

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

**Tayomi Dwi Larasati dan Bekticahyo 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](mailto:tayomidwi@gmail.com)<sup>1)</sup>, [bekticahyo@is.its.ac.id](mailto:bekticahyo@is.its.ac.id)<sup>2)</sup>

---

## Abstrak

*Live forensics digunakan untuk mendapatkan bukti digital pada RAM. Teknik ini diperlukan dumping data untuk dianalisa. Penelitian ini dilakukan untuk aplikasi Instant Messenger populer 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 populer 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 tertipnya 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 berpotensi menjadi barang bukti. Live forensics pada dasarnya memiliki kesamaan pada teknik forensik tradisional dalam hal metode yang dipakai yaitu identifikasi, penyimpanan, analisis, dan presentasi, hanya saja live forensics merupakan respon dari kekurangan teknik forensik tradisional 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 dibandingkan 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:

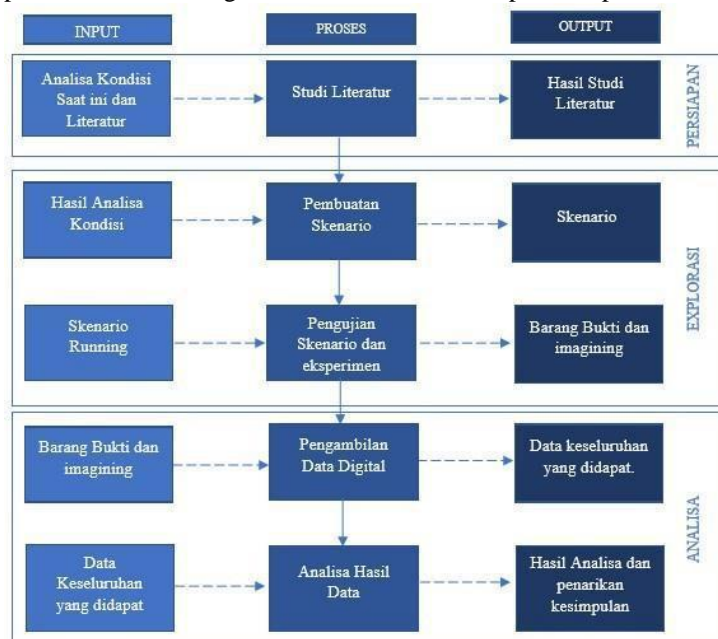
- Eksperimen 1: Aplikasi dijalankan dengan biasa. Pembicaraan meliputi percakapan antar pengguna dan pertukaran media (picture, video, dan audio).
- Eksperimen 2: Aplikasi dijalankan dengan biasa namun dengan adanya penghapusan beberapa pesan/percakapan melalui layanan aplikasi

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

```
11CF25C40 39 5F 34 4F 5F 42 45 5F 36 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 41 70 20 TO_USER U siap
11CF25C60 73 69 73 74 2C 20 64 69 74 75 6E 67 67 75 20 79 sirt, 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 69 20 73 75 64 61 68 20 kimakasih sudah
11CF25C90 62 65 72 62 65 6C 61 6E 4A 61 20 64 69 20 6F 6E berbelanja di om
11CF25CA0 6C 69 6E 65 20 73 68 6F 70 20 6B 61 6D 69 2E DA line shop kami.Ü
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*attache
11CF25CD0 6E 74 75 AC 01 24 5F 5F 46 42 5F 63 6C 61 73 73 nt- $ _FB_class
11CF25CE0 85 01 46 42 4D 4D 65 73 73 61 67 65 41 74 74 61 u FBMMessageActa
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 DA 00 03 B8 01 4E 53 41 72 pertiesÖ , NSAR
11CF25D10 72 61 79 2A 6A 73 6F 6E 41 74 74 61 63 68 6D 65 ray*jsonAttache
11CF25D20 6E 74 73 B6 01 4E 53 44 69 63 74 69 6F 6E 61 72 nce$ NSDictionar
11CF25D30 79 2A 73 68 61 72 65 4D 61 70 DA 00 34 01 46 42 y*shareMapÜ 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 enableAttache
11CF25D70 74 B8 01 4E 53 41 72 72 61 79 2A 6A 73 6F 6E 41 t, NSHrray*jsonA
11CF25D80 74 74 61 63 68 6D 65 6E 74 73 90 B6 01 4E 53 44 tchments* NSD
11CF25D90 69 63 74 69 6F 6E 61 72 79 2A 73 68 61 72 65 4D ictionary*shareM
```

