A34 Gold = 2	
-	-	-	Aku total ya sist, Tas = Rp.11.953.063 dan ongkir Rp.25.000. Total Rp.11.978.063 Transfer ke rek a/n Gucciies Olzhop No. rek BAC 0756-9852-3564. Kalau sudah di transfer, kirim bukti trfnya ya sist	Tidak Sesuai dan Tidak Terbukti
-	-	-	Send Picture	Tidak Sesuai dan Tidak Terbukti
1000180672 78807	1000181554 44443	5A1994BC	Ok, aku trf sekarang ya. Aku ke atm dulu.	Sama dan terbukti
1000180672 78807	1000181554 44443	45F170BD	Sudah aku trf ya sis, ditunggu tasnya.	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
			Kepengen banget sama tas itu	
10001 80672 78807	10001 81554 44443	16528C2 B	Send Picture	Sama dan terbukti
10001 80672 78807	10001 81554 44443	16781F9 7	Send Sticker	Sama dan terbukti
10001 80672 78807	10001 81554 44443	11CF25C AD	Siap sist, ditunggu yaa barangnya. Terimakasih sudah berbelanja di online shopping kami	Sama dan terbukti
10001 80672 78807	10001 81554 44443	90FD14 BC	Sist ? Barangnya kok belum sampai ? Sudah 2 hari saya tunggu. Katanya pengirimanny a ekspress.	Sama dan terbukti
10001 80672 78807	10001 81554 44443	1DA3D5 8	Send Voice note	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
10001 80672 78807	10001 81554 44443	4DE62C B5	Sist	Sama dan terbukti
10001 80672 78807	10001 81554 44443	235FD44 F	Jangan di read aja dong	Sama dan terbukti
10001 80672 78807	10001 81554 44443	78AE0C B3	Gimana barang saya?	Sama dan terbukti
10001 80672 78807	10001 81554 44443	1ACFC4 47	Sudah dikirim ?	Sama dan terbukti
10001 80672 78807	10001 81554 44443	84F1EC AD	Barang sedang dalam pengiriman sist, tenang saja. online shopping kami trusted 100% kok.	Sama dan terbukti
10001 80672 78807	10001 81554 44443	833DDC B4	Kalau pengiriman ekspress seharusnya 1 hari sudah sampai dong sist, jangan macem-macemnya. Aku bisa laporin online	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
			shop ini ke polisi.	
10001 80672 78807	10001 81554 44443	1010988 8D	Silahkan saja laporkan saya ke polisi, saya tidak takut!	Sama dan terbukti
10001 80672 78807	10001 81554 44443	9289BC7 E	Send Video	Sama dan terbukti
10001 80672 78807	10001 81554 44443	4729AC1 F	Aku udah lapor ke polisi, online shopping kamu harus ditindak karna biar ngga ada yg senasib kayak aku.	Sama dan terbukti
10001 80672 78807	10001 81554 44443	421552B C	Inget dosa mbak, udah nipu kok jahat bgt jadi orang.	Sama dan terbukti
10001 80672 78807	10001 81554 44443	278C00B D	Kembalikan uang saya	Sama dan terbukti
10001 80672 78807	10001 81554 44443	8A217C B4	Atau polisi akan datang ke tempat kamu.	Sama dan terbukti

Berdasarkan hasil pada Tabel 6.8 diatas, dapat ditarik kesimpulan bahwa aktivitas dan skenario percakapan pada aplikasi Facebook *Messenger* terbukti sama. Skenario berjalan dengan baik dan sama tanpa ada perbedaan sehingga dapat dijadikan bukti digital. Akan tetapi dari keseluruhan percakapan, terdapat percakapan yang tidak terekam jejaknya yaitu percakapan pertama sampai percakapan pengiriman picture yang diterangkan pada tabel diatas.

Dalam penelitian ini, penulis juga memiliki bukti dari kedua belah pihak. Oleh karena itu, kita juga dapat menganalisa menggunakan kunci percakapan yaitu RAW_CONTENT_VALUE_ONLY_TO_BE_VISIBLE_TO_USER.

Berdasarkan analisa diatas, terlihat dapat disimpulkan bahwa kunci percakapan menjadi primary key untuk membuktikan bahwa aktivitas percakapan antar perangkat melalui aplikasi Facebook *messenger* itu benar adanya tanpa ada rekayasa.

6.4.2 LINE *messenger*

Bagian ini membahas tentang analisa percakapan dari aplikasi Facebook *messenger*. Pada aplikasi Facebook *messenger*, penulis menganalisa hasil dump dari tools DumpIt dan Belkasoft RamCapturer, dimana hasilnya akan dianalisa dengan WinHex dan Belkasoft Evidence Center.

Untuk menganalisa aktivitas percakapan, maka penulis menggunakan kata kunci yang terdapat pada skenario. Berikut merupakan hasil analisa untuk membandingkan aktivitas percakapan pada aplikasi dengan skenario percakapan yang telah dibuat:

Tabel 6.19 Tabel Percakapan aplikasi LINE dan skenario

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380041dd023e57	3DEDC279	Hai sist, mau tanya. Gucci silvi totebag 189# A34 available ?	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380041dd023e57	55B6AB0D	Send Picture	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380041dd023e57	4CB51E76	Availabe sist, mau pesan warna apa ?	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380041dd023e57	55B6A9D1	Aku mau yang gold sist 2 ya	Sama dan terbukti
u85ca323e3	u89e12bb9f	55B6A86F	Send Emoji	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
415a3b6a584cbfde28442e6	043843cf11380040dd023e57			
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	55B6A780	Send Sticker	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	51436A19	Isi ini dulu sist: Format Pembelian Nama: Alamat: No. HP: Pesan:	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	55B6A586	Format Pembelian : Nama: Kurnia Ayu Alamat: jl. Kertajaya Indah Blok X No. 001 No.hp: 085424631524	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
			Pesan: Gucci Silvi Totebag 189# A34 Gold = 2	
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf1138004dd023e57	55B6A417	Aku total ya sist, Tas = Rp.11.953.063 dan ongkir Rp.25.000. Total Rp.11.978.063 Transfer ke rek a/n Gucciies Olzhop No. rek BAC 0756-9852-3564. Kalau sudah di transfer, kirim bukti trfnya ya sist	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf1138004dd023e57	55B6A249	Send Picture	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	55B6A0C4	Ok, aku trf sekarang ya. Aku ke atm dulu.	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	62BB75CC	Sudah aku trf ya sis, ditunggu tasnya. Kepengen banget sama tas itu	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	62BB76C2	Send Picture	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	62BB74CD	Send Sticker	Sama dan terbukti
u85ca323e3415a3b6a58	u89e12bb9f043843cf11	92A870BB	Siap sist, ditunggu yaa barangnya. Terimakasih	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
4cbfde28442e6	38004dd023e57		sudah berbelanja di online shopping kami	
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf1138004dd023e57	2BC8B5D1	Sist ? Barangnya kok belum sampai ? Sudah 2 hari saya tunggu. Katanya pengirimannya ekspress.	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf1138004dd023e57	129D00A5F	Send Voice note	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf1138004dd023e57	4DF75649	Sist	Sama dan terbukti
u85ca323e3415a3b6a58	u89e12bb9f043843cf11	1011C68AB	Jangan di read aja dong	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
4cbfde28442e6	38004dd023e57			
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380044dd023e57	1011C67FF	Gimana barang saya?	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380044dd023e57	1011C6758	Sudah dikirim ?	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380044dd023e57	222EBB59	Barang sedang dalam pengiriman sist, tenang saja. online shopping kami trusted 100% kok.	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380044dd023e57	1011C65D2	Kalau pengiriman ekspress seharusnya 1 hari sudah sampai dong sist, jangan	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
			macem-macemnya. Aku bisa laporin online shop ini ke polisi.	
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	4B1DC93F	Silahkan saja laporkan saya ke polisi, saya tidak takut!	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	129D00402	Send Video	Sama dan terbukti
u85ca323e3415a3b6a584cbfde28442e6	u89e12bb9f043843cf11380040dd023e57	222EB1B9	Aku udah lapor ke polisi, online shopping kamu harus ditindak karna biar ngga ada yg senasib kayak aku.	Sama dan terbukti
u85ca323e3415a3	u89e12bb9f04384	92457207	Inget dosa mbak, udah	Sama dan terbukti

Key ID TSK	Key ID KBN	OFFSET	Percakapan	Kesimpulan
b6a58 4cbfd e2844 2e6	3cf11 38004 dd023 e57		nipu kok jahat bgt jadi orang.	
u85ca 323e3 415a3 b6a58 4cbfd e2844 2e6	u89e1 2bb9f 04384 3cf11 38004 dd023 e57	1B3BBB 81	Kembalikan uang saya	Sama dan terbukti
u85ca 323e3 415a3 b6a58 4cbfd e2844 2e6	u89e1 2bb9f 04384 3cf11 38004 dd023 e57	15E2668 1	Atau polisi akan datang ke tempat kamu.	Sama dan terbukti

Berdasarkan hasil pada Tabel 6.9 diatas, dapat ditarik kesimpulan bahwa aktivitas dan skenario percakapan pada aplikasi LINE *Messenger* terbukti sama. Skenario berjalan dengan baik dan sama tanpa ada perbedaan sehingga dapat dijadikan bukti digital.

6.4.3 Telegram *messenger*

Untuk studi kasus Aplikasi Telegram *messenger* penulis tidak mendapatkan sesuatu pada data percakapan dari struktur pesan yang berkaitan dengan skenario yang telah dijalankan.

6.4.4 Hasil Akhir Pembuktian

Berdasarkan hasil analisa percakapan dan media, didapatkan hasil bahwa dari ketiga aplikasi instant *messenger* yang diuji hanya 2 aplikasi yaitu Facebook *Messenger* dan LINE *Messenger* yang dapat menghasilkan barang bukti yang kuat dan valid untuk sebuah kasus hukum di Indonesia karena berhasil membuktikan validitas percakapan. Untuk aplikasi LINE *messenger* memberikan bantuan bukti pendukung yang lebih lengkap dibandingkan Facebook *Messenger*. Dan untuk aplikasi Telegram *messenger* tidak memberikan informasi apapun mengenai skenario dan eksperimen yang dilakukan pada penelitian ini.

6.5 Perbandingan Data Digital

Berdasarkan hasil analisa dari ketersediaan, struktur, dan isi dari data digital yang dapat diambil melalui proses analisa, maka didapatkan beberapa hasil kesamaan dan perbedaan. Dalam melakukan proses perbadingan ini, penulis menggunakan pendekatan aplikasi, perangkat, dan eksperimen.

6.5.1 Perbandingan Data Aplikasi

Berdasarkan penelitian yang telah dilakukan, berikut merupakan perbandingan data dari aplikasi Facebook *Messenger*, LINE *Messenger* dan Telegram *Messenger*:

Pada tabel 6.19 merupakan tabel perbandingan data aplikasi yang didapatkan, perbandingan antar tools yang digunakan dan perbandingan aplikasi instant *messenger*, bobot persentase yang dilakukan pada setiap kategori yaitu kategori data primer percakapan dan media. Bobot persentase ini mempengaruhi tingkat kepentingan dari kategori tersebut, pada umumnya semua kategori memiliki tingkat kepentingan yang sama, akan tetapi dibutuhkan prioritas bukti digital yang nantinya akan digunakan dalam hukum. Data Primer percakapan yaitu userId, senderId, text chatId dan time, lebih

besar kepentingannya dibandingkan media yang terdiri dari picture, audio, video dan sticker dikarenakan data tersebut dapat dijadikan bukti digital untuk hukum.

Tabel 6.20 Perbandingan Data Aplikasi

Tools,Aplikasi / Data	Data Primer Percakapan					Media				Persentase
	userId	**sender Id**	**Text**	**chatId**	**Time**	**Picture**	**Audio**	**Video**	**Sticker**	
Bobot Persentase	12	12	12	12	12	10	10	10	10	
Winhex										
Facebook	Ada	Ada	Ada	Tidak Ada	Tidak Ada	Ada	Ada	Ada	Ada	76%
LINE	Ada	Ada	Ada	Ada	Ada	Ada	Ada	Ada	Ada	100%
Telegram	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	0%
Belkasoft										
Facebook	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Ada	Tidak Ada	Tidak Ada	Tidak Ada	10%
LINE	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Ada	Tidak Ada	Tidak Ada	Ada	20%
Telegram	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	Tidak Ada	0%

Keterangan : Ada (Data ditemukan), Tidak Ada (Data tidak ditemukan)

Dari tabel 6.19 merupakan hasil data aplikasi yang digunakan menggunakan tools winhex dan belkasoft untuk mengidentifikasi apakah data pada kategori data primer percakapan dan media terekam jejaknya pada *Random Access Memory* (RAM), apabila data-data tersebut terekam jejaknya, maka akan dianalisa apakah data-data pada kategori tersebut terbukti dengan melihat *cache* pada folder penyimpanan dari setiap aplikasi yang diuji. Pengujian dilakukan untuk setiap object pada struktur pesan yaitu text, picture, audio, video dan stiker. Persentase yang dinilai terdiri dari hasil perbandingan jumlah object yang dikirim dari skenario dengan jumlah object yang terdeteksi oleh tools dan terdapat jejak *cache* pada folder penyimpanan di setiap aplikasi instant messenger. Maka akan menghasilkan daftar jumlah artefak yang akan dijelaskan pada tabel 6.20, tabel 6.21 dan tabel 6.22.

Tabel 6.21 Persentase jumlah artefak yang didapatkan pada aplikasi Facebook Messenger

	WinHex			Belkasoft		
Object	Jumlah object yang dikirim	Jumlah object yang terdeteksi	Persentase (%)	Jumlah object yang dikirim	Jumlah object yang terdeteksi	Persentase (%)
Text	21	15	71,4	21	0	0,0
Picture	3	1	33,3	3	1	33,3
Audio	1	1	100,0	1	0	0,0
Video	1	1	100,0	1	0	0,0
Stiker	3	0	0,0	3	0	0,0
		rerata	60,95		rerata	6,67

Pada tabel 6.20 menjelaskan bahwa persentase jumlah artefak atau data yang didapatkan pada aplikasi Facebook messenger dilihat dari 2 tools yang digunakan yaitu Winhex dan Belkasoft Evidence Center, dan jumlah object dari data primer percakapan yaitu terdiri dari text, dan media yang terdiri dari picture, audio, video dan sticker. Dengan jumlah object yang dilakukan pada saat pelaksanaan skenario dan eksperimen, persentase jumlah object yang dikirim dengan jumlah object yang terdeteksi sebesar 60,95% menggunakan tools winhex dan 6,67% menggunakan tools belkasoft.

Tabel 6.22 Persentase jumlah artefak yang didapatkan pada aplikasi LINE Messenger

	WinHex			Belkasoft		
Object	Jumlah object yang dikirim	Jumlah object yang terdeteksi	Persentase (%)	Jumlah object yang dikirim	Jumlah object yang terdeteksi	Persentase (%)
Text	21	21	100,0	21	0	0,0
Picture	3	3	100,0	3	3	100,0
Audio	1	1	100,0	1	0	0,0
Video	1	1	100,0	1	0	0,0
Stiker	3	3	100,0	3	2	66,7
		rerata	100,00		rerata	33,33

Pada tabel 6.21 menjelaskan bahwa persentase jumlah artefak atau data yang didapatkan pada aplikasi LINE messenger dilihat dari 2 tools yang digunakan yaitu Winhex dan Belkasoft Evidence Center, dan jumlah object dari data primer percakapan yaitu terdiri dari text, dan media yang terdiri dari picture, audio, video dan sticker. Dengan jumlah object yang dilakukan pada saat

pelaksanaan skenario dan eksperimen, persentase jumlah object yang dikirim dengan jumlah object yang terdeteksi sebesar 100% menggunakan tools winhex dan 33,33% menggunakan tools belkasoft.

Tabel 6.23 Persentase jumlah artefak yang didapatkan pada aplikasi Telegram Messenger

	WinHex			Belkasoft		
Object	Jumlah object yang dikirim	Jumlah object yang terdeteksi	Persentase (%)	Jumlah object yang dikirim	Jumlah object yang terdeteksi	Persentase (%)
Text	21	0	0,0	21	0	0,0
Picture	3	0	0,0	3	0	0,0
Audio	1	0	0,0	1	0	0,0
Video	1	0	0,0	1	0	0,0
Stiker	3	0	0,0	3	0	0,0
		rerata	0,00		rerata	0,00

Pada tabel 6.22 menjelaskan bahwa persentase jumlah artefak atau data yang didapatkan pada aplikasi LINE messenger dilihat dari 2 tools yang digunakan yaitu Winhex dan Belkasoft Evidence Center, dan jumlah object dari data primer percakapan yaitu terdiri dari text, dan media yang terdiri dari picture, audio, video dan sticker. Dengan jumlah object yang dilakukan pada saat pelaksanaan skenario dan eksperimen, persentase jumlah object yang dikirim dengan jumlah object yang terdeteksi sebesar 0% menggunakan tools winhex dan 0% menggunakan tools belkasoft.

Pada tabel 6.23 akan menjelaskan keseluruhan dari 3 aplikasi instant messenger yang diteliti menggunakan 2 tools, yang memiliki persentase seperti berikut ini :

Tabel 6.24 Persentase rerata jumlah artefak

Aplikasi / Tools	Winhex	Belkasoft
Facebook	60,95%	6,67%
LINE	100%	33,33%
Telegram	0%	0%

Persentase rerata jumlah artefak yang didapatkan pada tabel 6.23 untuk aplikasi facebook menggunakan tools winhex sebesar 60,59% dan belkasoft 6,67%. Untuk aplikasi LINE messenger menggunakan tools winhex sebesar 100% dan belkasoft 33,33%. Untuk aplikasi telegram messenger menghasilkan persentase 0% pada kedua tools yang digunakan.

6.5.2 Perbandingan Data Eksperimen

Berdasarkan penelitian yang telah dilakukan, berikut merupakan perbandingan data dari eksperimen yang telah dilaksanakan dalam penelitian ini

Tabel 6.25 Perbandingan Data Eksperimen

Pembanding	Eksperimen 1	Eksperimen 2
Aktivitas Eksperimen	Aktivitas biasa	Penghapusan percakapan
Ketersediaan Data Aplikasi	Lengkap	Lengkap
Ketersediaan Data Pendukung	Ada	Ada

Aktivitas pada setiap eksperimen telah diatur pada bagian sebelumnya dimana setiap eksperimen memiliki aktivitas tersendiri. Eksperimen pertama merupakan aktivitas biasa pada penggunaan aplikasi. Eksperimen kedua merupakan penggunaan aplikasi dengan tambahan aktivitas penghapusan percakapan. Eksperimen ketiga merupakan penggunaan aplikasi dengan tambahan aktivitas penghapusan aplikasi.

Berdasarkan aktivitas yang dilakukan pada setiap eksperimen akan mempengaruhi ketersediaan data aplikasi. Untuk eksperimen pertama data yang didapatkan dari aplikasi telah lengkap didapatkan. Untuk eksperimen kedua, data yang didapatkan juga sama lengkapnya.

Untuk data pendukung, perbedaan terhadap aktivitas nyatanya tidak banyak mempengaruhi ketersediaan data. Indikator jumlah data hanya dapat berubah karena kondisi aktivitas aplikasi seperti adanya penambahan percakapan atau media sehingga secara menyeluruh data pendukung tidak terpengaruh atas aktivitas yang dilakukan pada aplikasi atau perangkat.

6.6 Analisa dan Rekomendasi Keamanan Aplikasi

6.6.1 Analisa Keamanan Aplikasi

Berdasarkan hasil analisa pada bagian sebelumnya, tingkat evaluasi untuk forensika digital pada ke-3 aplikasi instant *messenger* sudah cukup baik. Hal ini dibuktikan dengan 2 aplikasi dapat dilakukan forensika digital dan dapat digunakan sebagai alat pembuktian pada sebuah kasus atau sekedar menceritakan kronologi dan bentuk percakapan pada sebuah aplikasi instant *messenger*.

Untuk examiner, aplikasi Facebook dan LINE *messenger* tidak cukup baik dalam memberikan aspek keamanan pada pelayanannya pada versi ini. Dikarenakan mudahnya dalam melakukan forensik dan mendapatkan data-data yang tidak dienkripsi sama sekali, sehingga memudahkan untuk dijadikan barang bukti digital. Untuk aplikasi Telegram *Messenger* sendiri keamanan aplikasi harus diakui memiliki

tingkat kesulitan yang cukup tinggi. Hal ini terlihat pada akses datanya, baik melalui aplikasi maupun analisa secara manual. Selain itu membuka data pada aplikasi Telegram *Messenger* juga cukup sulit jika tidak dianalisa menggunakan tools WinHex, terlebih lagi menggunakan tools Belkasoft hanya mendapatkan media data saja tanpa adanya percakapan ataupun database pada ke3 aplikasi.

6.6.1 Rekomendasi Keamanan Aplikasi

Berdasarkan implementasi. penelitian dan perbandingan, maka penulis mendapatkan fakta-fakta menarik mengenai keamanan aplikasi instant *messenger* Facebook *messenger*, LINE *Messenger* dan Telegram *Messenger*. Oleh karena itu penulis dapat memberikan rekomendasi bahwa untuk Facebook dan LINE *messenger* merupakan aplikasi instant *messenger* yang sangat mudah untuk dilakukan analisa forensika digital karena kesederhanaan struktur data serta manajemen pengelolaan data pendukung yang baik. Hal ini mempermudah para analisa atau examiner untuk segera mengungkap kasus kejahatan maupun untuk membuktikan sebuah kronologi terkait pesan dalam aplikasi Facebook dan LINE *messenger*. Selain itu kemudahan untuk verifikasi tersangka dan korban menjadi keunggulan bagi Facebook *messenger* dikarenakan ID pengguna Facebook *messenger* menggunakan nomor telepon atau tidak dienkripsi menggunakan kode lain.

Namun untuk segi keamanan dan forensika digital untuk mendapatkan bukti digital, aplikasi Telegram *Messenger* sendiri harus diakui menempati posisi lebih baik dikarenakan percakapan pada aplikasi sangat dilindungi dari tangan-tangan yang tidak bertanggung jawab dan data-data yang dienkripsi. Selain itu mengungkapkan kasus pada aplikasi Telegram *Messenger* tidak semudah Facebook dan LINE *messenger* dikarenakan data-data lebih banyak bersifat artefak (*cache*) dan jika tersimpan maka data dapat berada di beberapa folder terpisah.

BAB VII
KESIMPULAN DAN SARAN

Pada bab ini akan dijelaskan mengenai kesimpulan dari hasil penelitian pada pengerjaan tugas akhir dan saran perbaikan untuk penelitian selanjutnya.

7.1. Kesimpulan

Berdasarkan hasil penelitian pada analisa forensika digital pada aplikasi instant *messenger* yaitu LINE *Messenger*, Facebook *Messenger* dan Telegram *Messenger*, didapatkan beberapa simpulan yang dijelaskan ke dalam beberapa poin berikut ini:

1. Aplikasi Instant *Messenger* seperti LINE *Messenger*, Facebook *Messenger* dan LINE *Messenger* memiliki karakteristik masing-masing sehingga data yang didapatkan juga berbeda bergantung bagaimana struktur data yang disusun pada aplikasi.
2. Penerapan dan pengimplementasian teknik live forensics untuk mendapatkan bukti digital dari aktivitas penggunaan Instant *Messenger* membutuhkan tools dan teknik yang berbeda untuk mendapatkan analisa yang sesuai dengan yang diinginkan, terlebih terdapatnya kekurangan dari teknik live forensics yaitu tidak semua data yang didapatkan sesuai dengan yang telah direncanakan. Teknik dan tools untuk live forensics sendiri juga tidak dapat digunakan pada waktu yang lama, dikarenakan apabila RAM mati maka tidak dapat dilakukan dumping dan analisa barang bukti.
3. Perbandingan bukti digital yang didapatkan dari Instant *Messenger* berupa data yang dapat diambil dari data utama pada aplikasi. Data utama percakapan berupa data primer yang berisikan struktur pesan percakapan dan artefak file penyusun aplikasi seperti pengaturan percakapan dan alur komunikasi. Dan media pada

aplikasi yaitu file-file seperti gambar, audio, video dan sticker.

