IMPLEMENTASI FORENSIK DIGITAL DI TELEGRAM PADA SISTEM OPERASI

DIGITAL FORENSIC IMPLEMENTATION FOR TELEGRAM APPS IN ANDROID OPERATING SYSTEM

Rizky Farras Aushaf [1], Setia Juli Irzal Ismail[2], Gandeva Bayu Satyra[3]

[1,2,3] Universitas Telkom, Bandung
rfarrasa@student.telkomuniversity.ac.id[1], jul@tass.telkomuniversity.ac.id,[2]
gandevabs@staff.telkomuniversity.ac.id[3]

Abstrak : Aplikasi perangkat lunak Instant Messaging adalah sebuah aplikasi pertukaran pesan yang banyak digunakan oleh seluruh lapisan masyarakat. Telegram pun digunakan sebagai media pertukaran pesan sesama pengguna tanpa terhalang batas waktu dan jarak. Telegram adalah salah satu aplikasi layanan pengirim pesan instan multiplatform berbasis awan dan banyak digunakan diseluruh dunia. Aplikasi tersebut sedang ramai digunakan saat ini karena bersifat gratis serta dapat digunakan melalui smartphone dan perangkat komputer. Para pengguna dapat bertukar pesan, foto, video, audio, stiker, dan tipe berkas lainnya. Telegram sering disalah gunakan untuk tindak kejahatan seperti penyebaran pornografi atau kasus cybercrime. Untuk menangani kasus cybercrime tersebut solusinya adalah melakukan forensik digital pada aplikasi Telegram di perangkat tersangka. Dalam contoh kasus kelompok teroris di wilayah Indonesia didapati memakai aplikasi Telegram sebagai alat komunikasi sesama anggota, atas dasar tersebut pengerjaan proyek akhir ini melakukan forensik pada aplikasi pesan instan Telegram dan sebuah perangkat Android dalam proses penyidikan. Dalam melakukan penyidikan, penyidik membuat model untuk menganalisa hasil forensik pada Android yang terdapat artefak atau yang sering disebut Data Remnant. Data Remnant adalah paket yang dihasilkan dari media penyimpanan yang didapat dari Telegram setelah melakukan kegiatan forensik digital terhadap bukti digital berupa artefak tersebut. akan mengatur semuanya dengan kendali melalui tampilan web yang terhubung dengan wifi rumah.

Kata Kunci: Cybercrime, Telegram, Digital Forensik, Data Remnant

***Abstract :** Instant Messaging software application is a messaging application that is widely used by all levels of society. As a medium for exchanging messages among users of the application without being hindered by time and distance limits Telegram is a cloud-based multiplatform instant messenger application that is widely used around the world. This application is being used today because it is free and can be used via smartphones and computer devices. Users can exchange messages, photos, videos, audios, stickers, and other types of files. Telegram also provides end-to-end message exchange. This technology can be misused for crimes such as the spread of pornography or cybercrime cases. Currently, the solution is to conduct digital forensics on cybercrime cases that have occurred. In the case of a terrorist group in Indonesian territory it was found using the Telegram application as a means of communicating among members, on this basis the work on this final project uses the Telegram instant messaging application and an Android device in the investigation process. In conducting an investigation, investigators create a model to analyze forensic results on Android that contain artifacts or what are often called Data Remnants. Data Remnant is a package generated from storage media obtained from Telegram after carrying out digital forensic activities on digital evidence in the form of these artifacts.*

***Keywords:** Cybercrime, Telegram, Digital Forensic, Data Remnant*

1. Pendahuluan

Kapolri Jenderal Pol Tito Karnavian mengatakan, penggunaan aplikasi Telegram oleh kelompok teroris di Indonesia bukan sebuah hal yang mengejutkan. Banyak teroris yang tertangkap mengakui bahwa komunikasi sesama anggota mereka dilakukan melalui aplikasi Telegram. Salah satunya digunakan pada saat kasus terror di kawasan MH Thamrin, Jakarta Pusat, Januari 2016 lalu. Tito mengatakan bahwa aplikasi tersebut menjadi favorit kelompok teroris karena melindungi privasi penggunanya [1]. kasus tersebut dapat di atasi dengan ilmu forensik yang dapat menganalisa barang bukti digital dari perangkat mobile di aplikasi Telegram. Metode yang cocok untuk kasus tersebut ialah dengan menggunakan ilmu forensik pada perangkat Android untuk aplikasi Telegram agar mendapatkan barang bukti digital.

Dalam pasal UU Nomor 19 Tahun 2016 mengenai Informasi dan Transaksi elektronik ("UU ITE") terkandung pada pasal 5 menyebutkan bahwa informasi elektronik atau dokumen elektronik merupakan alat bukti yang sah secara hukum di negara Indonesia [2]. Terkandung dalam pasal 6 informasi elektronik atau dokumen elektronik dianggap sah informasinya bila di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan [3].

