

**Laporan Tugas Media Sosial Forensik
IF-42-GAB**



Disusun Oleh Kelompok 3:

1301180379	Adabi Raihan Muhammad
1301198497	Muhammad Faisal Amir
1301174524	Muhammad Irfan Aldi
1301184219	Sya Raihan Heggi
1301184005	Gia Nusantara

**S1 INFORMATIKA
FAKULTAS INFORMATIKA
UNIVERSITAS TELKOM
BANDUNG
2021**

Daftar Isi

Daftar Isi	2
BAB 1	4
Pendahuluan	4
1.1 Aplikasi dan Framework	4
1.2 Metode Akuisisi.....	6
1.2.1 Metode Akuisisi dengan API	6
1.2.1.1 Metode yang dilakukan	6
1.2.1.2 Tantangan dalam menggunakan metode.	9
1.2.1.3 Integritas dari data yang diakuisisi	9
1.2.1.4 Analisis Manfaat dari data yang diakuisisi.....	9
1.2.2 Metode Akuisisi Manual	10
1.2.2.1 Metode yang dilakukan	10
1.2.2.2 Tantangan yang dihadapi.....	11
1.2.2.3 Integritas data	12
1.2.2.4 Analisis manfaat data yang didapatkan	12
1.3 Latar Belakang.....	13
BAB 2	14
ANALISIS TERHADAP DATA	14
2.1 Penjelasan Skenario.....	14
2.2 Tahapan Kegiatan	16
2.2.1 Preservation.....	16
2.2.2 Collection dan Examination	17
Versi Telegram Desktop dan keterangan tambahan	18
2.2.2.1 Cara Mengambil Data Chat	19
2.2.2.2 Cara Mengambil Data Login	21
2.2.2.3 Cara mengambil data yang dihapus.....	22
2.2.2.4 Cara Mengambil Data Cache.....	23
2.2.2.5 Cara mengambil data file.....	23
2.2.2.5 Hasil Pengambilan Data	24
2.2.3 Data Analysis	30

2.2.4 Reporting dan Verifikasi Hash Setelah Analisis	41
BAB 3	46
KESIMPULAN	46

BAB 1

Pendahuluan

1.1 Aplikasi dan Framework

Aplikasi yang diamati adalah Telegram, Telegram merupakan salah satu platform yang didirikan oleh Pavel Durov yang memungkinkan penggunanya untuk melakukan komunikasi baik itu berbagi foto, video, percakapan, maupun perangkat lainnya seperti Stiker dan Files

Telegram sendiri dapat diakses dari tiga jenis akses yaitu Website, Desktop, dan Mobile (iOS, Android, dan Windows Phone) untuk ketiga hal ini memiliki cara penyimpanan yang berbeda, namun telegram sendiri memiliki keuntungan yaitu datanya disimpan di cloud sehingga dapat diakses menggunakan API untuk melakukan akuisisi datanya.

untuk penyimpanan sendiri pada Telegram Android akan memiliki struktur seperti berikut ini.

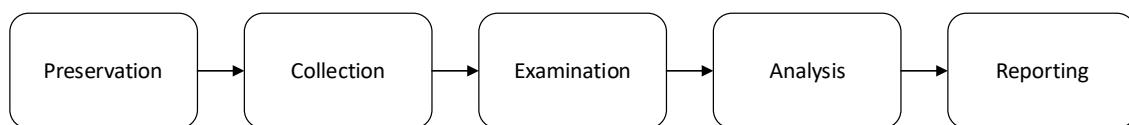
Jenis Data	Lokasi Penyimpanan
APK File (dex/java files)	/data/app
Telegram Files (Audio, Documents, Images, Video)	/sdcard/Telegram atau /internal-memory/Telegram
Cache Database (cache4.db) User Activities, Contact Information, Messages Exchange, Sharing Location/File. Delete Chat	/data/data/.org.telegram.messenger

Sementara itu pada Telegram Desktop yang dijalankan pada Windows 10 akan memiliki struktur penyimpanan seperti berikut ini.

Jenis Data	Lokasi Penyimpanan
Application Data	C:\Users\user\AppData\Roaming\Telegram Desktop
Telegram Files (Audio, Documents, Images, Video)	C:\Users\user\Downloads\Telegram Desktop
Telegram.exe files	C:\Users\user\AppData\Roaming\Telegram

	Desktop\Telegram.exe
Log data	C:\Users\user\AppData\Roaming\Telegram Desktop\Log.txt
Cache	C:\Users\user\AppData\Roaming\Telegram Desktop\tdata\user_data\cache

Untuk framework yang digunakan untuk pengerjaan dapat menggunakan kerangka model NIJ (*National Institute Of Justice*) di mana pada proses menggunakan framework ini akan menggunakan beberapa tahapan yaitu *Preservation*, *Collection*, *Examination*, *Analysis*, dan *Reporting*.



- **Preservation** merupakan tahap melakukan analisis mengenai aplikasi yang dilakukan.
- **Collection** merupakan tahap mengumpulkan data dari sumber yang terkait namun tetap menjaga integritas data tersebut.
- **Examination** merupakan tahap pemrosesan data yang dikumpulkan untuk dilakukan ke proses selanjutnya.
- **Analysis** merupakan tahap melakukan analisis sesuai dengan teknik dan hukum yang dibenarkan untuk mendapatkan informasi dan menjawab pertanyaan-pertanyaan.
- **Reporting** merupakan hasil laporan analisis meliputi penjelasan tindakan yang dilakukan sehingga dapat mengidentifikasi data yang dijadikan barang bukti pada skenario yang dilakukan.

untuk tahapan NIJ Framework yang digunakan pada uji coba kami dilakukan seperti berikut ini.

Tahapan	Proses Dilakukan
Preservation	Pada tahapan ini dilakukan analisis mengenai apa aplikasi yang digunakan, dimana saja penyimpanannya, dan metode akuisisi apa yang dapat dilakukan.
Collection	Pada tahapan ini dilakukan pengambilan dari public group Telegram dengan menggunakan beberapa cara seperti crawling dengan Telethon, export dari Telegram, dan terakhir mengamankan file-file yang ada di barang bukti komputer laptop (data-login, data-deleted, data-cache)

Examination	Melakukan pemisahan terlebih dahulu dengan membuat image-image dari setiap file yang sudah dikumpulkan agar analisis tidak terjadi proses write, untuk proses ini membutuhkan FTK Manager, dan beberapa tools lainnya yang terintegrasi agar dapat membuka filenya.
Analysis	Membuat analisis dari setiap proses yang dilakukan dan tahapan-tahapan yang dilakukan hingga hasil yang didapatkan.
Reporting	Membuat laporan dan menuliskan bukti bahwa barang bukti benar dan sah serta dapat digunakan untuk digunakan pada perkara hukum.

1.2 Metode Akuisisi

untuk melakukan akuisisi data pada Telegram Desktop terdapat dua metode yang dapat digunakan yaitu menggunakan API (Python, TaaS, dan Export Telegram) dan kemudian menggunakan metode *live forensics* (memdump, cache file Telegram Desktop), untuk lebih jelasnya ada pada pembahasan berikutnya.

1.2.1 Metode Akuisisi dengan API

1.2.1.1 Metode yang dilakukan

Untuk melakukan akuisisi menggunakan api dengan tahapan berikut ini.

1. Membuat Application di my.telegram.org
2. Kemudian simpan API_ID dan API_HASH yang anda miliki
3. Kemudian buat script menggunakan Python dengan library Telethon sehingga dapat dilakukan pengambilan metadata.

```

chat = <isi dengan id_chat>
api_id = <masukan API_ID>
api_hash = <masukan API_HASH>

from telethon.sync import TelegramClient
import pandas as pd

client=TelegramClient("session_id",api_id,
api_hash)

message = list()
with client:
    for msg in client.iter_messages(chat, 200):
        message.append(msg)

df = pd.DataFrame(message)
writer=pd.ExcelWriter("tele_data.xlsx",engine="

```

```

xlsxwriter")
df.to_excel(writer, sheet_name="data",
index=False)
writer.save()

```

4. Selanjutnya lakukan running code tersebut dan akan dihasilkan 2 buah file yaitu session dan file.xlsx data message yang terjadi di telegram.

Tables (5)

- entities
 - id: integer, CREATE TABLE entities (id integer primary key, hash integer not null, username text, phone integer, name text, date integer)
 - hash: integer, "hash" integer NOT NULL
 - username: text, "username" text
 - phone: integer, "phone" integer
 - name: text, "name" text
 - date: integer, "date" integer
- sent_files
 - md5_digest: blob, CREATE TABLE sent_files (md5_digest blob, file_size integer, type integer, id integer, hash integer, primary key(md5_digest, file_size, type))
 - file_size: integer, "file_size" integer
 - type: integer, "type" integer
 - id: integer, "id" integer
 - hash: integer, "hash" integer
- sessions
 - dc_id: integer, CREATE TABLE sessions (dc_id integer primary key, server_address text, port integer, auth_key blob, takeout_id integer)
 - server_address: text, "server_address" text
 - port: integer, "port" integer
 - auth_key: blob, "auth_key" blob
 - takeout_id: integer, "takeout_id" integer
- update_state
 - id: integer, CREATE TABLE update_state (id integer primary key, pts integer, qts integer, date integer, seq integer)
 - pts: integer, "pts" integer
 - qts: integer, "qts" integer
 - date: integer, "date" integer
 - seq: integer, "seq" integer
- version
 - version: integer, CREATE TABLE version (version integer primary key)
 - version: integer, "version" integer

Indices (0)
Views (0)
Triggers (0)

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: entities

	id	hash	username	phone	name	date
	Filter	Filter	Filter	Filter	Filter	Filter
1	-579189726	0	NULL	NULL	Bully-ers	1633440398
2	211246197	-770270870545169	rawdatabot	NULL	Telegram Bot Raw	1633440398
3	320967145	3390261759760785342	faisalamircs	NULL	Faisal Amir	1633440398
4	738888501	3071483658003699136	irfanaldii	NULL	irfan aldi	1633440398
5	784590528	-6006528188258352336	heggi_raihan	6281284549958	Sya Raihan Heggi	1633440398
6	1206830175	-7692370183596969562	NULL	NULL	Adabi	1633440398

Kemudian untuk data yang di didapatkan akan berbentuk seperti berikut ini.

```

Message(id=190,
peer_id=PeerChannel(channel_id=1600752976),
date=datetime.datetime(2021, 10, 16, 8, 32, 39,
tzinfo=datetime.timezone.utc), message='siap
siap', out=True, mentioned=False,
media_unread=False, silent=False, post=False,
from_scheduled=False, legacy=False,

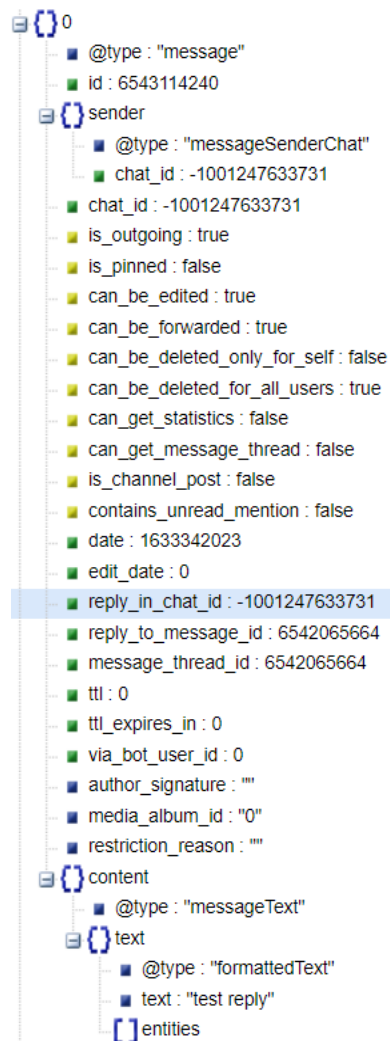
```

```

edit_hide=False, pinned=False,
from_id=PeerUser(user_id=784590528),
fwd_from=None, via_bot_id=None, reply_to=None,
media=None, reply_markup=None, entities=[],
views=None, forwards=None,
replies=MessageReplies(replies=0, replies_pts=194,
comments=False, recent_repliers=[],
channel_id=None, max_id=None, read_max_id=None),
edit_date=None, post_author=None, grouped_id=None,
restriction_reason=[], ttl_period=None))

```

Selain menggunakan script python kita dapat menggunakan aplikasi seperti TaaS yang dapat mendapatkan JSON filenya yang berformat kurang lebih seperti berikut ini.



Sehingga metadata yang didapatkan adalah chat_id, message_id, date, typenya dan textnya dan beberapa keterangan apakah sudah direply atau bukan dan penggunaan data lainnya

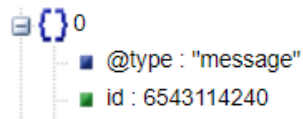
1.2.1.2 Tantangan dalam menggunakan metode.

Tantangan yang dihadapi jika menggunakan metode ini adalah untuk menemukan chat_id dari grup yang ditemukan, kemudian bagaimana menjaga integritas dan keutuhan data, dan terakhir pesan yang sudah dihapus tidak dapat ditemukan jika menggunakan API.

