ANALISIS *LIVE FORENSICS* UNTUK PERBANDINGAN APLIKASI *INSTANT MESSENGER* PADA SISTEM OPERASI WINDOWS 10

Tayomi Dwi Larasati dan Bekti Cahyo Hidayanto
Departemen Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi,
Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya 60111 Indonesia
e-mail: tayomidwi@gmail.com[1)], bekticahyo@is.its.ac.id[2)]

Abstrak

Live forensics digunakan untuk mendapatkan bukti digital pada RAM. Teknik ini diperlukan dumping data untuk dianalisa. Penelitian ini dilakukan untuk aplikasi Instant Messenger popular yaitu Facebook, LINE dan Telegram pada platform windows 10. Dari analisa ingin diketahui aplikasi yang mudah dan sulit untuk memperoleh data sebagai bukti digital. Dilakukan pengujian skenario dengan cara eksperimen berupa data percakapan biasa dan penghapusan pesan atau percakapan. Menggunakan tools Winhex dan Belkasoft Evidence Center digunakan untuk menganalisa data digital. Jenis data berupa data primer percakapan dan data media yang memiliki karakteristik unik sehingga data yang didapatkan juga berbeda bergantung struktur data yang disusun pada aplikasi. Berdasarkan analisa perbandingan data primer percakapan pada tools Winhex untuk 3 aplikasi tersebut sebesar 76%, 100%, dan 0% dan tools Belkasoft sebesar 10%, 20% dan 0%. Berdasarkan jumlah object yang dikirim dengan jumlah object yang terdeteksi pada tools Winhex sebesar 60,95%, 100%, dan 0%, untuk tools Belkasoft sebesar 6,67%, 33,33% dan 0%.

Kata kunci: *Live forensics, Facebook Messenger, LINE Messenger, Telegram Messenger*

1. PENDAHULUAN

Kejahatan dunia maya setiap tahunnya mengalami peningkatan yang sangat pesat [1], hal ini dikarenakan semakin berkembangnya teknologi komputer yang berdampak pada kehidupan manusia. Hal ini dikarenakan masih banyaknya cara untuk mendapatkan data orang lain dengan mudah, salah satunya adalah dengan memanfaatkan data yang tertinggal dari aktifitas penggunaan sebuah aplikasi pada Random Access Memory (RAM). RAM merupakan suatu memori tempat penyimpanan data sementara, ketika saat komputer dijalankan dan dapat diakses secara acak (random) [2]. 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 [3]. 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. Sistem Operasi yang popular saat ini adalah sistem operasi windows 10 yang digunakan oleh 23% dari seluruh penggunaan sistem operasi [4]. Penelitian terdahulu mengenai forensika digital pada aplikasi IM yang menggunakan aplikasi LINE dan Whatsapp. Hasil yang menunjukkan bahwa didapatkan data utama berupa database berisikan kontak, percakapan dan artefak file penyusun aplikasi serta menunjukkan bahwa aplikasi WhatsApp menjadi rujukan dalam forensika digital di Indonesia,sedangkan untuk LINE menjadi aplikasi yg lebih aman dikarenakan sulit untuk dilakukan forensika digital.

Permasalahan penelitian ini seperti apa saja karakteristik bukti digital yang didapat dari aktivitas penggunaan aplikasi Instant Messenger (IM), lalu bagaimana cara mengimplementasikan teknik live forensics untuk menginvestigasi bukti digital dari aktivitas penggunaan aplikasi IM, lalu bagaimana perbandingan bukti digital yang didapatkan oleh ke-3 aplikasi IM tersebut. Peneliti berinisiatif untuk melakukan penelitian mengenai tingkat keamanan dari aktifitas penggunaan aplikasi IM pada sistem operasi windows 10 menggunakan metode live forensics yang nantinya akan dijadikan bukti digital.