Penelitian melakukan Forensik Android pada aplikasi pesan Telegram. Smartphone yang di gunakan ialah Samsung Galaxy K Zoom SM-C11 versi Android 4.1.1. Model penelitian ini, meliputi penggunaan user seperti install, login, memasukan/memperbaharui/menghapus kontak, pertukaran pesan, berbagi lokasi, serta penghapusan komunikasi. Tools yang digunakan memakai software SQLite Browser dan Hex Editor Neo v6.54.01.6478 untuk menganalisis file cache4.db yang jadikan bukti digital dan untuk rooting device menggunakan aplikasi Android Debug tool v1.32, Odin v3.09, ADB Fastboot v1.4.3, CF Auto Root, serta untuk menemukan file db menggunakan aplikasi Root Browser Classic v2.7.9.0.

2. Tinjauan Pustaka

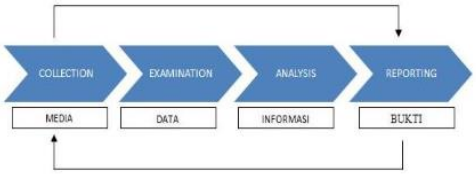
Berikut ini adalah teori yang digunakan dalam penyusunan Proyek Akhir ini.

2.1 Digital Forensik

Digital Forensik ialah sebuah cabang ilmu forensik, untuk penemuan bukti digital dan sering kali dikaitkan dengan kejahatan komputer digital. Awalnya istilah digital forensik ini disebut dengan forensik komputer tetapi kini di perluas untuk semua perangkat yang dapat menyimpan bukti digital. Landasan dari sebuah digital forensik ialah pengumpulan, analisis, dan pembuktian data digital [8].

2.2 NIST (National *Institute of Standards Technology)*

Metode forensic NIST (*National Institute of Standards Technology*) adalah tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan menggunakan metode NIST *(National Institute of Standards Technology).* Transformasi pertama terjadi saat data yang dikumpulkan diperiksa, lalu mengekstrak data dari Media dan mengubahnya menjadi format yang bisa diproses oleh alat forensik. Kedua, data ditransformasikan menjadi informasi melalui analisis.



Gambar 2.1 Tahap Analisa

1. *Collection* adalah pelabelan, identifikasi, rekaman, dan pengambilan data dari sumber data yang relevan dengan prosedur pada tahap analisa untuk menjaga integritas data.
2. *Examination* adalah pengolahan data yang dikumpulkan dalam penggunaan forensik kombinasi berbagai skenario, baik otomatis atau manual, serta menilai dan mengeluarkan data sesuai kebutuhan sambil mempertahankan integritas data.
3. *Analysis* adalah analisis hasil pemeriksaan dengan menggunakan metode teknis dibenarkan dan hukum.
4. *Reporting* adalah melaporkan hasil analisis yang meliputi penggambaran tindakan yang dilakukan.

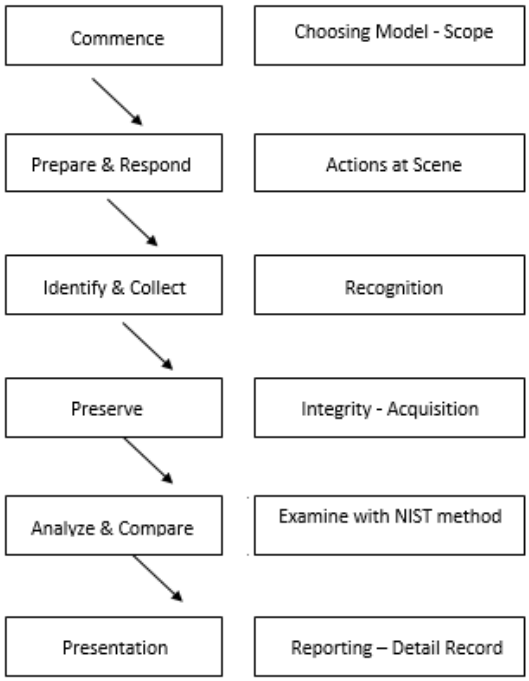
Telegram ialah sebuah aplikasi yang memungkinkan para penggunanya untuk bertukar pesan, menggunakan berbagai skema komunikasi (komunikasi satu ke satu, satu ke banyak, banyak ke banyak), Serta untuk melakukan panggilan suara, menggunakan berbagai teknik penjagaan privasi yang ketat.

Telegram mendukung pertukaran pesan teks (yang isinya teks biasa) dan non teks (digunakan untuk bertukar data dari jenis apa pun, termasuk informasi kontak, koordinat geografis, dan file jenis apapun) [9]

Android adalah sekumpulan software untuk perangkat mobile yang termasuk pada sistem operasi, middleware, dan key applications [10]. Android adalah sistem operasi perangkat mobile *opensource* yang dikembangkan berbasis dari sistem operasi Linux 2.6 dan dikelola oleh OpenHandset Alliance.

3. Analisis dan Perancangan

3.1 Gambaran Sistem Saat Ini



Gambar 3.1 Gambaran Sistem Saat Ini

Gambar 3.1 menunjukkan metodologi penelitian yang digunakan dalam makalah ini. Ini awali dengan 'memulai' yang berarti mendefinisikan lingkup penyelidikan yang akan ditangani. Berikutnya adalah 'mempersiapkan dan merespon' yang merupakan persiapan hardware dan software yang akan digunakan selama penyelidikan. Langkah berikutnya adalah 'mengidentifikasi dan mengumpulkan', identifikasi data yang dapat digunakan sebagai bukti serta koleksi. 'Menyimpan' berarti proses akuisisi dan duplikasi. 'Menganalisa' adalah proses analisis memeriksa data artefak dengan menggunakan metode NIST dari tahap identifikasi. 'Presentasi' adalah tahap penulisan laporan resmi yang akan disajikan dalam sidang.