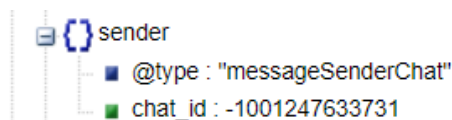
1.2.1.3 Integritas dari data yang diakuisisi

Untuk menjaga integritas dari data yang diakuisisi sebisa mungkin dilakukan isolasi dari data yang diambil dikarenakan sangat dimungkinkan untuk dilakukan perubahan karena hasilnya disimpan dalam program yang memiliki sifat *write data*, oleh karena itu dilakukan pembuatan image adl untuk analisis dan dibuktikan kembali dengan hash dari data.

1.2.1.4 Analisis Manfaat dari data yang diakuisisi



Dari data yang diakuisisi dapat diketahui pesan yang dikirim apakah adalah message atau message dari sistem dengan melihat kolom @type yang berada di file jsonnya kemudian dapat dipastikan integritasnya dengan id dari pesan tersebut.



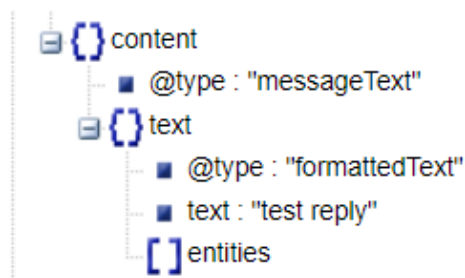
dan kemudian dapat diketahui siapa pengirimnya dari chat_idnya



dan dari data ini diketahui apakah pesan ini dikirimkan dari device dengan variabel *is_outgoing*, selanjutnya apakah ini pesan yang di pin di dalam grup

dengan variabel *is_pinned* kemudian apakah bisa di edit, forward dan di delete baik itu sendiri maupun keseluruhan dari variabel *can_be_edited*, *can_be_forwaded*, *can_be_deleted_only_for_self*, *can_be_deleted_for_all_users*, kemudian apakah data ini dapat dijadikan statistik, message thread dengan metadata *can_get_statistics*, *can_get_message* dan mengetahui apakah file ini merupakan postingan di channel dan apakah ada mention yang tidak di mention dengan metadata *is_channel_post* dan *contains_unread_mention* selanjutnya dapat diketahui dari metadata dapat diketahui atribut penanggalan yang digunakan.

date, *edit_date*, *reply_in_chat_id*, *reply_to_message_ud*, *message_thread_id*, *ttl*, *ttl_expires_id* yang menggambarkan waktu dari pesan ini, untuk *date* menggunakan timestamp UNIX saat pengiriman, kemudian *edit_date* untuk menampilkan kapan pesan diedit, selanjutnya ada metadata mengenai reply yang merujuk kepada *chat_id* dan *message_id* dan ttlnya hingga waktu ttl berakhir, selain itu ada beberapa metada berkenaan dengan signature, penggunaan album dan restriction.



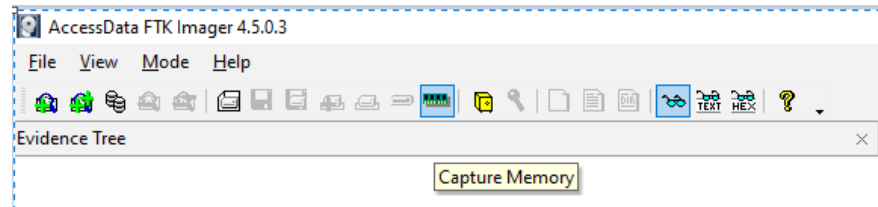
Selanjutnya dari data yang diakusisi dapat dilihat content yang dikandung apakah dokumen, text, stiker atau apapun itu dan didalamnya akan mengandung text apa, pada gambar ini terlihat text yang dikirim adalah “test reply”.

1.2.2 Metode Akuisisi Manual

untuk melakukan akuisisi data secara manual maka perlu dilakukan terlebih dahulu lokasi penyimpanan file-file yang digunakan oleh sistem.

1.2.2.1 Metode yang dilakukan

Metode akuisisi manual ini akan melakukan secara manual mengamankan tempat-tempat penyimpanan yang dapat dilihat pada pembahasan awal sehingga akan mengamankan (Lokasi Penyimpanan File, Telegram Data, Telegram Cache), beberapa teknik yang dapat digunakan yaitu dapat melakukan *dead forensics* yaitu dengan membuat image dari lokasi penyimpanan setelah aplikasi dimatikan atau dapat menggunakan metode *live forensics* dimana dengan melakukan capture data dan informasi yang berada pada RAM, untuk melakukan perekaman tersebut dapat menggunakan fitur yang ada pada FTK imager.



Kemudian dilakukan dengan cara *dead forensics* terlebih dahulu dengan melakukan penyimpanan dari cache, user_data, dan telegram file yang ada pada folder yang sudah diamati.

```

[Created By AccessData® FTK® Imager 4.5.0.3]

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 001
Evidence Number: 001
Unique Description: Telegram Application File
Examiner: Sya Raihan Heggil
Notes: Cache and User Data File

-----
Information for C:\Users\user\Desktop\Shorcut Aplikasi\Forensik Digital\Cases 01\Image\001-2021-Cyberbullying.ad1:
[Files Unable to be Added]
tdata\working
[Files With Read Errors (unreadable chunks replaced with 0s)]
tdata\user_data\cache\0\binlog
tdata\user_data\media_cache\0\binlog
[Computed Hashes]
MD5 checksum: 2d1ec7e5e02ae0b627bec7b08ad2614
SHA1 checksum: 00dacc7798687ebe2114616a667097f918d1edcd

Image Information:
Acquisition started: Wed Oct 6 23:41:09 2021
Acquisition finished: Wed Oct 6 23:41:50 2021
Segment list:
C:\Users\user\Desktop\Shorcut Aplikasi\Forensik Digital\Cases 01\Image\001-2021-Cyberbullying.ad1

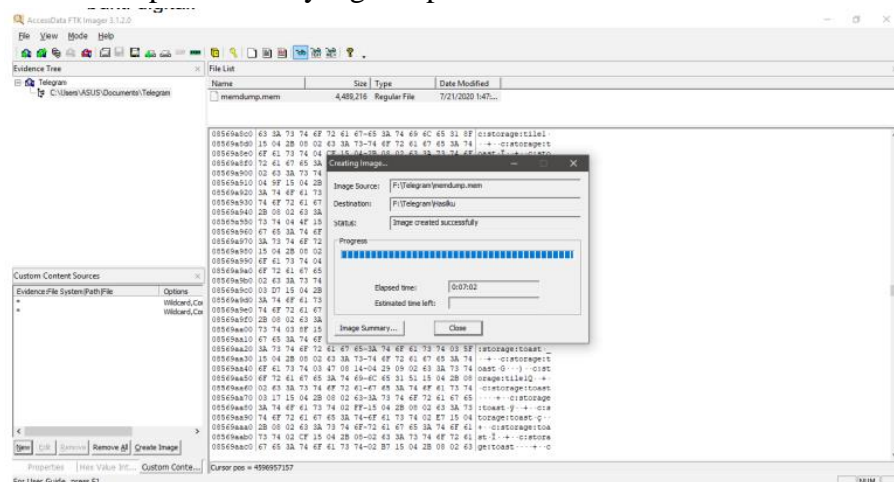
----- Errors during AD1 creation -----
AD Exception: The process cannot access the file because it is being used by another process. (32). Filename = "C:\Users\user\AppData\Roaming\Telegram Desktop\tdata\working"

Image Verification Results:
Verification started: Wed Oct 6 23:41:50 2021
Verification finished: Wed Oct 6 23:41:53 2021
MD5 checksum: 2d1ec7e5e02ae0b627bec7b08ad2614 : verified
SHA1 checksum: 00dacc7798687ebe2114616a667097f918d1edcd : verified

```

Setelah dilakukan imaging maka dapat dilakukan analisis data.

kemudian jika menggunakan metode *live forensics* yang dilakukan pertama kali adalah untuk mendapatkan data yang ada pada RAM.



1.2.2.2 Tantangan yang dihadapi

Untuk menggunakan metode ini jika menggunakan *dead forensics* ada kemungkinan untuk mendapatkan data lebih banyak, namun masih dikhawatirkan proses pengambilan akan mengganggu integritas dari datanya.

Selain itu jika menggunakan metode ini analisis yang dilakukan sedikit susah karena metadata yang didapat tidak tersusun rapi seperti baris data pada database karena data yang didapatkan hanya dari cache atau memdump sehingga perlu dilakukan analisis dengan perlahan.

0865172400	72 00 5F 00 64 00 61 00-74 00 61 00 5C 00 63 00	r--d-a-t-a-\c-
0865172416	61 00 63 00 68 00 65 00-5C 00 30 00 5C 00 43 00	a-c-h-e-\0-\c-
0865172432	31 00 5C 00 36 00 44 00-41 00 42 00 32 00 46 00	1-\-e-D-A-B-2-F-
0865172448	41 00 46 00 38 00 42 00-35 00 31 00 00 00 00 00	A-F-8-B-5-1-....
0865172464	65 DE 66 C7 A7 07 00 80-01 00 00 00 51 00 00 00	ePfCS-....Q-..
0865172480	52 00 00 00 10 00 00 00-4D 00 61 00 73 00 61 00	R-....M-a-s-a-
0865172496	20 00 75 00 64 00 61 00-68 00 20 00 64 00 69 00	-u-d-a-h- d-i-
0865172512	20 00 68 00 61 00 70 00-75 00 73 00 20 00 73 00	-h-a-p-u-s- s-
0865172528	65 00 20 00 67 00 61 00-6E 00 3F 00 20 00 49 00	l- g-a-n-? I-
0865172544	6E 00 69 00 20 00 75 00-64 00 61 00 68 00 20 00	n-i- u-d-a-h-
0865172560	73 00 65 00 4D 00 69 00-6E 00 67 00 67 00 75 00	s-e-m-i-n-g-u-
0865172576	20 00 6C 00 6F 00 68 00-2E 00 20 00 41 00 74 00	-l-o-h-.. A-t-
0865172592	61 00 75 00 20 00 6A 00-61 00 6E 00 67 00 61 00	a-u- j-a-n-g-a-
0865172608	6E 00 32 00 20 00 6B 00-61 00 6D 00 75 00 20 00	a-2- k-a-m-u-
0865172624	6E 00 69 00 70 00 75 00-20 00 73 00 61 00 79 00	n-i-p-u- s-a-y-
0865172640	61 00 20 00 79 00 61 00-3F 00 00 00 00 00 00 00	s- y-a-?
0865172656	8D DE 0E C7 0C 08 00 80-A8 5C 75 02 44 F7 D9 08	-b-C-....\u-D-b-
0865172672	00 00 00 00 C4 64 71 02-34 00 65 00 00 00 00 00Adq-4-e-...
0865172688	00 00 00 00 00 00 00 00-F8 07 D3 07 00 00 00 00e-D-....
0865172704	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0865172720	00 00 00 00 00 00 00 00-00 00 00 00 38 63 71 02Seq-
0865172736	38 63 71 02 A8 51 1E 0D-00 00 00 00 B8 51 1E 0D	Seq-Q-....,Q--
0865172752	00 00 00 00 00 00 00 00-F4 62 00 00 00 00 00 00db-....
0865172768	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0865172784	00 40 00 00 00 40 00 00-00 00 00 00 00 00 00 00	-B-..-B-.....
0865172800	00 00 63 00 02 00 00 00-00 00 00 00 5C 00 46 00	-c-.....\-F-
0865172816	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0865172832	00 00 38 00 37 00 35 00-F8 67 FF 10 00 00 E1 FF	-8-7-5-eggy-...4y
0865172848	B5 DE 16 C7 BB 09 00 80-10 E6 60 11 70 E6 60 11	uB-C-....-pe-
0865172864	D0 E6 60 11 30 E7 60 11-90 E7 60 11 F0 E7 60 11	B-e-0g-...-g-..-6g-
0865172880	50 E8 60 11 B0 E8 60 11-10 E9 60 11 70 E9 60 11	B-e-.*e-...-pe-
0865172896	D0 E9 60 11 30 EA 60 11-90 EA 60 11 F0 EA 60 11	B-e-0e-...-e-..-8e-
0865172912	50 EB 60 11 B0 EB 60 11-10 EC 60 11 70 EC 60 11	B-e-.*e-...-i-..-pi-

Sel start = 865172487, len = 163; clus = 7250712; log sec = 58005702

dan kemungkinan yang tercatat hanya yang dikirimkan dari perangkat yang disita, selain itu juga tidak ditemukan nomor telepon, pengirim, penerima, dan waktu percakapan namun memiliki kelebihan dapat melihat pesan-pesan yang sudah dihapus.

namun jika kita melakukan penyimpanan data dari database seperti melakukan export nilai terlebih dahulu maka akan mengalami permasalahan integritas dikarenakan tipe data yang didapatkan adalah json sehingga nilai hash dari setiap chat tidak diketahui namun masih ada chat_id, dan user_id.

1.2.2.3 Integritas data

Untuk integritas data dengan menggunakan metode ini, lebih terjamin karena proses yang dilakukan dapat dibuktikan dengan nilai hash dan file imagenya.