2. TINJAUAN PUSTAKA

Tinjauan Pustaka akan menjelaskan dasar teori yang dijadikan acuan dan memberikan gambaran secara umum dari landasan penjabaran paper ini.

2.1 Bukti Digital

Pada penyelidikan yang dilakukan, pasti terdapat bukti yang disimpan, baik bukti informasi atau data, Menurut [5] 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.

2.2 Live Forensics

Live forensic yaitu suatu teknik analisis dimana menyangkut data yang berjalan pada sistem atau data volatile yang umumnya tersimpan pada RAM atau transit pada jaringan [6]. 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. Tools yang dibandingan pada metode live forensics yaitu dari kemampuan penggunaan memory, waktu, jumlah langkah dan akurasi paling baik dalam melakukan live forensic.

2.3 Tahapan Forensics

Secara umum ada empat tahapan yang harus dilakukan dalam mengelola bukti pada forensika digital, yaitu pengumpulan, pemeliharaan, analisa, dan presentasi. Dalam penelitian ini, peneliti 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 : Identification, Collection, Examination, Analysis dan Reporting.

2.4 Random Access Memory (RAM)

RAM merupakan sebuah tipe penyimpanan komputer yang isinya dapat diakses dalam waktu yang tetap tidak memperdulikan letak data tersebut dalam memori [7]. 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 [8].

3. METODOLOGI

Pada penelitian ini terdapat 3 tahap yaitu tahap Persiapan, Eksplorasi dan Analisa, berikut ini akan dijelaskan secara lengkap:

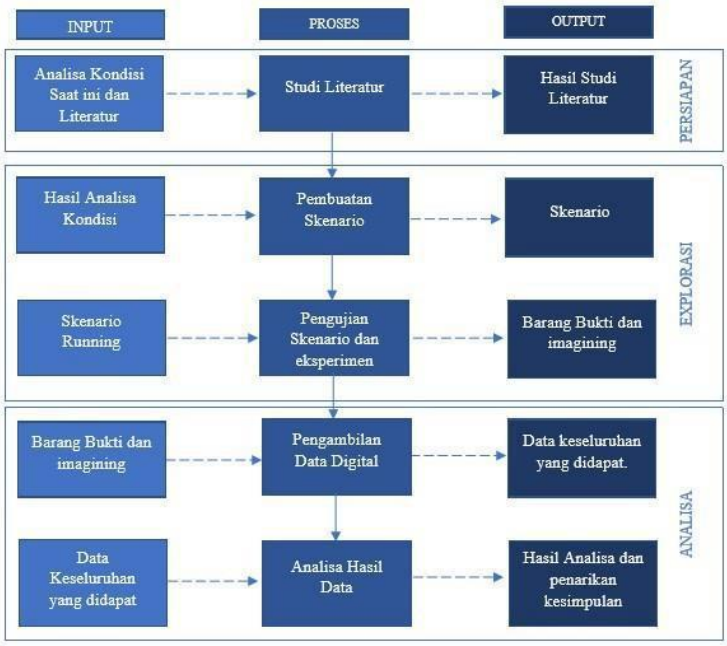
- Pada tahap persiapan dilakukan studi literatur mengenai teknik dan tahapan bagaimana melakukan live forensics, melakukan perbandingan tools yang akan digunakan dari tools yang ada yaitu tools DumpIt dan Belkasoft RamCapturer untuk pengambilan barang bukti digital dan tools Winhex dan Belkasoft Evidence Center untuk analisa barang bukti digital, dan melakukan analisa kondisi bagaimana penelitian sebelumnya untuk melakukan teknik live forensics.

3. Pada tahap eksplorasi, hasil analisa kondisi dan tahapan live forensics selanjutnya dilakukan pembuatan skenario dan eksperimen, pada penelitian ini terdapat 2 eksperimen yaitu:
   - Eksperimen 1: Aplikasi dijalankan dengan biasa. Pembicaraan meliputi percakapan antar pengguna dan pertukaran media (picture, video, dan audio).
   - Eksperimen 2: Aplikasi dijalankan dengan biasa namun dengan adanya penghapusan beberapa pesan/percakapan melalui layanan aplikasi

Setelah skenario dan eksperimen dijalankan maka akan terdapat hasil dari skenario dan eksperimen yang nantinya akan dianalisa pada tahapan selanjutnya.