3.2 Analisis Kebutuhan Sistem

Berdasarkan sistem yang akan dibuat, maka membutuhkan beberapa alat dan bahan berdasarkan fungsionalitas dan non-fungsionalitas, yaitu:

3.2.1 Fungsionalitas

Artefak atau *data remnant* yang ditemukan sebagai barang bukti digital saat proses investigasi berupa file cache4.db di Android yang dapat berguna sebagai laporan akhir hasil investigasi yang akan dibawa oleh penyidik.

3.2.2 Non Fungsional

Pada Bagian ini terdapat dua bagian yaitu *hardware* dan *software*.

3.2.3 Hardware

Hardware yang digunakan saat membuat sistem ini adalah satu buah Android yang akan di jadikan sebagai barang bukti pertama yang akan di investigasi oleh penyidik saat di temukan pada kejadian.

3.2.4 Software

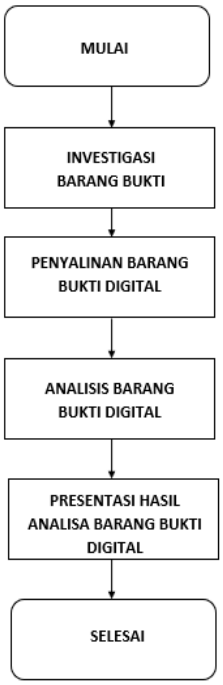
Berikut ini *Software* yang digunakan pada proyek ini adalah sebagai berikut.

Tabel 3.1 Software Yang Di Gunakan

No	Software	Fungsi
1.	Odin v3.09	Sebuah aplikasi yang menjadi penghubung atau komunikasi antara Samsung Galaxy dengan komputer
2.	Android Debug Tool	Sebuah aplikasi agar perangkat Android dapat mengembangkan aplikasi atau perangkatnya
3.	CF Auto Root	Untuk *rooting* perangkat Android melalui aplikasi Odin
4.	SQL DB Browser version 3.8.0	Untuk mendapatkan hasil verifikasi ke aslian dari sebuah file .db yang didapatkan
5.	Windows 10	Sebagai sistem Operasi
6.	Hex Editor Neo v6.54.01	Aplikasi yang dapat melihat pesan yang telah dihapus
7.	Root Explorer version 4.7.1	Untuk mengeksplorasi file sistem Smartphone Android yang telah di berikan akses rooting
8.	Oxygen Forensic v12	Untuk menganalisa sumber barang bukti digital yang perlu di duplikasi.

3.3 Perancangan Sistem

Berikut perancangan system yang dibuat pada Proyek akhir ini:



Gambar 3.2 Perancangan Sistem

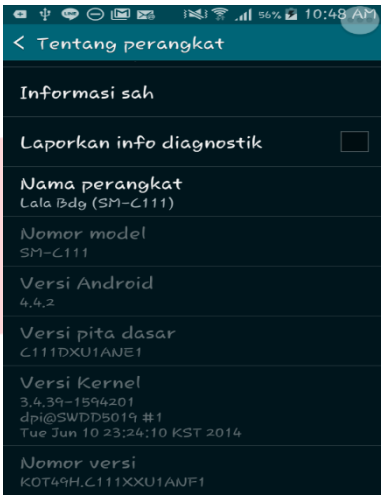
1. Saat menemukan Android sebagai barang bukti yang kita dapatkan, Android tersebut akan dilakukan investigasi terkait bukti digital yang sudah didapatkan sebelumnya
2. Setelah melakukan investigasi dan di dapatkan barang bukti digital chace4.db yaitu, penyalinan barang bukti digital dari Android ke laptop.
3. Dari hasil penyalinan barang bukti digital tersebut, dilakukan analisa terhadap barang bukti digital tersebut.
4. Dari hasil analisa yang telah dilakukan maka masuk ke tahap presentasi hasil analisa.
5. Ketika hasil analisa tersebut telah di presentasikan maka ini adalah langkah terakhir dari investigasi kasus masalah.
6. Selesai

4. IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Berikut ini adalah implementasi dari sistem pengerjaan Proyek Akhir ini

4.1.1 Tampilan Android menggunakan Stock ROM



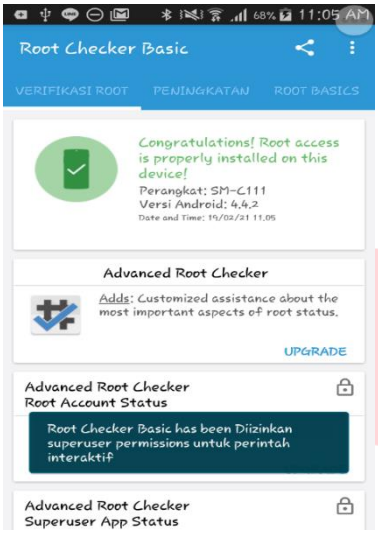
Gambar 4.1 Tampilan Android menggunakan Stock ROM