1.2.2.4 Analisis manfaat data yang didapatkan

Untuk menggunakan metode ini kurang lebih sama seperti dengan metode sebelumnya, kemudian kelebihan yang didapat adalah bisa didapatkan pesan yang sudah dihapus atau yang terkirim dari perangkat yang dikirim oleh perangkat yang disita, namun data ini yang didapatkan harus melalui perangkat yang disita karena semua file yang dijelaskan tersebut berada pada perangkat yang ada .

1.3 Latar Belakang

Kegiatan yang dilakukan memiliki latar belakang untuk membuktikan bahwa benar telah terjadi kegiatan Cyberbullying pada public group yang berada di Telegram Desktop, selain membuktikan akan dilakukan analisis bagaimana mendapatkan data dan juga menganalisis hingga didapatkan kesimpulan.

Seperti yang kita ketahui dengan berkembangnya teknologi saat ini maka berkembang juga metode kejahatan baru, *Cyber bullying* merupakan salah satu fenomena yang terjadi karena perkembangan teknologi internet. Pada kenyataannya terdapat banyak kasus baik di luar negeri maupun di Indonesia yang menyangkut tentang *cyber bullying*. *Cyber bullying* ini dapat dikatakan sebagai bentuk perluasan dari kejahatan *bullying*. *Cyber bullying* ini telah banyak terjadi di Indonesia terutama bagi anak-anak dan remaja, sebagaimana yang diketahui dengan melihat pembahasan di atas, masih banyak anak-anak yang belum mengerti peruntukan internet terutama media sosial, namun sudah banyak yang menggunakannya tentunya dengan pengetahuan yang masih terbatas, sehingga berpotensi menimbulkan *cyber bullying*.

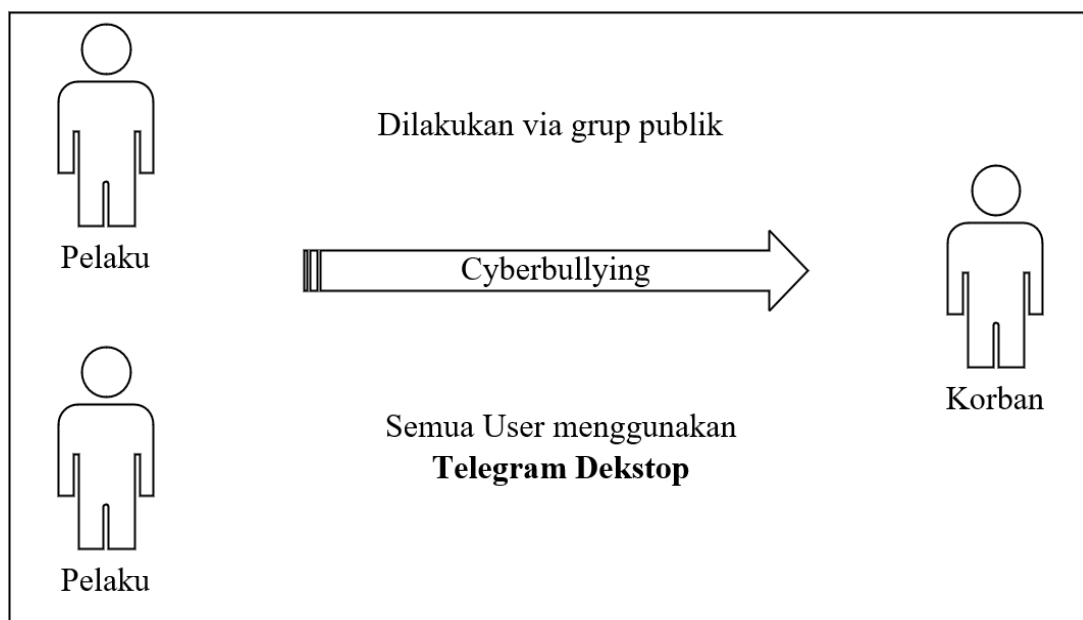
Dalam hukum Indonesia peraturan perundang-undangan yang mengatur mengenai *cyber bullying* adalah **Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)**. Sebelum adanya UU ITE, peraturan yang sering digunakan adalah **Pasal 310 ayat (1) dan (2) Kitab Undang-Undang Hukum Pidana terkait penghinaan dan pencemaran nama baik**. Namun menurut **Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008**, penghinaan dan pencemaran nama baik yang diatur di dalam **Pasal 310 ayat (1) dan (2) KUHP** tersebut **tidak dapat digunakan untuk perbuatan *cyber bullying***. Pada tahun 2016, diterbitkan peraturan baru terkait dengan ITE, **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik**.

BAB 2

ANALISIS TERHADAP DATA

2.1 Penjelasan Skenario

Untuk skenario pada pengujian ini akan topik kasus **Cyberbullying** yang dilakukan oleh sekelompok orang yang terdiri dari 5 orang dengan rincian 1 orang korban, 2 orang pelaku, dan 2 orang lagi orang awam dan pada proses ini akan dibuktikan siapa saja yang menjadi pelaku dalam kegiatan ini, kegiatan ini dilakukan dalam sebuah **public group** untuk lebih jelasnya dapat dilihat pada gambar berikut ini..

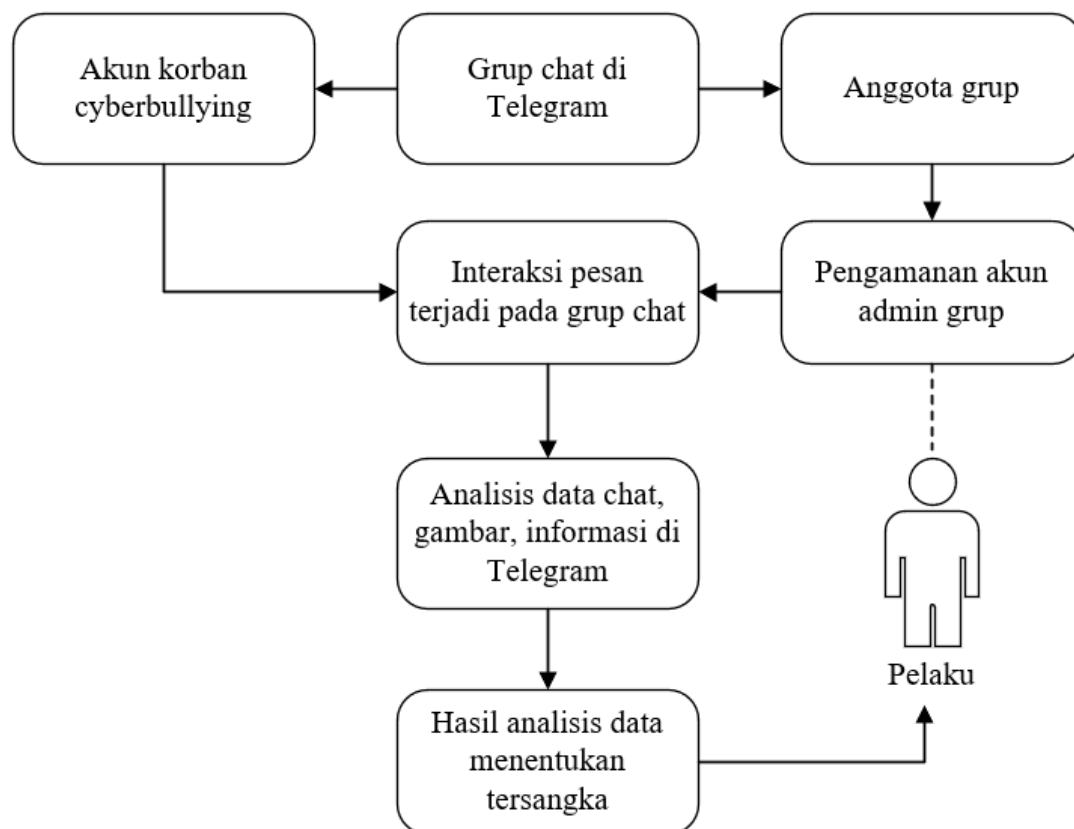


Untuk penjelasan lebih lengkap mengenai skenario yang akan dilakukan dapat dilihat pada tabel berikut ini .

Tahap 1	Pada sebuah grup telegram terdapat lima anggota yang berpartisipasi dalam grup. Satu dari 5 anggota merupakan korban. 2 di antara 4 lainnya merupakan tersangka sebagai pelaku yang melakukan cyber bullying. Pada kasus ini diharapkan penyelidik dapat mengetahui 2 di antara 4 orang yang merupakan pelaku cyberbullying.
Tahap 2	Penyelidik melakukan analisa terhadap grup telegram mengenai laporan Yang dilaporkan oleh korban yang merupakan satu dari 5 orang anggota grup telegram tersebut. Untuk mengetahui 2 pelaku di antara 4 anggota lainnya penyidik melakukan penyelidikan terhadap bukti chatting maupun informasi yang berada pada grup telegram tersebut.
Tahap 3	Penyelidik melakukan akuisisi data terhadap informasi ataupun data yang

	terdapat pada grup Telegram. Penyelidik juga melakukan pengamatan terhadap data-data yang sudah didapatkan dan melakukan sinkronisasi terhadap laporan yang diterima oleh korban atau pelapor.
Tahap 4	Menentukan siapa yang merupakan tersangka cyberbullying di antara 2 dari 4 anggota yang tercatat di grup telegram tersebut.

Atau kurang lebih bila digambarkan tahapan-tahapan tersebut menjadi diagram kurang-lebih skenario akan menjadi seperti berikut ini.



Karena percobaan ini merupakan sebuah percobaan yang terkontrol dalam hal ini percobaan yang sudah direncanakan dan tidak melebar hasilnya maka skenario akan mengirimkan pesan dan file kurang lebih seperti pada rincian di bawah ini.

Jenis Data	Jumlah Data
.png	2
.ipynb	1

.pdf	3
.xlsx	1
shared link	1
percakapan	191

2.2 Tahapan Kegiatan

Seperti yang kita ketahui bahwa pada tugas ini menggunakan acuan kerangka NIJ dalam melakukan kegiatan forensik maka akan dilakukan empat tahapan *preservation, collection, examination, analysis, reporting*, metode yang digunakan adalah melakukan akuisisi data melalui API terlebih dahulu kemudian jika tidak digunakan maka akan dilakukan *live forensics* sederhana seperti melihat memdump untuk membuktikan hal ini.

Oleh karena itu pada tugas ini diamankan sebuah akun yang merupakan admin dari grup tersebut dan memiliki akses terhadap api telegram, seperti yang sudah dijelaskan sebelumnya, selain mengamankan akun pihak berwajib juga mengamankan sebuah perangkat komunikasi yaitu satu buah laptop yang digunakan oleh terduga.

2.2.1 Preservation

Pada tahapan ini seperti yang sudah dijelaskan pada Bab 1 untuk aplikasi Telegram Desktop ini sendiri memiliki beberapa tempat penyimpanan yang dapat diamankan diantaranya lain adalah tempat file yang terunduh oleh sistem, data cache, file log, file *core system* dan untuk metode akuisisi yang dapat dilakukan adalah memanfaatkan fitur ekspor catatan percakapan dari Telegram namun membutuhkan akses akun sehingga perlu dilakukan penyimpanan terhadap satu akun dengan data seperti berikut ini.

No Telepon	Nama Akun	Kode Masuk
+628128454xxxx	Sya Raihan Heggi	79946

Selain itu dapat juga menggunakan API yang perlu dibuat dan diakses menggunakan bot atau akun yang berada pada suatu grup, selain dengan menggunakan metode ini dapat melakukan akuisisi secara manual yang akan dijelaskan tahapannya pada pembahasan tahap Collection, selain mengetahui metode yang digunakan maka pada tahapan ini juga akan dilakukan metode pencarian dimana untuk membuktikan dari scenario yang ada adalah mengecek *mention* terhadap akun korban dan kalimat yang dituliskan oleh pelaku, selanjutnya penelitian akan menggunakan peralatan seperti kode python (untuk melakukan crawling data dari API), telegram desktop (bahan analisis dan fungsi ekspor), FTK Imager (membuat image agar tidak ada proses write terjadi), dan terakhir adalah HashMyFiles/CMD command (untuk membuat nilai hash dari barang bukti yang

dihimpun pada tahapan Collection dan Juga melakukan verifikasi Kembali ketika membuat reporting).

2.2.2 Collection dan Examination

Pada tahapan ini dilakukan pengambilan semua data yang dapat diselamatkan dari barang bukti yang disita, data-data ini dapat berupa sebuah *cache*, *data percakapan*, *data percakapan yang hilang*, *data memori*, dan *data file-file yang dikirimkan* dan kemudian data-data tersebut disimpan menjadi image-image yang siap dilakukan tahapan berikutnya.

Skenario kegiatan ini dilakukan dengan perangkat laptop dengan menggunakan aplikasi Telegram Desktop dan skenario dijalankan di dalam sebuah public group yang berada di dalam aplikasi Telegram, untuk spesifikasi perangkat yang digunakan adalah seperti berikut ini.