Gambar 2 Hasil Winhex Text Facebook Messenger

##### B. Picture

```
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 B6 A3 01 49 64 B0 01 31 30 36 39 30 34 30 31 *id* 10690401
016528BD0 36 35 39 31 34 34 36 A5 01 46 62 69 64 B0 01 31 659144W fbid* 1
016528BE0 30 36 39 30 34 30 31 36 35 39 31 34 34 36 A9 01 0690401659144W
016528BF0 46 69 6C 45 6E 61 4D 65 B6 01 69 6D 61 47 65 2D filename$ image-
016528C00 31 30 36 39 30 34 30 31 36 35 39 31 34 34 36 AA 10690401659144W
016528C10 01 4D 69 6D 65 5F 74 79 70 65 A7 01 69 6D 61 67 mime_type$ imag
016528C20 45 2F A5 01 74 79 70 65 04 AB 01 69 6D 61 67 65 e/W type = image
016528C30 5F 64 41 74 61 84 B6 01 77 69 64 74 68 CD 01 C2 *data$: width$ Å
016528C40 A7 01 68 65 69 67 68 74 CD 03 20 A4 01 75 72 6C $ height$ = url
```

Gambar 3 Hasil Winhex Picture Facebook Messenger

##### D. Audio

```
001DA3CF0 69 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 B6 sonAttachments*
001DA3D10 A3 01 69 64 B0 01 31 30 36 39 30 39 32 30 39 39 id* 106902099
001DA3D20 32 34 32 36 30 A5 01 66 62 69 64 B0 01 31 30 36 24260W fbid* 106
001DA3D30 39 30 39 32 30 39 39 32 34 32 36 30 AA 01 66 69 909209924260* fi
001DA3D40 6C 65 5F 73 69 7A 65 CD 78 00 A9 01 66 69 6C 65 le_size$X © file
001DA3D50 6E 61 4D 65 DA 00 21 01 61 75 64 69 6F 63 6C 69 nameÜ ! audiccli
001DA3D60 70 2D 31 34 39 37 36 39 32 35 34 38 30 30 30 2D p-1497692548000-
001DA3D70 37 30 34 30 2E 6D 70 34 AA 01 6D 69 6D 65 5F 74 7040.mp4* mime_t
001DA3D80 79 70 65 A7 01 61 75 64 69 6F 2F A5 01 74 79 70 ype$ audio/W typ
001DA3D90 65 06 B6 01 4E 53 44 69 63 74 69 6F 6E 61 72 79 e$ NSDictionary
```

Gambar 5 Hasil Winhex Audio Facebook Messenger

##### C. Video

```
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 B8 A3 01 69 Attachments*f 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 93W fbid* 106923
0541975A0 35 34 36 35 38 39 34 39 33 AA 01 66 69 6C 65 5F 546589493* file
0541975B0 73 69 7A 65 CE 00 1C 29 8C A9 01 66 69 6C 65 6E size$ )GE filen
0541975C0 61 6D 65 B5 01 76 69 64 65 6F 2D 31 34 39 37 36 ameu video-14976
0541975D0 39 33 35 37 35 2E 6D 70 34 AA 01 6D 69 6D 65 5F 93573.mp4* mime_
0541975E0 74 79 70 65 A7 01 76 69 64 65 6F 2F A5 01 74 79 type$ video/W ty
0541975F0 70 65 05 AB 01 69 6D 61 67 65 5F 64 61 74 61 B2 pe = image, data,
054197600 A6 01 77 69 64 74 68 CD 01 E0 A7 01 68 65 69 67 width$ Å heig
```

Gambar 4 Hasil Winhex Video Facebook

##### E. Sticker

```
016781EF0 B8 01 4E 53 41 72 72 61 79 2A 6A 73 6F 6E 41 74 , NSArray*jsonAu
016781F00 74 61 63 68 6D 65 6E 74 73 B6 01 4E 53 44 69 63 tachment$ 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 Ü 4 FBMMessageEx
016781F30 74 65 6E 73 69 62 6C 65 41 74 74 61 63 68 6D 65 enableAttache
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 * share
016781F90 5F 6D 61 70 81 AB 01 73 74 69 63 68 65 72 5F 69 _map = sticker_i
```

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

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	"to":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	ku":"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	68	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	68	61	6D	69	2E	22	2C	22	hopping kami.",