4. Pada sisi examiner, aplikasi Facebook dan LINE *messenger* merupakan aplikasi instant *messenger* yang memiliki kerentanan tinggi karena kemudahan dalam menganalisa dan validasi untuk pembuktian tersangka dan kronologi percakapan, serta kelengkapan dalam manajemen file terkait struktur pesan dan media. Sedangkan untuk Telegram *Messenger* menjadi aplikasi instant *messenger* yang penuh tantangan untuk dilakukan proses analisa forensika digital karena kerumitan data dan pembuktian percakapan untuk mendapatkan bukti digital. Dan pada sisi pelaku kejahatan, aplikasi Facebook dan LINE *messenger* merupakan aplikasi yang dalam penggunaannya dapat dijadikan barang bukti digital, sedangkan aplikasi Telegram *Messenger* menjadi aplikasi yang aman digunakan.

7.2. Saran

Berdasarkan hasil penelitan terhadap analisa *Live forensics* terhadap *Instant Messenger* yaitu LINE *Messenger*, Facebook *Messenger* dan Telegram *Messenger*, dibutuhkan penyempurnaan dalam penelitian lebih lanjut agar didapatkan hasil yang lebih baik dalam penyajian barang bukti digital untuk sebuah kasus hukum. Adapun saran yang dapat disampaikan penulis untuk penelitian selanjutnya adalah sebagai berikut :

1. Penggunaan tools lain atau tools yang berbayar seperti Belkasoft Evidence Center Ultimate dan Registry Recon. Menggunakan objek penelitian yang berbeda untuk dapat mengetahui lebih dalam bukti-bukti digital yang dapat dihasilkan.

2. Untuk pelaksanaan live forensika digital pada RAM dibutuhkan metode baku agar dapat menjamin validitas dan integritas serta kelengkapan data yang dibutuhkan.

“Halaman ini sengaja dikosongkan”

DAFTAR PUSTAKA

[1] Y. Setyorini, "Digilib ITS," September 2014. [Online]. Available: http://digilib.its.ac.id/public/ITS-Undergraduate-31303-1309100008-Chapter%201.pdf.

[2] wearesocial.com, "Annual Growth "Year on year growth trends for key digital statistic indicator"," Januari 2016. [Online]. Available: https://image.slidesharecdn.com/wearesocialdigitalin2016v02-160126235031/95/digital-in-2016-8-638.jpg?cb=1453953587.

[3] S. N, "Pengertian Random Access Memory (RAM) dan Fungsinya pada Komputer," September 2014. [Online]. Available: http://www.pengertianku.net/2014/09/pengertian-ram-dan-fungsinya-pada-komputer.html.

[4] Y. P. Galih Wicaksono, "Teknik Forensik Audio Untuk Analisa Suara Pada Barang Bukti Digital," 2013.

[5] Y. Y. Prayudi, 2016. [Online]. Available: master-fit.uii.ac.id.

[6] wearesocial.com, "Top Active Social Platforms in Indonesia," Januari 2016. [Online]. Available: https://image.slidesharecdn.com/wearesocialdigitalin2016v02-160126235031/95/digital-in-2016-224-638.jpg?cb=1453953587.

[7] wearesocial.com, "Global Digital Snapshot "A snapshot of the world key digital statistic indicators"," Januari 2016. [Online]. Available: https://image.slidesharecdn.com/wearesocialdigitalin2016v02-160126235031/95/digital-in-2016-7-638.jpg?cb=1453953587.

[8] R. U. A. Y. Muhammad Nur Faiz, "ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN KEMANANAN EMAIL PADA SISTEM OPERASI PROPRIETARY," April 2016.

[9] F. S. Fenu Gianni, "Live Digital Forensics: Windows XP vs Windows 7," Desember 2013.

[10] A. Y. M. N. F. Rusydi Umar, "ANALISIS KINERJA METODE LIVE FORENSICS UNTUK INVESTIGASI RANDOM ACCESS MEMORY PADA SISTEM PROPRIETARY," 2014.

[11] Y. P. Aan Kurniawan, "Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics," 2014.

[12] A. Chandra, Y. Kurniawan and K.-H. Rhee, "Security Analysis Testing for Secure Instant Messaging in Android with Study Case: Telegram," 2016.

[13] G. B. Satrya, P. T. Daely and M. A. Nugroho, "Digital Forensic Analysis of Telegram Messenger on Android Devices," 2016.

[14] S. Ikhsani, "Analisa Forensik Whatsapp dan LINE Messenger pada Smartphone Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia," 2016.

[15] Marshall, Digital Forensics: Digital Evidence in Criminal Investigations, 2008.

[16] S. T., "Forensik Komputer Prinsip-Prinsip Dasar," 2012.

[17] K. Amari, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory," 2009.

[18] Wikipedia, "Random Access Memory (RAM)," 2016. [Online]. Available: https://id.wikipedia.org/wiki/Memori_akses_acak.

[19] Wikipedia, "Facebook Messeger," Oktober 2016. [Online]. Available: https://en.wikipedia.org/wiki/Facebook_Messenger.

[20] Wikipedia, "Line Messenger," Februari 2016. [Online]. Available: https://id.wikipedia.org/wiki/LINE.

[21] Wikipedia, "Telegram Messenger," 2016. [Online]. Available: https://id.wikipedia.org/wiki/Telegram_(perangkat_lunak).

[22] Winhex, "Winhex," 2017. [Online]. Available: http://www.x-ways.net/winhex/.

[23] Belkasoft Evidence Center, "Belkasoft Evidence Center," 2017. [Online]. Available: https://belkasoft.com/ec.

[24] Wikipedia, "FTK Imager," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Forensic_Toolkit.

[25] Arsenal Recon, "Registry Recon," 2017. [Online]. Available: http://arsenalrecon.com/apps/recon/#features.

[26] Bounga, "Encase Forensics," 2017. [Online]. Available: https://bounga.id/id/content/encase-forensic.

[27] D. Sudyana, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory," *Akuisisi dan Imagining menggunakan FTK Imager*, 2016.

[28] R. Diansyah, "Instant Messaging," April 2011. [Online]. Available: http://besokmasihkuliah.blogspot.co.id/2011/04/instant-messaging.html.

“Halaman ini sengaja dikosongkan”

BIODATA PENULIS

Penulis memiliki nama lengkap Tayomi Dwi Larasati. Lahir di Serang, tanggal 06 Mei 1995, penulis menempuh masa sekolah di Serang-Banten, bersekolah di SD Negeri 7 Kota Serang. Dilanjutkan menempuh masa SMP di SMP Negeri 15 Kota Serang dan selanjutnya menempuh SMK Negeri 1 Kota Serang jurusan Teknik Komputer dan Jaringan. Setelah tamat pendidikan Sekolah Menengah Kejuruan, selanjutnya studi di Institut Teknologi Sepuluh Nopember Surabaya, melewati tes SBMPTN dan diterima di Departemen Sistem Informasi dengan NRP 5213100099.

Penulis aktif di organisasi tingkat Jurusan, seperti menjadi staff BEM Fakultas Teknologi Informasi (FTIf) ITS dan Lembaga Dakwah Jurusan Kajian Islam Sistem Informasi (KISI). Selain itu, penulis juga aktif pada beberapa pelatihan dan kepanitiaan dari setingkat jurusan hingga nasional, seperti LKMM, ISE! dan GERIGI ITS.

Selain bidang manajerial, Penulis juga aktif mengikuti beberapa lomba keprofesian dan minat bakat hingga berhasil menjadi Juara 2 Lomba Keamanan Jaringan dari FTIf ITS. Penulis juga pernah melakukan kerja praktik di Divisi Research and Development ID-SIRTII/CC. Selain itu, di departemen Sistem Informasi ITS sendiri, penulis juga pernah bekerja sebagai Asisten Praktikum pada mata kuliah Desian dan Manajemen Jaringan Komputer, mata kuliah Keamanan Aset dan Informasi dan mata kuliah Forensika Digital untuk masing-masing satu semester. Pada pengerjaan Tugas Akhir di Departemen Sistem Informasi ITS, penulis mengambil bidang minat Infrastruktur dan Keamanan Teknologi Informasi dengan topik Forensika Digital .Penulis dapat dihubungi melalui e-mail tayomidwi@gmail.com atau tayomidwi@outlook.com.

“Halaman ini sengaja dikosongkan”

LAMPIRAN A – Skenario Percakapan

Lampiran ini berisikan skenario percakapan yang digunakan dalam penelitian ini

Aktor	Percakapan
Korban	Hai sist, mau tanya. Gucci silvi totebag 189# A34 available ?
Korban	Send Picture
Tersangka	Availabe sist, mau pesan warna apa ?
Korban	Aku mau yang gold sist 2 ya
Korban	Send Emoji
Korban	Send Sticker
Tersangka	Isi ini dulu sist: Format Pembelian Nama: Alamat: No. HP: Pesan:
Korban	Format Pembelian : Nama: Kurnia Ayu Alamat: jl. Kertajaya Indah Blok X No. 001 No.hp: 085424631524 Pesan: Gucci Silvi Totebag 189# A34 Gold = 2
Tersangka	Aku total ya sist, Tas = Rp.11.953.063 dan ongkir Rp.25.000. Total Rp.11.978.063 Transfer ke rek a/n Gucciies Olzhop No. rek BAC 0756-9852-3564. Kalau sudah di transfer, kirim bukti trfnya ya sist
Tersangka	Send Picture
Korban	Ok, aku trf sekarang ya. Aku ke atm dulu.

A-2

Aktor	Percakapan
Korban	Sudah aku trf ya sis, ditunggu tasnya. Kepengen banget sama tas itu
Korban	Send Picture
Korban	Send Sticker
Tersangka	Siap sist, ditunggu yaa barangnya. Terimakasih sudah berbelanja di online shopping kami
Korban	Sist ? Barangnya kok belum sampai ? Sudah 2 hari saya tunggu. Katanya pengirimannya ekspress.
Korban	Send Voice note
Korban	Sist
Korban	Jangan di read aja dong
Korban	Gimana barang saya?
Korban	Sudah dikirim ?
Tersangka	Barang sedang dalam pengiriman sist, tenang saja. online shopping kami trusted 100% kok.
Korban	Kalau pengiriman ekspress seharusnya 1 hari sudah sampai dong sist, jangan macem-macemnya. Aku bisa laporin online shop ini ke polisi.
Tersangka	Silahkan saja laporkan saya ke polisi, saya tidak takut!
Korban	Send Video
Korban	Aku udah lapor ke polisi, online shopping kamu harus ditindak karna biar ngga ada yg senasib kayak aku.
Korban	Inget dosa mbak, udah nipu kok jahat bgt jadi orang.
Korban	Kembalikan uang saya
Korban	Atau polisi akan datang ke tempat kamu.

LAMPIRAN B – Hasil Winhex

Berikut ini merupakan lampiran hasil winhex dari 3 aplikasi yaitu Facebook messenger, LINE messenger dan Telegram Messenger :

FACEBOOK *MESSENGER*

OFFSET	Aktor	Percakapan
5A1994BC	Korban	Ok, aku trf sekarang ya. Aku ke atm dulu.

Hasil Winhex:

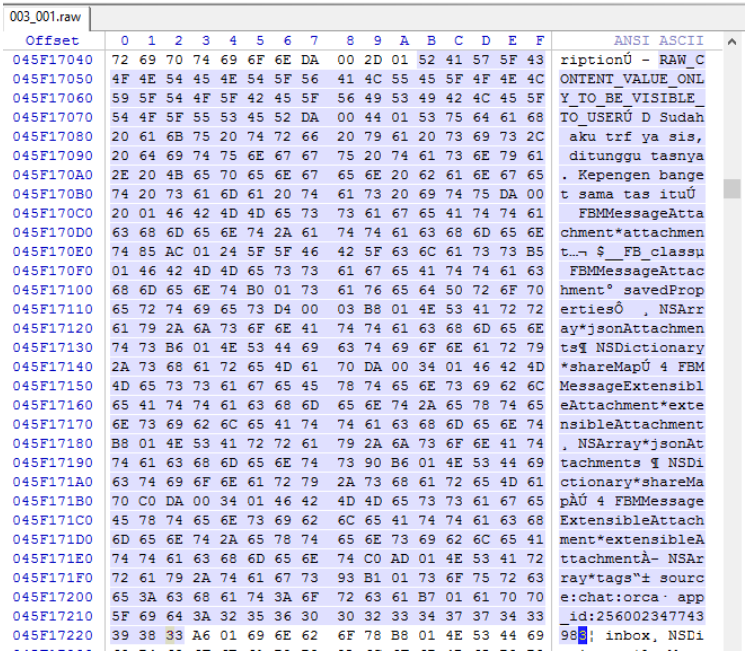
003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
05A199400	35	35	34	34	34	34	34	33	DA	00	25	01	46	42	53	74	55444443Ú % FBSt
05A199410	72	69	6E	67	57	69	74	68	52	65	64	61	63	74	65	64	ringWithRedacted
05A199420	44	65	73	63	72	69	70	74	69	6F	6E	2A	74	65	78	74	Description*text
05A199430	82	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	DA	00	,¬ $__FB_classÚ
05A199440	20	01	46	42	53	74	72	69	6E	67	57	69	74	68	52	65	FBStringWithRe
05A199450	64	61	63	74	65	64	44	65	73	63	72	69	70	74	69	6F	dactedDescriptio
05A199460	6E	DA	00	2D	01	52	41	57	5F	43	4F	4E	54	45	4E	54	nÚ - RAW_CONTENT
05A199470	5F	56	41	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	5F	42	_VALUE_ONLY_TO_B
05A199480	45	5F	56	49	53	49	42	4C	45	5F	54	4F	5F	55	53	45	E_VISIBLE_TO_USE
05A199490	52	DA	00	2A	01	4F	6B	2C	20	61	6B	75	20	74	72	66	RÚ * Ok, aku trf
05A1994A0	20	73	65	6B	61	72	61	6E	67	20	79	61	2E	20	41	6B	sekarang ya. Ak
05A1994B0	75	20	6B	65	20	61	74	6D	20	64	75	6C	75	2E	DA	00	u ke atm dulu.Ú
05A1994C0	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	FBMMessageAtta
05A1994D0	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	65	6E	chment*attachmen
05A1994E0	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	B5	t…¬ $__FB_classµ
05A1994F0	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	63	FBMMessageAttac
05A199500	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	6F	70	hment° savedProp
05A199510	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	72	72	ertiesÔ ¸ NSArr
05A199520	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	ay*jsonAttachmen
05A199530	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	ts¶ NSDictionary
05A199540	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	42	4D	*shareMapÚ 4 FBM
05A199550	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	6C	MessageExtensibl
05A199560	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	65	eAttachment*exte
05A199570	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	nsibleAttachment
05A199580	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	¸ NSArray*jsonAt
05A199590	74	61	63	68	6D	65	6E	74	73	90	B6	01	4E	53	44	69	tachments ¶ NSDi
05A1995A0	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	ctionary*shareMa
05A1995B0	70	C0	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	pÀÚ 4 FBMMessage
05A1995C0	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	ExtensibleAttach
05A1995D0	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	ment*extensibleA
05A1995E0	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	41	72	ttachmentÀ- NSAr
05A1995F0	72	61	79	2A	74	61	67	73	93	B1	01	73	6F	75	72	63	ray*tags“± sourc
05A199600	65	3A	63	68	61	74	3A	6F	72	63	61	B7	01	61	70	70	e:chat:orca· app
05A199610	5F	69	64	3A	32	35	36	30	30	32	33	34	37	37	34	33	_id:256002347743
05A199620	39	38	33	A6	01	69	6E	62	6F	78	B8	01	4E	53	44	69	983¦ inbox¸ NSDi

B-2

OFFSET	Aktor	Percakapan
45F170BD	Korban	Sudah aku trf ya sis, ditunggu tasnya. Kepengen banget sama tas itu

Hasil Winhex:

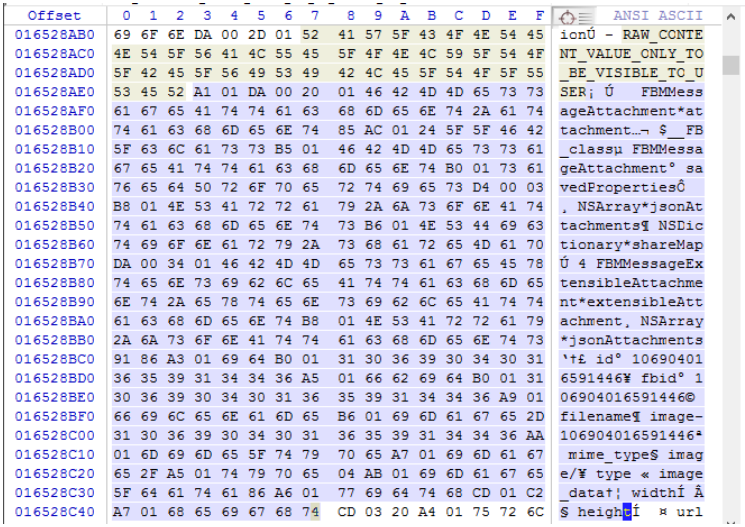


003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
045F17040	72	69	70	74	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	riptionÚ - RAW_C
045F17050	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	ONTENT_VALUE_ONL
045F17060	59	5F	54	4F	5F	42	45	5F	56	49	53	49	42	4C	45	5F	Y_TO_BE_VISIBLE_
045F17070	54	4F	5F	55	53	45	52	DA	00	44	01	53	75	64	61	68	TO_USERÚ D Sudah
045F17080	20	61	6B	75	20	74	72	66	20	79	61	20	73	69	73	2C	aku trf ya sis,
045F17090	20	64	69	74	75	6E	67	67	75	20	74	61	73	6E	79	61	ditunggu tasnya
045F170A0	2E	20	4B	65	70	65	6E	67	65	6E	20	62	61	6E	67	65	. Kepengen bange
045F170B0	74	20	73	61	6D	61	20	74	61	73	20	69	74	75	DA	00	t sama tas ituÚ
045F170C0	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	FBMMessageAtta
045F170D0	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	65	6E	chment*attachmen
045F170E0	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	B5	t…¬ $__FB_classµ
045F170F0	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	63	FBMMessageAttac
045F17100	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	6F	70	hment° savedProp
045F17110	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	72	72	ertiesÔ ¸ NSArr
045F17120	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	ay*jsonAttachmen
045F17130	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	ts¶ NSDictionary
045F17140	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	42	4D	*shareMapÚ 4 FBM
045F17150	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	6C	MessageExtensibl
045F17160	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	65	eAttachment*exte
045F17170	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	nsibleAttachment
045F17180	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	¸ NSArray*jsonAt
045F17190	74	61	63	68	6D	65	6E	74	73	90	B6	01	4E	53	44	69	tachments ¶ NSDi
045F171A0	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	ctionary*shareMa
045F171B0	70	C0	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	pÀÚ 4 FBMMessage
045F171C0	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	ExtensibleAttach
045F171D0	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	ment*extensibleA
045F171E0	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	41	72	ttachmentÀ- NSAr
045F171F0	72	61	79	2A	74	61	67	73	93	B1	01	73	6F	75	72	63	ray*tags“± sourc
045F17200	65	3A	63	68	61	74	3A	6F	72	63	61	B7	01	61	70	70	e:chat:orca· app
045F17210	5F	69	64	3A	32	35	36	30	30	32	33	34	37	37	34	33	_id:256002347743
045F17220	39	38	33	A6	01	69	6E	62	6F	78	B8	01	4E	53	44	69	983¦ inbox¸ NSDi

OFFSET	Aktor	Percakapan
16528C2B	Korban	Send Picture

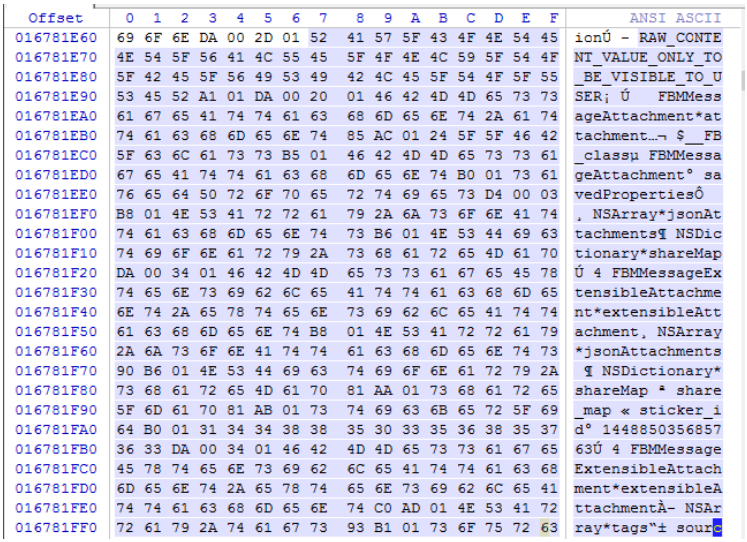
Hasil Winhex:



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
016528AB0	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	4F	4E	54	45	ionÚ - RAW_CONTE
016528AC0	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	NT_VALUE_ONLY_TO
016528AD0	5F	42	45	5F	56	49	53	49	42	4C	45	5F	54	4F	5F	55	_BE_VISIBLE_TO_U
016528AE0	53	45	52	A1	01	DA	00	20	01	46	42	4D	4D	65	73	73	SER¡ Ú FBMMess
016528AF0	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	74	ageAttachment*at
016528B00	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	42	tachment…¬ $__FB
016528B10	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	61	_classµ FBMMessa
016528B20	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	61	geAttachment° sa
016528B30	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	00	03	vedPropertiesÔ
016528B40	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	¸ NSArray*jsonAt
016528B50	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	63	tachments¶ NSDic
016528B60	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	70	tionary*shareMap
016528B70	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	45	78	Ú 4 FBMMessageEx
016528B80	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	tensibleAttachme
016528B90	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	74	nt*extensibleAtt
016528BA0	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	79	achment¸ NSArray
016528BB0	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	73	*jsonAttachments
016528BC0	91	86	A3	01	69	64	B0	01	31	30	36	39	30	34	30	31	‘†£ id° 10690401
016528BD0	36	35	39	31	34	34	36	A5	01	66	62	69	64	B0	01	31	6591446¥ fbid° 1
016528BE0	30	36	39	30	34	30	31	36	35	39	31	34	34	36	A9	01	069040165914466©
016528BF0	66	69	6C	65	6E	61	6D	65	B6	01	69	6D	61	67	65	2D	filename¶ image-
016528C00	31	30	36	39	30	34	30	31	36	35	39	31	34	34	36	AA	106904016591446ª
016528C10	01	6D	69	6D	65	5F	74	79	70	65	A7	01	69	6D	61	67	mime_type§ imag
016528C20	65	2F	A5	01	74	79	70	65	04	AB	01	69	6D	61	67	65	e/¥ type « image
016528C30	5F	64	61	74	61	86	A6	01	77	69	64	74	68	CD	01	C2	_data†¦ widthÍ Â
016528C40	A7	01	68	65	69	67	68	74	CD	03	20	A4	01	75	72	6C	§ heightÍ ¤ url

OFFSET	Aktor	Percakapan
16781F97	Korban	Send Sticker

Hasil Winhex:

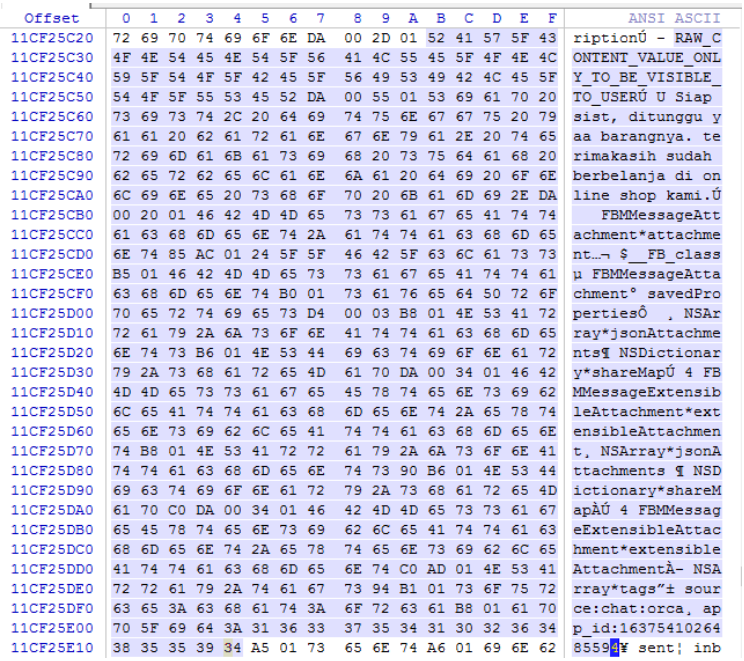


Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
016781E60	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	4F	4E	54	45	ionÚ - RAW_CONTE
016781E70	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	NT_VALUE_ONLY_TO
016781E80	5F	42	45	5F	56	49	53	49	42	4C	45	5F	54	4F	5F	55	_BE_VISIBLE_TO_U
016781E90	53	45	52	A1	01	DA	00	20	01	46	42	4D	4D	65	73	73	SER¡ Ú FBMMess
016781EA0	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	74	ageAttachment*at
016781EB0	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	42	tachment…¬ $__FB
016781EC0	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	61	_classµ FBMMessa
016781ED0	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	61	geAttachment° sa
016781EE0	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	00	03	vedPropertiesÔ
016781EF0	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	¸ NSArray*jsonAt
016781F00	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	63	tachments¶ NSDic
016781F10	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	70	tionary*shareMap
016781F20	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	45	78	Ú 4 FBMMessageEx
016781F30	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	tensibleAttachme
016781F40	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	74	nt*extensibleAtt
016781F50	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	79	achment¸ NSArray
016781F60	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	73	*jsonAttachments
016781F70	90	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	2A	¶ NSDictionary*
016781F80	73	68	61	72	65	4D	61	70	81	AA	01	73	68	61	72	65	shareMap ª share
016781F90	5F	6D	61	70	81	AB	01	73	74	69	63	6B	65	72	5F	69	_map « sticker_i
016781FA0	64	B0	01	31	34	34	38	38	35	30	33	35	36	38	35	37	d° 1448850356857
016781FB0	36	33	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	63Ú 4 FBMMessage
016781FC0	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	ExtensibleAttach
016781FD0	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	ment*extensibleA
016781FE0	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	41	72	ttachmentÀ- NSAr
016781FF0	72	61	79	2A	74	61	67	73	93	B1	01	73	6F	75	72	63	ray*tags“± sourc

B-4

OFFSET	Aktor	Percakapan
11CF25CAD	Tersangka	Siap sist, ditunggu yaa barangnya. Terimakasih sudah berbelanja di online shopping kami

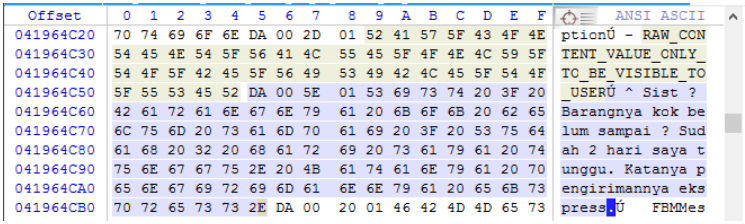
Hasil Winhex:



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
11CF25C20	72	69	70	74	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	riptionÚ - RAW_C
11CF25C30	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	ONTENT_VALUE_ONL
11CF25C40	59	5F	54	4F	5F	42	45	5F	56	49	53	49	42	4C	45	5F	Y_TO_BE_VISIBLE_
11CF25C50	54	4F	5F	55	53	45	52	DA	00	55	01	53	69	61	70	20	TO_USERÚ U Siap
11CF25C60	73	69	73	74	2C	20	64	69	74	75	6E	67	67	75	20	79	sist, ditunggu y
11CF25C70	61	61	20	62	61	72	61	6E	67	6E	79	61	2E	20	74	65	aa barangnya. te
11CF25C80	72	69	6D	61	6B	61	73	69	68	20	73	75	64	61	68	20	rimakasih sudah
11CF25C90	62	65	72	62	65	6C	61	6E	6A	61	20	64	69	20	6F	6E	berbelanja di on
11CF25CA0	6C	69	6E	65	20	73	68	6F	70	20	6B	61	6D	69	2E	DA	line shop kami.Ú
11CF25CB0	00	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	FBMMessageAtt
11CF25CC0	61	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	65	achment*attachme
11CF25CD0	6E	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	nt…¬ $__FB_class
11CF25CE0	B5	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	µ FBMMessageAtta
11CF25CF0	63	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	6F	chment° savedPro
11CF25D00	70	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	72	pertiesÔ ¸ NSAr
11CF25D10	72	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	ray*jsonAttachme
11CF25D20	6E	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	nts¶ NSDictionar
11CF25D30	79	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	42	y*shareMapÚ 4 FB
11CF25D40	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	MMessageExtensib
11CF25D50	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	leAttachment*ext
11CF25D60	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	ensibleAttachmen
11CF25D70	74	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	t¸ NSArray*jsonA
11CF25D80	74	74	61	63	68	6D	65	6E	74	73	90	B6	01	4E	53	44	ttachments ¶ NSD
11CF25D90	69	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	ictionary*shareM
11CF25DA0	61	70	C0	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	apÀÚ 4 FBMMessag
11CF25DB0	65	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	eExtensibleAttac
11CF25DC0	68	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	hment*extensible
11CF25DD0	41	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	41	AttachmentÀ- NSA
11CF25DE0	72	72	61	79	2A	74	61	67	73	94	B1	01	73	6F	75	72	rray*tags”± sour
11CF25DF0	63	65	3A	63	68	61	74	3A	6F	72	63	61	B8	01	61	70	ce:chat:orca¸ ap
11CF25E00	70	5F	69	64	3A	31	36	33	37	35	34	31	30	32	36	34	p_id:16375410264
11CF25E10	38	35	35	39	34	A5	01	73	65	6E	74	A6	01	69	6E	62	85594¥ sent¦ inb

OFFSET	Aktor	Percakapan
90FD14BC	Korban	Sist ? Barangnya kok belum sampai ? Sudah 2 hari saya tunggu. Katanya pengirimannya ekspress.

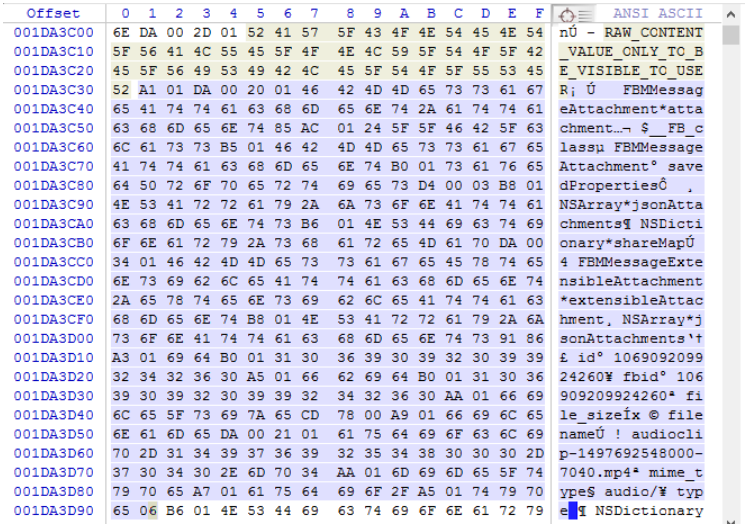
Hasil Winhex:



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
041964C20	70	74	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	4F	4E	ptionÚ - RAW_CON
041964C30	54	45	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	59	5F	TENT_VALUE_ONLY_
041964C40	54	4F	5F	42	45	5F	56	49	53	49	42	4C	45	5F	54	4F	TO_BE_VISIBLE_TO
041964C50	5F	55	53	45	52	DA	00	5E	01	53	69	73	74	20	3F	20	_USERÚ ^ Sist ?
041964C60	42	61	72	61	6E	67	6E	79	61	20	6B	6F	6B	20	62	65	Barangnya kok be
041964C70	6C	75	6D	20	73	61	6D	70	61	69	20	3F	20	53	75	64	lum sampai ? Sud
041964C80	61	68	20	32	20	68	61	72	69	20	73	61	79	61	20	74	ah 2 hari saya t
041964C90	75	6E	67	67	75	2E	20	4B	61	74	61	6E	79	61	20	70	unggu. Katanya p
041964CA0	65	6E	67	69	72	69	6D	61	6E	6E	79	61	20	65	6B	73	engirimannya eks
041964CB0	70	72	65	73	73	2E	DA	00	20	01	46	42	4D	4D	65	73	press.Ú FBMMes

OFFSET	Aktor	Percakapan
1DA3D58	Korban	Send Voice note

Hasil Winhex:



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
001DA3C00	6E	DA	00	2D	01	52	41	57	5F	43	4F	4E	54	45	4E	54	nÚ - RAW_CONTENT
001DA3C10	5F	56	41	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	5F	42	_VALUE_ONLY_TO_B
001DA3C20	45	5F	56	49	53	49	42	4C	45	5F	54	4F	5F	55	53	45	E_VISIBLE_TO_USE
001DA3C30	52	A1	01	DA	00	20	01	46	42	4D	4D	65	73	73	61	67	R¡ Ú FBMMessag
001DA3C40	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	74	74	61	eAttachment*atta
001DA3C50	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	42	5F	63	chment…¬ $__FB_c
001DA3C60	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	61	67	65	lassµ FBMMessage
001DA3C70	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	61	76	65	Attachment° save
001DA3C80	64	50	72	6F	70	65	72	74	69	65	73	D4	00	03	B8	01	dPropertiesÔ ¸
001DA3C90	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	74	61	NSArray*jsonAtta
001DA3CA0	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	63	74	69	chments¶ NSDicti
001DA3CB0	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	70	DA	00	onary*shareMapÚ
001DA3CC0	34	01	46	42	4D	4D	65	73	73	61	67	65	45	78	74	65	4 FBMMessageExte
001DA3CD0	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	nsibleAttachment
001DA3CE0	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	*extensibleAttac
001DA3CF0	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	79	2A	6A	hment¸ NSArray*j
001DA3D00	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	73	91	86	sonAttachments'†
001DA3D10	A3	01	69	64	B0	01	31	30	36	39	30	39	32	30	39	39	£ id° 1069092099
001DA3D20	32	34	32	36	30	A5	01	66	62	69	64	B0	01	31	30	36	24260¥ fbid° 106
001DA3D30	39	30	39	32	30	39	39	32	34	32	36	30	AA	01	66	69	909209924260ª fi
001DA3D40	6C	65	5F	73	69	7A	65	CD	78	00	A9	01	66	69	6C	65	le_sizeÍx © file
001DA3D50	6E	61	6D	65	DA	00	21	01	61	75	64	69	6F	63	6C	69	nameÚ ! audiocli
001DA3D60	70	2D	31	34	39	37	36	39	32	35	34	38	30	30	30	2D	p-1497692548000-
001DA3D70	37	30	34	30	2E	6D	70	34	AA	01	6D	69	6D	65	5F	74	7040.mp4ª mime_t
001DA3D80	79	70	65	A7	01	61	75	64	69	6F	2F	A5	01	74	79	70	ype§ audio/¥ typ
001DA3D90	65	06	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	e¶ NSDictionary

B-6

OFFSET	Aktor	Percakapan
4DE62CB5	Korban	Sist

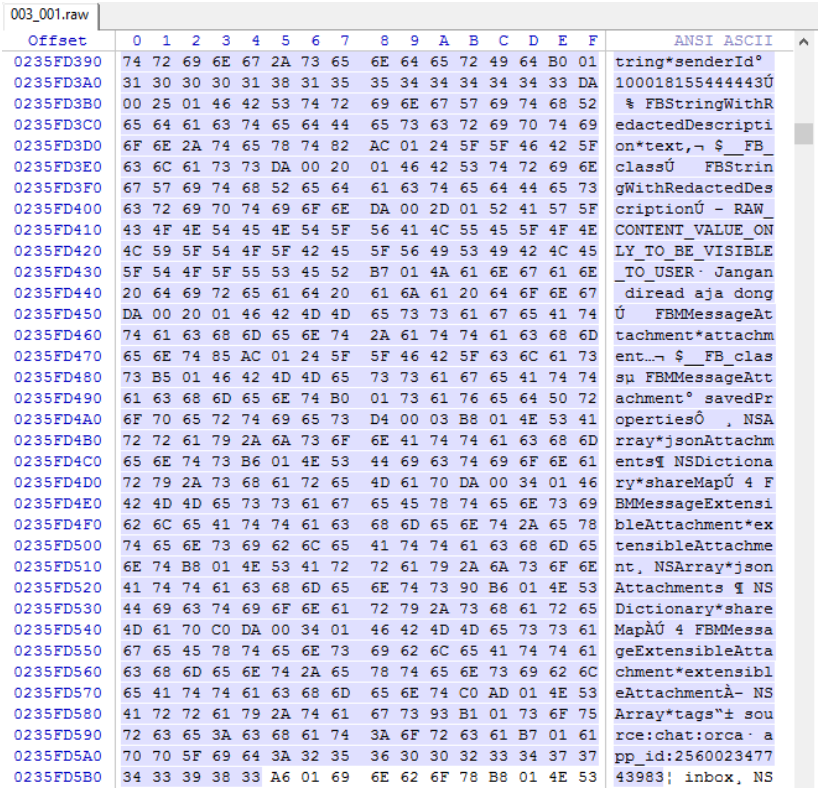
Hasil Winhex:

003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
04DE62C10	6E	64	65	72	49	64	B0	01	31	30	30	30	31	38	31	35	nderId° 10001815
04DE62C20	35	34	34	34	34	34	33	DA	00	25	01	46	42	53	74	72	5444443Ú % FBStr
04DE62C30	69	6E	67	57	69	74	68	52	65	64	61	63	74	65	64	44	ingWithRedactedD
04DE62C40	65	73	63	72	69	70	74	69	6F	6E	2A	74	65	78	74	82	escription*text,
04DE62C50	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	DA	00	20	¬ $__FB_classÚ
04DE62C60	01	46	42	53	74	72	69	6E	67	57	69	74	68	52	65	64	FBStringWithRed
04DE62C70	61	63	74	65	64	44	65	73	63	72	69	70	74	69	6F	6E	actedDescription
04DE62C80	DA	00	2D	01	52	41	57	5F	43	4F	4E	54	45	4E	54	5F	Ú - RAW_CONTENT_
04DE62C90	56	41	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	5F	42	45	VALUE_ONLY_TO_BE
04DE62CA0	5F	56	49	53	49	42	4C	45	5F	54	4F	5F	55	53	45	52	_VISIBLE_TO_USER
04DE62CB0	A5	01	53	69	73	74	DA	00	20	01	46	42	4D	4D	65	73	¥ SistÚ FBMMes
04DE62CC0	73	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	sageAttachment*a
04DE62CD0	74	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	ttachment…¬ $__F
04DE62CE0	42	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	B_classµ FBMMess
04DE62CF0	61	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	ageAttachment° s
04DE62D00	61	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	00	avedPropertiesÔ
04DE62D10	03	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	¸ NSArray*jsonA
04DE62D20	74	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	ttachments¶ NSDi
04DE62D30	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	ctionary*shareMa
04DE62D40	70	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	45	pÚ 4 FBMMessageE
04DE62D50	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	xtensibleAttachm
04DE62D60	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	ent*extensibleAt
04DE62D70	74	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	tachment¸ NSArra
04DE62D80	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	y*jsonAttachment
04DE62D90	73	90	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	s ¶ NSDictionary
04DE62DA0	2A	73	68	61	72	65	4D	61	70	C0	DA	00	34	01	46	42	*shareMapÀÚ 4 FB
04DE62DB0	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	MMessageExtensib
04DE62DC0	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	leAttachment*ext
04DE62DD0	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	ensibleAttachmen
04DE62DE0	74	C0	AD	01	4E	53	41	72	72	61	79	2A	74	61	67	73	tÀ- NSArray*tags
04DE62DF0	93	B1	01	73	6F	75	72	63	65	3A	63	68	61	74	3A	6F	"± source:chat:o
04DE62E00	72	63	61	B7	01	61	70	70	5F	69	64	3A	32	35	36	30	rca· app_id:2560
04DE62E10	30	32	33	34	37	37	34	33	39	38	33	A6	01	69	6E	62	0234774398¦ inb

OFFSET	Aktor	Percakapan
235FD44F	Korban	Jangan di read aja dong

Hasil Winhex:



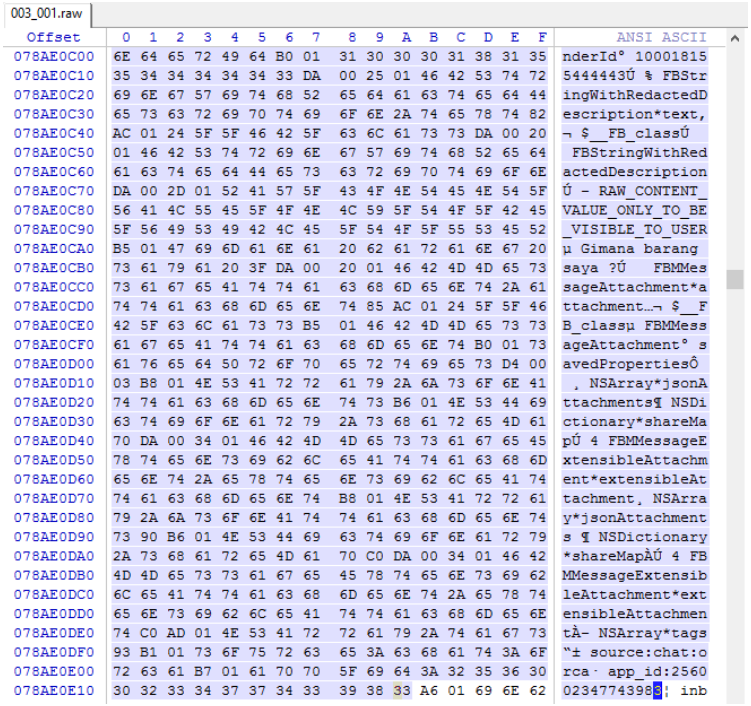
003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0235FD390	74	72	69	6E	67	2A	73	65	6E	64	65	72	49	64	B0	01	tring*senderId°
0235FD3A0	31	30	30	30	31	38	31	35	35	34	34	34	34	34	33	DA	1000181554444433Ú
0235FD3B0	00	25	01	46	42	53	74	72	69	6E	67	57	69	74	68	52	% FBStringWithR
0235FD3C0	65	64	61	63	74	65	64	44	65	73	63	72	69	70	74	69	edactedDescripti
0235FD3D0	6F	6E	2A	74	65	78	74	82	AC	01	24	5F	5F	46	42	5F	on*text,¬ $__FB_
0235FD3E0	63	6C	61	73	73	DA	00	20	01	46	42	53	74	72	69	6E	classÚ FBStrin
0235FD3F0	67	57	69	74	68	52	65	64	61	63	74	65	64	44	65	73	gWithRedactedDes
0235FD400	63	72	69	70	74	69	6F	6E	DA	00	2D	01	52	41	57	5F	criptionÚ - RAW_
0235FD410	43	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	5F	4F	4E	CONTENT_VALUE_ON
0235FD420	4C	59	5F	54	4F	5F	42	45	5F	56	49	53	49	42	4C	45	LY_TO_BE_VISIBLE
0235FD430	5F	54	4F	5F	55	53	45	52	B7	01	4A	61	6E	67	61	6E	_TO_USER· Jangan
0235FD440	20	64	69	72	65	61	64	20	61	6A	61	20	64	6F	6E	67	diread aja dong
0235FD450	DA	00	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	Ú FBMMessageAt
0235FD460	74	61	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	tachment*attachm
0235FD470	65	6E	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	ent…¬ $__FB_clas
0235FD480	73	B5	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	sµ FBMMessageAtt
0235FD490	61	63	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	achment° savedPr
0235FD4A0	6F	70	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	opertiesÔ ¸ NSA
0235FD4B0	72	72	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	rray*jsonAttachm
0235FD4C0	65	6E	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	ents¶ NSDictiona
0235FD4D0	72	79	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	ry*shareMapÚ 4 F
0235FD4E0	42	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	BMMessageExtensi
0235FD4F0	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	bleAttachment*ex
0235FD500	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	tensibleAttachme
0235FD510	6E	74	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	nt¸ NSArray*json
0235FD520	41	74	74	61	63	68	6D	65	6E	74	73	90	B6	01	4E	53	Attachments ¶ NS
0235FD530	44	69	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	Dictionary*share
0235FD540	4D	61	70	C0	DA	00	34	01	46	42	4D	4D	65	73	73	61	MapÀÚ 4 FBMMessa
0235FD550	67	65	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	geExtensibleAtta
0235FD560	63	68	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	chment*extensibl
0235FD570	65	41	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	eAttachmentÀ- NS
0235FD580	41	72	72	61	79	2A	74	61	67	73	93	B1	01	73	6F	75	Array*tags“± sou
0235FD590	72	63	65	3A	63	68	61	74	3A	6F	72	63	61	B7	01	61	rce:chat:orca· a
0235FD5A0	70	70	5F	69	64	3A	32	35	36	30	30	32	33	34	37	37	pp_id:2560023477
0235FD5B0	34	33	39	38	33	A6	01	69	6E	62	6F	78	B8	01	4E	53	43983¦ inbox¸ NS

B-8

OFFSET	Aktor	Percakapan
78AE0CB3	Korban	Gimana barang saya?

Hasil Winhex:

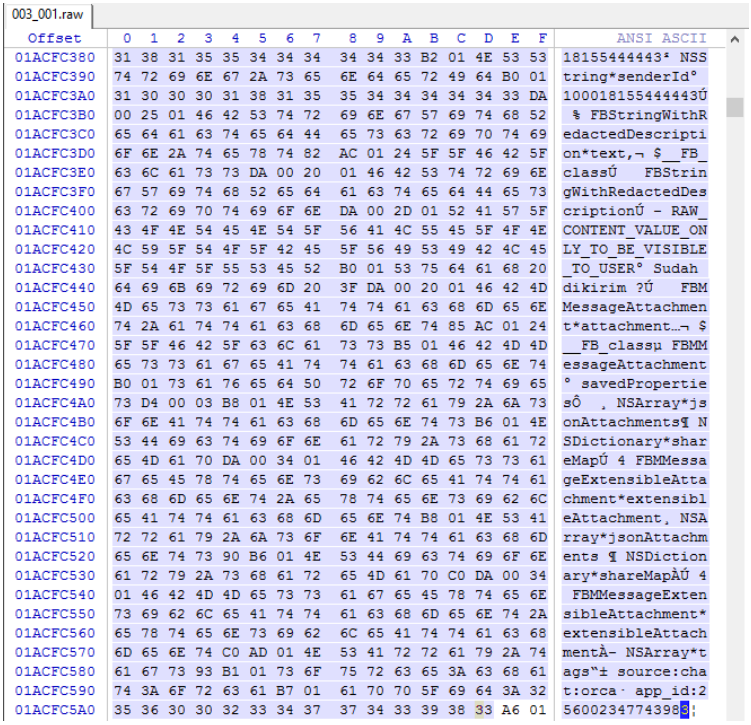


003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
078AE0C00	6E	64	65	72	49	64	B0	01	31	30	30	30	31	38	31	35	nderId° 10001815
078AE0C10	35	34	34	34	34	34	33	DA	00	25	01	46	42	53	74	72	5444443Ú % FBStr
078AE0C20	69	6E	67	57	69	74	68	52	65	64	61	63	74	65	64	44	ingWithRedactedD
078AE0C30	65	73	63	72	69	70	74	69	6F	6E	2A	74	65	78	74	82	escription*text,
078AE0C40	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	DA	00	20	¬ $__FB_classÚ
078AE0C50	01	46	42	53	74	72	69	6E	67	57	69	74	68	52	65	64	FBStringWithRed
078AE0C60	61	63	74	65	64	44	65	73	63	72	69	70	74	69	6F	6E	actedDescription
078AE0C70	DA	00	2D	01	52	41	57	5F	43	4F	4E	54	45	4E	54	5F	Ú - RAW_CONTENT_
078AE0C80	56	41	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	5F	42	45	VALUE_ONLY_TO_BE
078AE0C90	5F	56	49	53	49	42	4C	45	5F	54	4F	5F	55	53	45	52	_VISIBLE_TO_USER
078AE0CA0	B5	01	47	69	6D	61	6E	61	20	62	61	72	61	6E	67	20	µ Gimana barang
078AE0CB0	73	61	79	61	20	3F	DA	00	20	01	46	42	4D	4D	65	73	saya ?Ú FBMMes
078AE0CC0	73	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	sageAttachment*a
078AE0CD0	74	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	ttachment…¬ $__F
078AE0CE0	42	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	B_classµ FBMMess
078AE0CF0	61	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	ageAttachment° s
078AE0D00	61	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	00	avedPropertiesÔ
078AE0D10	03	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	¸ NSArray*jsonA
078AE0D20	74	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	ttachments¶ NSDi
078AE0D30	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	ctionary*shareMa
078AE0D40	70	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	45	pÚ 4 FBMMessageE
078AE0D50	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	xtensibleAttachm
078AE0D60	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	ent*extensibleAt
078AE0D70	74	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	tachment¸ NSArra
078AE0D80	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	y*jsonAttachment
078AE0D90	73	90	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	s ¶ NSDictionary
078AE0DA0	2A	73	68	61	72	65	4D	61	70	C0	DA	00	34	01	46	42	*shareMapÀÚ 4 FB
078AE0DB0	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	MMessageExtensib
078AE0DC0	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	leAttachment*ext
078AE0DD0	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	ensibleAttachmen
078AE0DE0	74	C0	AD	01	4E	53	41	72	72	61	79	2A	74	61	67	73	tÀ- NSArray*tags
078AE0DF0	93	B1	01	73	6F	75	72	63	65	3A	63	68	61	74	3A	6F	"± source:chat:o
078AE0E00	72	63	61	B7	01	61	70	70	5F	69	64	3A	32	35	36	30	rca· app_id:2560
078AE0E10	30	32	33	34	37	37	34	33	39	38	33	A6	01	69	6E	62	0234774398¦ inb

OFFSET	Aktor	Percakapan
1ACFC447	Korban	Sudah dikirim ?