Spesifikasi	Detail
Nama Perangkat	Laptop HP ENVY 13-aq000x
Sistem Operasi	Windows 10
Firmware revision number	8310A80002C00
Hardware revision number	SK_hynix_BC501_HFM512GDJTNG
Microprocessor	Intel® Core™ i7 8565U (1.8 GHz base frequency, up to 4.6 GHz with Intel® Turbo Boost Technology, 8 MB cache, 4 cores)
Chipset	Intel® Integrated SoC
Memory Standard	16 GB DDR4-2400 SDRAM (onboard)
Hard drive	512 GB PCIe® NVMe™ M.2 SSD
Display	13.3" diagonal FHD IPS BrightView micro-edge WLED-backlit touch screen (1920 x 1080)
Wireless Connectivity	Intel® Wireless-AC 9560 802.11a/b/g/n/ac (2x2) Wi-Fi® and Bluetooth® 5 Combo
Expansion slot	1 microSD media card reader
External Port	1 USB 3.1 Gen 1 Type-C™ (5 Gb/s signaling rate, Power

	Delivery 3.0, DisplayPort™ 1.2, HP Sleep and Charge); 1 USB 3.1 Gen 1 Type-A (HP Sleep and Charge); 1 USB 3.1 Gen 1 Type-A (Data Transfer Only); 1 AC smart pin; 1 headphone/microphone combo
Webcam	HP Wide Vision HD Camera with integrated dual array digital microphone
Audio Features	B&O, quad speakers, HP Audio Boost, HP Far-field Cortana support

Kemudian untuk spesifikasi aplikasi Telegram Desktop seperti berikut ini .

- Nama Aplikasi : Telegram Desktop on Windows
- Version : v 3.1.8 (Launched version: **3001008**, install beta: [FALSE], alpha: 0, debug mode: [FALSE])

dan jika melihat log yang terdapat pada direktori penyimpanan dari Telegram Desktop maka didapat informasi seperti berikut ini

Versi Telegram Desktop dan keterangan tambahan
[2021.10.14 20:40:39] Launched version: 3001008, install beta: [FALSE], alpha: 0, debug mode: [FALSE]
Lokasi file .exe dari Telegram Desktop
[2021.10.14 20:40:39] Executable dir: C:/Users/user/AppData/Roaming/Telegram Desktop/, name: Telegram.exe
Lokasi initial working dir dari Telegram Desktop
[2021.10.14 20:40:39] Initial working dir: C:/Users/user/AppData/Roaming/Telegram Desktop/.
Lokasi working dir dari Telegram Desktop
[2021.10.14 20:40:39] Working dir: C:/Users/user/AppData/Roaming/Telegram Desktop/
Eksekusi Telegram Desktop
[2021.10.14 20:40:39] Command line: C:\Users\user\AppData\Roaming\Telegram Desktop\Telegram.exe
Lokasi .exe yang valid
[2021.10.14 20:40:39] Executable path before check:

C:/Users/user/AppData/Roaming/Telegram Desktop/Telegram.exe .
Socket yang digunakan [2021.10.14 20:40:39] Connecting local socket to Global\4fcd644764302e0e4eb0ad7a5595f0f5-{87A94AB0-E370-4cde-98D3-ACC110C5967D}....
Process ID dari aplikasi [2021.10.14 20:40:39] Show command response received, pid = 15252, activating and quitting

Kemudian tahapan dari *collection* kurang lebih akan seperti pada tabel dibawah ini yang menjelaskan tahapan dan bagaimana file tersebut disimpan..

Tahapan	Keterangan Tambahan
Akuisisi bukti Telegram	Untuk File Image Telegram disimpan dengan nama Data_Cache
Akuisisi bukti Login	Untuk File Image Telegram disimpan dengan nama Data_Login
Akuisisi bukti Aktivitas Cyberbullying	Untuk File Image Telegram disimpan dengan nama Data_Chat dan Data_Chat_Deleted
Akuisisi Data File yang dikirim	Untuk File Image Telegram disimpan dengan nama Data_Chat dan Data_Chat_Deleted

2.2.2.1 Cara Mengambil Data Chat

Untuk melakukan pengambilan data chat digunakan kode python yang menggunakan library telethon yang memang dikhususkan untuk melakukan pengambilan data melalui API Telegram atau dapat melakukan ekspor dari aplikasi Telegram.

Pertama akan dibahas menggunakan telethon untuk menggunakan telethon maka kurang lebih akan membutuhkan *channel_id/user_id* , *api_id*, *api_hash* untuk membuatnya dapat mengunjungi my.telegram.org dan tahapannya bisa seperti pada pembahasan pada bab 1 metode akuisisi data dengan API, setelah melengkapi kebutuhan tersebut maka cukup membuat coding seperti berikut ini.

```

chat = "CHANNEL_ID"
api_id = "API_ID"
api_hash = "API_HASH"

from telethon.sync import TelegramClient
import pandas as pd

client = TelegramClient("session_id", api_id, api_hash)






with open("cyberbullying_evidence.txt", "w", encoding="utf-8") as f:
    message = list()

    with client:
        # 10 is the limit on how many messages to fetch. Remove or change for
        # more.
        for msg in client.iter_messages(chat, 200):
            message.append(msg)
            f.write("%s\n" % str(msg))

df = pd.DataFrame(message)
writer = pd.ExcelWriter("tele_data.xlsx", engine="xlsxwriter")
df.to_excel(writer, sheet_name="data", index=False)
writer.save()

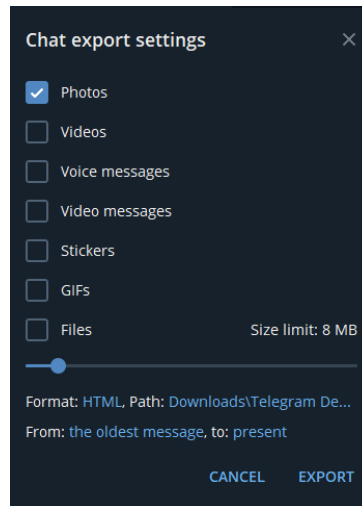
```

bagaimana untuk mendapatkan channel_id ada dua metode yang dapat digunakan **menggunakan getIDBots atau menggunakan versi terdahulu dari Telegram Web**, kemudian dengan kode tersebut nanti akan dihasilkan data chat berbentuk txt, file session dan sebuah file xlsx seperti pada gambar berikut ini.

 cyberbullying_evidence.txt	16/10/2021 16:09	Text Document	140 KB
 session_id.session	16/10/2021 16:09	SESSION File	28 KB
 tele_data.xlsx	16/10/2021 16:09	Microsoft Excel W...	18 KB
 telegram_2.py	16/10/2021 15:43	Python Source File	1 KB
 telegram_3.py	16/10/2021 16:09	Python Source File	1 KB

Namun pesan yang diambil ini merupakan pesan-pesan yang belum dihapus karena jika pesan sudah dihapus maka perlu penanganan khusus untuk mendapatkan kembali datanya. Selain menggunakan library Telethon dapat menggunakan fungsi export bawaan yang sudah disediakan oleh telegram untuk melakukan export ini cukup mudah dapat melakukan dengan mengakses *Pilih*

Chat => Hamburger Button => Export Chat History => Pilih Settingan yang diinginkan atau kurang lebih dapat dijelaskan pada gambar berikut ini.



pada pengambilan data ini dilakukan pengambilan semua komponen yang dirasa penting dan untuk formatnya diubah menjadi .json agar lebih mudah terlihat key dari setiap objectnya.

```
1  {
2    "name": "Forensik Cyberbullying",
3    "type": "private_supergroup",
4    "id": 1600752976,
5    "messages": [
6      {
7        "id": -999953919,
8        "type": "service",
9        "date": "2021-10-16T14:41:00",
10       "actor": "Sya Raihan Heggi",
11       "actor_id": "user784590528",
12       "action": "create_group",
13       "title": "Forensik Cyberbullying",
14       "members": [
15         "Sya Raihan Heggi",
16         "Adabi",
17         "Gia N",
18         "Faisal Amir",
19         "irfan aldi"
20       ],
21       "text": ""
22     },
```

Namun dengan metode ini kurang lebih pesan yang ditampilkan kurang lengkap meta datanya dibandingkan mengambil dengan telethon.

2.2.2.2 Cara Mengambil Data Login

Proses untuk mengambil data login dikarenakan informasi ini dari channel resmi telegram terdapat kesulitan untuk mengambil secara langsung dengan api, karena aksesnya terbatas oleh karena itu memanfaatkan fungsi ekspor yang sudah

dijelaskan pada bagian sebelumnya dan akan didapatkan file .json berisi riwayat kode dan permintaan login yang ada.

2.2.2.3 Cara mengambil data yang dihapus



Metode pengambilan yang dapat dilakukan adalah mengambil dari admin logs dengan menggunakan telethon, karena tidak ada jejak dari pesan yang sudah dihapus di telegram sehingga satu-satunya kemungkinan adalah mengambil di admin logs dalam kurun waktu 48 jam setelah chat tersebut diakuisisi, untuk kode yang digunakan seperti berikut ini.

```
from telethon import TelegramClient, events, sync
from telethon.tl.types import InputChannel, PeerChannel
from telethon.tl.types import Channel
import time

api_id = "API_ID"
api_hash = "API_HASH"
group_chat_id = "CHANNEL_ID"

client = TelegramClient('session_name', api_id, api_hash)
client.start()

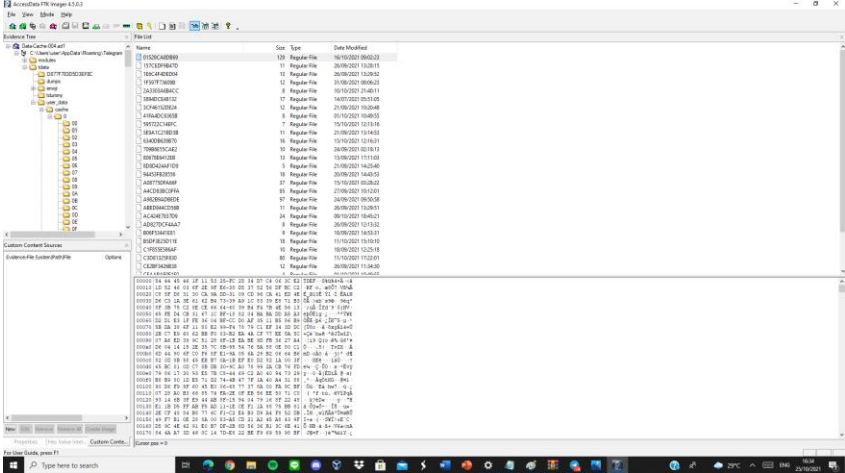
group = client.get_entity(PeerChannel(group_chat_id))
#messages = client.get_admin_log(group)

file1 = open("dump.json", "w")
c = 0
m = 0
for event in client.iter_admin_log(group):
    if event.deleted_message:
        print("Dumping message", c, "(", event.old.id, event.old.date, ")")
        file1.write(event.old.to_json() + ",")
        c += 1
    if event.old.media:
```

```
m+=1
#print(event.old.media.to_dict()['Document']['id'])
client.download_media(event.old.media, str(event.old.id))
print(" Dumped media", m)
time.sleep(0.1)
```

dan setelah kode tersebut dijalankan maka akan didapatkan data dari pesan yang dihapus tersebut maka akan dihasilkan file json dan session dari pengambilan data tersebut, namun untuk pesan masih bisa teridentifikasi karena masih ada user_id di dalamnya.

2.2.2.4 Cara Mengambil Data Cache



Untuk data cache sendiri diamankan karena bisa jadi ada data percakapan yang dihapus masih berada di file tersebut, namun alternatif dari cache ini dapat dilakukan memory capture dari perangkat yang digunakan oleh pelaku atau orang-orang yang berada di grup tersebut.

Untuk data cache sendiri akan berada pada direktori utama program Telegram Desktop namun masih terenkripsi oleh format *tdf* dan *tdef* sehingga yang memungkinkan untuk di analisis adalah data yang berasal dari memdump untuk mendapatkan memdump sendiri digunakan FTK Imager.

2.2.2.5 Cara mengambil data file

Secara default untuk penyimpanan file yang dikirim atau dipertukarkan pada Telegram Desktop akan berada pada folder Downloads dengan nama Telegram Desktop, sehingga dapat langsung diamankan dengan membuat image atau membuat salinan dari folder tersebut.

2.2.2.5 Hasil Pengambilan Data

Dari pengambilan data ini didapati enam buah folder data yang berisi masing-masing data yang berkaitan dengan keperluan analisis nantinya , folder-folder tersebut memiliki nama dan isi sebagai berikut ini.

Nama	Keterangan
Data_Chat	Folder ini berisi data berkaitan dengan bukti percakapan yang terjadi pada public group yang ada di telegram.
Data_Chat_Deleted	Folder ini berisi data percakapan yang dihapus pada public group yang berhasil diambil dalam jangka 48 jam.
Data_Foto	Folder ini berisi file-file yang dikirim tidak hanya foto namun pdf, xlsx, rar dll
Data_Login	Folder berisi bukti data login dengan akun yang digunakan, atau bisa dibilang bukti pengamanan akun untuk bukti bahwa ada akses masuk ke akun yang digunakan
Memdump	Folder berisi memdump dari hasil capture dengan FTK Imager
New_Analysis	Folder yang berisi percobaan kedua yang berisi untuk percobaan tambahan yang dilakukan, yang merupakan bukti tambahan

dan berikut ini kurang lebih dokumentasi dari folder-folder yang berhasil dikumpulkan pada tahapan collection ini.