Pada gambar 4.1 dilakukan tahap percobaan Android menggunakan Stock ROM karena untuk proses rooting tidak diperlukan perubahan ROM menjadi Custom ROM seperti di beberapa *device* lainnya, hal tersebut dikarenakan pada *smartphone* samsung proses rooting dapat dilakukan pada Stock ROM atau ROM orisinil dari *device* itu sendiri.
Langkah rooting pada smartphone Android tersebut ialah:

1. Siapkan software Odin v3.09, ADB Fastboot Tools v1.4.3, dan CF Auto Root.
2. Aktifkan mode USB Debuggin.
3. Buka aplikasi Odin v3.09.
4. Masukan device ke dalam Download Mode lalu sambungkan ke Laptop.
5. Klik AP lalu masukan file CF Auto Root dan klik Start.
6. Proses akan bertulisan Reset tunggu hingga bertulisan Pass maka device

dapat di putuskan dari Laptop dan device sudah diberi akses root.

4.1.2 Tampilan Verifikasi Android Telah Di Beri Akses Root



Gambar 4.2 Tampilan Verifikasi Android Telah Di Beri Akses Root

Pada gambar 4.2 adalah proses verifikasi Android telah diberi akses root. Proses verfikasi menggunakan aplikasi Root Checker yang tersedia di playstore, setelah proses rooting selesai lalu langkah selanjutnya ialah melakukan tahap forensik digital terhadap keseluruhan aktivitas pelaku pada saat penggunaan aplikasi *Telegram*.

4.1.3 Tabel Aktivitas User Untuk Mendapatkan Artefak atau Data Remnant Pada Android

No	*Aktivitas User*	*Data Yang Akan Di Dapatkan*
1	Sign up data	cache4.db
2	Informasi Kontak	cache4.db
3	Pertukaran Pesan	cache4.db
4	Berbagi File	cache4.db
5	Pertukaran pesan yang dihapus	cache4.db

Pada tabel 4.1 didapatkan bahwa untuk mengetahui aktivitas *user* maka perlu didapatkannya data artefak atau *data remnant* yang bernama cache4.db agar dapat di analisa sehingga diketahui aktivitas *user* apa saja yang telah dilakukan melalui aplikasi pesan instan *Telegram*.

4.2 Pengujian

Pengujian pada Implementasi Forensic Digital di *Telegram* Pada Sistem Operasi Android ini dilakukan dengan menggunakan pengujian keseluruhan. Proses pengujian akan dilakukan terhadap semua kebutuhan fungsional yang telah dirancang sebelumnya.

4.2.1 Rencana Skenario Pengujian

Pada rencana pengujian skenario kali ini akun teroris bernama “Rizky Aushaf” akan bertukar pesan dengan akun teroris bernama “RFarrasA”. barang bukti digital diambil melalui Telegram pada akun “Rizky Aushaf “. Sehingga pada tahap analisisnya menggunakan barang bukti digital dari akun “Rizky Aushaf “untuk diketahui isi pertukaran pesan, pesan yang dihapus, dan informasi akun dan kontak yang dimiliki oleh akun “Rizky Aushaf “.

Gambar 4.3 Skenario Pengujian

4.2.2 Pengujian Mendapatkan Barang Bukti Digital

Pada pengambilan atau tahap duplikasi barang bukti dilakukan pengujian untuk menemukan dua cara yaitu pertama dengan aplikasi *root explorer* dan kedua dengan aplikasi *oxygen forensic*. Pada pengambilan barang bukti pun kita mencari cache4.db untuk menemukan database aktivitas *user* selama menggunakan *Telegram*, pengambilan cache4.db berdasarkan hasil analisa menggunakan *oxygen forensic* karena untuk mengetahui informasi *user* itu berada di cache4.db

4.2.2.1 Duplikasi Barang Bukti Digital Melalui Root Explorer

Gambar 4.4 Pengujian Mendapatkan Barang Digital

Pada tahap duplikasi file cache4.db, digunakan aplikasi root explorer dengan direktori data/data/org.*Telegram*.messenger/files/ maka ketika folder files terbuka disitu tertera file cache4.db yang akan kita analisis menggunakan SQL DB Browser seperti gambar dibawah

Gambar 4.5 Pengujian Mendapatkan Barang Bukti Digital

Setelah dilakukan step diatas maka file sudah ditemukan lalu lakukan duplikasi folder org. *Telegram* messenger menjadi org.*Telegram*.messenger.tar. dan pindahkan file tersebut ke dalam *internal storage*.

Pada saat file masuk kedalam *internal storage*, lakukan duplikasi file ke perangkat laptop melalui kabel USB dan inputkan kedalam folder di perangkat laptop yang sudah di sediakan untuk melakukan penelitian.

Gambar 4.6 Pengujian Mendapatkan Barang Digital

Gambar 4.7 Pengujian Mendapatkan Barang Digital

Ketika file org.*Telegram*.messenger.tar.tar sudah di pindahkan atau di duplikasi menuju folder yang sudah disiapkan maka langkah selanjutnya adalah lakukan ekstrak pada file dari hp agar bisa terbuka di aplikasi DB SQL DB Browser untuk mengetahui barang bukti digital yang ada di dalam file tersebut.