Hasil Winhex:



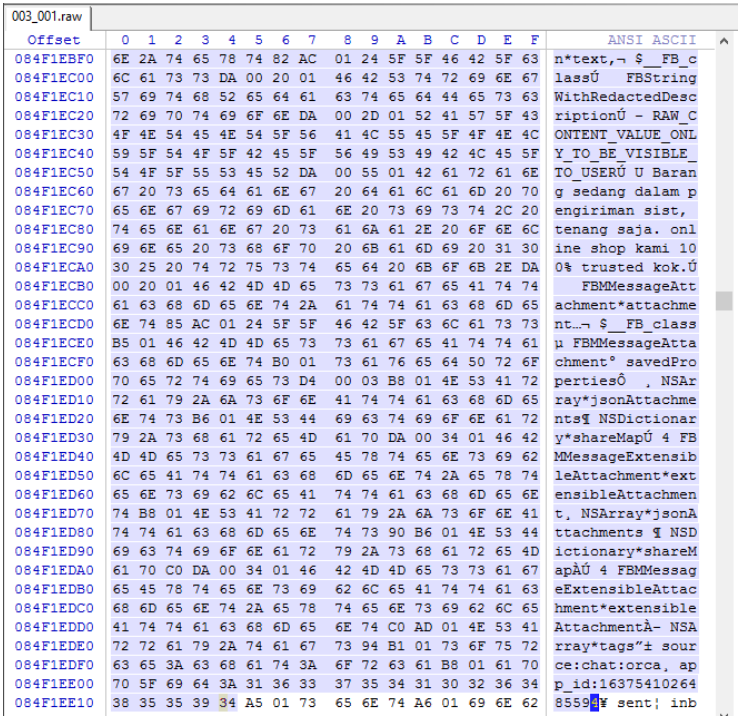
003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
01ACFC380	31	38	31	35	35	34	34	34	34	34	33	B2	01	4E	53	53	181554444443² NSS
01ACFC390	74	72	69	6E	67	2A	73	65	6E	64	65	72	49	64	B0	01	tring*senderId°
01ACFC3A0	31	30	30	30	31	38	31	35	35	34	34	34	34	34	33	DA	10001815544444 3Ú
01ACFC3B0	00	25	01	46	42	53	74	72	69	6E	67	57	69	74	68	52	% FBStringWithR
01ACFC3C0	65	64	61	63	74	65	64	44	65	73	63	72	69	70	74	69	edactedDescripti
01ACFC3D0	6F	6E	2A	74	65	78	74	82	AC	01	24	5F	5F	46	42	5F	on*text,¬ $__FB_
01ACFC3E0	63	6C	61	73	73	DA	00	20	01	46	42	53	74	72	69	6E	classÚ FBStrin
01ACFC3F0	67	57	69	74	68	52	65	64	61	63	74	65	64	44	65	73	gWithRedactedDes
01ACFC400	63	72	69	70	74	69	6F	6E	DA	00	2D	01	52	41	57	5F	criptionÚ - RAW_
01ACFC410	43	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	5F	4F	4E	CONTENT_VALUE_ON
01ACFC420	4C	59	5F	54	4F	5F	42	45	5F	56	49	53	49	42	4C	45	LY_TO_BE_VISIBLE
01ACFC430	5F	54	4F	5F	55	53	45	52	B0	01	53	75	64	61	68	20	_TO_USER° Sudah
01ACFC440	64	69	6B	69	72	69	6D	20	3F	DA	00	20	01	46	42	4D	dikirim ?Ú FBM
01ACFC450	4D	65	73	73	61	67	65	41	74	74	61	63	68	6D	65	6E	MessageAttachmen
01ACFC460	74	2A	61	74	74	61	63	68	6D	65	6E	74	85	AC	01	24	t*attachment…¬ $
01ACFC470	5F	5F	46	42	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	__FB_classµ FBMM
01ACFC480	65	73	73	61	67	65	41	74	74	61	63	68	6D	65	6E	74	essageAttachment
01ACFC490	B0	01	73	61	76	65	64	50	72	6F	70	65	72	74	69	65	° savedPropertie
01ACFC4A0	73	D4	00	03	B8	01	4E	53	41	72	72	61	79	2A	6A	73	sÔ ¸ NSArray*js
01ACFC4B0	6F	6E	41	74	74	61	63	68	6D	65	6E	74	73	B6	01	4E	onAttachments¶ N
01ACFC4C0	53	44	69	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	SDictionary*shar
01ACFC4D0	65	4D	61	70	DA	00	34	01	46	42	4D	4D	65	73	73	61	eMapÚ 4 FBMMessa
01ACFC4E0	67	65	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	geExtensibleAtta
01ACFC4F0	63	68	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	chment*extensibl
01ACFC500	65	41	74	74	61	63	68	6D	65	6E	74	B8	01	4E	53	41	eAttachment¸ NSA
01ACFC510	72	72	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	rray*jsonAttachm
01ACFC520	65	6E	74	73	90	B6	01	4E	53	44	69	63	74	69	6F	6E	ents ¶ NSDiction
01ACFC530	61	72	79	2A	73	68	61	72	65	4D	61	70	C0	DA	00	34	ary*shareMapÀÚ 4
01ACFC540	01	46	42	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	FBMMessageExten
01ACFC550	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	sibleAttachment*
01ACFC560	65	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	extensibleAttach
01ACFC570	6D	65	6E	74	C0	AD	01	4E	53	41	72	72	61	79	2A	74	mentÀ- NSArray*t
01ACFC580	61	67	73	93	B1	01	73	6F	75	72	63	65	3A	63	68	61	ags“± source:cha
01ACFC590	74	3A	6F	72	63	61	B7	01	61	70	70	5F	69	64	3A	32	t:orca· app_id:2
01ACFC5A0	35	36	30	30	32	33	34	37	37	34	33	39	38	33	A6	01	560023477439 8¦

B-10

OFFSET	Aktor	Percakapan
84F1ECAD	Tersangka	Barang sedang dalam pengiriman sist, tenang saja. online shopping kami trusted 100% kok.

Hasil Winhex

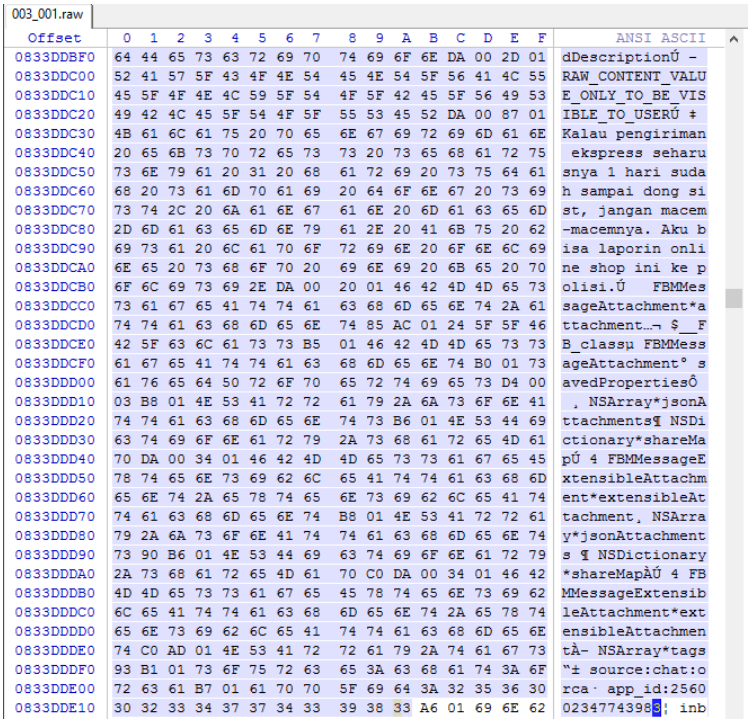


003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
084F1EBF0	6E	2A	74	65	78	74	82	AC	01	24	5F	5F	46	42	5F	63	n*text,¬ $__FB_c
084F1EC00	6C	61	73	73	DA	00	20	01	46	42	53	74	72	69	6E	67	lassÚ FBString
084F1EC10	57	69	74	68	52	65	64	61	63	74	65	64	44	65	73	63	WithRedactedDesc
084F1EC20	72	69	70	74	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	riptionÚ - RAW_C
084F1EC30	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	ONTENT_VALUE_ONL
084F1EC40	59	5F	54	4F	5F	42	45	5F	56	49	53	49	42	4C	45	5F	Y_TO_BE_VISIBLE_
084F1EC50	54	4F	5F	55	53	45	52	DA	00	55	01	42	61	72	61	6E	TO_USERÚ U Baran
084F1EC60	67	20	73	65	64	61	6E	67	20	64	61	6C	61	6D	20	70	g sedang dalam p
084F1EC70	65	6E	67	69	72	69	6D	61	6E	20	73	69	73	74	2C	20	engiriman sist,
084F1EC80	74	65	6E	61	6E	67	20	73	61	6A	61	2E	20	6F	6E	6C	tenang saja. onl
084F1EC90	69	6E	65	20	73	68	6F	70	20	6B	61	6D	69	20	31	30	ine shop kami 10
084F1ECA0	30	25	20	74	72	75	73	74	65	64	20	6B	6F	6B	2E	DA	0% trusted kok.Ú
084F1ECB0	00	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	FBMMessageAtt
084F1ECC0	61	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	65	achment*attachme
084F1ECD0	6E	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	nt…¬ $__FB_class
084F1ECE0	B5	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	µ FBMMessageAtta
084F1ECF0	63	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	6F	chment° savedPro
084F1ED00	70	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	72	pertiesÔ ¸ NSAr
084F1ED10	72	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	ray*jsonAttachme
084F1ED20	6E	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	nts¶ NSDictionar
084F1ED30	79	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	42	y*shareMapÚ 4 FB
084F1ED40	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	MMessageExtensib
084F1ED50	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	leAttachment*ext
084F1ED60	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	ensibleAttachmen
084F1ED70	74	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	t¸ NSArray*jsonA
084F1ED80	74	74	61	63	68	6D	65	6E	74	73	90	B6	01	4E	53	44	ttachments ¶ NSD
084F1ED90	69	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	ictionary*shareM
084F1EDA0	61	70	C0	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	apÀÚ 4 FBMMessag
084F1EDB0	65	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	eExtensibleAttac
084F1EDC0	68	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	hment*extensible
084F1EDD0	41	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	41	AttachmentÀ- NSA
084F1EDE0	72	72	61	79	2A	74	61	67	73	94	B1	01	73	6F	75	72	rray*tags"± sour
084F1EDF0	63	65	3A	63	68	61	74	3A	6F	72	63	61	B8	01	61	70	ce:chat:orca¸ ap
084F1EE00	70	5F	69	64	3A	31	36	33	37	35	34	31	30	32	36	34	p_id:16375410264
084F1EE10	38	35	35	39	34	A5	01	73	65	6E	74	A6	01	69	6E	62	85594¥ sent¦ inb

OFFSET	Aktor	Percakapan
833DDCB4	Korban	Kalau pengiriman ekspress seharusnya 1 hari sudah sampai dong sist, jangan macem-macemnya. Aku bisa laporin online shop ini ke polisi.

Hasil Winhex:



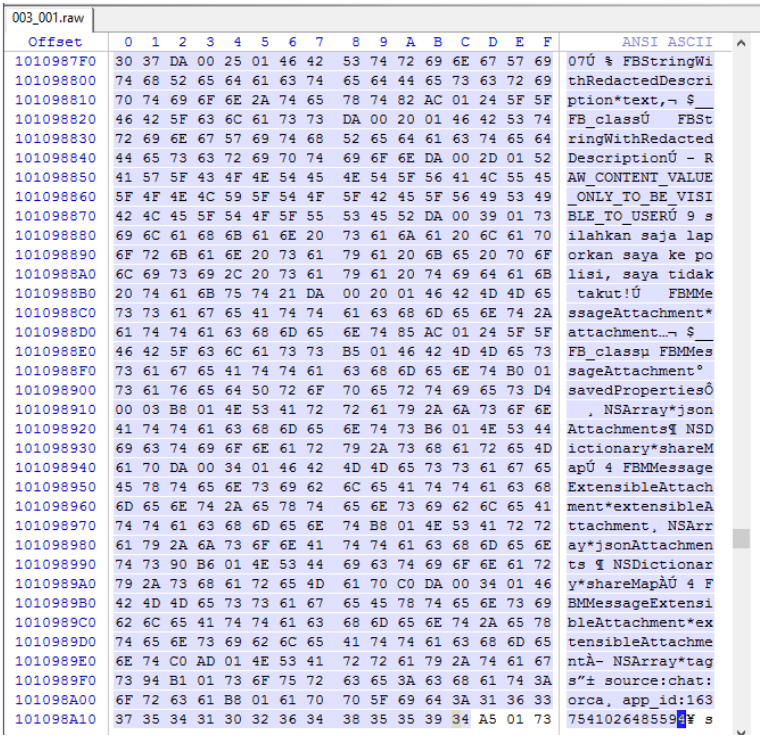
003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0833DDBF0	64	44	65	73	63	72	69	70	74	69	6F	6E	DA	00	2D	01	dDescriptionÚ -
0833DDC00	52	41	57	5F	43	4F	4E	54	45	4E	54	5F	56	41	4C	55	RAW_CONTENT_VALU
0833DDC10	45	5F	4F	4E	4C	59	5F	54	4F	5F	42	45	5F	56	49	53	E_ONLY_TO_BE_VIS
0833DDC20	49	42	4C	45	5F	54	4F	5F	55	53	45	52	DA	00	87	01	IBLE_TO_USERÚ ‡
0833DDC30	4B	61	6C	61	75	20	70	65	6E	67	69	72	69	6D	61	6E	Kalau pengiriman
0833DDC40	20	65	6B	73	70	72	65	73	73	20	73	65	68	61	72	75	ekspress seharu
0833DDC50	73	6E	79	61	20	31	20	68	61	72	69	20	73	75	64	61	snya 1 hari suda
0833DDC60	68	20	73	61	6D	70	61	69	20	64	6F	6E	67	20	73	69	h sampai dong si
0833DDC70	73	74	2C	20	6A	61	6E	67	61	6E	20	6D	61	63	65	6D	st, jangan macem
0833DDC80	2D	6D	61	63	65	6D	6E	79	61	2E	20	41	6B	75	20	62	-macemnya. Aku b
0833DDC90	69	73	61	20	6C	61	70	6F	72	69	6E	20	6F	6E	6C	69	isa laporin onli
0833DDCA0	6E	65	20	73	68	6F	70	20	69	6E	69	20	6B	65	20	70	ne shop ini ke p
0833DDCB0	6F	6C	69	73	69	2E	DA	00	20	01	46	42	4D	4D	65	73	olisi.Ú FBMMes
0833DDCC0	73	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	sageAttachment*a
0833DDCD0	74	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	ttachment…¬ $__F
0833DDCE0	42	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	B_classµ FBMMess
0833DDCF0	61	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	ageAttachment° s
0833DDD00	61	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	00	avedPropertiesÔ
0833DDD10	03	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	¸ NSArray*jsonA
0833DDD20	74	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	ttachments¶ NSDi
0833DDD30	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	ctionary*shareMa
0833DDD40	70	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	45	pÚ 4 FBMMessageE
0833DDD50	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	xtensibleAttachm
0833DDD60	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	ent*extensibleAt
0833DDD70	74	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	tachment¸ NSArra
0833DDD80	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	y*jsonAttachment
0833DDD90	73	90	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	s ¶ NSDictionary
0833DDDA0	2A	73	68	61	72	65	4D	61	70	C0	DA	00	34	01	46	42	*shareMapÀÚ 4 FB
0833DDDB0	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	MMessageExtensib
0833DDDC0	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	leAttachment*ext
0833DDDD0	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	ensibleAttachmen
0833DDDE0	74	C0	AD	01	4E	53	41	72	72	61	79	2A	74	61	67	73	tÀ- NSArray*tags
0833DDDF0	93	B1	01	73	6F	75	72	63	65	3A	63	68	61	74	3A	6F	"± source:chat:o
0833DDE00	72	63	61	B7	01	61	70	70	5F	69	64	3A	32	35	36	30	rca· app_id:2560
0833DDE10	30	32	33	34	37	37	34	33	39	38	33	A6	01	69	6E	62	0234774398¦ inb

B-12

OFFSET	Aktor	Percakapan
10109888D	Tersangka	Silahkan saja laporkan saya ke polisi, saya tidak takut!

Hasil Winhex:

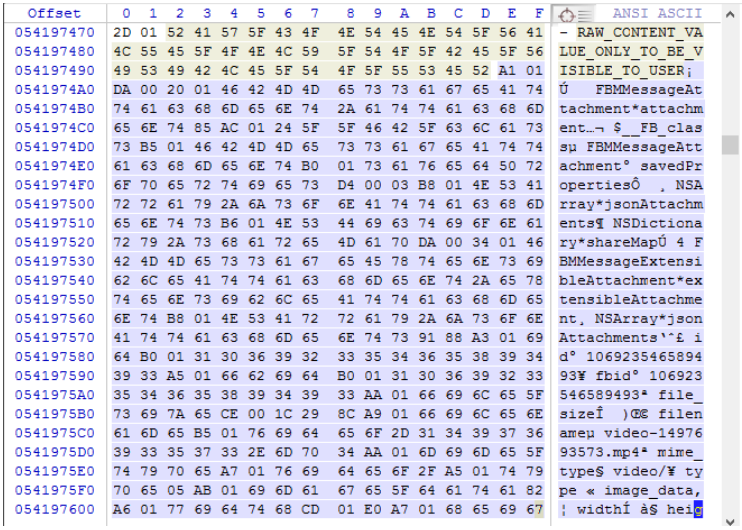


003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
1010987F0	30	37	DA	00	25	01	46	42	53	74	72	69	6E	67	57	69	07Ú % FBStringWi
101098800	74	68	52	65	64	61	63	74	65	64	44	65	73	63	72	69	thRedactedDescri
101098810	70	74	69	6F	6E	2A	74	65	78	74	82	AC	01	24	5F	5F	ption*text,¬ $__
101098820	46	42	5F	63	6C	61	73	73	DA	00	20	01	46	42	53	74	FB_classÚ FBSt
101098830	72	69	6E	67	57	69	74	68	52	65	64	61	63	74	65	64	ringWithRedacted
101098840	44	65	73	63	72	69	70	74	69	6F	6E	DA	00	2D	01	52	DescriptionÚ - R
101098850	41	57	5F	43	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	AW_CONTENT_VALUE
101098860	5F	4F	4E	4C	59	5F	54	4F	5F	42	45	5F	56	49	53	49	_ONLY_TO_BE_VISI
101098870	42	4C	45	5F	54	4F	5F	55	53	45	52	DA	00	39	01	73	BLE_TO_USERÚ 9 s
101098880	69	6C	61	68	6B	61	6E	20	73	61	6A	61	20	6C	61	70	ilahkan saja lap
101098890	6F	72	6B	61	6E	20	73	61	79	61	20	6B	65	20	70	6F	orkan saya ke po
1010988A0	6C	69	73	69	2C	20	73	61	79	61	20	74	69	64	61	6B	lisi, saya tidak
1010988B0	20	74	61	6B	75	74	21	DA	00	20	01	46	42	4D	4D	65	takut!Ú FBMMe
1010988C0	73	73	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	ssageAttachment*
1010988D0	61	74	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	attachment…¬ $__
1010988E0	46	42	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	FB_classµ FBMMes
1010988F0	73	61	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	sageAttachment°
101098900	73	61	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	savedPropertiesÔ
101098910	00	03	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	¸ NSArray*json
101098920	41	74	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	Attachments¶ NSD
101098930	69	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	ictionary*shareM
101098940	61	70	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	apÚ 4 FBMMessage
101098950	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	ExtensibleAttach
101098960	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	ment*extensibleA
101098970	74	74	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	ttachment¸ NSArr
101098980	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	ay*jsonAttachmen
101098990	74	73	90	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	ts ¶ NSDictionar
1010989A0	79	2A	73	68	61	72	65	4D	61	70	C0	DA	00	34	01	46	y*shareMapÀÚ 4 F
1010989B0	42	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	BMMessageExtensi
1010989C0	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	bleAttachment*ex
1010989D0	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	tensibleAttachme
1010989E0	6E	74	C0	AD	01	4E	53	41	72	72	61	79	2A	74	61	67	ntÀ- NSArray*tag
1010989F0	73	94	B1	01	73	6F	75	72	63	65	3A	63	68	61	74	3A	s"± source:chat:
101098A00	6F	72	63	61	B8	01	61	70	70	5F	69	64	3A	31	36	33	orca¸ app_id:163
101098A10	37	35	34	31	30	32	36	34	38	35	35	39	34	A5	01	73	7541026485594¥ s

OFFSET	Aktor	Percakapan
9289BC7E	Korban	Send Video

Hasil Winhex:



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
054197470	2D	01	52	41	57	5F	43	4F	4E	54	45	4E	54	5F	56	41	- RAW_CONTENT_VA
054197480	4C	55	45	5F	4F	4E	4C	59	5F	54	4F	5F	42	45	5F	56	LUE_ONLY_TO_BE_V
054197490	49	53	49	42	4C	45	5F	54	4F	5F	55	53	45	52	A1	01	ISIBLE_TO_USER¡
0541974A0	DA	00	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	Ú FBMMessageAt
0541974B0	74	61	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	tachment*attachm
0541974C0	65	6E	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	ent…¬ $__FB_clas
0541974D0	73	B5	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	sµ FBMMessageAtt
0541974E0	61	63	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	achment° savedPr
0541974F0	6F	70	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	opertiesÔ ¸ NSA
054197500	72	72	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	rray*jsonAttachm
054197510	65	6E	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	ents¶ NSDictiona
054197520	72	79	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	ry*shareMapÚ 4 F
054197530	42	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	BMMessageExtensi
054197540	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	bleAttachment*ex
054197550	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	tensibleAttachme
054197560	6E	74	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	nt¸ NSArray*json
054197570	41	74	74	61	63	68	6D	65	6E	74	73	91	88	A3	01	69	Attachments'^£ i
054197580	64	B0	01	31	30	36	39	32	33	35	34	36	35	38	39	34	d° 1069235465894
054197590	39	33	A5	01	66	62	69	64	B0	01	31	30	36	39	32	33	93¥ fbid° 106923
0541975A0	35	34	36	35	38	39	34	39	33	AA	01	66	69	6C	65	5F	546589493ª file_
0541975B0	73	69	7A	65	CE	00	1C	29	8C	A9	01	66	69	6C	65	6E	sizeÎ)Œ© filen
0541975C0	61	6D	65	B5	01	76	69	64	65	6F	2D	31	34	39	37	36	ameµ video-14976
0541975D0	39	33	35	37	33	2E	6D	70	34	AA	01	6D	69	6D	65	5F	93573.mp4ª mime_
0541975E0	74	79	70	65	A7	01	76	69	64	65	6F	2F	A5	01	74	79	types§ video/¥ ty
0541975F0	70	65	05	AB	01	69	6D	61	67	65	5F	64	61	74	61	82	pe « image_data,
054197600	A6	01	77	69	64	74	68	CD	01	E0	A7	01	68	65	69	67	¦ widthÍ à§ heig

B-14

OFFSET	Aktor	Percakapan
4729AC1F	Korban	Aku udah lapor ke polisi, online shopping kamu harus ditindak karna biar ngga ada yg senasib kayak aku.