<input type="checkbox"/>	Data_Chat	16/10/2021 16:11	File folder
<input type="checkbox"/>	Data_Chat_Deleted	16/10/2021 16:29	File folder
<input type="checkbox"/>	Data_Foto	25/10/2021 12:12	File folder
<input type="checkbox"/>	Data_Login	16/10/2021 16:13	File folder
<input type="checkbox"/>	Decrypt Cache	18/10/2021 13:52	File folder
<input type="checkbox"/>	Images File	25/10/2021 13:28	File folder
<input type="checkbox"/>	Memdump	25/10/2021 12:54	File folder
<input type="checkbox"/>	New_Analysis	25/10/2021 13:26	File folder

selanjutnya dilakukan tahapan Examination dimana data-data ini disiapkan untuk dilakukan analisis, yang dilakukan pada tahapan ini adalah membuat image-image file yang berguna melakukan pemisahan bukti yang didapatkan dan bahan analisis sehingga terjamin integritas datanya dan kurang lebih dihimpun menjadi seperti berikut ini.

Data-Cache-004	16/10/2021 16:28	File folder
Data-Chat-001	16/10/2021 16:15	File folder
Data-Delete Chat- 005	16/10/2021 16:31	File folder
Data-Files-003	16/10/2021 16:23	File folder
Data-Login-002	16/10/2021 16:20	File folder
Data-New-Testing-006	25/10/2021 13:28	File folder

Pembuatan folder ini menggunakan FTK Imager sehingga akan dihasilkan file-file berikut ini.

Data-Chat-001.ad1	16/10/2021 16:15	AD1 File	1.682 KB
Data-Chat-001.ad1.csv	16/10/2021 16:15	Microsoft Excel C...	25 KB
Data-Chat-001.ad1.txt	16/10/2021 16:24	Text Document	2 KB

File .ad1 ini merupakan file yang berisi image dari folder, file csv merupakan kumpulan metadata dari file yang ada di image jika dibuka maka akan menampilkan hal berikut ini.

	A	B	C	D	E	F	G	H
1	Filename	Full Path	Size (byte	Created	Modified	Accessed	Is Deleted	Stored MD5 Hash
2	ChatExport_2021-10-16	C:\Users\user\Documents\Co	0	2021-Oct-	2021-Oct-	2021-Oct-	no	
3	cyberbullying_evidence.txt	C:\Users\user\Documents\Co	142703	2021-Oct-	2021-Oct-	2021-Oct-	no	208f1026bbe41f5f442697786159ff56
4	session_id.session	C:\Users\user\Documents\Co	28672	2021-Oct-	2021-Oct-	2021-Oct-	no	dae921c8e2f2a864be1bfa0bc5a4df2d
5	telegram_2.py	C:\Users\user\Documents\Co	442	2021-Oct-	2021-Oct-	2021-Oct-	no	7869ccca91805cf70f4342b163127604
6	telegram_3.py	C:\Users\user\Documents\Co	719	2021-Oct-	2021-Oct-	2021-Oct-	no	a57c3197986847e3df0882e0ba391f6f
7	tele_data.xlsx	C:\Users\user\Documents\Co	17563	2021-Oct-	2021-Oct-	2021-Oct-	no	3774f885c1f2012ece185174ce63f8b3

Di mana akan berisi beberapa data yang berkaitan dengan tanggal akses, apakah ada perubahan dan nilai hash dari file tersebut, mengapa dibuat image ini karena bertujuan agar integritas terjaga kemudian bagaimana membuktikan bahwa image tersebut tidak dibuat dari bukti yang dibangun maka dapat dilakukan verifikasi balik dengan bukti awal yang dihimpun sehingga akan dijelaskan secara detail nilai hash dari masing-masing folder.

- **Data_Chat**

Nama File	Nilai Hash (MD5)
cyberbullying_evidence.txt	208f1026bbe41f5f442697786159ff56
session_id.session	dae921c8e2f2a864be1bfa0bc5a4df2d
tele_data.xlsx	3774f885c1f2012ece185174ce63f8b3

telegram_2.py	7869ccca91805cf70f4342b163127604
telegram_3.py	a57c3197986847e3df0882e0ba391f6f
CII-2M3 Pengantar Kecerdasan Buatan - Tugas 01.pdf	503f07fe8959a5d90ae464ea227a04f8
CII-2M3 Pengantar Kecerdasan Buatan - Tugas 01.pdf_thumb.jpg	a07fa02bbcc8259b1ec1e6048fb0f750
DataTugasPengantar.xlsx	34626bd864096fe43ce122f40c005c1e
image_2021-10-16_14-53-23.png	aa9c094287ae4174573289e464bf6a40
image_2021-10-16_14-53-23.png_thumb.jpg	d485ce9f22e54d37c8cde47509f9e7e0
image_2021-10-16_15-16-37.png	c5b0e5df1f9ae6b174de45c4b0da5bf4
image_2021-10-16_15-16-37.png_thumb.jpg	146543274d33c383fd7a7193714d1b73
Overview_of_the_General_Framework.pdf	ca8296db1b9d26bcf0fc58e717956710
Overview_of_the_General_Framework.pdf_thumb.jpg	2f921dad2a4b0996c0609bb2265be436
TensorFlow.ipynb	1243023b85b3ded59f95fe301af9fbea
Tugas PKKMB.pdf	781b7c7c34db1f5b36f6d4da76f27ac3
Tugas PKKMB.pdf_thumb.jpg	35bec91a2aec6d50ec1841616dc7b74
photo_1@16-10-2021_14-41-01.jpg	f2154672a7772fe94de165d9eacc0976
photo_2@16-10-2021_14-48-56.jpg	a82a5a3df33bca6847f701744095310e
photo_3@16-10-2021_14-49-25.jpg	6f8444b26d3e4b01a33236317550ec24

sticker (1).webp	a805f7682e49ecbe5e2ce84493279ff4
sticker (1).webp_thumb.jpg	afe51b25fa07462e536645a827fca2ef
sticker (2).webp	c48a8c9571234703eb79905046416ca8
sticker (2).webp_thumb.jpg	9b0b1cc5e1b7a76404a839c4abd251c0
sticker (3).webp	4a6fd02aa7bb63b4efb0bb98c90333fa
sticker (3).webp_thumb.jpg	e788eafd764618ff150dbfee73570c05
sticker.webp	55eee8a3902c5b7119807e083e6acd84
sticker.webp_thumb.jpg	163086a6138df9d8d6a03a472086a07a
mp4.mp4	8a5be7813131640e273e8f42a1b42336
result.json	bde67bd781702268f77b5055da5e6ff7

- **Data Delete Chat**

Nama File	Nilai Hash (MD5)
dump.json	0f453e5292701eea58dac6c727a0faec
restore_data.py	6b3f9fc5ec35dcc5629eb7fe762383c1
session_name.session	c8969a7a9a497597524122ceb44140ad

- **Data Files** (sebenarnya ada file lainnya namun saat ini berfokus pada file yang digunakan pada skenario)

Nama File	Nilai Hash (MD5)
DataTugasPengantar.xlsx	34626bd864096fe43ce122f40c005cle

TensorFlow.ipynb	1243023b85b3ded59f95fe301af9fbaea
Overview_of_the_General_Framework.pdf	ca8296db1b9d26bcf0fc58e717956710
image_2021-10-16_14-53-23.png	aa9c094287ae4174573289e464bf6a40
image_2021-10-16_15-16-37.png	c5b0e5df1f9ae6b174de45c4b0da5bf4
Tugas PKKMB.pdf	(Tidak Ditemukan Karena Dikirimkan oleh Korban Sehingga File berasal dari Korban)
File Pengantar Kecerdasan Buatan	(Tidak Ditemukan Karena Dikirimkan oleh Korban Sehingga File berasal dari Korban)

- **Data Login**

Nama File	Nilai Hash (MD5)
result.json	a5f07f448efa9086186d0438c7992efe
result.json	e31157e664a8761c9c8f11e6034efb84
session_id.session	4fc6d9fc7e2964bca3971fb171ca0c5a
telegram_3.py	f1d2a1d12e0cee83bc78575d36135ed4

- **Data Cache**

Nama File	Nilai Hash (MD5)
Memdump	Tidak Ada

- **Data New_Analysis**

Nama File	Nilai Hash (MD5)
Bukti Live Forensics.PNG	e77a6304cc58c882748b7f05aa32a73f
bukti_deleted.jpg	f105d9b8352e460249c191fc0d3954e1

cyberbullying_evidence.txt	04b9cd3edfaffae6f527b68f2bc16563
dump.json	084467fadd5f97578da90255416f5ee5
Hash_Data.txt	1f43b08d741091c150c70b045e144f36
restore_data.py	6b3f9fc5ec35dcc5629eb7fe762383c1
session_id.session	1cedffc5445a0c77c2961f5753cd9b45
session_name.session	1c09c8b6330f8a22cc887d316c6f7bdb
tele_data.xlsx	b6355b38980dcf60209a8706a14cee7d
telegram_3.py	a57c3197986847e3df0882e0ba391f6f
Bukti Live Forensics.PNG	e77a6304cc58c882748b7f05aa32a73f

- **Data Image**

Nama File	Nilai Hash (MD5)
Data-Chat-001.ad1	97623193f556170352b4354ca233deb2
Data-Login-002.ad1	55126cd2daf5607b6199e96a32a56b0f
Data-Files-003.ad1	a5a9d65fead30b158d2e5d85f7769acd
Data-Cache-004.ad1	e755677ff003b5401f36ba0b6b5f59dc
Delete-Chat-005.ad1	b555b191505ca0eec5d0efeba9d33931
006-New-Testing.ad1	4d7235e8632c92a9c9f536ebd3bb5d25

Untuk proses pengambilan data ini dilakukan dengan menggunakan masuk dengan akun korban Sya Raihan Heggi yang dibuktikan dengan adanya bukti akses masuk ke dalam akun tersebut.

```
{
  "id": 46089,
  "type": "message",
  "date": "2021-10-16T15:37:12",
  "from": "Telegram",
  "from_id": "user777000",
  "text": "Kode masuk Anda: 97436
},
{
  "id": 46091,
  "type": "message",
  "date": "2021-10-16T15:44:18",
  "from": "Telegram",
  "from_id": "user777000",
  "text": "Kode masuk Anda: 79946
}
]
```

2.2.3 Data Analysis

Data yang sudah dipersiapkan sebelumnya pada tahapan *Collection dan Examination* kemudian akan dilakukan analisis tahapan analisis yang dilakukan adalah.

1. Membuat Duplicate File digunakan untuk file yang tidak dapat dilihat pada FTK imager atau file-file yang perlu dirapikan,
2. Menggunakan program yang memblok proses *write* dalam hal ini menggunakan FTK Imager untuk analisis program.
3. Analisis Data chat yang ada dan dapat ditemukan
4. Analisis Data chat yang dihapus
5. Analisis File yang dikirim
6. Membuat kesimpulan dari data yang ditemukan

Seperti yang sudah disiapkan hal pertama yang akan dianalisis adalah data chat untuk data chat sendiri yang di crawling menggunakan kode python disimpan dalam bentuk .txt untuk menganalisisnya sebenarnya bisa dilakukan tanpa merubah namun akan lebih mudah untuk membagi setiap key yang didapatkan dari data yang di crawling oleh karena itu data yang ada di duplicate dan dibuatkan sebuah file excel yang mempermudah untuk analisis dari chat ini didapati kurang lebih ada key/fitur yang ada pada data yang diambil yang bisa dijelaskan sebagai berikut ini.