Gambar 7 Hasil Winhex Text LINE Messenger

##### B. Picture

055B6A190	45	4E	54	5F	49	4E	4E	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	tegrity":{"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\\":"JFEG\\","a
055B6A1D0	6E	69	6D	61	74	65	64	5C	22	3A	66	61	6C	73	65	2C	imated":{"false,
055B6A1E0	5C	22	77	69	64	74	68	5C	22	3A	31	38	33	36	2C	5C	\\width":"1336\\
055B6A1F0	22	68	65	69	67	65	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 ("cate
055B6A240	72	79	22	3A	74	72	75	65	2C	22	66	69	6C	65	4E	61	zy":{"true,"file
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	", "patch":"C:\\U
055B6A280	65	72	73	5C	5C	68	61	72	72	6D	5C	5C	41	70	70	44	era\\\\hazrm\\AppD
055B6A290	61	74	61	5C	5C	4C	6F	63	61	6C	5C	4C	49	4E	45	45	ata\\Local\\LINE
055B6A2A0	5C	5C	43	61	63	68	65	5C	5C	74	6D	70	2F	66	36	34	\\Cache\\tmp\\264

Gambar 8 Hasil Winhex Picture LINE Messenger

##### C. Video

129D002F0	33	32	33	65	33	34	31	35	61	33	62	36	61	35	38	34	323e9415a3b6a584
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	64	C6	14	18	02	634913806 \\Z
129D00320	7B	22	44	55	52	41	54	49	4F	4E	22	3A	22	39	33	35	("DURATION":"935
129D00330	35	22	5C	22	4F	42	53	5F	50	4F	50	22	3A	22	62	22	5","OBS_PCP":"b
129D00340	2C	22	53	52	43	5F	53	56	43	5F	43	4F	44	45	22	3A	,"SRC_SVC_CODE":
129D00350	72	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("sendC
129D00380	6E	74	65	6E	74	22	3A	74	72	75	65	2C	22	74	68	75	ntent":true,"chu
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\\hazrm\\Ap
129D003C0	70	44	61	74	61	5C	5C	4C	6F	63	61	6C	2F	4C	49	4E	pdata\\Local\\LIN

Gambar 9 Hasil Winhex Video LINE Messenger

##### E. Sticker

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 \\ < e ("STR
062BB74D0	49	44	22	3A	22	34	32	38	22	2C	22	53	54	4B	50	4B	ID":"42g","STRE
062BB74E0	47	49	44	22	3A	22	31	22	2C	22	53	54	4B	54	59	54	GIP":"1","STREX
062BB74F0	22	3A	22	5B	53	74	69	63	68	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	IKVER":"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 11 Hasil Winhex Sticker LINE Messenger

#### 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, tunggu 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
id	id percakapan, jika percakapan bersifat unicast maka id percakapan sama dengan id dari lawan bicaranya.
chatId:"u89e12bb9f043843cf1138004dd023e57"	isi dari pesan yang dikirim
text:"Siap sist, tunggu 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
FBMessageAttachment* attachment\$ _FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMessageExtensibleAttachment* extensibleAttachmentNSArray *jsonAttachmentsNSDictionary* shareMap4	Deskripsi Ekstensi Attachment
FBMessageExtensibleAttachment *extensibleAttachmentNSArray *tagssource:chat:orcaapp_id:1637541026 485594	Deskripsi ekstensi Attachment dengan tagssource

##### C. Video

Tabel 8. Type Data Video Facebook Messenger

Type Object	Keterangan
FBMessageAttachment* attachment\$ _FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMessageExtensibleAttachment* extensibleAttachmentNSArray*jsonA ttachmentsid106923546589493fbid1 06923546589493file_size)	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
filenamevideo-1497693573.mp4	nama file video yang dikirim
mime_typevideo/typeimage_datawi dthheight	Deskripsi data mime type 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

##### E. Sticker

Tabel 9. Type Data Sticker Facebook Messenger

Type Object	Keterangan
FBMessageAttachment* attachment\$ _FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMessageExtensibleAttachment* extensibleAttachmentNSArray*jsonA ttachments	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
NSDictionary*shareMapshare_maps ticker_id144885035685763	identitas stiker yang dikirim
FBMessageExtensibleAttachment* extensibleAttachmentNSArray*tagss ource:chat:orcaapp_id:25600234774 3983	Deskripsi ekstensi Attachment dengan tagssource

##### B. Picture

Tabel 6. Type Data Picture Facebook Messenger

Type Object	Keterangan
FBMessageAttachment* attachment\$ _FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMessageExtensibleAttachment *extensibleAttachmentNSArray *jsonAttachmentsid1069040165914 46fbid106904016591446	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
filenameimage-106904016591446	Nama file gambar yang dikirim
mime_typeimage/typeimage_datawi dthheight	Deskripsi data mime type image
urlhttps://scontent.xx.fbcdn.net/v/ t34.0-12/ 19251246_106904016591446_ 1240998779_n.jpg? oh=086f8004d88b69359a3c80c27 b093d7d&oe=594745DB	url file gambar yang dikirim
preview_urlhttps://scontent.xx. fbcdn.net /v/t34.00/s480x480/19251246_ 106904016591446_ 1240998779_n.jpg? oh=9df2fda172c7ce7fc8e5f7a61f3be 3f1&oe=59471518	url file thumbnail gambar yang dikirim