- Pada tahap analisa, setelah mendapatkan hasil dari skenario dan eksperimen maka dilakukan analisa untuk mendapatkan barang bukti digital, dilihat dari data-data yang didapatkan melalui tools yang telah ditentukan, pengambilan dari barang bukti digital seperti data percakapan aplikasi, data pendukung aplikasi

dan data media. Dari pengambilan data barang bukti digital yang sesuai dengan skenario dan eksperimen yang nantinya dilakukan kesimpulan dan perbandingan dari aplikasi IM.
Metodologi pengerjaan penelitian ini secara garis besar terdiri atas tahapan-tahapan berikut:



Gambar 1. Metodologi Penelitian

4. PEMBAHASAN

Berikut merupakan hasil dan pembahasan penelitian.

4.1 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

4.1.1 Hasil Data Eksperimen 1

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

Tabel 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
Belkasoft Evidence	Hanya data Media	Hanya data Media	Hanya data Media

Pada Tabel 1 merupakan eksperimen pertama yang berupa aktivitas penggunaan aplikasi dengan kondisi normal, tanpa ada modifikasi penggunaan maupun penanganan terhadap aplikasi. Oleh karena itu, peneliti 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.

4.1.2 Hasil Data Eksperimen 2

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

Tabel 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

Pada Tabel 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, peneliti 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.

4.2 Analisa Data Digital

Pada analisa Data digital, 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.

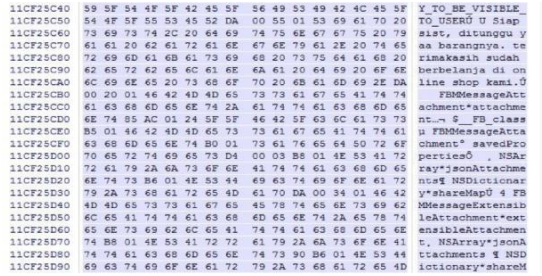
4.2.1 Struktur Pesan

Berikut ini merupakan struktur pesan dari 3 aplikasi instant messenger (IM):

4.2.1.1 Struktur Pesan Facebook Messenger

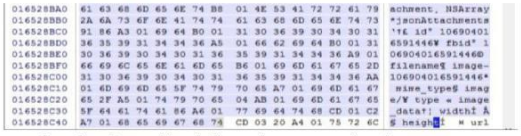
Pada Struktur Pesan aplikasi LINE Messenger terdiri dari struktur dan type data yang berbeda, terdiri dari pengambilan sample dari text, picture, video, audio dan sticker untuk mendapatkan bukti digital.

A. Text



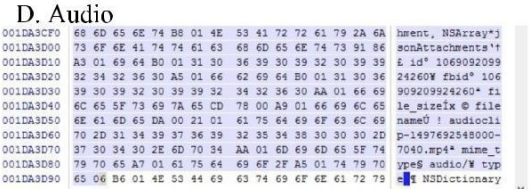
Gambar 2 Hasil Winhex Text Facebook Messenger

B. Picture



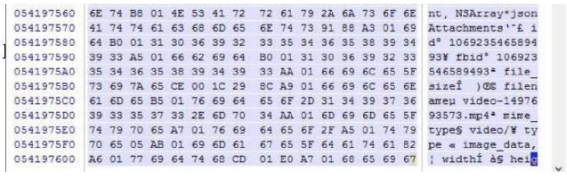
Gambar 3 Hasil Winhex Picture Facebook Messenger