Hasil Winhex:

003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
04729ABF0	46	42	5F	63	6C	61	73	73	DA	00	20	01	46	42	53	74	FB_classÚ FBSt
04729AC00	72	69	6E	67	57	69	74	68	52	65	64	61	63	74	65	64	ringWithRedacted
04729AC10	44	65	73	63	72	69	70	74	69	6F	6E	DA	00	2D	01	52	DescriptionÚ - R
04729AC20	41	57	5F	43	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	AW_CONTENT_VALUE
04729AC30	5F	4F	4E	4C	59	5F	54	4F	5F	42	45	5F	56	49	53	49	_ONLY_TO_BE_VISI
04729AC40	42	4C	45	5F	54	4F	5F	55	53	45	52	DA	00	68	01	41	BLE_TO_USERÚ h A
04729AC50	6B	75	20	75	64	61	68	20	6C	61	70	6F	72	20	6B	65	ku udah lapor ke
04729AC60	20	70	6F	6C	69	73	69	2C	20	6F	6E	6C	69	6E	65	20	polisi, online
04729AC70	73	68	6F	70	70	69	6E	67	20	6B	61	6D	75	20	68	61	shopping kamu ha
04729AC80	72	75	73	20	64	69	74	69	6E	64	61	6B	20	6B	61	72	rus ditindak kar
04729AC90	6E	61	20	62	69	61	72	20	6E	67	67	61	20	61	64	61	na biar ngga ada
04729ACA0	20	79	67	20	73	65	6E	61	73	69	62	20	6B	61	79	61	yg senasib kaya
04729ACB0	6B	20	61	6B	75	2E	DA	00	20	01	46	42	4D	4D	65	73	k aku.Ú FBMMes
04729ACC0	73	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	sageAttachment*a
04729ACD0	74	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	ttachment…¬ $__F
04729ACE0	42	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	B_classµ FBMMess
04729ACF0	61	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	ageAttachment° s
04729AD00	61	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	00	avedPropertiesÔ
04729AD10	03	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	¸ NSArray*jsonA
04729AD20	74	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	ttachments¶ NSDi
04729AD30	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	ctionary*shareMa
04729AD40	70	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	45	pÚ 4 FBMMessageE
04729AD50	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	xtensibleAttachm
04729AD60	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	ent*extensibleAt
04729AD70	74	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	tachment¸ NSArra
04729AD80	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	y*jsonAttachment
04729AD90	73	90	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	s ¶ NSDictionary
04729ADA0	2A	73	68	61	72	65	4D	61	70	C0	DA	00	34	01	46	42	*shareMapÀÚ 4 FB
04729ADB0	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	MMessageExtensib
04729ADC0	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	leAttachment*ext
04729ADD0	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	ensibleAttachmen
04729ADE0	74	C0	AD	01	4E	53	41	72	72	61	79	2A	74	61	67	73	tÀ- NSArray*tags
04729ADF0	93	B1	01	73	6F	75	72	63	65	3A	63	68	61	74	3A	6F	"± source:chat:o
04729AE00	72	63	61	B7	01	61	70	70	5F	69	64	3A	32	35	36	30	rca· app_id:2560
04729AE10	30	32	33	34	37	37	34	33	39	38	33	A6	01	69	6E	62	023477439[illegible]¦ inb

OFFSET	Aktor	Percakapan
421552BC	Korban	Inget dosa mbak, udah nipu kok jahat bgt jadi orang.

Hasil Winhex:

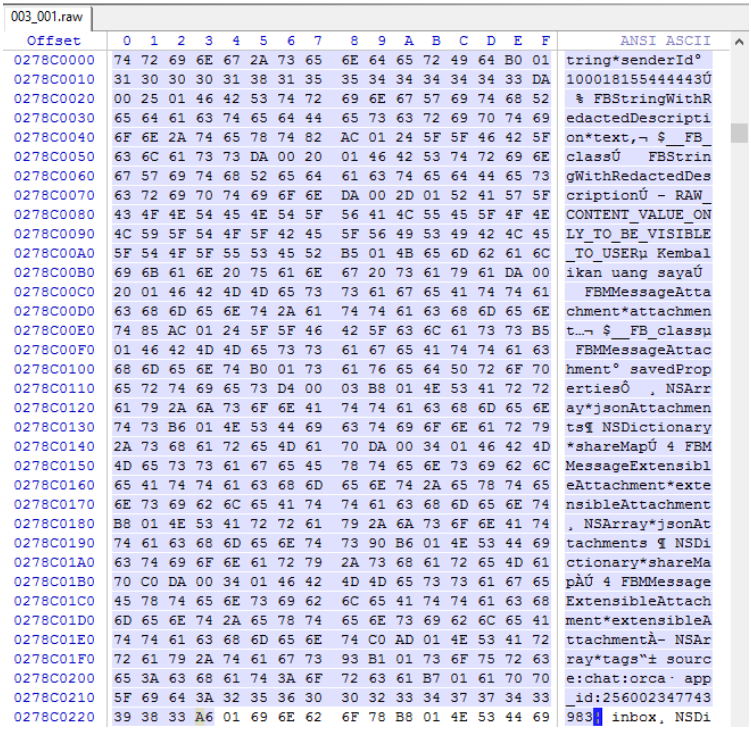
003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
042155200	01	46	42	53	74	72	69	6E	67	57	69	74	68	52	65	64	FBStringWithRed
042155210	61	63	74	65	64	44	65	73	63	72	69	70	74	69	6F	6E	actedDescription
042155220	2A	74	65	78	74	82	AC	01	24	5F	5F	46	42	5F	63	6C	*text,¬ $__FB_cl
042155230	61	73	73	DA	00	20	01	46	42	53	74	72	69	6E	67	57	assÚ FBStringW
042155240	69	74	68	52	65	64	61	63	74	65	64	44	65	73	63	72	ithRedactedDescr
042155250	69	70	74	69	6F	6E	DA	00	2D	01	52	41	57	5F	43	4F	iptionÚ - RAW_CO
042155260	4E	54	45	4E	54	5F	56	41	4C	55	45	5F	4F	4E	4C	59	NTENT_VALUE_ONLY
042155270	5F	54	4F	5F	42	45	5F	56	49	53	49	42	4C	45	5F	54	_TO_BE_VISIBLE_T
042155280	4F	5F	55	53	45	52	DA	00	35	01	49	6E	67	65	74	20	O_USERÚ 5 Inget
042155290	64	6F	73	61	20	6D	62	61	6B	2C	20	75	64	61	68	20	dosa mbak, udah
0421552A0	6E	69	70	75	20	6B	6F	6B	20	6A	61	68	61	74	20	62	nipu kok jahat b
0421552B0	67	74	20	6A	61	64	69	20	6F	72	61	6E	67	2E	DA	00	gt jadi orang.Ú
0421552C0	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	FBMMessageAtta
0421552D0	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	65	6E	chment*attachmen
0421552E0	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	B5	t…¬ $__FB_classµ
0421552F0	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	63	FBMMessageAttac
042155300	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	6F	70	hment° savedProp
042155310	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	72	72	ertiesÔ ¸ NSArr
042155320	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	ay*jsonAttachmen
042155330	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	ts¶ NSDictionary
042155340	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	42	4D	*shareMapÚ 4 FBM
042155350	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	6C	MessageExtensibl
042155360	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	65	eAttachment*exte
042155370	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	nsibleAttachment
042155380	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	¸ NSArray*jsonAt
042155390	74	61	63	68	6D	65	6E	74	73	90	B6	01	4E	53	44	69	tachments ¶ NSDi
0421553A0	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	ctionary*shareMa
0421553B0	70	C0	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	pÀÚ 4 FBMMessage
0421553C0	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	ExtensibleAttach
0421553D0	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	ment*extensibleA
0421553E0	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	41	72	ttachmentÀ- NSAr
0421553F0	72	61	79	2A	74	61	67	73	93	B1	01	73	6F	75	72	63	ray*tags"± sourc
042155400	65	3A	63	68	61	74	3A	6F	72	63	61	B7	01	61	70	70	e:chat:orca· app
042155410	5F	69	64	3A	32	35	36	30	30	32	33	34	37	37	34	33	_id:256002347743
042155420	39	38	33	A6	01	69	6E	62	6F	78	B8	01	4E	53	44	69	983¦ inbox¸ NSDi

B-16

OFFSET	Aktor	Percakapan
278C00BD	Korban	Kembalikan uang saya

Hasil Winhex:



003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0278C0000	74	72	69	6E	67	2A	73	65	6E	64	65	72	49	64	B0	01	tring*senderId°
0278C0010	31	30	30	30	31	38	31	35	35	34	34	34	34	34	33	DA	1000181554444443Ú
0278C0020	00	25	01	46	42	53	74	72	69	6E	67	57	69	74	68	52	% FBStringWithR
0278C0030	65	64	61	63	74	65	64	44	65	73	63	72	69	70	74	69	edactedDescripti
0278C0040	6F	6E	2A	74	65	78	74	82	AC	01	24	5F	5F	46	42	5F	on*text,¬ $__FB_
0278C0050	63	6C	61	73	73	DA	00	20	01	46	42	53	74	72	69	6E	classÚ FBStrin
0278C0060	67	57	69	74	68	52	65	64	61	63	74	65	64	44	65	73	gWithRedactedDes
0278C0070	63	72	69	70	74	69	6F	6E	DA	00	2D	01	52	41	57	5F	criptionÚ - RAW_
0278C0080	43	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	5F	4F	4E	CONTENT_VALUE_ON
0278C0090	4C	59	5F	54	4F	5F	42	45	5F	56	49	53	49	42	4C	45	LY_TO_BE_VISIBLE
0278C00A0	5F	54	4F	5F	55	53	45	52	B5	01	4B	65	6D	62	61	6C	_TO_USERµ Kembal
0278C00B0	69	6B	61	6E	20	75	61	6E	67	20	73	61	79	61	DA	00	ikan uang sayaÚ
0278C00C0	20	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	FBMMessageAtta
0278C00D0	63	68	6D	65	6E	74	2A	61	74	74	61	63	68	6D	65	6E	chment*attachmen
0278C00E0	74	85	AC	01	24	5F	5F	46	42	5F	63	6C	61	73	73	B5	t…¬ $__FB_classµ
0278C00F0	01	46	42	4D	4D	65	73	73	61	67	65	41	74	74	61	63	FBMMessageAttac
0278C0100	68	6D	65	6E	74	B0	01	73	61	76	65	64	50	72	6F	70	hment° savedProp
0278C0110	65	72	74	69	65	73	D4	00	03	B8	01	4E	53	41	72	72	ertiesÔ ¸ NSArr
0278C0120	61	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	ay*jsonAttachmen
0278C0130	74	73	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	ts¶ NSDictionary
0278C0140	2A	73	68	61	72	65	4D	61	70	DA	00	34	01	46	42	4D	*shareMapÚ 4 FBM
0278C0150	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	6C	MessageExtensibl
0278C0160	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	65	eAttachment*exte
0278C0170	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	74	nsibleAttachment
0278C0180	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	74	¸ NSArray*jsonAt
0278C0190	74	61	63	68	6D	65	6E	74	73	90	B6	01	4E	53	44	69	tachments ¶ NSDi
0278C01A0	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	ctionary*shareMa
0278C01B0	70	C0	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	pÀÚ 4 FBMMessage
0278C01C0	45	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	ExtensibleAttach
0278C01D0	6D	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	ment*extensibleA
0278C01E0	74	74	61	63	68	6D	65	6E	74	C0	AD	01	4E	53	41	72	ttachmentÀ- NSAr
0278C01F0	72	61	79	2A	74	61	67	73	93	B1	01	73	6F	75	72	63	ray*tags“± sourc
0278C0200	65	3A	63	68	61	74	3A	6F	72	63	61	B7	01	61	70	70	e:chat:orca· app
0278C0210	5F	69	64	3A	32	35	36	30	30	32	33	34	37	37	34	33	_id:256002347743
0278C0220	39	38	33	A6	01	69	6E	62	6F	78	B8	01	4E	53	44	69	983¦ inbox¸ NSDi

OFFSET	Aktor	Percakapan
8A217CB4	Korban	Atau polisi akan datang ke tempat kamu.

Hasil Winhex:

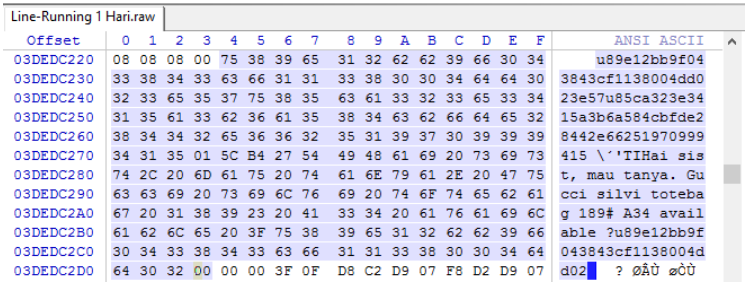
003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
08A217BF0	64	B0	01	31	30	30	30	31	38	31	35	35	34	34	34	34	d° 1000181554444
08A217C00	34	33	DA	00	25	01	46	42	53	74	72	69	6E	67	57	69	43Ú % FBStringWi
08A217C10	74	68	52	65	64	61	63	74	65	64	44	65	73	63	72	69	thRedactedDescri
08A217C20	70	74	69	6F	6E	2A	74	65	78	74	82	AC	01	24	5F	5F	ption*text,¬ $__
08A217C30	46	42	5F	63	6C	61	73	73	DA	00	20	01	46	42	53	74	FB_classÚ FBSt
08A217C40	72	69	6E	67	57	69	74	68	52	65	64	61	63	74	65	64	ringWithRedacted
08A217C50	44	65	73	63	72	69	70	74	69	6F	6E	DA	00	2D	01	52	DescriptionÚ - R
08A217C60	41	57	5F	43	4F	4E	54	45	4E	54	5F	56	41	4C	55	45	AW_CONTENT_VALUE
08A217C70	5F	4F	4E	4C	59	5F	54	4F	5F	42	45	5F	56	49	53	49	_ONLY_TO_BE_VISI
08A217C80	42	4C	45	5F	54	4F	5F	55	53	45	52	DA	00	28	01	41	BLE_TO_USERÚ (A
08A217C90	74	61	75	20	70	6F	6C	69	73	69	20	61	6B	61	6E	20	tau polisi akan
08A217CA0	64	61	74	61	6E	67	20	6B	65	20	74	65	6D	70	61	74	datang ke tempat
08A217CB0	20	6B	61	6D	75	2E	DA	00	20	01	46	42	4D	4D	65	73	kamu.Ú FBMMes
08A217CC0	73	61	67	65	41	74	74	61	63	68	6D	65	6E	74	2A	61	sageAttachment*a
08A217CD0	74	74	61	63	68	6D	65	6E	74	85	AC	01	24	5F	5F	46	ttachment…¬ $__F
08A217CE0	42	5F	63	6C	61	73	73	B5	01	46	42	4D	4D	65	73	73	B_classµ FBMMess
08A217CF0	61	67	65	41	74	74	61	63	68	6D	65	6E	74	B0	01	73	ageAttachment° s
08A217D00	61	76	65	64	50	72	6F	70	65	72	74	69	65	73	D4	00	avedPropertiesÔ
08A217D10	03	B8	01	4E	53	41	72	72	61	79	2A	6A	73	6F	6E	41	¸ NSArray*jsonA
08A217D20	74	74	61	63	68	6D	65	6E	74	73	B6	01	4E	53	44	69	ttachments¶ NSDi
08A217D30	63	74	69	6F	6E	61	72	79	2A	73	68	61	72	65	4D	61	ctionary*shareMa
08A217D40	70	DA	00	34	01	46	42	4D	4D	65	73	73	61	67	65	45	pÚ 4 FBMMessageE
08A217D50	78	74	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	xtensibleAttachm
08A217D60	65	6E	74	2A	65	78	74	65	6E	73	69	62	6C	65	41	74	ent*extensibleAt
08A217D70	74	61	63	68	6D	65	6E	74	B8	01	4E	53	41	72	72	61	tachment¸ NSArra
08A217D80	79	2A	6A	73	6F	6E	41	74	74	61	63	68	6D	65	6E	74	y*jsonAttachment
08A217D90	73	90	B6	01	4E	53	44	69	63	74	69	6F	6E	61	72	79	s ¶ NSDictionary
08A217DA0	2A	73	68	61	72	65	4D	61	70	C0	DA	00	34	01	46	42	*shareMapÀÚ 4 FB
08A217DB0	4D	4D	65	73	73	61	67	65	45	78	74	65	6E	73	69	62	MMessageExtensib
08A217DC0	6C	65	41	74	74	61	63	68	6D	65	6E	74	2A	65	78	74	leAttachment*ext
08A217DD0	65	6E	73	69	62	6C	65	41	74	74	61	63	68	6D	65	6E	ensibleAttachmen
08A217DE0	74	C0	AD	01	4E	53	41	72	72	61	79	2A	74	61	67	73	tÀ- NSArray*tags
08A217DF0	93	B1	01	73	6F	75	72	63	65	3A	63	68	61	74	3A	6F	"± source:chat:o
08A217E00	72	63	61	B7	01	61	70	70	5F	69	64	3A	32	35	36	30	rca· app_id:2560
08A217E10	30	32	33	34	37	37	34	33	39	38	33	A6	01	69	6E	62	0234774398¦ inb

LINE *MESSENGER*

OFFSET	Aktor	Percakapan
3DEDC279	Korban	Hai sist, mau tanya. Gucci silvi totebag 189# A34 available ?

Hasil Winhex :

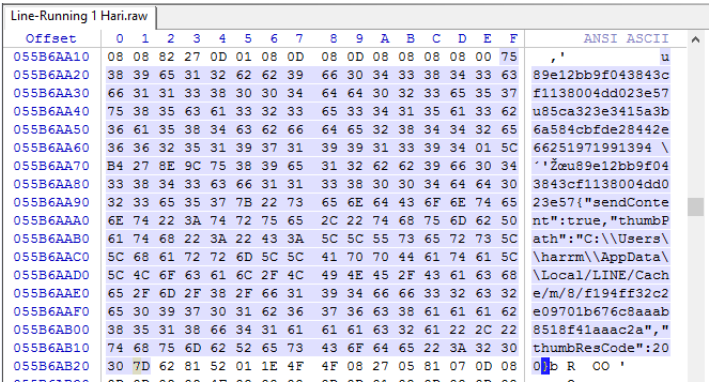


Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
03DEDC220	08	08	08	00	75	38	39	65	31	32	62	62	39	66	30	34	u89e12bb9f04
03DEDC230	33	38	34	33	63	66	31	31	33	38	30	30	34	64	64	30	3843cf1138004dd0
03DEDC240	32	33	65	35	37	75	38	35	63	61	33	32	33	65	33	34	23e57u85ca323e34
03DEDC250	31	35	61	33	62	36	61	35	38	34	63	62	66	64	65	32	15a3b6a584cbfde2
03DEDC260	38	34	34	32	65	36	36	32	35	31	39	37	30	39	39	39	8442e66251970999
03DEDC270	34	31	35	01	5C	B4	27	54	49	48	61	69	20	73	69	73	415 \´'TIHai sis
03DEDC280	74	2C	20	6D	61	75	20	74	61	6E	79	61	2E	20	47	75	t, mau tanya. Gu
03DEDC290	63	63	69	20	73	69	6C	76	69	20	74	6F	74	65	62	61	cci silvi toteba
03DEDC2A0	67	20	31	38	39	23	20	41	33	34	20	61	76	61	69	6C	g 189# A34 avail
03DEDC2B0	61	62	6C	65	20	3F	75	38	39	65	31	32	62	62	39	66	able ?u89e12bb9f
03DEDC2C0	30	34	33	38	34	33	63	66	31	31	33	38	30	30	34	64	043843cf1138004d
03DEDC2D0	64	30	32	00	00	00	3F	0F	D8	C2	D9	07	F8	D2	D9	07	d02 ? ØÂÙ øÒÙ

OFFSET	Aktor	Percakapan
55B6AB0D	Korban	Send Picture

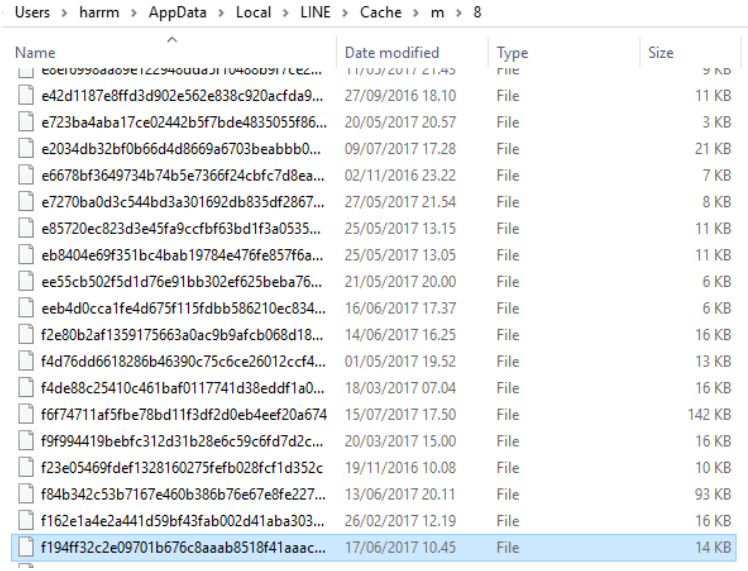
Hasil Winhex :



Line-Running 1 Hari.raw

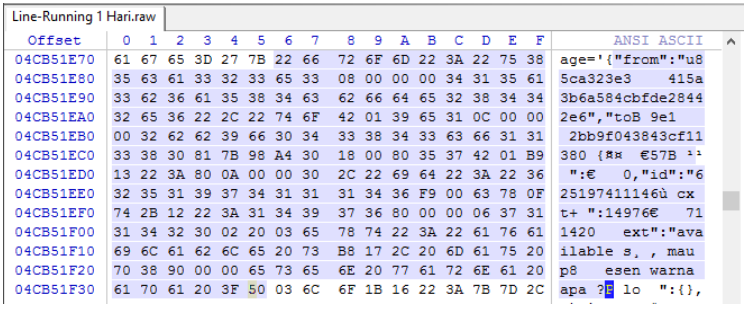
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
055B6AA10	08	08	82	27	0D	01	08	0D	08	0D	08	08	08	08	00	75	,' u
055B6AA20	38	39	65	31	32	62	62	39	66	30	34	33	38	34	33	63	89e12bb9f043843c
055B6AA30	66	31	31	33	38	30	30	34	64	64	30	32	33	65	35	37	f1138004dd023e57
055B6AA40	75	38	35	63	61	33	32	33	65	33	34	31	35	61	33	62	u85ca323e3415a3b
055B6AA50	36	61	35	38	34	63	62	66	64	65	32	38	34	34	32	65	6a584cbfde28442e
055B6AA60	36	36	32	35	31	39	37	31	39	39	31	33	39	34	01	5C	66251971991394 \
055B6AA70	B4	27	8E	9C	75	38	39	65	31	32	62	62	39	66	30	34	´'Žœu89e12bb9f04
055B6AA80	33	38	34	33	63	66	31	31	33	38	30	30	34	64	64	30	3843cf1138004dd0
055B6AA90	32	33	65	35	37	7B	22	73	65	6E	64	43	6F	6E	74	65	23e57{"sendConte
055B6AAA0	6E	74	22	3A	74	72	75	65	2C	22	74	68	75	6D	62	50	nt":true,"thumbP
055B6AAB0	61	74	68	22	3A	22	43	3A	5C	5C	55	73	65	72	73	5C	ath":"C:\\Users\
055B6AAC0	5C	68	61	72	72	6D	5C	5C	41	70	70	44	61	74	61	5C	\harrm\\AppData\
055B6AAD0	5C	4C	6F	63	61	6C	2F	4C	49	4E	45	2F	43	61	63	68	\Local/LINE/Cach
055B6AAE0	65	2F	6D	2F	38	2F	66	31	39	34	66	66	33	32	63	32	e/m/8/f194ff32c2
055B6AAF0	65	30	39	37	30	31	62	36	37	36	63	38	61	61	61	62	e09701b676c8aaab
055B6AB00	38	35	31	38	66	34	31	61	61	61	63	32	61	22	2C	22	8518f41aaac2a","
055B6AB10	74	68	75	6D	62	52	65	73	43	6F	64	65	22	3A	32	30	thumbResCode":20
055B6AB20	30	7D	62	81	52	01	1E	4F	4F	08	27	05	81	07	0D	08	0}b R OO '

Cache Penyimpanan Data :



OFFSET	Aktor	Percakapan
4CB51E76	Tersangka	Availabe sist, mau pesan warna apa ?