##### D. Audio

Tabel 7. Type Data Audio Facebook Messenger

Type Object	Keterangan
FBMessageAttachment* attachment\$ _FB_class	Deskripsi Kelas Fb Berupa Attachment
FBMessageAttachmentsaved PropertiesNSArray*jsonAttachments NSDictionary*shareMap4	Deskripsi Attachment Properties
FBMessageExtensibleAttachment* extensibleAttachmentNSArray*jsonA ttachments	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
NSArray*jsonAttachmentsid1069092 09924260fbid106909209924260	Deskripsi Ekstensi Attachment dengan id attachment dan id fb
file_sizefilename!audioclip- 1497692548000-7040.mp4	nama file audio yang dikirim
mime_typeaudio/typeNSDictionary* shareMap4	Deskripsi data mime type audio
FBMessageExtensibleAttachment* extensibleAttachmentNSArray*tagss ource:chat:orcaapp_id:25600234774 3983	Deskripsi ekstensi Attachment dengan tagssource



### 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:{},	Metadana 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:"u89e12bb9f043843cf1138004dd023e57",	id percakapan, jika percakapan bersifat unicast maka id

#### C. Video

Tabel 10. Type Data Video LINE Messenger

Type Object	Keterangan
u89e12bb9f043843cf1138004dd023e57	identitas pengirim pesan
u85ca323e3415a3b6a584cbfde28442e6	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/4/504fa8efa3f97947a18fb3c2a16224439abeb1e"}	lokasi gambar thumbnail
u89e12bb9f043843cf1138004dd023e57	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:

#### B. Picture

Tabel 11. Type Data Picture LINE Messenger

Type Object	Keterangan
u89e12bb9f043843cf1138004dd023e57	identitas pengirim pesan
u85ca323e3415a3b6a584cbfde28442e6	identitas penerima pesan
6251971991394	identitas pesan
89e12bb9f043843cf1138004dd023e57	identitas percakapan
{"sendContent":true,	informasi pengiriman konten
thumbPath:"C:\\Users\\harrm\\AppData\\Local\\LINE\\Cache\\m/8/f194ff32c2e09701b676c8aaab8518f41aac2a",	lokasi file thumbnail
thumbResCode:200}	ukuran gambar thumbnail

#### D. Audio

Tabel 11. Type Data Audio LINE Messenger

Type Object	Keterangan
u89e12bb9f043843cf1138004dd023e57	identitas pengirim pesan
u85ca323e3415a3b6a584cbfde28442e6	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
u89e12bb9f043843cf1138004dd023e57	identitas percakapan

#### E. Sticker

Tabel 12. Type Data Sticker LINE Messenger

Type 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
STKTX:"[Sticker]",	teks dari stiker yang dikirim
STKVER:"100"}	versi dari stiker yang dikirim
u89e12bb9f043843cf1138004dd023e57	identitas percakapan

### 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 dijalankan dengan nama file Screenshot\_2017-06-16-15-37-53.jpg.



Gambar 12 Media Picture Facebook Messenger



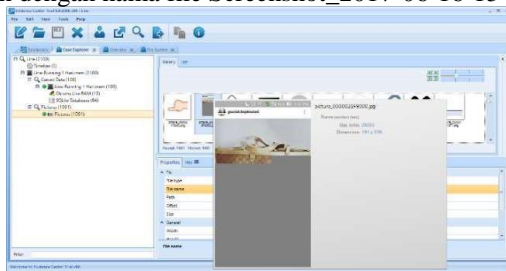
Gambar 13 Media Picture Skenario Facebook Messenger

### 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 dijalankan dengan nama file Screenshot\_2017-06-16-15-37-53.jpg



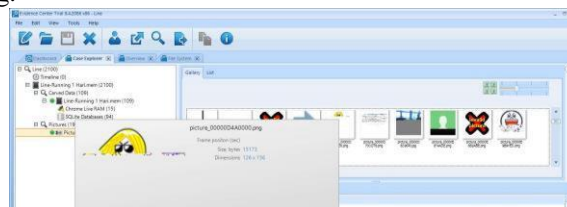
Gambar 14 Media Picture LINE Messenger



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 perbandingan 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	
<b>Bobot Persentase</b>	12	12	12	12	12	10	10	10	10	
<b>Winhex</b>										
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%
<b>Belkasoft</b>										
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

Object	WinHex			Belkasoft		
	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

Object	WinHex			Belkasoft		
	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

Object	WinHex			Belkasoft		
	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 artefak pada 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 penelitian 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] Available:[https://id.wikipedia.org/wiki/Memori\\_akses\\_acak](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*