- **Message** (Merupakan Pesan yang dikirimkan oleh user ke dalam sebuah group)

Nama Header	Penjelasan
id	id dari pesan atau urutan pesan yang dikirim.
channel_id	id channel dimana pesan itu berada.
date	berisi metadata yang berkaitan dengan tanggal pesan dikirimkan didalamnya akan berisi date_time, tzinfo
date_time	waktu pesan dikirim ditulis dengan format YYYY-MM-DD HH:MM:SS'.
tzinfo	kelas abstrak yang digunakan untuk konversi waktu ke UTC.
message	isi pesan yang dikirimkan .
out	mengetahui pesan tersebut dikirim dari sesi user atau sesi lain, misalnya orang lain. akan selalu bernilai true jika user sendiri yang mengirim pesan.
mentioned	mengetahui berupa pesan biasa atau memiliki

	balasan/mention.
media_unread	mengetahui pesan tersebut sudah dibaca atau belum.
silent	mengetahui notifikasi pesan dinyalakan dengan suara atau tidak.
post	mengetahui pesan di posting di channel atau tidak.
from_scheduled	mengetahui berupa pesan yang dijadwalkan atau tidak.
legacy	mengetahui pesan berupa pesan legacy atau tidak.
edit_hide	mengetahui pesan yang diubah ditampilkan atau disembunyikan.
pinned	mengetahui pesan disematkan atau tidak.
from_id	mengetahui pesan dikirim oleh PeerUser (User), PeerChat (Chat), PeerChannel (Channel) atau None.
fwd_from	mengetahui pesan merupakan hasil forward dari pesan lain atau tidak
reply_to	mengetahui key balasan pesan seperti reply_to_msg_id.
media	mengetahui key seperti dokumen id atau datetime dan jenis media seperti photo, dokumen, dsb.
Dokumentasi lebih lengkap dapat dibaca pada message (telegram.org)	

- **MessageReplies** (Merupakan pesan yang di reply oleh user tertentu pada)

Nama Header	Penjelasan
replies	Menjelaskan pesan ini sudah berapa kali dilakukan reply.
replies_pts	Menandakan chat yang merupakan asal dari replies.
comments	Isi dari reply terhadap suatu pesan.
recent_replies	Menjelaskan pesan terakhir yang melakukan reply terhadap suatu pesan
channel_id	Merupakan channel_id dari comment

max_id	Id dari replies terakhir yang berada pada suatu chat session atau pada comment session
read_max_id	Id dari read terakhir dari suatu chat session atau pada comment session.
edit_Date	Waktu saat pesan ini terakhir diedit.
post_author	Nama tampilan pengirim pesan untuk ditampilkan dalam pesan.
grouped_id	Jika pesan ini milik sekelompok pesan (album foto atau album video), semuanya akan memiliki nilai yang sama.
restriction_reason	Daftar opsional alasan mengapa pesan ini dibatasi. Jika daftarnya tidak ada, pesan ini belum dibatasi.
ttl_period	Periode Time To Live dikonfigurasi untuk pesan ini jika melewati waktu ini maka pesan dihapus dari manapun itu disimpan (memori, database lokal, dll.)
Dokumentasi lebih lengkap dapat dibaca pada messageReplies (telegram.org)	

- **MessageMediaDocument** (Merupakan Media (video, audio, voice, sticker) yang dikirimkan pada Message)

Nama Header	Penjelasan
document_id	Merupakan id dari document yang dikirim
access_hash	Hash dari file yang dikirim
file_reference	Merupakan data dari file yang dikirim
date	Tanggal dimana dokumen tersebut dikirimkan
thumbs	Merupakan data Thumbnail yang akan ditampilkan biasanya berisi data foto atau contoh dari suatu file/dokumen.
PhotoStrippedSize	Foto yang ditampilkan pada thumbnail dari file yang dikirim, metadata yang terdapat pada header ini ada type , ttl_seconds dan bytes untuk contoh. (type='i', bytes=b"\x01(\x1c\xd9\xc8\xf5\xa6\x16a\xd0\x0f\xce\x

	95\x88\x07\x91\xfaP\x00=\xbfJ\x00@;\x93\xfa\xd3\xe8\x03\x14P\x03\x1f\xb5\x00\x1fsJ\xc3"xa5(\xc8\xe3\x03\xf3\xa0\x05\x1fB(\xa4\xe7\xd0~t\xb4\x00QE\x14\x00QE\x14\x01")), ttl_seconds=None)
PhotoSize	Merupakan parameter ukuran foto yang ditampilkan terdiri dari type , w (width) , h (height) , size , video_thumbs (type='m', w=226, h=320, size=9543)], video_thumbs=[])
Dokumentasi lebih lengkap dapat dibaca pada MessageMedia (telegram.org) , untuk penjelasan lebih spesifik mengenai dokumen yang dikirim dapat dibaca pada messageMediaDocument (telegram.org)	

- **MessageService**(Merupakan Pesan yang dikirimkan oleh telegram atau aplikasi jika terjadi suatu event seperti leave, join, created group, dll)

Nama Header	Penjelasan
id	id atau urutan pesan yang dikirim.
channel_id	id channel.
date	berisi metadata yang berkaitan dengan tanggal pesan dikirimkan didalamnya akan berisi date_time , tzinfo
date_time	waktu pesan dikirim.
tzinfo	kelas abstrak yang digunakan untuk konversi waktu ke UTC.
action	berisi action atau hal yang terjadi dan mengapa message ini dikirimkan pada pengujian skenario didapatkan MessageActionChatDeleteUser (User Leave Group) dan MessageActionChannelMigrateFrom (Group Created dari specific Chat dalam hal ini chat antar anggota grup) . namun sebenarnya masih banyak lagi action yang dapat terjadi dokumentasi ini ada pada tautan berikut ini MessageAction (telegram.org) .
out	Menjelaskan pesan berasal dari sesi user atau bukan
mentioned	Menjelaskan pesan melakukan mention terhadap suatu entitas atau tidak

media_unread	Mengetahui pesan tersebut sudah dibaca atau belum.
silent	Mengetahui notifikasi pesan dinyalakan dengan suara atau tidak.
post	Mengetahui pesan di posting di channel atau tidak.
legacy	Mengetahui berupa pesan yang dijadwalkan atau tidak.
from_id	mengetahui pesan dikirim oleh PeerUser (User), PeerChat (Chat), PeerChannel (Channel) atau None.
reply_to	Menjelaskan bawa message melakukan reply kepada suatu chat atau hal lainnya.
ttl_period	Waktu yang menjelaskan Time to Live dari suatu dokumen sebelum dihapus dari semua media penyimpanan.
Dokumentasi lebih lengkap dapat dibaca pada messageService (telegram.org)	

Kemudian selain dari header-header yang ditemukan tersebut terdapat sebuah data log dari sesi dimana akan tercatat nilai hash, user_id dan nama dari semua pengguna yang ada di dalam data yang dilakukan crawling.

	id	hash	username	phone	name	date
	Filter	Filter	Filter	Filter	Filter	Filter
1	-1001600752976	-638835477837235065	NULL	NULL	Forensik Cyberbullying	1634375382
2	-1001525881369	-3399693992427597443	joinn1111	NULL	Tanam duit saham binomo	1634375179
3	-619871710	0	NULL	NULL	Forensik Cyberbullying	1634375382
4	140267078	-7474907206538251593	gif	NULL	Tenor GIF Search	1634375382
5	320967145	3390261759760785342	faisalamircs	NULL	Faisal Amir	1634375382
6	738888501	3071483658003699136	irfanaldii	NULL	irfan aldi	1634375382
7	784590528	-6006528188258352336	heggi_raihan	6281284549958	Sya Raihan Heggi	1634375382
8	910287747	-1795591771625251566	NULL	NULL	Gia N	1634375382
9	1087968824	125032246693351047	groupanonymousbot	NULL	Group	1634375382
10	1206830175	-7692370183596969562	NULL	NULL	Adabi	1634375382
11	1504012575	-271594398012089092	obaja202020	NULL	Mr Simamora02	1634375179
12	1922576398	8371841608142456106	wahyuhalin	NULL	Wahyu halin	1634375179
13	2015563188	8374304811314898677	NULL	NULL	Rudi Tabudi	1634375179
14	2033434433	6365249099783027455	NULL	NULL	Warhamni 04	1634375179
15	2049444082	3604685483120267233	NULL	NULL	Sinar	1634375179

dengan mendapatkan id dari pengguna ini akan mudah untuk melakukan pengecekan terhadap siapa sebenarnya pelaku perbuatan *cyberbullying* ini untuk mengetahui secara pasti siapa saja anggotanya data ini dapat didapatkan dari hasil ekspor chat yang dilakukan dengan bantuan Telegram Desktop

```
{
  "name": "Forensik Cyberbullying",
  "type": "private_supergroup",
  "id": 1600752976,
  "messages": [
    {
      "id": -999953919,
      "type": "service",
      "date": "2021-10-16T14:41:00",
      "actor": "Sya Raihan Heggi",
      "actor_id": "user784590528",
      "action": "create_group",
      "title": "Forensik Cyberbullying",
      "members": [
        "Sya Raihan Heggi",
        "Adabi",
        "Gia N",
        "Faisal Amir",
        "irfan aldi"
      ],
      "text": ""
    },
  ],
}
```

Dari data ini diketahui anggota dari grup ini adalah Sya Raihan Heggi, Adabi, Gia N, Faisal Amir. dan Irfan aldi dan dengan data ini pula diketahui bahwa grup ini dibuat oleh Sya Raihan Heggi dengan maksud dan tujuan tertentu.

Kemudian didapati beberapa chat yang mengandung unsur cyberbullying yang dapat berguna sebagai barang bukti jika kasus tersebut dibawa ke ranah hukum, dan kurang lebih pesan yang didapatkan adalah sebagai berikut ini.

id_message	id_pengirim	message	datetime
165	320967145(Faisal Amir)	‘iya iya penggila cumlaude’	2021-10-16 8:20:32
166	320967145(Faisal Amir)	‘makan tuh sana cumlaude’	2021-10-16 8:20:37
167	320967145(Faisal Amir)	‘pas lulus juga nilai ga kepake’	2021-10-16 8:20:57
168	320967145(Faisal Amir)	‘yang kepake koneksi broh inget tuh’	2021-10-16 8:21:03
169	320967145(Faisal Amir)	‘@Heggi_raihan dasar nerdy’	2021-10-16 8:21:10

id_message	id_pengirim	message	datetime
150	320967145(Faisal Amir)	'bodo amat lah gw', out	2021-10-16 8:16:44
151	320967145(Faisal Amir)	biarin si rajin yang menang @Heggi_raihan	2021-10-16 8:16:57

id_message	id_pengirim	message	datetime
97	320967145(Faisal Amir)	'mintaa maaf lu @Heggi_raihan ama gia'	2021-10-16 8:02:12
98	320967145(Faisal Amir)	'sok banget jadi orang'	2021-10-16 8:02: 20
99	910287747(Gia N)	'udah males gw'	2021-10-16 8:02:31
100	320967145(Faisal Amir)	'sabar bro Gia'	2021-10-16 8:02:40
101	320967145(Faisal Amir)	'rada rada tuh emang dia @Heggi_raihan'	2021-10-16 8:02:49
102	320967145(Faisal Amir)	'egonya ga ada akhlakj'	2021-10-16 8:02:53
103	320967145(Faisal Amir)	'@Heggi_raihan mana nih ga muncul lagi'	2021-10-16 8:04:30
104	320967145(Faisal Amir)	'katanya jagoan kok diem skrng'	2021-10-16 8:04:45

Terdapat beberapa user yang berada di grup tersebut memojokan Heggi, dapat dilihat beberapa user melakukan tag kepada username Heggi_raihan dengan menggunakan kata kata yang bisa dibilang menjurus ke cyberbullying, kemudian selain dari, terdapat

beberapa files yang dikirimkan melalui media telegram ini yang kurang lebih datanya sebagai berikut ini.

id_message	id_pengirim	document_id	name	message	datetime
2	784590528 (Sya Raihan Heggi)	629397414791 5580329 (Document)	CII-2M3 Pengantar Kecerdasan Buatan - Tugas 01.pdf	Pengiriman File Tanpa Pesan (,)	2021-10-16 7:43:1
35	784590528 (Sya Raihan Heggi)	629397414837 1820402 (Photo)	photos/photo_2@16-10-2021_14-48-56.jpg	Pengiriman File Tanpa Pesan (,)	2021-10-16 7:48:56
39	784590528 (Sya Raihan Heggi)	629397414837 1820403 (Photo)	photos/photo_3@16-10-2021_14-49-25.jpg	Pengiriman File Tanpa Pesan (,)	2021-10-16 7:49:25
54	784590528 (Sya Raihan Heggi)	629397414791 5580331 (Document)	image_2021-10-16_14-53-23.png	'mana tuh udah gw kasih''	2021-10-16 7:53:25
72	784590528 (Sya Raihan Heggi)	458135382551 1670060 (Sticker)	'👉'	Pengiriman File Tanpa Pesan (,)	2021-10-16 7:55:59
74	320967145 (Faisal Amir)	598212262416 1940017 (Video File)	mp4.mp4	Pengiriman File Tanpa Pesan (,)	2021-10-16 7:56:34
75	784590528 (Sya Raihan Heggi)	629397414791 5580332 (Dokumen)	Tugas PKKMB.pdf	'neh'	2021-10-16 7:57:32
86	320967145 (Faisal Amir)	629397414791 5580333 (Dokumen)	'Overview_of_the_General_Framework.pdf	Pengiriman File Tanpa Pesan (,)	2021-10-16 7:59:26)

131	910287747 (Gia N)	629397414791 5580334 (Dokumen)	files/TensorFlow.ipynb	'nih udah gw kerjain bagian ini;'	2021-10-16 8:9:30
148	738888501 (Irfan aldi)	629397414791 5580335 (Dokumen)	files/DataTugasPengerantar.xlsx	'ini yaa dataset nya udah kubuat'	2021-10-16 8:16:11
149	320967145 (Faisal Amir)	629397414791 5580336 (Dokumen)	files/image_2021-10-16_15-16-37.png	'ini code yang di kerjain gw ama adabi ga lu anggep, sebanyak ini'	2021-10-16 8:16:41
173	784590528 (Sya Raihan Heggi)	614292480385 9808965 (Sticker)	'😊'	Pengiriman File Tanpa Pesan (,)	2021-10-16 8:21:47
185	784590528 (Sya Raihan Heggi)	436061904939 516837 (Sticker)	'👍'	Pengiriman File Tanpa Pesan (,)	2021-10-16 8:25:41