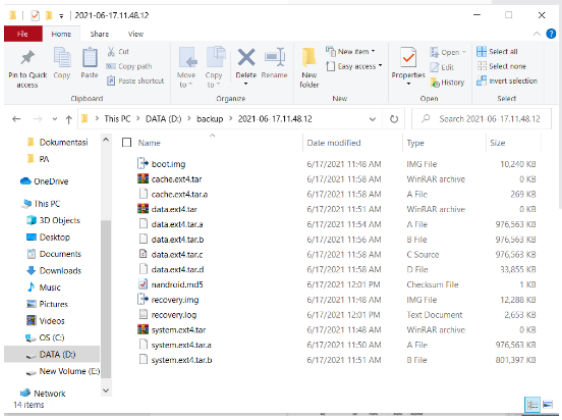
4.2.2.2 Duplikasi Barang Bukti Digital Melalui Oxygen Forensic

Gambar 4.8 CWM Mode

1. Masuk mode cwm dengan mematikan perangkat Android lalu tekan tombol *power+home+volume up*.

2. Arahkan pada bagian backup and restore dengan cara menekan tombol *volume down* lalu tekan tombol *power*, " *volume down* " untuk ke bawah, " volume up " untuk ke atas, dan tombol " power " untuk memilih pilihan.

3. Lalu tentukan penyimpanan *back up* akan disimpan dimana, untuk pengujian ini penulis melakukan penyimpanan pada memori eksternal.

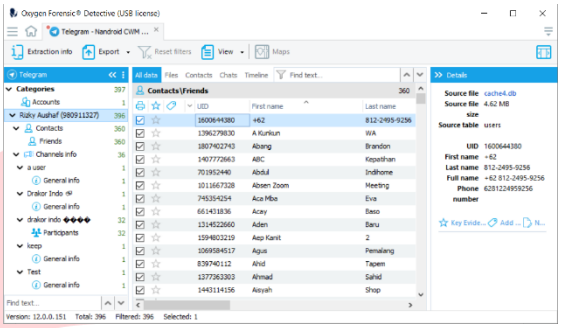


Gambar 4.9 Penyimpanan Back Up CWM

1. Ketika *back up* cwm sudah dilakukan dan sudah masuk ke mode *smartphone* biasa maka selanjutnya adalah sambungkan *smartphone* dengan laptop melalui kabel USB.

2. Lalu cari penyimpanan di *storage* yang sudah ditentukan maka muncul direktori clockworkmod -> *backup* -> dan duplikasi hasil backup sesuai tanggal melakukan *back up*.

3. Simpan pada folder yang sudah ditentukan maka hasilnya akan seperti gambar 4.9



Gambar 4.10 Oxygen Forensic

1. Buka aplikasi *oxygen forensic* lalu pilih *backup import* dan masukan *file* data.ext4.tar.

2. Lalu cari daftar *application* dan klik *Telegram*.

3. Klik bagian *username* pengguna (pada kasus ini username bernama Rizky Aushaf).

4. Maka sesuai gambar 4.2.2.3 muncul tulisan *source file* atau sumber *file*.

5. Klik pada bagian cache4.db lalu *save to* dan arahkan pada folder yang sudah disiapkan.

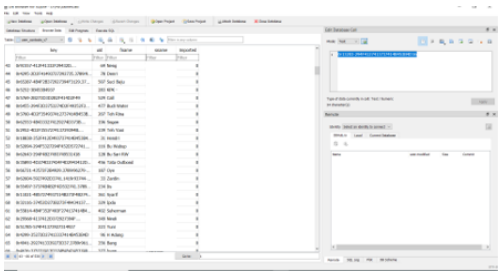
4.2.3 Pengujian Hash

Fungsi hash dalam kriptografi memiliki fungsi dalam autentikasi pesan, hash dirancang untuk melindungi pesan yang sudah di hash dan mengembalikan teks aslinya. Hash ini di cek menggunakan aplikasi yang bernama FTK yang berfungsi untuk melakukan preview dan pembuatan image lalu melakukan pengecekkan melalui *properties* pada file cache4.db dan melalui *command prompt* (CMD)

Hasil dari pengujian hash ini ialah nilai md5 dan sha1 itu sama yaitu "a191173f0fc39dfde54a45f15d96dc7c" sehingga hasil dari pengujian ini adalah dibuktikan bahwa barang bukti digital antara user tidak ada yang dirubah semenjak proses

duplikasi dari perangkat android ke perangkat laptop

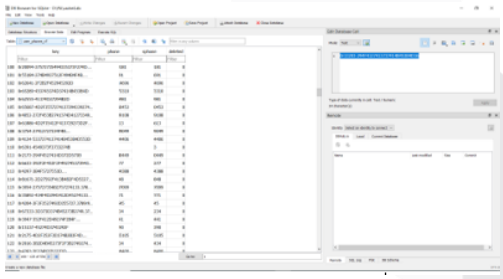
4.2.4 Tampilan Informasi Kontak Tersimpan



Gambar 4.11 Tampilan Nama Informasi Kontak

Pada gambar 4.12 diketahui bahwa kontak siapa saja yang disimpan oleh *user* dan nama tersebut merupakan nama yang disimpan oleh *user* melalui penyimpanan kontak telepon.
Berikut langkah – langkah untuk mengetahui informasi nama kontak:

1. Buka aplikasi DB SQLite Browser.
2. Duplikasi file cache4.db dari perangkat Android ke laptop.
3. Pada aplikasi DB SQLite Browser menuju *open database* lalu buka *file* cache4.db.
4. Tekan *browse data* lalu telusuri tabel pada bagian *user_contact_v7*. Tercantum informasi nama kontak yang disimpan oleh *user*.