D. Audio



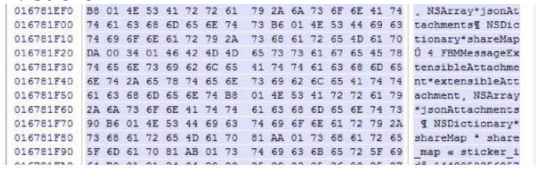
Gambar 5 Hasil Winhex Audio Facebook Messenger

C. Video



Gambar 4 Hasil Winhex Video Facebook

E. Sticker



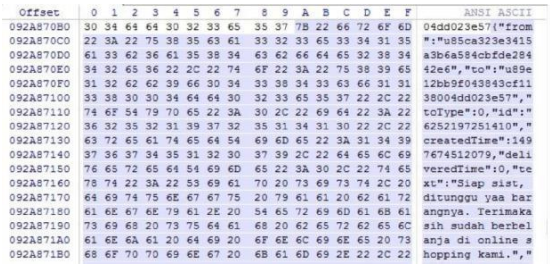
Gambar 6 Hasil Winhex Sticker Facebook

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

4.2.1.2 Struktur Pesan LINE Messenger

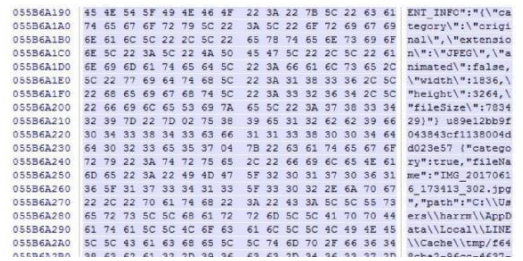
Pada Struktur Pesan aplikasi LINE Messenger terdiri dari struktur dan type data yang berbeda, terdiri dari pengambilan sample dari text, picture, video, audio dan sticker untuk mendapatkan bukti digital.

A. Text



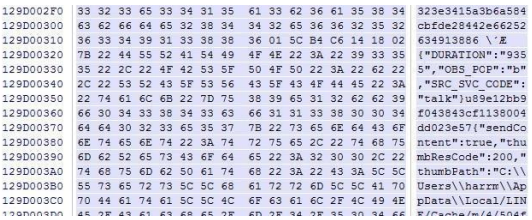
Gambar 7 Hasil Winhex Text LINE Messenger

B. Picture



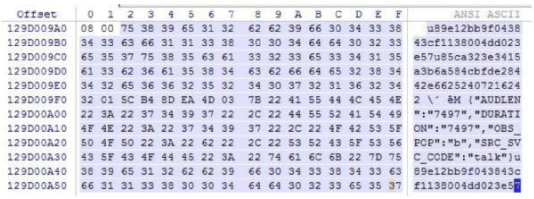
Gambar 8 Hasil Winhex Picture LINE Messenger

C.Video



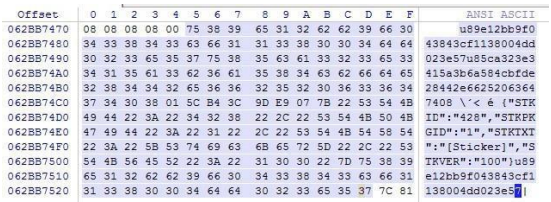
Gambar 9 Hasil Winhex Video LINE Messenger

D. Audio



Gambar 10 Hasil Winhex Audio LINE Messenger

E. Sticker



Gambar 11 Hasil Winhex Sticker LINE Messenger

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

4.2.1.3 Struktur Pesan Telegram Messenger

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

4.2.2 Analisa Data Primer Percakapan

Berikut ini adalah analisa data primer percakapan yang digunakan untuk bukti pendukung:

4.2.2.1 Facebook Messenger

Tabel 3. Type Data Facebook Messenger

Type 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

4.2.2.2 LINE Messenger

Tabel 4. Type Data LINE Messenger

Type 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 berbelanja di onLINE shopping kami.",	isi dari pesan yang dikirim
createdTime:1497674512079,	waktu saat pesan dibuat. Berbentuk unix hex