- **Bukti Foto yang Diamankan**

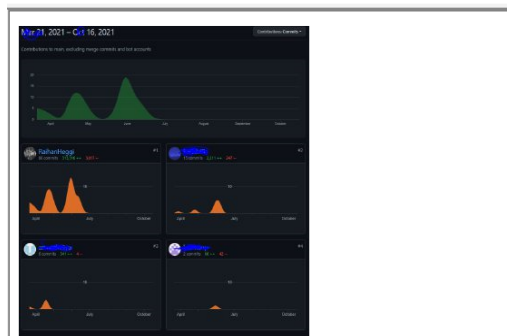


- **Bukti Video yang Diamankan**

Name	Size	Type	Date Modified
🔊 mp4.mp4	125	Regular File	16/10/2021 08:50:41

- **Bukti Dokumen yang Diamankan**

Name	Size	Type	Date Modified
CII-2M3 Pengantar Kecerdasan Buatan - ...	270	Regular File	16/10/2021 08:50:31
CII-2M3 Pengantar Kecerdasan Buatan - ...	10	Regular File	16/10/2021 08:50:32
image_2021-10-16_14-53-23.png	49	Regular File	16/10/2021 08:50:32
image_2021-10-16_14-53-23.png_thumb...	13	Regular File	16/10/2021 08:50:33
Tugas PKKMB.pdf	180	Regular File	16/10/2021 08:50:41
Tugas PKKMB.pdf_thumb.jpg	7	Regular File	16/10/2021 08:50:41
Overview_of_the_General_Framework.pdf	285	Regular File	16/10/2021 08:50:42
Overview_of_the_General_Framework.pdf...	5	Regular File	16/10/2021 08:50:42
TensorFlow.ipynb	28	Regular File	16/10/2021 08:50:43
DataTugasPengantar.xlsx	9	Regular File	16/10/2021 08:50:43
image_2021-10-16_15-16-37.png	544	Regular File	16/10/2021 08:50:44
image_2021-10-16_15-16-37.png_thumb...	8	Regular File	16/10/2021 08:50:44



(bukti yang didapatkan dari ekspor Telegram)

image_2021-10-16_14-53-23.png	49	Regular File	16/10/2021 07:53:46
Overview_of_the_General_Framework.pdf	285	Regular File	16/10/2021 07:59:26
TensorFlow.ipynb	28	Regular File	16/10/2021 08:09:30
DataTugasPengantar.xlsx	9	Regular File	16/10/2021 08:17:36

(bukti yang didapatkan dari perangkat keras yang diamankan)

Kemudian dari rekam percakapan sendiri keadaan mulai memanaskan ketika Gia N (910287747) keluar dari grup tanpa alasan apapun, sehingga ada kecenderungan untuk merundung Sya Raihan Heggi (784590528), seperti yang ditemukan pada chat_id 60 dan kemudian masuk kembali pada chat_id 96 masuk melalui tautan undangan.

```
MessageService(id=60, peer_id=PeerChannel(channel_id=1600752976), date=datetime.datetime(2021, 10, 16, 7, 54, 28, tzinfo=datetime.timezone.utc), action=MessageActionChatDeleteUser(user_id=910287747), out=False, mentioned=False, media_unread=False, silent=False, post=False, legacy=False, from_id=PeerUser(user_id=910287747), reply_to=None, ttl_period=None)
```

(bukti user_id 910287747 keluar dari grup)

Selanjutnya menurut keterangan korban terdapat pesan-pesan yang dihapus untuk menghilangkan bukti kegiatan percakapan.



Namun pesan tersebut sempat di reply dan dilakukan tangkapan layar oleh korban sehingga untuk membuktikan hal ini dilakukan pengambilan data yang berada pada admin log yang memiliki batas waktu 48 jam sebelum data tersebut dihapus selamanya.

Data yang berhasil di capture

```
{ "_": "Message", "id": 196, "peer_id": { "_": "PeerChannel", "channel_id": 1600752976 },
  "date": "2021-10-25T05:47:27+00:00", "message": "nah reply", "out": true, "mentioned":
  false, "media_unread": false, "silent": false, "post": false, "from_scheduled": false, "legacy":
  false, "edit_hide": false, "pinned": false, "from_id": { "_": "PeerUser", "user_id":
  784590528 }, "fwd_from": null, "via_bot_id": null, "reply_to": null, "media": null,
  "reply_markup": null, "entities": [], "views": null, "forwards": null, "replies": { "_":
  "MessageReplies", "replies": 1, "replies_pts": 203, "comments": false, "recent_repliers": [],
  "channel_id": null, "max_id": 197, "read_max_id": null }, "edit_date": null, "post_author":
  null, "grouped_id": null, "restriction_reason": [], "ttl_period": null },
```

pesan ini dikirimkan oleh id_user (784590528) dan dikirimkan sebagai pesan dengan id 196, selain dengan metode ini dapat didapatkan data dengan melakukan metode live forensic dengan melakukan memdump namun ada baiknya untuk mendapatkan data ini dilakukan hanya ketika komputer atau barang bukti belum dimatikan.


```

26b66c430 D:0R-Dÿÿ0Râ@....4-if05:47:27+00:00", \"message\": \"nah reply\", \"out\": true,
26b66c480 \"mentioned\": false, \"media_unread\": false, \"silent\": false, \"post\": fal
26b66c4d0 se, \"from_scheduled\": false, \"legacy\": false, \"edit_hide\": false, \"pinned
26b66c520 \": false, \"from_id\": {\"_\": \"PeerUser\", \"user_id\": 784590528}, \"fwd_fro
26b66c570 m\": null, \"via_bot_id\": null, \"reply_to\": null, \"media\": null, \"reply_ma
26b66c5c0 rkup\": null, \"entities\": [], \"views\": null, \"forwards\": null, \"replies\"
26b66c610 : {\"_\": \"MessageReplies\", \"replies\": 1, \"replies_pts\": 203, \"comments\"
26b66c660 : false, \"recent_repliers\": [], \"channel_id\": null, \"max_id\": 197, \"read_
26b66c6b0 max_id\": null}, \"edit_date\": null, \"post_author\": null, \"grouped_id\": nul
26b66c700 l, \"restriction_reason\": [], \"ttl_period\": null}, \"}} .....øÿÿ
26b66c750 z·pD·t%.....8l>×·çÿÿ.....x.....ç.....D·t%.....δ!··çÿÿéÿÿ!·çÿÿ

```

(bukti komputer masih melakukan get data admin log)

```

27d502610 73 00 65 00 6D 00 75 00-61 00 20 00 6B 00 65 00 s·e·m·u·a· ·k·e·
27d502620 67 00 69 00 61 00 74 00-61 00 6E 00 20 00 6C 00 g·i·a·t·a·n· ·l·
27d502630 61 00 62 00 20 00 61 00-61 00 64 00 61 00 20 00 a·b· ·a·a·d·a· ·
27d502640 64 00 61 00 20 00 77 00-6B 00 77 00 6D 00 6F 00 d·a· ·w·k·w·m·o·
27d502650 73 00 74 00 6C 00 20 00-79 00 20 00 6D 00 61 00 s·t·l· ·y· ·m·a·
27d502660 6C 00 61 00 68 00 20 00-6B 00 6F 00 6D 00 75 00 l·a·h· ·k·o·m·u·
27d502670 6E 00 69 00 6B 00 61 00-73 00 69 00 20 00 6C 00 n·i·k·a·s·i· ·l·
27d502680 61 00 62 00 20 00 6B 00-75 00 20 00 64 00 69 00 a·b· ·k·u· ·d·i·
27d502690 20 00 74 00 65 00 6C 00-65 00 20 00 77 00 6B 00 ·t·e·l·e· ·w·k·
27d5026a0 77 00 77 00 6B 00 77 00-6B 00 77 00 20 00 70 00 w·w·k·w·k·w· ·p·
27d5026b0 61 00 73 00 20 00 70 00-61 00 6B 00 20 00 61 00 a·s· ·p·a·k· ·a·
27d5026c0 75 00 6C 00 20 00 6F 00-6E 00 20 00 6C 00 61 00 u·l· ·o·n· ·l·a·
27d5026d0 67 00 69 00 20 00 77 00-6B 00 77 00 77 00 6B 00 g·i· ·w·k·w·w·k·
27d5026e0 77 00 6B 00 20 00 6E 00-67 00 65 00 72 00 74 00 w·k· ·n·g·e·r·t·
27d5026f0 69 00 20 00 62 00 61 00-74 00 20 00 74 00 61 00 i· ·b·a·t· ·t·a·
27d502700 77 00 6B 00 6F 00 77 00-6B 00 6F 00 77 00 6B 00 w·k·o·w·k·o·w·k·
27d502710 6F 00 47 00 61 00 69 00-73 00 20 00 54 00 6F 00 o·G·a·i·s· ·T·o·
27d502720 6C 00 6F 00 67 00 20 00-6E 00 67 00 20 00 64 00 l·o·g· ·n·g· ·d·
27d502730 69 00 20 00 52 00 65 00-70 00 6C 00 79 00 20 00 i· ·R·e·p·l·y· ·
27d502740 64 00 75 00 6E 00 64 00-73 00 74 00 65 00 72 00 d·u·n·d·s·t·e·r·
27d502750 75 00 73 00 20 00 64 00-69 00 20 00 73 00 73 00 u·s· ·d·i· ·s·s·
27d502760 68 00 65 00 65 00 68 00-20 00 6D 00 61 00 73 00 h·e·e·h· ·m·a·s·
27d502770 69 00 68 00 20 00 61 00-6E 00 6F 00 6E 00 79 00 i·h· ·a·n·o·n·y·
27d502780 6D 00 6F 00 75 00 73 00-6E 00 61 00 68 00 20 00 m·o·u·s· ·n·a·h· ·
27d502790 72 00 65 00 70 00 6C 00-79 00 73 00 73 00 20 00 r·e·p·l·y·s· ·
27d5027a0 64 00 75 00 6E 00 64 00-73 00 20 00 62 00 69 00 d·u·n·d·s· ·b·i·
27d5027b0 6B 00 69 00 72 00 69 00-6D 00 20 00 64 00 69 00 k·i·r·i·m· ·d·i·
27d5027c0 20 00 6C 00 69 00 6E 00-65 00 00 00 00 00 00 ·l·i·n·e·.....

```

(bukti message yang dihapus masih ada di memory)

Sehingga dapat dipastikan bahwa pesan yang dihapus bernilai 'nah reply' yang dikirimkan oleh id_user (784590528), sehingga untuk membuktikan penghapusan dalam sebuah file dapat dilakukan selama tempo waktu 48 jam bila tidak maka harapan untuk menganalisa adalah pada file cache memory atau cache telegram namun untuk cache telegram tidak dapat dianalisis dikarenakan di enkripsi dengan metode yang tidak diketahui metode dekripsinya.

2.2.4 Reporting dan Verifikasi Hash Setelah Analisis

Untuk reporting dituliskan pada laporan yang telah ditulis ini dan untuk tahapan verifikasi bahwa tidak ada bukti yang dimanipulasi maka dilakukan verifikasi terhadap nilai hash dari image bukti yang dianalisis sehingga lebih membuktikan tidak ada perubahan terhadap isi dari suatu file.