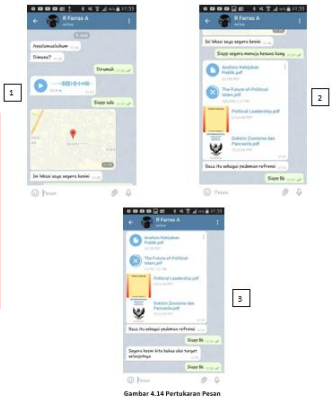


Gambar 4.12 Tampilan Nomor Telepon Kontak

Pada gambar 4.13 tabel *user_phones_v7* terdeteksi nomor telepon kontak yang tersimpan, nantinya dicocokan dengan tabel *user_contacts_v7* melalui *key* sehingga diketahui nama dan nomor telepon target.
Berikut langkah – langkah untuk mengetahui informasi nomor telepon kontak:

1. Buka aplikasi DB SQLite Browser.
2. Duplikasi file cache4.db dari perangkat Android ke laptop.
3. Pada aplikasi DB SQLite Browser menuju *open database* lalu buka *file* cache4.db.
4. Tekan *browse data* lalu telusuri tabel pada bagian *user_phones_v7*. Tercantum informasi nama kontak yang disimpan oleh *user*.

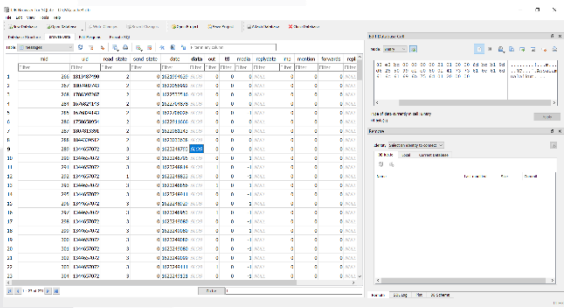
4.2.5 Pengujian Pertukaran Pesan



Gambar 4.13 Pertukaran Pesan

Pada Gambar 4.6 adalah pengujian pertukaran pesan yang dilakukan antar user melalui aplikasi *Telegram* untuk mengetahui apakah user mengirim atau menerima pesan yang terdapat sesuatu mencurigakan sesuai dengan alur dari gambar diatas.

4.2.5.1 Tampilan Pertukaran Pesan



Gambar 4.14 Tampilan Isi Pesan Masuk

Pada gambar 4.15 diketahui bahwa *user* melakukan pertukaran pesan dengan siapa saja dan apa isi pesan dari pertukaran pesan *user* tersebut, agar diketahui user melakukan pesan dengan siapa saja kita tinggal mencocokan kolom *uid* pada tabel *messages* dengan kolom *uid* pada tabel *users*. Untuk mengetahui pesan keluar dengan pesan masuk pada kolom out jika value itu “0” maka artinya pesan masuk kepada user lain dan apabila value itu “1” maka user tersebut mengirimkan kepada user lain.
Berikut langkah – langkah untuk mengetahui

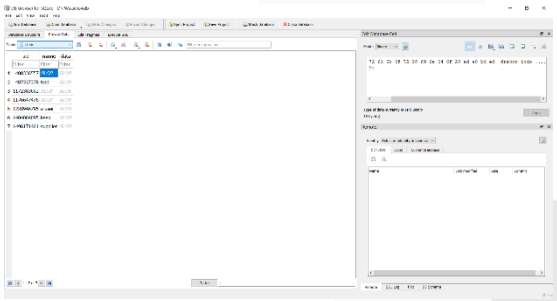
pertukaran pesan:

1. Buka aplikasi DB SQLite Browser.
2. Duplikasi file cache4.db dari perangkat Android ke laptop.
3. Pada aplikasi DB SQLite Browser menuju *open database* lalu buka *file* cache4.db.
4. Tekan *browse data* lalu telusuri tabel pada bagian *messages*. Tercantum mulai dari isi pesan, bertukar pesan dengan siapa, dan pesan keluar masuk.