4.2.2.3 Telegram Messenger

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

4.2.3 Analisa Data Pendukung Percakapan

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

4.2.3.1 Facebook Messenger

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

A. Text

Tabel 5. Type Data Text Facebook Messenger

Type 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

B. Picture

Tabel 6. Type Data Picture Facebook Messenger

Type 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_typeimage/typeimage_datawidthheight	Deskripsi data mime type 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

C. Video

Tabel 8. Type Data Video Facebook Messenger

Type Object	Keterangan
FBMMessageAttachment* attachment$__FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMMessageExtensibleAttachment* extensibleAttachmentNSArray*jsonAttachmentsid106923546589493fbid106923546589493file_size)	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
filenamevideo-1497693573.mp4	nama file video yang dikirim
mime_typevideo/typeimage_datawidthheight	Deskripsi data mime type video dengan image
video_dataurlhttps://video.xx.fbcdn.net/v/t42.3356-2/19288123_106923563256158_8384727728976297984_n.mp4/video-1497693573.mp4?vabr=1640572&o	url file video yang dikirim

D. Audio

Tabel 7. Type Data Audio Facebook Messenger

Type 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_typeaudio/typeNSDictionary* shareMap4	Deskripsi data mime type audio
FBMMessageExtensibleAttachment* extensibleAttachmentNSArray*tagssource:chat:orcaapp_id:256002347743983	Deksripsi ekstensi Attachment dengan tagsource

E. Sticker

Tabel 9. Type Data Sticker Facebook Messenger

Type 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
NSDictionary*shareMapshare_mapsticker_id144885035685763	identitas stiker yang dikirim
FBMMessageExtensibleAttachment* extensibleAttachmentNSArray*tagssource:chat:orcaapp_id:256002347743983	Deksripsi ekstensi Attachment dengan tagsource

4.2.3.2 LINE Messenger

A. Text

Tabel 10. Type Data Text LINE Messenger

Type Object	Keterangan
toType: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
contentType: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.
type: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

B. Picture

Tabel 11. Type Data Picture LINE Messenger

Type Object	Keterangan
u89e12bb9f043843cf1138004dd02 3e57	identitas pengirim pesan
u85ca323e3415a3b6a584cbfde284 42e6	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

C. Video

Tabel 10. Type Data Video LINE Messenger

Type 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

D. Audio

Tabel 11. Type Data Audio LINE Messenger

Type 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

E. Sticker

Tabel 12. Type Data Sticker LINE Messenger

Type Object	Keterangan
u89e12bb9f043843cf1138004dd02 3e57	identitas pengirim pesan
u85ca323e3415a3b6a584cbfde284 42e6	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
u89e12bb9f043843cf1138004dd02 3e57	identitas percakapan

4.2.3.3 Telegram Messenger

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

4.3 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:

4.3.1 Facebook Messenger

A. Picture

Pada tools Belkasoft Evidence Center hanya didapatkan data-data picture pada Facebook messenger. Pada gambar 12 menggambarkan hasil yang didapatkan yaitu gambar dengan nama file picture_00006212D5C8.jpg dan Pada gambar 13 perbandingan dengan nama file pada saat skenario dijalan kan dengan nama file Screenshot_2017-06-16-15-37-53.jpg.