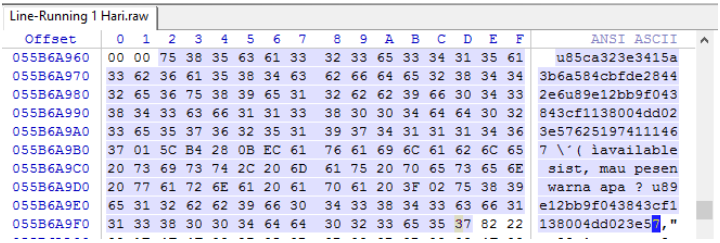
Hasil Winhex:



B-20

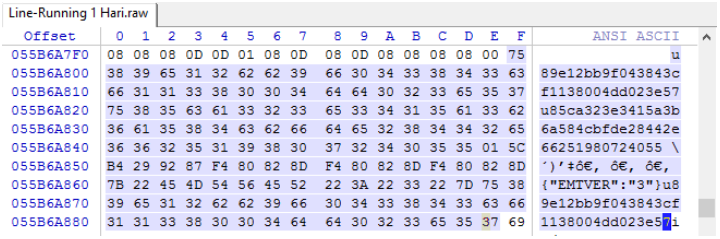
OFFSET	Aktor	Percakapan
55B6A9D1	Korban	Aku mau yang gold sist 2 ya

Hasil Winhex:



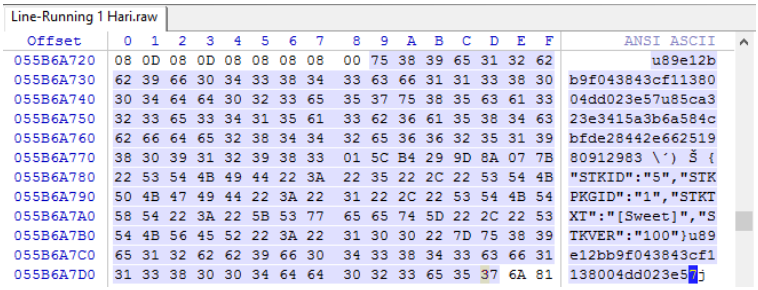
OFFSET	Aktor	Percakapan
55B6A86F	Korban	Send Emoji

Hasil Winhex:



OFFSET	Aktor	Percakapan
55B6A780	Korban	Send Sticker

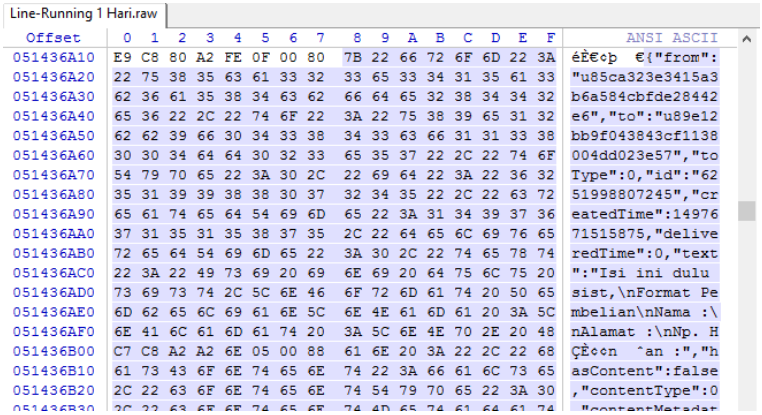
Hasil Winhex:


Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
055B6A720	08	0D	08	0D	08	08	08	08	00	75	38	39	65	31	32	62	u89e12b
055B6A730	62	39	66	30	34	33	38	34	33	63	66	31	31	33	38	30	b9f043843cf11380
055B6A740	30	34	64	64	30	32	33	65	35	37	75	38	35	63	61	33	04dd023e57u85ca3
055B6A750	32	33	65	33	34	31	35	61	33	62	36	61	35	38	34	63	23e3415a3b6a584c
055B6A760	62	66	64	65	32	38	34	34	32	65	36	36	32	35	31	39	bfde28442e662519
055B6A770	38	30	39	31	32	39	38	33	01	5C	B4	29	9D	8A	07	7B	80912983 \´) Š {
055B6A780	22	53	54	4B	49	44	22	3A	22	35	22	2C	22	53	54	4B	"STKID":"5","STK
055B6A790	50	4B	47	49	44	22	3A	22	31	22	2C	22	53	54	4B	54	PKGID":"1","STKT
055B6A7A0	58	54	22	3A	22	5B	53	77	65	65	74	5D	22	2C	22	53	XT":"[Sweet]","S
055B6A7B0	54	4B	56	45	52	22	3A	22	31	30	30	22	7D	75	38	39	TKVER":"100"}u89
055B6A7C0	65	31	32	62	62	39	66	30	34	33	38	34	33	63	66	31	e12bb9f043843cf1
055B6A7D0	31	33	38	30	30	34	64	64	30	32	33	65	35	37	6A	81	138004dd023e57j

OFFSET	Aktor	Percakapan
51436A19	Tersangka	Isi ini dulu sist: Format Pembelian Nama: Alamat: No. HP: Pesan:

Hasil Winhex:

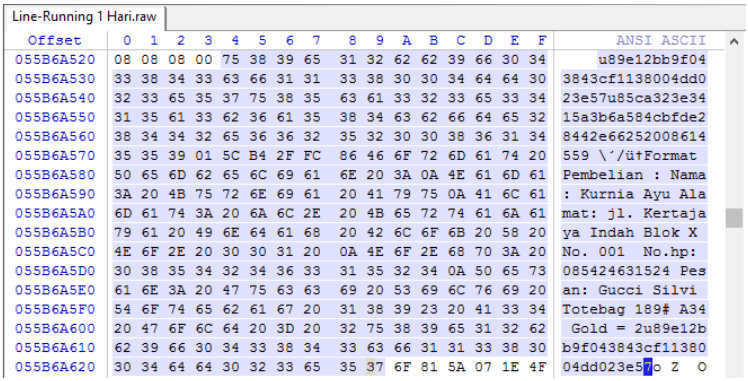

Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
051436A10	E9	C8	80	A2	FE	0F	00	80	7B	22	66	72	6F	6D	22	3A	éÈ€¢þ €{"from":
051436A20	22	75	38	35	63	61	33	32	33	65	33	34	31	35	61	33	"u85ca323e3415a3
051436A30	62	36	61	35	38	34	63	62	66	64	65	32	38	34	34	32	b6a584cbfde28442
051436A40	65	36	22	2C	22	74	6F	22	3A	22	75	38	39	65	31	32	e6","to":"u89e12
051436A50	62	62	39	66	30	34	33	38	34	33	63	66	31	31	33	38	bb9f043843cf1138
051436A60	30	30	34	64	64	30	32	33	65	35	37	22	2C	22	74	6F	004dd023e57","to
051436A70	54	79	70	65	22	3A	30	2C	22	69	64	22	3A	22	36	32	Type":0,"id":"62
051436A80	35	31	39	39	38	38	30	37	32	34	35	22	2C	22	63	72	51998807245","cr
051436A90	65	61	74	65	64	54	69	6D	65	22	3A	31	34	39	37	36	eatedTime":14976
051436AA0	37	31	35	31	35	38	37	35	2C	22	64	65	6C	69	76	65	71515875,"delive
051436AB0	72	65	64	54	69	6D	65	22	3A	30	2C	22	74	65	78	74	redTime":0,"text
051436AC0	22	3A	22	49	73	69	20	69	6E	69	20	64	75	6C	75	20	":"Isi ini dulu
051436AD0	73	69	73	74	2C	5C	6E	46	6F	72	6D	61	74	20	50	65	sist,\nFormat Pe
051436AE0	6D	62	65	6C	69	61	6E	5C	6E	4E	61	6D	61	20	3A	5C	mbelian\nNama :\
051436AF0	6E	41	6C	61	6D	61	74	20	3A	5C	6E	4E	70	2E	20	48	nAlamat :\nNp. H
051436B00	C7	C8	A2	A2	6E	05	00	88	61	6E	20	3A	22	2C	22	68	ÇÈ¢¢n ˆan :","h
051436B10	61	73	43	6F	6E	74	65	6E	74	22	3A	66	61	6C	73	65	asContent":false
051436B20	2C	22	63	6F	6E	74	65	6E	74	54	79	70	65	22	3A	30	,"contentType":0
051436B30	2C	22	63	6F	6E	74	65	6E	74	4D	65	74	61	64	61	74	"contentMetadat

OFFSET	Aktor	Percakapan
55B6A586	Korban	Format Pembelian : Nama: Kurnia Ayu

		Alamat: jl. Kertajaya Indah Blok X No. 001 No.hp: 085424631524 Pesan: Gucci Silvi Totebag 189# A34 Gold = 2

Hasil Winhex:



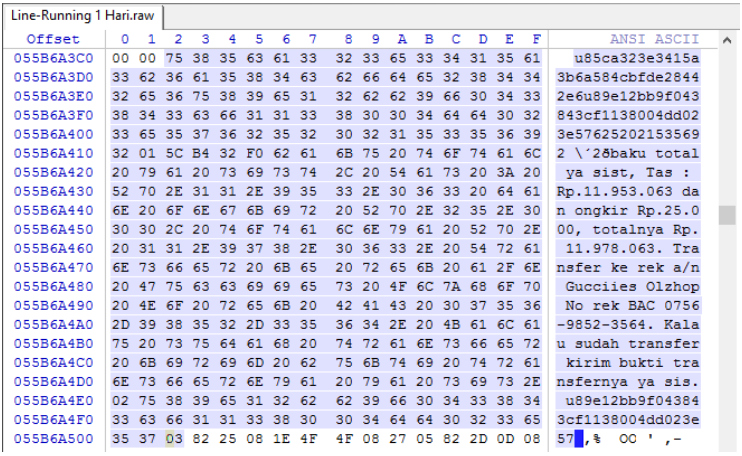
Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
055B6A520	08	08	08	00	75	38	39	65	31	32	62	62	39	66	30	34	u89e12bb9f04
055B6A530	33	38	34	33	63	66	31	31	33	38	30	30	34	64	64	30	3843cf1138004dd0
055B6A540	32	33	65	35	37	75	38	35	63	61	33	32	33	65	33	34	23e57u85ca323e34
055B6A550	31	35	61	33	62	36	61	35	38	34	63	62	66	64	65	32	15a3b6a584cbfde2
055B6A560	38	34	34	32	65	36	36	32	35	32	30	30	38	36	31	34	8442e66252008614
055B6A570	35	35	39	01	5C	B4	2F	FC	86	46	6F	72	6D	61	74	20	559 \´/ütFormat
055B6A580	50	65	6D	62	65	6C	69	61	6E	20	3A	0A	4E	61	6D	61	Pembelian : Nama
055B6A590	3A	20	4B	75	72	6E	69	61	20	41	79	75	0A	41	6C	61	: Kurnia Ayu Ala
055B6A5A0	6D	61	74	3A	20	6A	6C	2E	20	4B	65	72	74	61	6A	61	mat: jl. Kertaja
055B6A5B0	79	61	20	49	6E	64	61	68	20	42	6C	6F	6B	20	58	20	ya Indah Blok X
055B6A5C0	4E	6F	2E	20	30	30	31	20	0A	4E	6F	2E	68	70	3A	20	No. 001 No.hp:
055B6A5D0	30	38	35	34	32	34	36	33	31	35	32	34	0A	50	65	73	085424631524 Pes
055B6A5E0	61	6E	3A	20	47	75	63	63	69	20	53	69	6C	76	69	20	an: Gucci Silvi
055B6A5F0	54	6F	74	65	62	61	67	20	31	38	39	23	20	41	33	34	Totebag 189# A34
055B6A600	20	47	6F	6C	64	20	3D	20	32	75	38	39	65	31	32	62	Gold = 2u89e12b
055B6A610	62	39	66	30	34	33	38	34	33	63	66	31	31	33	38	30	b9f043843cf11380
055B6A620	30	34	64	64	30	32	33	65	35	37	6F	81	5A	07	1E	4F	04dd023e57o Z O

OFFSET	Aktor	Percakapan
55B6A417	Tersangka	Aku total ya sist, Tas = Rp.11.953.063 dan ongkir Rp.25.000. Total Rp.11.978.063 Transfer ke rek a/n Gucciies Olzhop No. rek BAC 0756-9852-3564. Kalau sudah di transfer,

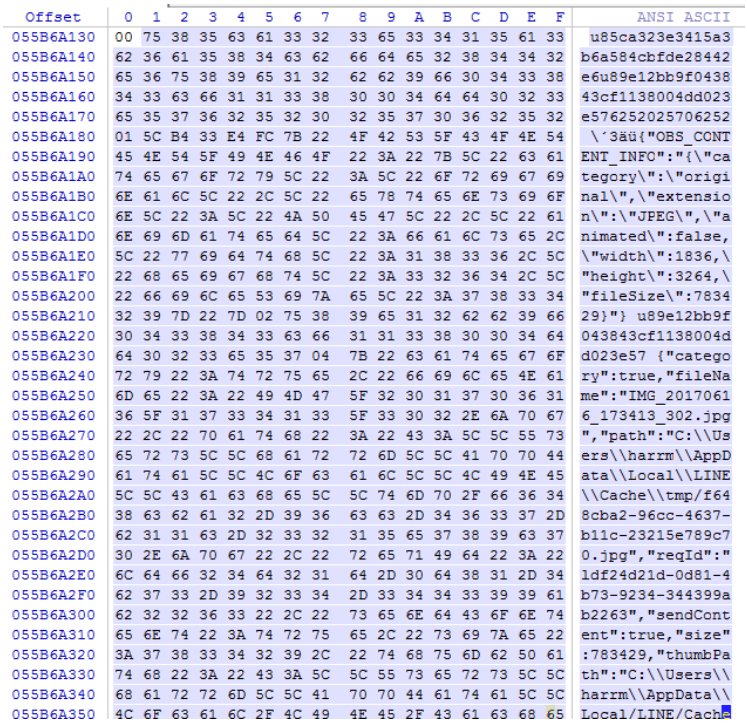
		kirim bukti trfnya ya sist

Hasil Winhex:



OFFSET	Aktor	Percakapan
55B6A249	Tersangka	Send Picture

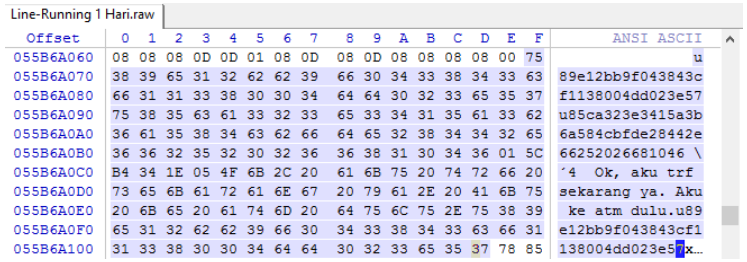
Hasil Winhex:



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
055B6A130	00	75	38	35	63	61	33	32	33	65	33	34	31	35	61	33	u85ca323e3415a3
055B6A140	62	36	61	35	38	34	63	62	66	64	65	32	38	34	34	32	b6a584cbfde28442
055B6A150	65	36	75	38	39	65	31	32	62	62	39	66	30	34	33	38	e6u89e12bb9f0438
055B6A160	34	33	63	66	31	31	33	38	30	30	34	64	64	30	32	33	43cf1138004dd023
055B6A170	65	35	37	36	32	35	32	30	32	35	37	30	36	32	35	32	e576252025706252
055B6A180	01	5C	B4	33	E4	FC	7B	22	4F	42	53	5F	43	4F	4E	54	\´3äü{"OBS_CONT
055B6A190	45	4E	54	5F	49	4E	46	4F	22	3A	22	7B	5C	22	63	61	ENT_INFO":"{\"ca
055B6A1A0	74	65	67	6F	72	79	5C	22	3A	5C	22	6F	72	69	67	69	tegory\":\"origi
055B6A1B0	6E	61	6C	5C	22	2C	5C	22	65	78	74	65	6E	73	69	6F	nal\",\"extensio
055B6A1C0	6E	5C	22	3A	5C	22	4A	50	45	47	5C	22	2C	5C	22	61	n\":\"JPEG\",\"a
055B6A1D0	6E	69	6D	61	74	65	64	5C	22	3A	66	61	6C	73	65	2C	nimated\":false,
055B6A1E0	5C	22	77	69	64	74	68	5C	22	3A	31	38	33	36	2C	5C	\"width\":1836,\
055B6A1F0	22	68	65	69	67	68	74	5C	22	3A	33	32	36	34	2C	5C	"height\":3264,\
055B6A200	22	66	69	6C	65	53	69	7A	65	5C	22	3A	37	38	33	34	"fileSize\":7834
055B6A210	32	39	7D	22	7D	02	75	38	39	65	31	32	62	62	39	66	29}"} u89e12bb9f
055B6A220	30	34	33	38	34	33	63	66	31	31	33	38	30	30	34	64	043843cf1138004d
055B6A230	64	30	32	33	65	35	37	04	7B	22	63	61	74	65	67	6F	d023e57 {"catego
055B6A240	72	79	22	3A	74	72	75	65	2C	22	66	69	6C	65	4E	61	ry":true,"fileNa
055B6A250	6D	65	22	3A	22	49	4D	47	5F	32	30	31	37	30	36	31	me":"IMG_2017061
055B6A260	36	5F	31	37	33	34	31	33	5F	33	30	32	2E	6A	70	67	6_173413_302.jpg
055B6A270	22	2C	22	70	61	74	68	22	3A	22	43	3A	5C	5C	55	73	","path":"C:\\Us
055B6A280	65	72	73	5C	5C	68	61	72	72	6D	5C	5C	41	70	70	44	ers\\harrm\\AppD
055B6A290	61	74	61	5C	5C	4C	6F	63	61	6C	5C	5C	4C	49	4E	45	ata\\Local\\LINE
055B6A2A0	5C	5C	43	61	63	68	65	5C	5C	74	6D	70	2F	66	36	34	\\Cache\\tmp/f64
055B6A2B0	38	63	62	61	32	2D	39	36	63	63	2D	34	36	33	37	2D	8cba2-96cc-4637-
055B6A2C0	62	31	31	63	2D	32	33	32	31	35	65	37	38	39	63	37	b11c-23215e789c7
055B6A2D0	30	2E	6A	70	67	22	2C	22	72	65	71	49	64	22	3A	22	0.jpg","reqId":"
055B6A2E0	6C	64	66	32	34	64	32	31	64	2D	30	64	38	31	2D	34	ldf24d21d-0d81-4
055B6A2F0	62	37	33	2D	39	32	33	34	2D	33	34	34	33	39	39	61	b73-9234-344399a
055B6A300	62	32	32	36	33	22	2C	22	73	65	6E	64	43	6F	6E	74	b2263","sendCont
055B6A310	65	6E	74	22	3A	74	72	75	65	2C	22	73	69	7A	65	22	ent":true,"size"
055B6A320	3A	37	38	33	34	32	39	2C	22	74	68	75	6D	62	50	61	:783429,"thumbPa
055B6A330	74	68	22	3A	22	43	3A	5C	5C	55	73	65	72	73	5C	5C	th":"C:\\Users\\
055B6A340	68	61	72	72	6D	5C	5C	41	70	70	44	61	74	61	5C	5C	harrm\\AppData\\
055B6A350	4C	6F	63	61	6C	2F	4C	49	4E	45	2F	43	61	63	68	65	Local/LINE/Cache

OFFSET	Aktor	Percakapan
55B6A0C4	Korban	Ok, aku trf sekarang ya. Aku ke atm dulu.

Hasil Winhex:

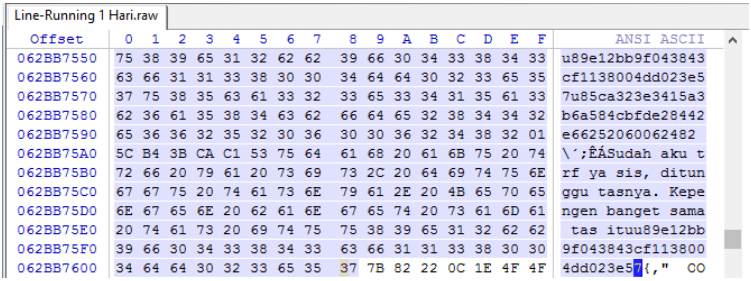


Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
055B6A060	08	08	08	0D	0D	01	08	0D	08	0D	08	08	08	08	00	75	u
055B6A070	38	39	65	31	32	62	62	39	66	30	34	33	38	34	33	63	89e12bb9f043843c
055B6A080	66	31	31	33	38	30	30	34	64	64	30	32	33	65	35	37	f1138004dd023e57
055B6A090	75	38	35	63	61	33	32	33	65	33	34	31	35	61	33	62	u85ca323e3415a3b
055B6A0A0	36	61	35	38	34	63	62	66	64	65	32	38	34	34	32	65	6a584cbfde28442e
055B6A0B0	36	36	32	35	32	30	32	36	36	38	31	30	34	36	01	5C	66252026681046 \
055B6A0C0	B4	34	1E	05	4F	6B	2C	20	61	6B	75	20	74	72	66	20	´4 Ok, aku trf
055B6A0D0	73	65	6B	61	72	61	6E	67	20	79	61	2E	20	41	6B	75	sekarang ya. Aku
055B6A0E0	20	6B	65	20	61	74	6D	20	64	75	6C	75	2E	75	38	39	ke atm dulu.u89
055B6A0F0	65	31	32	62	62	39	66	30	34	33	38	34	33	63	66	31	e12bb9f043843cf1
055B6A100	31	33	38	30	30	34	64	64	30	32	33	65	35	37	78	85	138004dd023e5x…

OFFSET	Aktor	Percakapan
62BB75CC	Korban	Sudah aku trf ya sis, ditunggu tasnya. Kepengen banget sama tas itu

Hasil Winhex:

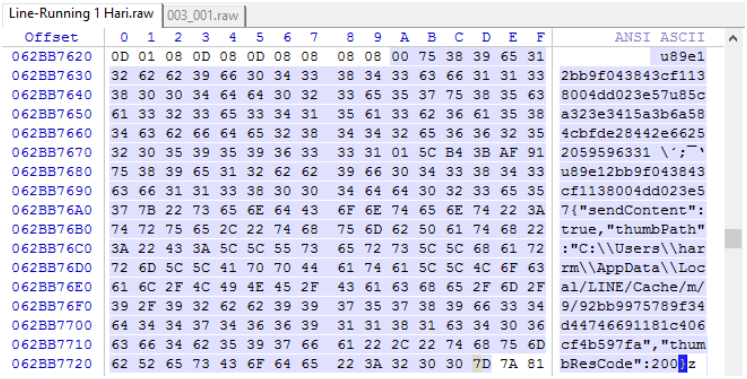


Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
062BB7550	75	38	39	65	31	32	62	62	39	66	30	34	33	38	34	33	u89e12bb9f043843
062BB7560	63	66	31	31	33	38	30	30	34	64	64	30	32	33	65	35	cf1138004dd023e5
062BB7570	37	75	38	35	63	61	33	32	33	65	33	34	31	35	61	33	7u85ca323e3415a3
062BB7580	62	36	61	35	38	34	63	62	66	64	65	32	38	34	34	32	b6a584cbfde28442
062BB7590	65	36	36	32	35	32	30	36	30	30	36	32	34	38	32	01	e66252060062482
062BB75A0	5C	B4	3B	CA	C1	53	75	64	61	68	20	61	6B	75	20	74	\´;ÊÁSudah aku t
062BB75B0	72	66	20	79	61	20	73	69	73	2C	20	64	69	74	75	6E	rf ya sis, ditun
062BB75C0	67	67	75	20	74	61	73	6E	79	61	2E	20	4B	65	70	65	ggu tasnya. Kepe
062BB75D0	6E	67	65	6E	20	62	61	6E	67	65	74	20	73	61	6D	61	ngen banget sama
062BB75E0	20	74	61	73	20	69	74	75	75	38	39	65	31	32	62	62	tas ituu89e12bb
062BB75F0	39	66	30	34	33	38	34	33	63	66	31	31	33	38	30	30	9f043843cf113800
062BB7600	34	64	64	30	32	33	65	35	37	7B	82	22	0C	1E	4F	4F	4dd023e57{," OO