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 001-Cyberbullying Telegram
Evidence Number: 001-Bukti-Percakapan
Unique Description: 001-Chat
Examiner: Sya Raihan Hegg
Notes: Bukti Percakapan Di Grup

Information for C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Chat-001\Data-Chat-001.ad1:
[Computed Hashes]
MD5 checksum: 97623193f556170352b4354ca233deb2
SHA1 checksum: 7c3568fb4f28037a43dcdbac5796c5c64dd49bc4

Image information:
Acquisition started: Sat Oct 16 16:15:37 2021
Acquisition finished: Sat Oct 16 16:15:37 2021
Segment list:
C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Chat-001\Data-Chat-001.ad1

Image Verification Results:
Verification started: Sat Oct 16 16:15:37 2021
Verification finished: Sat Oct 16 16:15:37 2021
MD5 checksum: 97623193f556170352b4354ca233deb2 : verified
SHA1 checksum: 7c3568fb4f28037a43dcdbac5796c5c64dd49bc4 : verified

Image Verification Results:
Verification started: Sat Oct 16 16:24:53 2021
Verification finished: Sat Oct 16 16:24:53 2021
MD5 checksum: 97623193f556170352b4354ca233deb2 : verified
SHA1 checksum: 7c3568fb4f28037a43dcdbac5796c5c64dd49bc4 : verified

Image Verification Results:
Verification started: Sat Oct 16 16:24:57 2021
Verification finished: Sat Oct 16 16:24:57 2021
MD5 checksum: 97623193f556170352b4354ca233deb2 : verified
SHA1 checksum: 7c3568fb4f28037a43dcdbac5796c5c64dd49bc4 : verified

Image Verification Results:
Verification started: Thu Oct 28 01:33:32 2021
Verification finished: Thu Oct 28 01:33:32 2021
MD5 checksum: 97623193f556170352b4354ca233deb2 : verified
SHA1 checksum: 7c3568fb4f28037a43dcdbac5796c5c64dd49bc4 : verified

(Bukti Verifikasi Image Folder Data_Chat)

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 001-Cyberbullying Telegram
Evidence Number: 002 Login Data on Telegram
Unique Description: JSON file of login data
Examiner: Sya Raihan Hegg
Notes: JSON File for Access Code

Information for C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Login-002\Data-Login-002.ad1:
[Computed Hashes]
MD5 checksum: 55126cd2daf5607b6199e96a32a56b0f
SHA1 checksum: 998b84ffef27307f9dcc5138ed42605a22b2c141

Image information:
Acquisition started: Sat Oct 16 16:20:41 2021
Acquisition finished: Sat Oct 16 16:20:41 2021
Segment list:
C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Login-002\Data-Login-002.ad1

Image Verification Results:
Verification started: Sat Oct 16 16:20:41 2021
Verification finished: Sat Oct 16 16:20:41 2021
MD5 checksum: 55126cd2daf5607b6199e96a32a56b0f : verified
SHA1 checksum: 998b84ffef27307f9dcc5138ed42605a22b2c141 : verified

(Bukti Verifikasi Folder Data_Login)

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 001-Cyberbullying on Telegram
Evidence Number: 003-Image and Files
Unique Description: Image and Files In telegram
Examiner: Sya Raihan Heggi
Notes: Contains Sent File

Information for C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Files-003\Data-Files-003.ad1:
[Computed Hashes]
MD5 checksum: a5a9d65fead30b158d2e5d85f7769acd
SHA1 checksum: 1e61be41a0d0a1bb2471113a7f7533e3e30dfc85

Image information:
Acquisition started: Sat Oct 16 16:22:46 2021
Acquisition finished: Sat Oct 16 16:23:27 2021
Segment list:
C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Files-003\Data-Files-003.ad1

Image Verification Results:
Verification started: Sat Oct 16 16:23:27 2021
Verification finished: Sat Oct 16 16:23:33 2021
MD5 checksum: a5a9d65fead30b158d2e5d85f7769acd : verified
SHA1 checksum: 1e61be41a0d0a1bb2471113a7f7533e3e30dfc85 : verified

Image Verification Results:
Verification started: Thu Oct 28 01:33:34 2021
Verification finished: Thu Oct 28 01:33:38 2021
MD5 checksum: a5a9d65fead30b158d2e5d85f7769acd : verified
SHA1 checksum: 1e61be41a0d0a1bb2471113a7f7533e3e30dfc85 : verified

(Bukti Verifikasi Folder Data_Files)

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 001-Cyberbullying on Telegram
Evidence Number: 004-Cache Files
Unique Description: Cache and Application File on Telegram
Examiner: Sya Raihan Heggi
Notes: Cache File

Information for C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Cache-004\Data-Cache-004.ad1:
[Computed Hashes]
MD5 checksum: e755677ff003b5401f36ba0b6b5f59dc
SHA1 checksum: dd1cf3f41cd7a3398a25cd93f0c795130aab2cb1

Image information:
Acquisition started: Sat Oct 16 16:27:40 2021
Acquisition finished: Sat Oct 16 16:28:39 2021
Segment list:
C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Cache-004\Data-Cache-004.ad1

Image Verification Results:
Verification started: Sat Oct 16 16:28:42 2021
Verification finished: Sat Oct 16 16:28:56 2021
MD5 checksum: e755677ff003b5401f36ba0b6b5f59dc : verified
SHA1 checksum: dd1cf3f41cd7a3398a25cd93f0c795130aab2cb1 : verified

Image Verification Results:
Verification started: Fri Oct 22 18:55:23 2021
Verification finished: Fri Oct 22 18:55:39 2021
MD5 checksum: e755677ff003b5401f36ba0b6b5f59dc : verified
SHA1 checksum: dd1cf3f41cd7a3398a25cd93f0c795130aab2cb1 : verified

Image Verification Results:
Verification started: Mon Oct 25 12:28:48 2021
Verification finished: Mon Oct 25 12:28:51 2021
MD5 checksum: 232b3fc1b55a19b321d0803a529caa2a : FAILED
SHA1 checksum: 18e9b02d6f381dada28fa69191503b92a64e538a : FAILED

(Bukti Verifikasi Folder Data_Cache)

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 001-Cyberbullying on Telegram
Evidence Number: 005-Deleted Chat
Unique Description: Deleted Chat Content
Examiner: Sya Raihan Heggi
Notes: Deleted Chat

Information for C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Delete Chat- 005\Delete-Chat-005.ad1:
[Computed Hashes]
MD5 checksum: b555b191505ca0eec5d0efeba9d33931
SHA1 checksum: 340b01c42b0eda23b014e5b21397b11d4b497665

Image information:
Acquisition started: Sat Oct 16 16:31:47 2021
Acquisition finished: Sat Oct 16 16:31:47 2021
Segment list:
C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-Delete Chat- 005\Delete-Chat-005.ad1

Image Verification Results:
Verification started: Sat Oct 16 16:31:47 2021
Verification finished: Sat Oct 16 16:31:47 2021
MD5 checksum: b555b191505ca0eec5d0efeba9d33931 : verified
SHA1 checksum: 340b01c42b0eda23b014e5b21397b11d4b497665 : verified

(Bukti Verifikasi Folder Deleted_Chat)

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 001-Telegram Cyberbullying
Evidence Number: 002- New_testing_file
Unique Description: newest testing
Examiner: Sya Raihan Heggi
Notes: Contain Deleted, SS, Chat Files

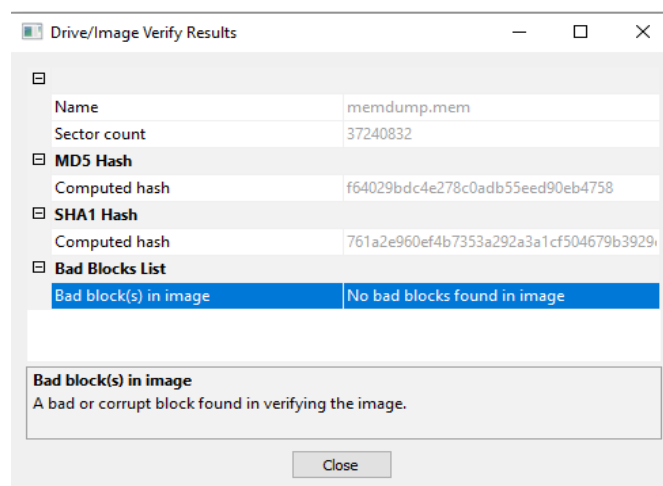
Information for C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-New-Testing-006\006-New-Testing.ad1:
[Computed Hashes]
MD5 checksum: 4d7235e8632c92a9c9f536ebd3bb5d25
SHA1 checksum: 26b268fdeb1b6da024de352eb31dbe3b2b2675e5

Image information:
Acquisition started: Mon Oct 25 13:28:49 2021
Acquisition finished: Mon Oct 25 13:28:49 2021
Segment list:
C:\Users\user\Documents\College Stuff's\PPT Kuliah\Semester 7\Forensik Digital\Pengujian Media Sosial Forensik\Images File\Data-New-Testing-006\006-New-Testing.ad1

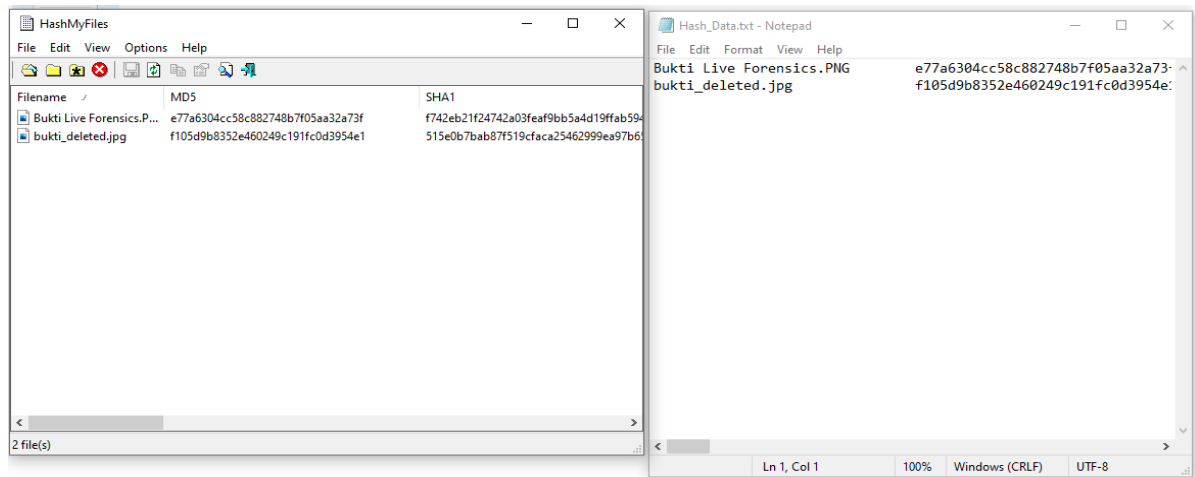
Image Verification Results:
Verification started: Mon Oct 25 13:28:49 2021
Verification finished: Mon Oct 25 13:28:49 2021
MD5 checksum: 4d7235e8632c92a9c9f536ebd3bb5d25 : verified
SHA1 checksum: 26b268fdeb1b6da024de352eb31dbe3b2b2675e5 : verified

Image Verification Results:
Verification started: Thu Oct 28 01:43:51 2021
Verification finished: Thu Oct 28 01:43:51 2021
MD5 checksum: 4d7235e8632c92a9c9f536ebd3bb5d25 : verified
SHA1 checksum: 26b268fdeb1b6da024de352eb31dbe3b2b2675e5 : verified

(Bukti Verifikasi Folder New_Analysis)



(Verifikasi memdump.mem)



(Verifikasi Bukti SS tidak diubah)

BAB 3

KESIMPULAN

Setelah kami menganalisis aplikasi telegram dengan studi kasus cyberbullying dapat disimpulkan sebagai berikut :

- Pelaksanaan kegiatan Digital Forensik pada aplikasi telegram dapat dilakukan dengan 2 metode akuisisi, yang pertama menggunakan metode akuisisi dengan API dan yang kedua menggunakan metode akuisisi manual.
- Perbandingan metode akuisisi dengan API dan metode akuisisi manual secara detail terdapat pada tabel di bawah ini :

Perbedaan	Metode Akuisisi API	Metode Akuisisi Manual
Sistem Operasi	Untuk metode akuisisi dengan API dapat dilakukan di perangkat dengan sistem operasi windows, linux, dan macOS. dikarenakan metode ini merequest data menggunakan bahasa pemrograman python yang bisa dijalankan disemua sistem operasi	Untuk metode akuisisi manual hanya dapat dilakukan di perangkat windows di karenakan FTK Imager hanya mensupport untuk perangkat windows
Kebutuhan Device	Untuk metode akuisisi dengan API data bisa didapatkan dengan cara merequest langsung dari API Telegram.	Untuk metode akuisisi manual data bisa didapatkan melalui device. jika device di lenyapkan tidak dapat dilakukan metode akuisisi manual
Tantangan yang dihadapi	Tantangan yang dihadapi jika menggunakan metode ini adalah untuk menemukan chat_id dari grup yang ditemukan, kemudian bagaimana menjaga integritas dan keutuhan data, dan terakhir pesan yang sudah dihapus tidak dapat ditemukan jika menggunakan API	Untuk menggunakan metode ini jika menggunakan dead forensics ada kemungkinan untuk mendapatkan data lebih banyak, namun masih dikhawatirkan proses pengambilan akan mengganggu integritas dari datanya.
Integritas Data	Untuk menjaga integritas dari data yang diakuisisi sebisa mungkin dilakukan isolasi dari data yang diambil dikarenakan sangat dimungkinkan untuk dilakukan	Untuk integritas data dengan menggunakan metode ini, lebih terjamin karena proses yang dilakukan dapat dibuktikan

	perubahan karena hasilnya disimpan dalam program yang memiliki sifat <i>write data</i> , oleh karena itu dilakukan pembuatan image ad1 untuk analisis dan dibuktikan kembali dengan hash dari data.	dengan nilai hash dan file imagenya.
--	---	--------------------------------------

Dari hasil analisis ini berhasil didapatkan bukti kalimat-kalimat yang masuk ke kategori perundungan kepada korban, selain itu diketahui bahwa memang ada dua buah akun yang memberikan kalimat yang memojokkan korban dari bukti yang dihimpun pelaku memiliki uid 320967145 dan uid 910287747, kemudian untuk pesan yang berusaha untuk dihilangkan oleh pihak perundung dapat diselamatkan dengan metode API dalam jangka waktu 48 jam, jika sudah lewat maka harus melakukan pembacaan cache atau melakukan pembacaan memdump dalam kata lain melakukan *live forensics*.

Selanjutnya dalam studi kasus ini dilakukan pengujian mengikuti kerangka kerja NIJ dimana tahapan yang dilakukan dimulai dari *preservation, collection, examination, analysis*, dan *reporting* dimana penggunaan kerangka kerja ini diharapkan agar pengujian pada studi kasus ini lebih terarah dan lebih baik, serta diharapkan memenuhi kaidah forensik.