Gambar 12 Media Picture Facebook Messenger

Gambar 13 Media Picture Skenario Facebook Messenger

4.3.2 LINE Messenger

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

A. Picture

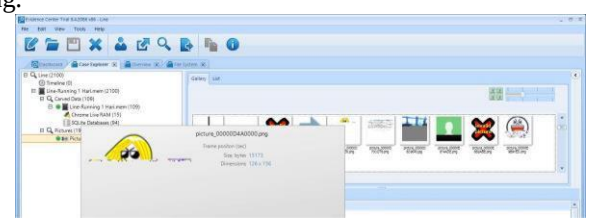
Pada tools Belkasoft Evidence Center hanya didapatkan data-data picture pada LINE messenger. Pada gambar 14 menggambarkan hasil yang didapatkan yaitu gambar dengan nama file picture_0000028F9000.jpg dan pada gambar 15 perbandingan dengan nama file pada saat skenario dijalan kan dengan nama file Screenshot_2017-06-16-15-37-53.jpg

Gambar 14 Media Picture LINE Messenger

Gambar 15 Media Picture Skenario Line Messenger

B. Sticker

Pada tools Belkasoft Evidence Center hanya didapatkan data-data Sticker pada LINE messenger. Pada gambar 16 menggambarkan hasil yang didapatkan yaitu sticker dengan nama file picture_00000D4A0000.png.



Gambar 16 Media Sticker LINE Messenger

4.3.3 Telegram Messenger

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

4.4 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, peneliti menggunakan pendekatan aplikasi, perangkat, dan eksperimen.

4.4.1 Perbandingan Data Aplikasi

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

Tabel 13. Perbandingan Data Aplikasi

Tools,Aplikasi / Data	Data Primer Percakapan					Media				Persentase
	userId	senderId	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%

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.

Dari hasil perbandingan data aplikasi pada tabel 15 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 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. Maka akan menghasilkan daftar jumlah artefak yang akan dijelaskan pada tabel 16, tabel 17 dan tabel 18.

Tabel 16. 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

Tabel 17. 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

Tabel 18. Persentase jumlah artefak yang didapatkan

	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 19 akan menjelaskan keseluruhan dari 3 aplikasi

Tabel 19. Persentase rerata jumlah artefakpada aplikasi Telegram Messenger

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.

4.4.2 Perbandingan Data Eksperimen

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

Tabel 20. Perbandingan Data Eksperimen

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

5. KESIMPULAN DAN SARAN

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

- Penerapan dan pengimplementasian teknik live forensics untuk mendapatkan bukti digital dari aktivitas penggunaan aplikasi IM 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.
- Perbandingan bukti digital yang didapatkan dari aplikasi IM 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.
- Pada sisi examiner, aplikasi Facebook dan LINE messenger merupakan aplikasi IM 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 IM 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.

Berdasarkan hasil penelitan ini adapun saran yang dapat disampaikan untuk penelitian selanjutnya adalah sebagai berikut :

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

6. DAFTAR PUSTAKA

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

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

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

[4] R. U. A. Y. Muhammad Nur Faiz, "ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN KEMANANAN EMAIL PADA SISTEM OPERASI PROPRIETARY," April 2016.
[5] Marshall, Digital Forensics: Digital Evidence in Criminal Investigations, 2008.
[6] A. Y. M. N. F. Rusydi Umar, "ANALISIS KINERJA METODE LIVE FORENSICS UNTUK INVESTIGASI RANDOM ACCESS MEMORY PADA SISTEM PROPRIETARY," 2014.
[7] Wikipedia, "Rndom Access Memory (RAM)," 2016. [Online] Aailable:https://id.wikipedia.org/wiki/Memori_akses_acak.
[8] K. Amari, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory," 2009.
[9] Y. P. Aan Kurniawan, "Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics," 2014.
[10] F. S. Fenu Gianni, "Live Digital Forensics: Windows XP vs Windows 7," Desember 2013.
[11] D. Sudyana, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory," Akuisisi dan Imagining menggunakan FTK Imager, 2016.
[12] R. Diansyah, "Instant Messaging," April 2011. [Online]. Available: http://besokmasihkuliah.blogspot.co.id/2011/04/instant-messaging.html.
[13] A. Chandra, Y. Kurniawan dan K.-H. Rhee, "Security Analysis Testing for Secure Instant Messaging in Android with Study Case: Telegram," 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.

Halaman ini sengaja dikosongkan