OFFSET	Aktor	Percakapan
62BB76C2	Korban	Send Picture

Hasil Winhex:

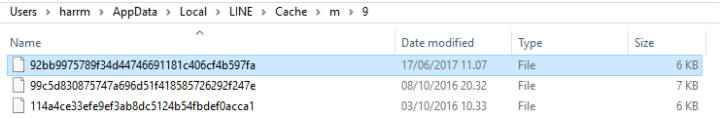


Line-Running 1 Hari.raw | 003_001.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
062BB7620	0D	01	08	0D	08	0D	08	08	08	08	00	75	38	39	65	31	u89e1
062BB7630	32	62	62	39	66	30	34	33	38	34	33	63	66	31	31	33	2bb9f043843cf113
062BB7640	38	30	30	34	64	64	30	32	33	65	35	37	75	38	35	63	8004dd023e57u85c
062BB7650	61	33	32	33	65	33	34	31	35	61	33	62	36	61	35	38	a323e3415a3b6a58
062BB7660	34	63	62	66	64	65	32	38	34	34	32	65	36	36	32	35	4cbfde28442e6625
062BB7670	32	30	35	39	35	39	36	33	33	31	01	5C	B4	3B	AF	91	2059596331 \´;¯`
062BB7680	75	38	39	65	31	32	62	62	39	66	30	34	33	38	34	33	u89e12bb9f043843
062BB7690	63	66	31	31	33	38	30	30	34	64	64	30	32	33	65	35	cf1138004dd023e5
062BB76A0	37	7B	22	73	65	6E	64	43	6F	6E	74	65	6E	74	22	3A	7{"sendContent":
062BB76B0	74	72	75	65	2C	22	74	68	75	6D	62	50	61	74	68	22	true,"thumbPath"
062BB76C0	3A	22	43	3A	5C	5C	55	73	65	72	73	5C	5C	68	61	72	:"C:\\Users\\har
062BB76D0	72	6D	5C	5C	41	70	70	44	61	74	61	5C	5C	4C	6F	63	rm\\AppData\\Loc
062BB76E0	61	6C	2F	4C	49	4E	45	2F	43	61	63	68	65	2F	6D	2F	al/LINE/Cache/m/
062BB76F0	39	2F	39	32	62	62	39	39	37	35	37	38	39	66	33	34	9/92bb9975789f34
062BB7700	64	34	34	37	34	36	36	39	31	31	38	31	63	34	30	36	d44746691181c406
062BB7710	63	66	34	62	35	39	37	66	61	22	2C	22	74	68	75	6D	cf4b597fa","thum
062BB7720	62	52	65	73	43	6F	64	65	22	3A	32	30	30	7D	7A	81	bResCode":200}z

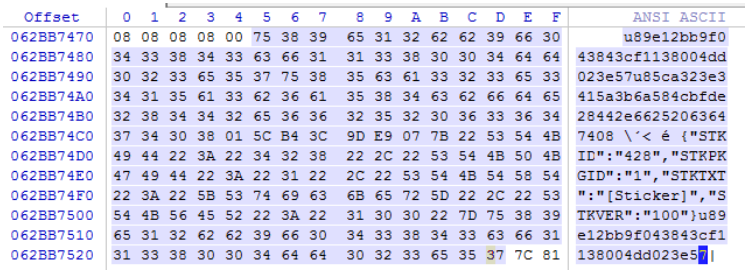
Cache Penyimpanan Data

B-26



OFFSET	Aktor	Percakapan
62BB74CD	Korban	Send Sticker

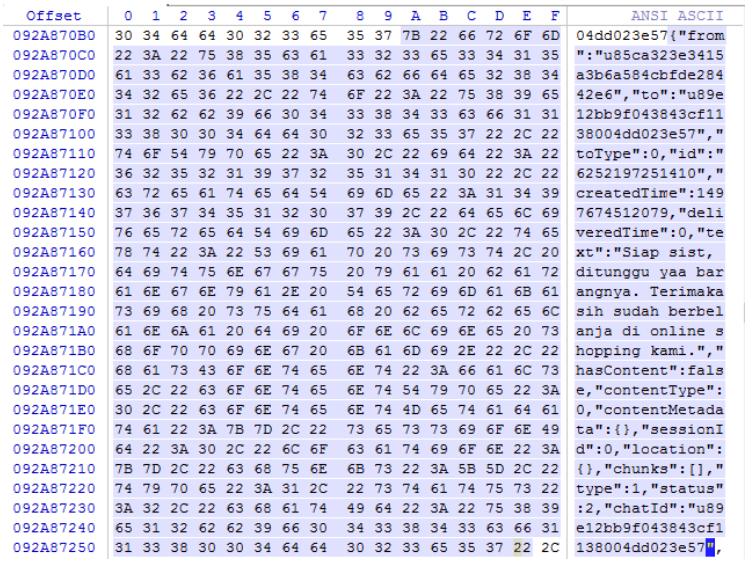
Hasil Winhex:



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
062BB7470	08	08	08	08	00	75	38	39	65	31	32	62	62	39	66	30	u89e12bb9f0
062BB7480	34	33	38	34	33	63	66	31	31	33	38	30	30	34	64	64	43843cf1138004dd
062BB7490	30	32	33	65	35	37	75	38	35	63	61	33	32	33	65	33	023e57u85ca323e3
062BB74A0	34	31	35	61	33	62	36	61	35	38	34	63	62	66	64	65	415a3b6a584cbfde
062BB74B0	32	38	34	34	32	65	36	36	32	35	32	30	36	33	36	34	28442e6625206364
062BB74C0	37	34	30	38	01	5C	B4	3C	9D	E9	07	7B	22	53	54	4B	7408 \´< é {"STK
062BB74D0	49	44	22	3A	22	34	32	38	22	2C	22	53	54	4B	50	4B	ID":"428","STKPK
062BB74E0	47	49	44	22	3A	22	31	22	2C	22	53	54	4B	54	58	54	GID":"1","STKTXT
062BB74F0	22	3A	22	5B	53	74	69	63	6B	65	72	5D	22	2C	22	53	":"[Sticker]","S
062BB7500	54	4B	56	45	52	22	3A	22	31	30	30	22	7D	75	38	39	TKVER":"100"}u89
062BB7510	65	31	32	62	62	39	66	30	34	33	38	34	33	63	66	31	e12bb9f043843cf1
062BB7520	31	33	38	30	30	34	64	64	30	32	33	65	35	37	7C	81	138004dd023e57

OFFSET	Aktor	Percakapan
92A870BB	Tersangka	Siap sist, ditunggu yaa barangnya. Terimakasih sudah berbelanja di online shopping kami

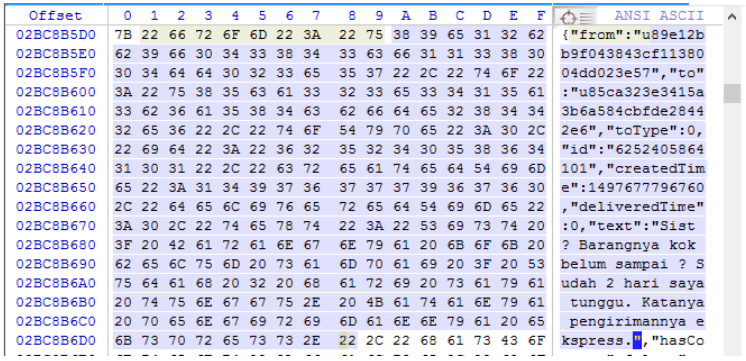
Hasil Winhex:



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
092A870B0	30	34	64	64	30	32	33	65	35	37	7B	22	66	72	6F	6D	04dd023e57{"from
092A870C0	22	3A	22	75	38	35	63	61	33	32	33	65	33	34	31	35	":"u85ca323e3415
092A870D0	61	33	62	36	61	35	38	34	63	62	66	64	65	32	38	34	a3b6a584cbfde284
092A870E0	34	32	65	36	22	2C	22	74	6F	22	3A	22	75	38	39	65	42e6","to":"u89e
092A870F0	31	32	62	62	39	66	30	34	33	38	34	33	63	66	31	31	12bb9f043843cf11
092A87100	33	38	30	30	34	64	64	30	32	33	65	35	37	22	2C	22	38004dd023e57","
092A87110	74	6F	54	79	70	65	22	3A	30	2C	22	69	64	22	3A	22	toType":0,"id":"
092A87120	36	32	35	32	31	39	37	32	35	31	34	31	30	22	2C	22	6252197251410","
092A87130	63	72	65	61	74	65	64	54	69	6D	65	22	3A	31	34	39	createdTime":149
092A87140	37	36	37	34	35	31	32	30	37	39	2C	22	64	65	6C	69	7674512079,"deli
092A87150	76	65	72	65	64	54	69	6D	65	22	3A	30	2C	22	74	65	veredTime":0,"te
092A87160	78	74	22	3A	22	53	69	61	70	20	73	69	73	74	2C	20	xt":"Siap sist,
092A87170	64	69	74	75	6E	67	67	75	20	79	61	61	20	62	61	72	ditunggu yaa bar
092A87180	61	6E	67	6E	79	61	2E	20	54	65	72	69	6D	61	6B	61	angnya. Terimaka
092A87190	73	69	68	20	73	75	64	61	68	20	62	65	72	62	65	6C	sih sudah berbel
092A871A0	61	6E	6A	61	20	64	69	20	6F	6E	6C	69	6E	65	20	73	anja di online s
092A871B0	68	6F	70	70	69	6E	67	20	6B	61	6D	69	2E	22	2C	22	hopping kami.","
092A871C0	68	61	73	43	6F	6E	74	65	6E	74	22	3A	66	61	6C	73	hasContent":fals
092A871D0	65	2C	22	63	6F	6E	74	65	6E	74	54	79	70	65	22	3A	e,"contentType":
092A871E0	30	2C	22	63	6F	6E	74	65	6E	74	4D	65	74	61	64	61	0,"contentMetada
092A871F0	74	61	22	3A	7B	7D	2C	22	73	65	73	73	69	6F	6E	49	ta":{},"sessionI
092A87200	64	22	3A	30	2C	22	6C	6F	63	61	74	69	6F	6E	22	3A	d":0,"location":
092A87210	7B	7D	2C	22	63	68	75	6E	6B	73	22	3A	5B	5D	2C	22	{},"chunks":[],"
092A87220	74	79	70	65	22	3A	31	2C	22	73	74	61	74	75	73	22	type":1,"status"
092A87230	3A	32	2C	22	63	68	61	74	49	64	22	3A	22	75	38	39	:2,"chatId":"u89
092A87240	65	31	32	62	62	39	66	30	34	33	38	34	33	63	66	31	e12bb9f043843cf1
092A87250	31	33	38	30	30	34	64	64	30	32	33	65	35	37	22	2C	138004dd023e57",

OFFSET	Aktor	Percakapan
2BC8B5D1	Korban	Sist ? Barangnya kok belum sampai ? Sudah 2 hari saya tunggu. Katanya pengirimannya ekspress.

Hasil Winhex:

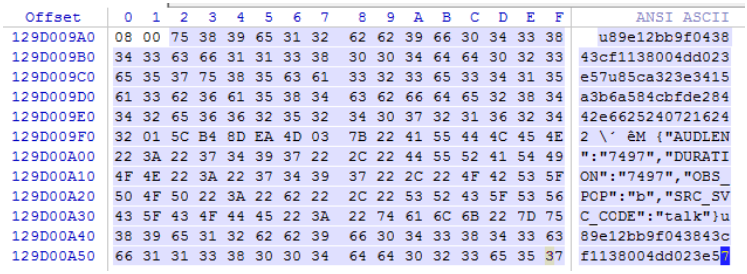


Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
02BC8B5D0	7B	22	66	72	6F	6D	22	3A	22	75	38	39	65	31	32	62	{"from":"u89e12b
02BC8B5E0	62	39	66	30	34	33	38	34	33	63	66	31	31	33	38	30	b9f043843cf11380
02BC8B5F0	30	34	64	64	30	32	33	65	35	37	22	2C	22	74	6F	22	04dd023e57","to"
02BC8B600	3A	22	75	38	35	63	61	33	32	33	65	33	34	31	35	61	:"u85ca323e3415a
02BC8B610	33	62	36	61	35	38	34	63	62	66	64	65	32	38	34	34	3b6a584cbfde2844
02BC8B620	32	65	36	22	2C	22	74	6F	54	79	70	65	22	3A	30	2C	2e6","toType":0,
02BC8B630	22	69	64	22	3A	22	36	32	35	32	34	30	35	38	36	34	"id":"6252405864
02BC8B640	31	30	31	22	2C	22	63	72	65	61	74	65	64	54	69	6D	101","createdTim
02BC8B650	65	22	3A	31	34	39	37	36	37	37	37	39	36	37	36	30	e":1497677796760
02BC8B660	2C	22	64	65	6C	69	76	65	72	65	64	54	69	6D	65	22	,"deliveredTime"
02BC8B670	3A	30	2C	22	74	65	78	74	22	3A	22	53	69	73	74	20	:0,"text":"Sist
02BC8B680	3F	20	42	61	72	61	6E	67	6E	79	61	20	6B	6F	6B	20	? Barangnya kok
02BC8B690	62	65	6C	75	6D	20	73	61	6D	70	61	69	20	3F	20	53	belum sampai ? S
02BC8B6A0	75	64	61	68	20	32	20	68	61	72	69	20	73	61	79	61	udah 2 hari saya
02BC8B6B0	20	74	75	6E	67	67	75	2E	20	4B	61	74	61	6E	79	61	tunggu. Katanya
02BC8B6C0	20	70	65	6E	67	69	72	69	6D	61	6E	6E	79	61	20	65	pengirimannya e
02BC8B6D0	6B	73	70	72	65	73	73	2E	22	2C	22	68	61	73	43	6F	kspress.","hasCo

B-28

OFFSET	Aktor	Percakapan
129D00A5F	Korban	Send Voice note

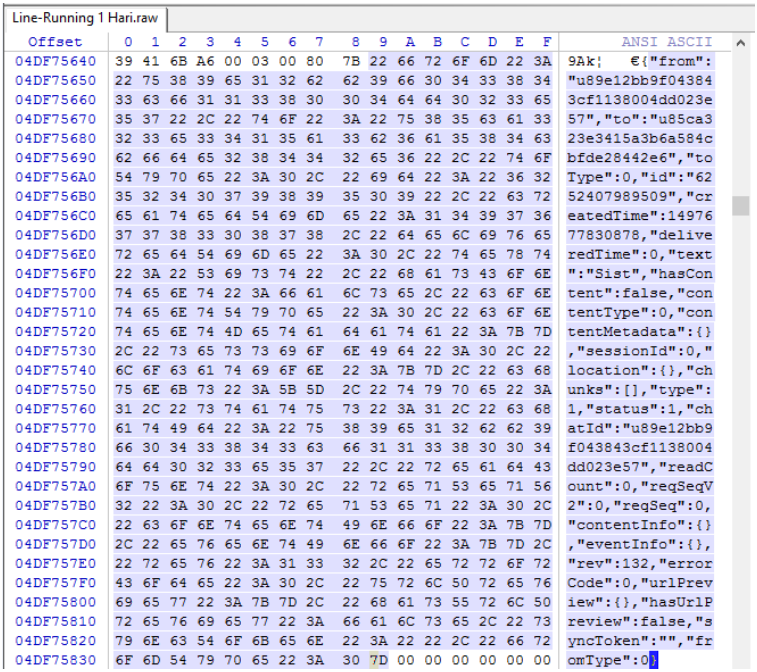
Hasil Winhex:



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
129D009A0	08	00	75	38	39	65	31	32	62	62	39	66	30	34	33	38	u89e12bb9f0438
129D009B0	34	33	63	66	31	31	33	38	30	30	34	64	64	30	32	33	43cf1138004dd023
129D009C0	65	35	37	75	38	35	63	61	33	32	33	65	33	34	31	35	e57u85ca323e3415
129D009D0	61	33	62	36	61	35	38	34	63	62	66	64	65	32	38	34	a3b6a584cbfde284
129D009E0	34	32	65	36	36	32	35	32	34	30	37	32	31	36	32	34	42e6625240721624
129D009F0	32	01	5C	B4	8D	EA	4D	03	7B	22	41	55	44	4C	45	4E	2 \´ êM {"AUDLEN
129D00A00	22	3A	22	37	34	39	37	22	2C	22	44	55	52	41	54	49	":"7497","DURATI
129D00A10	4F	4E	22	3A	22	37	34	39	37	22	2C	22	4F	42	53	5F	ON":"7497","OBS_
129D00A20	50	4F	50	22	3A	22	62	22	2C	22	53	52	43	5F	53	56	POP":"b","SRC_SV
129D00A30	43	5F	43	4F	44	45	22	3A	22	74	61	6C	6B	22	7D	75	C_CODE":"talk"}u
129D00A40	38	39	65	31	32	62	62	39	66	30	34	33	38	34	33	63	89e12bb9f043843c
129D00A50	66	31	31	33	38	30	30	34	64	64	30	32	33	65	35	37	f1138004dd023e57

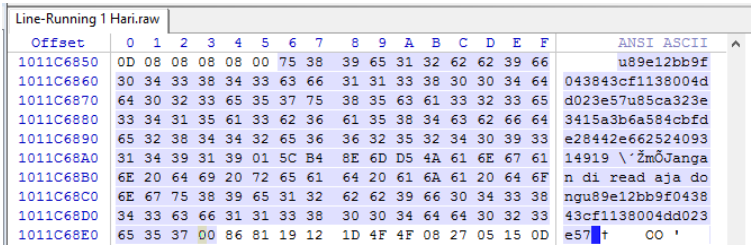
OFFSET	Aktor	Percakapan
4DF75649	Korban	Sist

Hasil Winhex:



OFFSET	Aktor	Percakapan
1011C68AB	Korban	Jangan di read aja dong

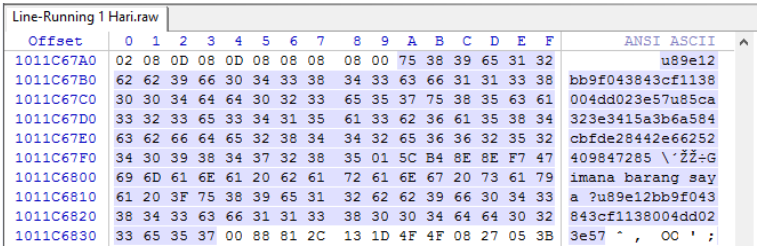
Hasil Winhex:



B-30

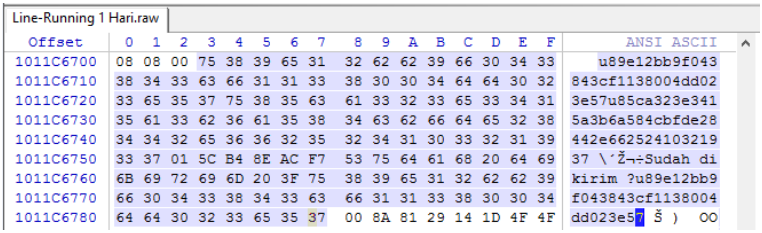
OFFSET	Aktor	Percakapan
1011C67FF	Korban	Gimana barang saya?

Hasil Winhex:



OFFSET	Aktor	Percakapan
1011C6758	Korban	Sudah dikirim ?

Hasil Winhex:



OFFSET	Aktor	Percakapan
222EBB59	Tersangka	Barang sedang dalam pengiriman sist, tenang saja. online shopping kami trusted 100% kok.

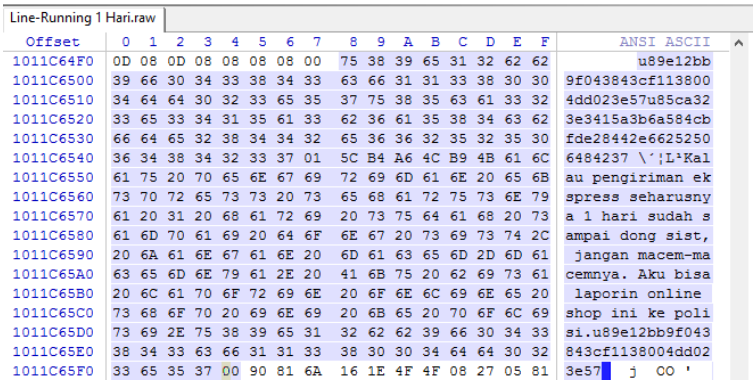
Hasil Winhex:

Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0222EBB50	9B	1C	BA	A5	00	0B	00	80	7B	22	66	72	6F	6D	22	3A	› °¥ €{"from":
0222EBB60	22	75	38	35	63	61	33	32	33	65	33	34	31	35	61	33	"u85ca323e3415a3
0222EBB70	62	36	61	35	38	34	63	62	66	64	65	32	38	34	34	32	b6a584cbfde28442
0222EBB80	65	36	22	2C	22	74	6F	22	3A	22	75	38	39	65	31	32	e6","to":"u89e12
0222EBB90	62	62	39	66	30	34	33	38	34	33	63	66	31	31	33	38	bb9f043843cf1138
0222EBBA0	30	30	34	64	64	30	32	33	65	35	37	22	2C	22	74	6F	004dd023e57","to
0222EBBB0	54	79	70	65	22	3A	30	2C	22	69	64	22	3A	22	36	32	Type":0,"id":"62
0222EBBC0	35	32	34	39	35	37	36	31	31	34	35	22	2C	22	63	72	52495761145","cr
0222EBBD0	65	61	74	65	64	54	69	6D	65	22	3A	31	34	39	37	36	eatedTime":14976
0222EBBE0	37	39	32	34	35	31	31	31	2C	22	64	65	6C	69	76	65	79245111,"delive
0222EBBF0	72	65	64	54	69	6D	65	22	3A	30	2C	22	74	65	78	74	redTime":0,"text
0222EBC00	22	3A	22	42	61	72	61	6E	67	20	73	65	64	61	6E	67	":"Barang sedang
0222EBC10	20	64	61	6C	61	6D	20	70	65	6E	67	69	72	69	6D	61	dalam pengirima
0222EBC20	6E	20	73	69	73	74	2C	20	74	65	6E	61	6E	67	20	73	n sist, tenang s
0222EBC30	61	6A	61	2E	20	6F	6E	6C	69	6E	65	20	73	68	6F	70	aja. online shop
0222EBC40	20	6B	61	6D	69	20	74	72	75	73	74	65	64	20	31	30	kami trusted 10
0222EBC50	30	25	20	6B	6F	6B	2E	22	2C	22	68	61	73	43	6F	6E	0% kok.","hasCon
0222EBC60	74	65	6E	74	22	3A	66	61	6C	73	65	2C	22	63	6F	6E	tent":false,"con
0222EBC70	74	65	6E	74	54	79	70	65	22	3A	30	2C	22	63	6F	6E	tentType":0,"con
0222EBC80	74	65	6E	74	4D	65	74	61	64	61	74	61	22	3A	7B	7D	tentMetadata":{}
0222EBC90	2C	22	73	65	73	73	69	6F	6E	49	64	22	3A	30	2C	22	,"sessionId":0,"
0222EBCA0	6C	6F	63	61	74	69	6F	6E	22	3A	7B	7D	2C	22	63	68	location":{},"ch
0222EBCB0	75	6E	6B	73	22	3A	5B	5D	2C	22	74	79	70	65	22	3A	unks":[],"type":
0222EBCC0	31	2C	22	73	74	61	74	75	73	22	3A	32	2C	22	63	68	1,"status":2,"ch
0222EBCD0	61	74	49	64	22	3A	22	75	38	39	65	31	32	62	62	39	atId":"u89e12bb9
0222EBCE0	66	30	34	33	38	34	33	63	66	31	31	33	38	30	30	34	f043843cf1138004
0222EBCF0	64	64	30	32	33	65	35	37	22	2C	22	72	65	61	64	43	dd023e57","readC
0222EBD00	6F	75	6E	74	22	3A	30	2C	22	72	65	71	53	65	71	56	ount":0,"reqSeqV
0222EBD10	32	22	3A	36	2C	22	72	65	71	53	65	71	22	3A	30	2C	2":6,"reqSeq":0,
0222EBD20	22	63	6F	6E	74	65	6E	74	49	6E	66	6F	22	3A	7B	7D	"contentInfo":{}
0222EBD30	2C	22	65	76	65	6E	74	49	6E	66	6F	22	3A	7B	7D	2C	,"eventInfo":{},
0222EBD40	22	72	65	76	22	3A	31	34	30	2C	22	65	72	72	6F	72	"rev":140,"error
0222EBD50	43	6F	64	65	22	3A	30	2C	22	75	72	6C	50	72	65	76	Code":0,"urlPrev
0222EBD60	69	65	77	22	3A	7B	7D	2C	22	68	61	73	55	72	6C	50	iew":{},"hasUrlP
0222EBD70	72	65	76	69	65	77	22	3A	66	61	6C	73	65	2C	22	73	revlew":false,"s

OFFSET	Aktor	Percakapan
1011C65D2	Korban	Kalau pengiriman ekspress seharusnya 1 hari sudah sampai dong sist, jangan macem-macemnya. Aku bisa laporin online shop ini ke polisi.

Hasil Winhex:

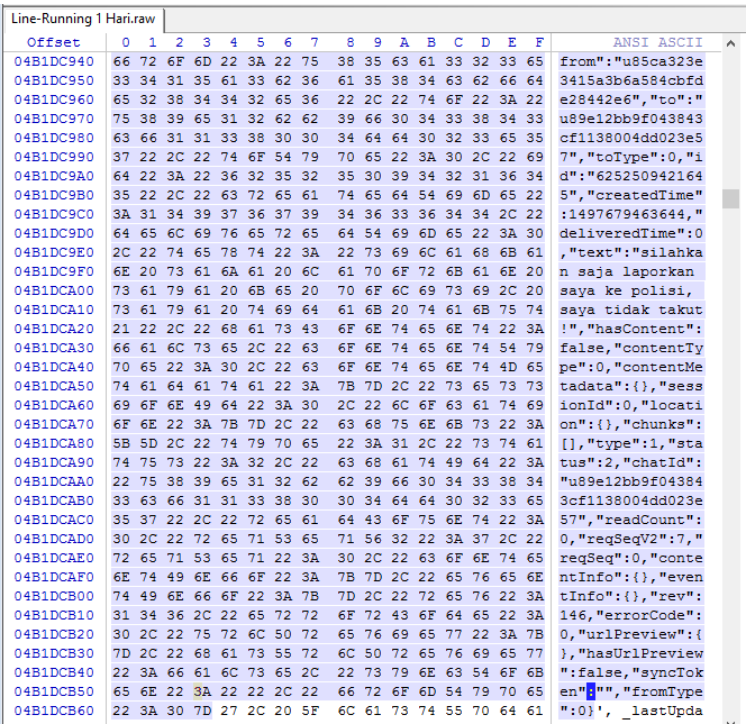


Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
1011C64F0	0D	08	0D	08	08	08	08	00	75	38	39	65	31	32	62	62	u89e12bb
1011C6500	39	66	30	34	33	38	34	33	63	66	31	31	33	38	30	30	9f043843cf113800
1011C6510	34	64	64	30	32	33	65	35	37	75	38	35	63	61	33	32	4dd023e57u85ca32
1011C6520	33	65	33	34	31	35	61	33	62	36	61	35	38	34	63	62	3e3415a3b6a584cb
1011C6530	66	64	65	32	38	34	34	32	65	36	36	32	35	32	35	30	fde28442e6625250
1011C6540	36	34	38	34	32	33	37	01	5C	B4	A6	4C	B9	4B	61	6C	6484237 \´¦L¹Kal
1011C6550	61	75	20	70	65	6E	67	69	72	69	6D	61	6E	20	65	6B	au pengiriman ek
1011C6560	73	70	72	65	73	73	20	73	65	68	61	72	75	73	6E	79	spress seharusny
1011C6570	61	20	31	20	68	61	72	69	20	73	75	64	61	68	20	73	a 1 hari sudah s
1011C6580	61	6D	70	61	69	20	64	6F	6E	67	20	73	69	73	74	2C	ampai dong sist,
1011C6590	20	6A	61	6E	67	61	6E	20	6D	61	63	65	6D	2D	6D	61	jangan macem-ma
1011C65A0	63	65	6D	6E	79	61	2E	20	41	6B	75	20	62	69	73	61	cemnya. Aku bisa
1011C65B0	20	6C	61	70	6F	72	69	6E	20	6F	6E	6C	69	6E	65	20	laporin online
1011C65C0	73	68	6F	70	20	69	6E	69	20	6B	65	20	70	6F	6C	69	shop ini ke poli
1011C65D0	73	69	2E	75	38	39	65	31	32	62	62	39	66	30	34	33	si.u89e12bb9f043
1011C65E0	38	34	33	63	66	31	31	33	38	30	30	34	64	64	30	32	843cf1138004dd02
1011C65F0	33	65	35	37	00	90	81	6A	16	1E	4F	4F	08	27	05	81	3e57 j OO '

OFFSET	Aktor	Percakapan
4B1DC93F	Tersangka	Silahkan saja laporkan saya ke polisi, saya tidak takut!

Hasil Winhex:



Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
04B1DC940	66	72	6F	6D	22	3A	22	75	38	35	63	61	33	32	33	65	from":"u85ca323e
04B1DC950	33	34	31	35	61	33	62	36	61	35	38	34	63	62	66	64	3415a3b6a584cbfd
04B1DC960	65	32	38	34	34	32	65	36	22	2C	22	74	6F	22	3A	22	e28442e6","to":"
04B1DC970	75	38	39	65	31	32	62	62	39	66	30	34	33	38	34	33	u89e12bb9f043843
04B1DC980	63	66	31	31	33	38	30	30	34	64	64	30	32	33	65	35	cf1138004dd023e5
04B1DC990	37	22	2C	22	74	6F	54	79	70	65	22	3A	30	2C	22	69	7","toType":0,"i
04B1DC9A0	64	22	3A	22	36	32	35	32	35	30	39	34	32	31	36	34	d":"625250942164
04B1DC9B0	35	22	2C	22	63	72	65	61	74	65	64	54	69	6D	65	22	5","createdTime"
04B1DC9C0	3A	31	34	39	37	36	37	39	34	36	33	36	34	34	2C	22	:1497679463644,"
04B1DC9D0	64	65	6C	69	76	65	72	65	64	54	69	6D	65	22	3A	30	deliveredTime":0
04B1DC9E0	2C	22	74	65	78	74	22	3A	22	73	69	6C	61	68	6B	61	,"text":"silahka
04B1DC9F0	6E	20	73	61	6A	61	20	6C	61	70	6F	72	6B	61	6E	20	n saja laporkan
04B1DCA00	73	61	79	61	20	6B	65	20	70	6F	6C	69	73	69	2C	20	saya ke polisi,
04B1DCA10	73	61	79	61	20	74	69	64	61	6B	20	74	61	6B	75	74	saya tidak takut
04B1DCA20	21	22	2C	22	68	61	73	43	6F	6E	74	65	6E	74	22	3A	!","hasContent":
04B1DCA30	66	61	6C	73	65	2C	22	63	6F	6E	74	65	6E	74	54	79	false,"contentTy
04B1DCA40	70	65	22	3A	30	2C	22	63	6F	6E	74	65	6E	74	4D	65	pe":0,"contentMe
04B1DCA50	74	61	64	61	74	61	22	3A	7B	7D	2C	22	73	65	73	73	tadata":{},"sess
04B1DCA60	69	6F	6E	49	64	22	3A	30	2C	22	6C	6F	63	61	74	69	ionId":0,"locati
04B1DCA70	6F	6E	22	3A	7B	7D	2C	22	63	68	75	6E	6B	73	22	3A	on":{},"chunks":
04B1DCA80	5B	5D	2C	22	74	79	70	65	22	3A	31	2C	22	73	74	61	[],"type":1,"sta
04B1DCA90	74	75	73	22	3A	32	2C	22	63	68	61	74	49	64	22	3A	tus":2,"chatId":
04B1DCAA0	22	75	38	39	65	31	32	62	62	39	66	30	34	33	38	34	"u89e12bb9f04384
04B1DCAB0	33	63	66	31	31	33	38	30	30	34	64	64	30	32	33	65	3cf1138004dd023e
04B1DCAC0	35	37	22	2C	22	72	65	61	64	43	6F	75	6E	74	22	3A	57","readCount":
04B1DCAD0	30	2C	22	72	65	71	53	65	71	56	32	22	3A	37	2C	22	0,"reqSeqV2":7,"
04B1DCAE0	72	65	71	53	65	71	22	3A	30	2C	22	63	6F	6E	74	65	reqSeq":0,"conte
04B1DCAF0	6E	74	49	6E	66	6F	22	3A	7B	7D	2C	22	65	76	65	6E	ntInfo":{},"even
04B1DCB00	74	49	6E	66	6F	22	3A	7B	7D	2C	22	72	65	76	22	3A	tInfo":{},"rev":
04B1DCB10	31	34	36	2C	22	65	72	72	6F	72	43	6F	64	65	22	3A	146,"errorCode":
04B1DCB20	30	2C	22	75	72	6C	50	72	65	76	69	65	77	22	3A	7B	0,"urlPreview":{
04B1DCB30	7D	2C	22	68	61	73	55	72	6C	50	72	65	76	69	65	77	},"hasUrlPreview
04B1DCB40	22	3A	66	61	6C	73	65	2C	22	73	79	6E	63	54	6F	6B	":false,"syncTok
04B1DCB50	65	6E	22	3A	22	22	2C	22	66	72	6F	6D	54	79	70	65	en":"","fromType
04B1DCB60	22	3A	30	7D	27	2C	20	5F	6C	61	73	74	55	70	64	61	":0}', _lastUpda

OFFSET	Aktor	Percakapan
129D00402	Korban	Send Video

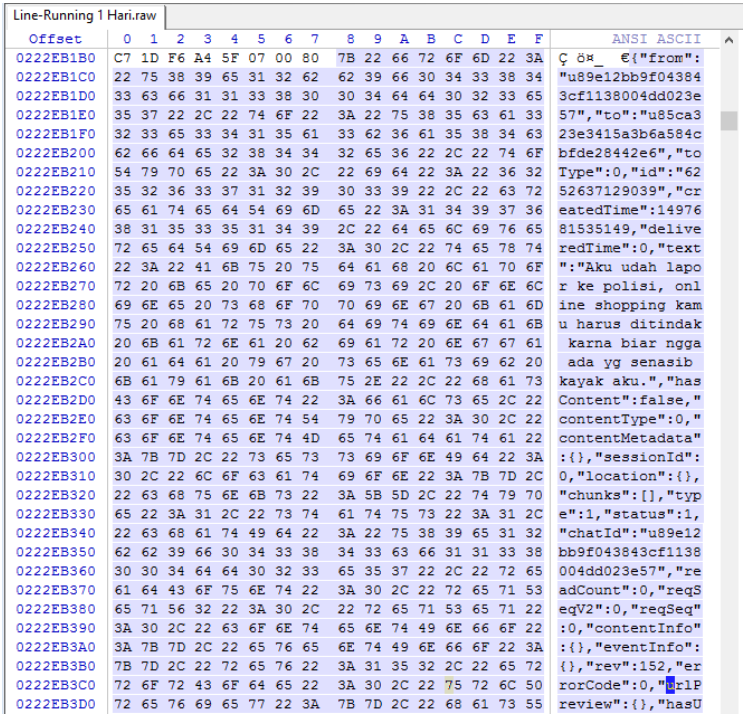
Hasil Winhex:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
129D009A0	08	00	75	38	39	65	31	32	62	62	39	66	30	34	33	38	u89e12bb9f0438
129D009B0	34	33	63	66	31	31	33	38	30	30	34	64	64	30	32	33	43cf1138004dd023
129D009C0	65	35	37	75	38	35	63	61	33	32	33	65	33	34	31	35	e57u85ca323e3415
129D009D0	61	33	62	36	61	35	38	34	63	62	66	64	65	32	38	34	a3b6a584cbfde284
129D009E0	34	32	65	36	36	32	35	32	34	30	37	32	31	36	32	34	42e6625240721624
129D009F0	32	01	5C	B4	8D	EA	4D	03	7B	22	41	55	44	4C	45	4E	2 \´ êM {"AUDLEN
129D00A00	22	3A	22	37	34	39	37	22	2C	22	44	55	52	41	54	49	":"7497","DURATI
129D00A10	4F	4E	22	3A	22	37	34	39	37	22	2C	22	4F	42	53	5F	ON":"7497","OBS_
129D00A20	50	4F	50	22	3A	22	62	22	2C	22	53	52	43	5F	53	56	POP":"b","SRC_SV
129D00A30	43	5F	43	4F	44	45	22	3A	22	74	61	6C	6B	22	7D	75	C_CODE":"talk"}u
129D00A40	38	39	65	31	32	62	62	39	66	30	34	33	38	34	33	63	89e12bb9f043843c
129D00A50	66	31	31	33	38	30	30	34	64	64	30	32	33	65	35	37	f1138004dd023e57

B-34

OFFSET	Aktor	Percakapan
222EB1B9	Korban	Aku udah lapor ke polisi, online shopping kamu harus ditindak karna biar ngga ada yg senasib kayak aku.

Hasil Winhex:

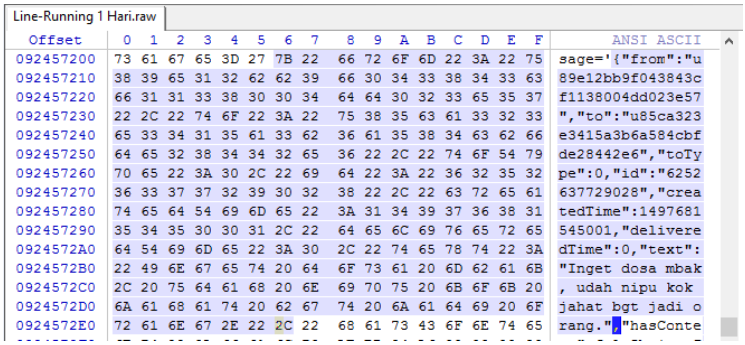


Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0222EB1B0	C7	1D	F6	A4	5F	07	00	80	7B	22	66	72	6F	6D	22	3A	Ç ö¤_ €{"from":
0222EB1C0	22	75	38	39	65	31	32	62	62	39	66	30	34	33	38	34	"u89e12bb9f04384
0222EB1D0	33	63	66	31	31	33	38	30	30	34	64	64	30	32	33	65	3cf1138004dd023e
0222EB1E0	35	37	22	2C	22	74	6F	22	3A	22	75	38	35	63	61	33	57","to":"u85ca3
0222EB1F0	32	33	65	33	34	31	35	61	33	62	36	61	35	38	34	63	23e3415a3b6a584c
0222EB200	62	66	64	65	32	38	34	34	32	65	36	22	2C	22	74	6F	bfde28442e6","to
0222EB210	54	79	70	65	22	3A	30	2C	22	69	64	22	3A	22	36	32	Type":0,"id":"62
0222EB220	35	32	36	33	37	31	32	39	30	33	39	22	2C	22	63	72	52637129039","cr
0222EB230	65	61	74	65	64	54	69	6D	65	22	3A	31	34	39	37	36	eatedTime":14976
0222EB240	38	31	35	33	35	31	34	39	2C	22	64	65	6C	69	76	65	81535149,"delive
0222EB250	72	65	64	54	69	6D	65	22	3A	30	2C	22	74	65	78	74	redTime":0,"text
0222EB260	22	3A	22	41	6B	75	20	75	64	61	68	20	6C	61	70	6F	":"Aku udah lapo
0222EB270	72	20	6B	65	20	70	6F	6C	69	73	69	2C	20	6F	6E	6C	r ke polisi, onl
0222EB280	69	6E	65	20	73	68	6F	70	70	69	6E	67	20	6B	61	6D	ine shopping kam
0222EB290	75	20	68	61	72	75	73	20	64	69	74	69	6E	64	61	6B	u harus ditindak
0222EB2A0	20	6B	61	72	6E	61	20	62	69	61	72	20	6E	67	67	61	karna biar ngga
0222EB2B0	20	61	64	61	20	79	67	20	73	65	6E	61	73	69	62	20	ada yg senasib
0222EB2C0	6B	61	79	61	6B	20	61	6B	75	2E	22	2C	22	68	61	73	kayak aku.","has
0222EB2D0	43	6F	6E	74	65	6E	74	22	3A	66	61	6C	73	65	2C	22	Content":false,"
0222EB2E0	63	6F	6E	74	65	6E	74	54	79	70	65	22	3A	30	2C	22	contentType":0,"
0222EB2F0	63	6F	6E	74	65	6E	74	4D	65	74	61	64	61	74	61	22	contentMetadata"
0222EB300	3A	7B	7D	2C	22	73	65	73	73	69	6F	6E	49	64	22	3A	:{},"sessionId":
0222EB310	30	2C	22	6C	6F	63	61	74	69	6F	6E	22	3A	7B	7D	2C	0,"location":{},
0222EB320	22	63	68	75	6E	6B	73	22	3A	5B	5D	2C	22	74	79	70	"chunks":[],"typ
0222EB330	65	22	3A	31	2C	22	73	74	61	74	75	73	22	3A	31	2C	e":1,"status":1,
0222EB340	22	63	68	61	74	49	64	22	3A	22	75	38	39	65	31	32	"chatId":"u89e12
0222EB350	62	62	39	66	30	34	33	38	34	33	63	66	31	31	33	38	bb9f043843cf1138
0222EB360	30	30	34	64	64	30	32	33	65	35	37	22	2C	22	72	65	004dd023e57","re
0222EB370	61	64	43	6F	75	6E	74	22	3A	30	2C	22	72	65	71	53	adCount":0,"reqS
0222EB380	65	71	56	32	22	3A	30	2C	22	72	65	71	53	65	71	22	eqV2":0,"reqSeq"
0222EB390	3A	30	2C	22	63	6F	6E	74	65	6E	74	49	6E	66	6F	22	:0,"contentInfo"
0222EB3A0	3A	7B	7D	2C	22	65	76	65	6E	74	49	6E	66	6F	22	3A	:{},"eventInfo":
0222EB3B0	7B	7D	2C	22	72	65	76	22	3A	31	35	32	2C	22	65	72	{},"rev":152,"er
0222EB3C0	72	6F	72	43	6F	64	65	22	3A	30	2C	22	75	72	6C	50	rorCode":0,"urlP
0222EB3D0	72	65	76	69	65	77	22	3A	7B	7D	2C	22	68	61	73	55	review":{},"hasU

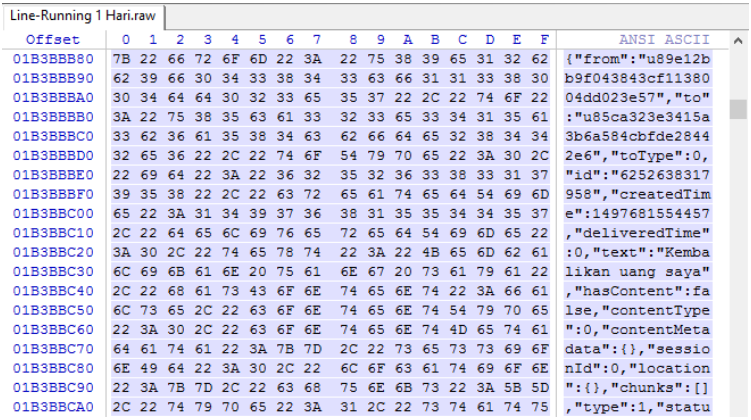
OFFSET	Aktor	Percakapan
92457207	Korban	Inget dosa mbak, udah nipu kok jahat bgt jadi orang.

Hasil Winhex:



OFFSET	Aktor	Percakapan
1B3BBB81	Korban	Kembalikan uang saya

Hasil Winhex:



B-36

OFFSET	Aktor	Percakapan
15E26681	Korban	Atau polisi akan datang ke tempat kamu.

Hasil Winhex:

Line-Running 1 Hari.raw

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
015E26680	7B	22	66	72	6F	6D	22	3A	22	75	38	39	65	31	32	62	{"from":"u89e12b
015E26690	62	39	66	30	34	33	38	34	33	63	66	31	31	33	38	30	b9f043843cf11380
015E266A0	30	34	64	64	30	32	33	65	35	37	22	2C	22	74	6F	22	04dd023e57","to"
015E266B0	3A	22	75	38	35	63	61	33	32	33	65	33	34	31	35	61	:"u85ca323e3415a
015E266C0	33	62	36	61	35	38	34	63	62	66	64	65	32	38	34	34	3b6a584cbfde2844
015E266D0	32	65	36	22	2C	22	74	6F	54	79	70	65	22	3A	30	2C	2e6","toType":0,
015E266E0	22	69	64	22	3A	22	36	32	35	32	36	34	31	33	34	30	"id":"6252641340
015E266F0	38	31	38	22	2C	22	63	72	65	61	74	65	64	54	69	6D	818","createdTim
015E26700	65	22	3A	31	34	39	37	36	38	31	36	30	33	36	32	38	e":1497681603628
015E26710	2C	22	64	65	6C	69	76	65	72	65	64	54	69	6D	65	22	,"deliveredTime"
015E26720	3A	30	2C	22	74	65	78	74	22	3A	22	41	74	61	75	20	:0,"text":"Atau
015E26730	70	6F	6C	69	73	69	20	61	6B	61	6E	20	64	61	74	61	polisi akan data
015E26740	6E	67	20	6B	65	20	74	65	6D	70	61	74	20	6B	61	6D	ng ke tempat kam
015E26750	75	2E	22	2C	22	68	61	73	43	6F	6E	74	65	6E	74	22	u.","hasContent"
015E26760	3A	66	61	6C	73	65	2C	22	63	6F	6E	74	65	6E	74	54	:false,"contentT
015E26770	79	70	65	22	3A	30	2C	22	63	6F	6E	74	65	6E	74	4D	ype":0,"contentM
015E26780	65	74	61	64	61	74	61	22	3A	7B	7D	2C	22	73	65	73	etadata":{},"ses
015E26790	73	69	6F	6E	49	64	22	3A	30	2C	22	6C	6F	63	61	74	sionId":0,"locat
015E267A0	69	6F	6E	22	3A	7B	7D	2C	22	63	68	75	6E	6B	73	22	ion":{},"chunks"
015E267B0	3A	5B	5D	2C	22	74	79	70	65	22	3A	31	2C	22	73	74	:[],"type":1,"st
015E267C0	61	74	75	73	22	3A	31	2C	22	63	68	61	74	49	64	22	atus":1,"chatId"
015E267D0	3A	22	75	38	39	65	31	32	62	62	39	66	30	34	33	38	:"u89e12bb9f0438
015E267E0	34	33	63	66	31	31	33	38	30	30	34	64	64	30	32	33	43cf1138004dd023
015E267F0	65	35	37	22	2C	22	72	65	61	64	43	6F	75	6E	74	22	e57","readCount"
015E26800	3A	30	2C	22	72	65	71	53	65	71	56	32	22	3A	30	2C	:0,"reqSeqV2":0,
015E26810	22	72	65	71	53	65	71	22	3A	30	2C	22	63	6F	6E	74	"reqSeq":0,"cont
015E26820	65	6E	74	49	6E	66	6F	22	3A	7B	7D	2C	22	65	76	65	entInfo":{},"eve
015E26830	6E	74	49	6E	66	6F	22	3A	7B	7D	2C	22	72	65	76	22	ntInfo":{},"rev"
015E26840	3A	31	35	35	2C	22	65	72	72	6F	72	43	6F	64	65	22	:155,"errorCode"
015E26850	3A	30	2C	22	75	72	6C	50	72	65	76	69	65	77	22	3A	:0,"urlPreview":
015E26860	7B	7D	2C	22	68	61	73	55	72	6C	50	72	65	76	69	65	{},"hasUrlPrevie
015E26870	77	22	3A	66	61	6C	73	65	2C	22	73	79	6E	63	54	6F	w":false,"syncTo
015E26880	6B	65	6E	22	3A	22	22	2C	22	66	72	6F	6D	54	79	70	ken":"","fromTyp
015E26890	65	22	3A	30	7D	00	00	00	00	00	00	00	00	00	00	00	e":0}