Tabel 4.2 Pengujian Pertukaran Pesan

R Farras A				Risky Aushaf			
mid	uid	Waktu dan Tanggal	data	mid	uid	Waktu dan Tanggal	data
289	1344657072	Rabu, 9 Juni 2021 9:26:33	Assalamualaikum				
290	1344657072	Rabu, 9 Juni 2021 9:26:35	Dimana?	291	980911327	Rabu, 9 Juni 2021 9:26:54	Dirumah
292	1344657072	Rabu, 9 Juni 2021 9:27:13	(Mengirim pesan suara (audio/ogg))	293	980911327	Rabu, 9 Juni 2021 9:27:36	Siapp ada
295	1344657072	Rabu, 9 Juni 2021 9:28:31	(Mengirim lokasi)				
296	1344657072	Rabu, 9 Juni 2021 9:28:49	Ini lokasi saya segera kesini	297	980911327	Rabu, 9 Juni 2021 9:27:36	Siapp segera menuju kesana kang
298	1344657072	Rabu, 9 Juni 2021 9:31:20	(mengirim file pdf) Analisis Kebijakan Publik.pdf				
299	1344657072	Rabu, 9 Juni 2021 9:31:20	(mengirim file pdf) The Future Of Political Islam.pdf				
300	1344657072	Rabu, 9 Juni 2021 9:31:20	(mengirim file pdf) Political Leadership.pdf				
301	1344657072	Rabu, 9 Juni 2021 9:31:20	(mengirim file pdf) Doktrin Zionisme dan				
302	1344657072	Rabu, 9 Juni 2021 9:31:39	Baca itu sebagai pedoman refrensi	303	980911327	Rabu, 9 Juni 2021 9:31:51	Siapp 86
304	1344657072	Rabu, 9 Juni 2021 9:32:11	Segera kesini kita bahas aksi target selanjutnya	305	980911327	Rabu, 9 Juni 2021 9:32:21	Siapp 86

Pada tabel 4.2 merupakan hasil analisa percakapan yang telah disusun sesuai hari dan waktu pengiriman, *message id* (mid), *user id* (uid), dan isi teks percakapan pesan

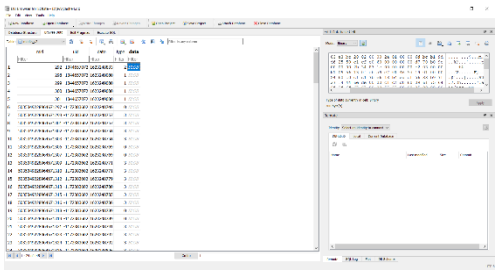


Gambar 4.15 Informasi Pertukaran Pesan

Pada gambar 4.16 diketahui bahwa *user* menerima pesan masuk atau mengikuti *group* apa saja pada aplikasi *Telegram*.

Berikut langkah – langkah untuk mengetahui *group chat*:

1. Buka aplikasi DB SQLite Browser.
2. Duplikasi file cache4.db dari perangkat Android ke laptop.
3. Pada aplikasi DB SQLite Browser menuju *open database* lalu buka *file* cache4.db.
4. Tekan *browse data* lalu telusuri tabel pada bagian *chats*. Tercantum *user* mengikuti *group* atau *group* apa saja yang *user* terima pesan masuknya



Gambar 4.16 Pertukaran Pesan Media

Pada gambar 4.17 tabel *media_v2* terlihat isi pesan yang mengirimkan sebuah *audio* atau *voice note* dan melalui *uid* akan diketahui pada percakapan siapa isi pesan tersebut muncul. Kolom type pun diketahui bahwa tiap tipe tipe media memiliki *value* masing – masing salah satu contohnya tipe dengan *value* “2” artinya user menerima *voice note*.

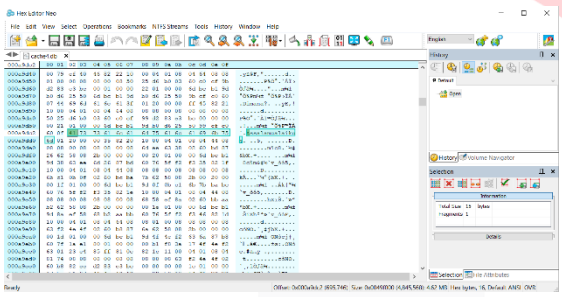
Berikut langkah – langkah untuk mengetahui penerimaan pesan *media*:

1. Buka aplikasi DB SQLite Browser.
2. Duplikasi file cache4.db dari perangkat Android ke laptop.
3. Pada aplikasi DB SQLite Browser menuju *open database* lalu buka *file* cache4.db.
4. Tekan *browse data* lalu telusuri tabel pada bagian *media_v2*. Tercantum *user* menerima pesan media apa saja.

4.2.6 Tampilan Pertukaran Pesan di Hapus

Pada pertukaran pesan di hapus terdapat isi pesan seperti pertukaran pesan media contohnya file “ Analisa Kebijakan Publik.pdf “ dan isi pesan “ Segera kesini kita bahas aksi target selanjutnya “ pada smartphone pesan tersebut tidak ada namun setelah di analisa cache4.db isi pesan tersebut didapatkan

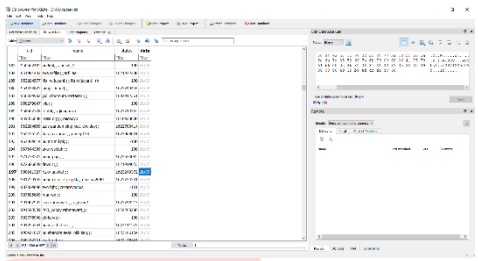
Gambar 4.17 Pertukaran Pesan Di Hapus



Gambar 4.18 *Tampilan isi chat pada akun user dan akun R Farras A*

Pada tampilan gambar 4.19 terlihat bahwa *user* menghapus pesan dengan akun R Farras A sehingga pada akun *user* dan akun R Farras A history pesan tersebut sudah hilang. Terlihat bahwa isi *chat* telah dihapus oleh *user* saat bertukar pesan dengan akun R Farras A dengan asumsi kita mengetahui *clue* isi pesan tersebut.
Berikut langkah – langkah untuk mengetahui pertukaran pesan yang dihapus:

1. Buka aplikasi DB SQLite Browser.
2. Duplikasi file cache4.db dari perangkat Android ke laptop.
3. Pada aplikasi DB SQLite Browser menuju *open database* lalu buka *file* cache4.db.
4. Tekan *browse data* lalu telusuri tabel pada bagian *messages*. Tercantum mulai dari isi pesan, bertukar pesan dengan siapa, dan pesan keluar masuk.
5. Buka aplikasi Hex Editor Neo.
6. Buka *file* cache4.db pada aplikasi Hex Editor Neo.
7. Temukan atau telusuri kata kunci atau *clue* dari salah satu isi pesan tersebut.



Gambar 4.19 Tampilan Data Sign Up Data

Pada gambar 4.20 didapatkan bahwa untuk mengetahui data *sign up user* untuk diketahui *username* dan nomor telepon yang terdaftar pada aplikasi *Telegram* tabel *users*.
Berikut langkah – langkah untuk mengetahui informasi *sign up*:

1. Buka aplikasi DB SQLite Browser.
2. Duplikasi file cache4.db dari perangkat Android ke laptop.
3. Pada aplikasi DB SQLite Browser menuju *open database* lalu buka *file* cache4.db.
4. Tekan *browse data* lalu telusuri tabel pada bagian *users*. Tercantum mulai dari *username*, dan nomor telepon.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil pengujian pada BAB 4 dapat diambil kesimpulan sebagai berikut.

1. Hasil penerapan metode Android forensik yang dilakukan barang bukti dapat ditemukan *file* cache4.db terletak pada direktori yang sama dan diperlukannya akses *root* agar *file* cache4.db tersebut dapat ditemukan, pada saat proses *rooting* diperlukan langkah yang hati-hati, karena apabila *device* Android ingin di root melalui *software* seperti Odin, Super SU, King Root, dan lain-lain. Bila terjadi salah langkah dapat menyebabkan *bootloop* atau mati total.

2. Setelah dilakukan investigasi, hasil identifikasi file barang bukti digital dan analisa telah berhasil dilakukan. data tidak ada yang dirubah oleh user sehingga ketika identifikasi file berlangsung tidak ditemukan kejanggalan data yang diambil dari aplikasi *Telegram*.

5.2 Saran

Dari hasil pengerjaan Proyek Akhir ini, saran untuk yang ingin mengerjakan Proyek Akhir yang sama maka haruslah membuat suatu perbedaan seperti metode pengerjaan atau penambahan temuan investigasi dari aktivitas user seperti *sharing location*, gambar, video, kontak terhapus, dan lain-lain.

REFERENSI

[1] Ambaranie Nadia Kemala Movanita, "Teroris Pengguna Telegram, Kasus Bom Thamrin hingga Penusukan Polisi di Masjid Falatehan," *Kompas.com*, 2017. https://nasional.kompas.com/read/2017/07/16/09033181/teroris-pengguna-telegram-kasus-bom-thamrin-hingga-penusukan-polisi-di?page=all. 2020-05-09

[2] Republik Indonesia, "Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Lembaran Negara Republik Indones. Tahun 2016 Nomor 251*, pp. 1689–1699, 2016.

[3] K. H. D. H. A. M. R. Indonesia, "Undang Undang ITE," *Kemenkeu*, 2018. https://jdih.kemenkeu.go.id/fulltext/2008/11tahun2008uu.htm#:~:text=Setiap Orang dengan sengaja dan,menyebabkan perubahan apa pun maupun. 2020-05-09

[4] G. B. Satrya, P. T. Daely, M. Arief, and M. A. Nugroho, "Digital Forensic Analysis of Telegram Messenger on Android Devices Creative Capstone Design Using LoRa Wireless Communication View project Color Temperature Varying LED StreetLight and Control/Monitoring SW Development using Weather Big Data View project Digital Forensic Analysis of Telegram Messenger on Android Devices," *ieeexplore.ieee.org*, doi: 10.1109/ICTS.2016.7910263.

[5] I. S. Wijaya, H. Riadi, "Analisis Forensik Digital Aplikasi Telegram," *Semantikom*, pp. 95–98, 2017.

[6] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, "Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST," *J. Repos.*, vol. 2, no. 10, pp. 1400–1405, 2020, doi: 10.22219/repositor.v2i10.1066.

[7] I. G. N. Guna Wicaksana and I. K. Gede Suhartana, "Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 8, no. 4, p. 381, 2020, doi: 10.24843/jlk.2020.v08.i04.p03.

[8] J. Lyle, "DIGITAL FORENSIC RESEARCH CONFERENCE Testing Disk Imaging Tools." Accessed: Apr. 20, 2020. [Online]. Available: http://www.cftt.nist.gov/. 2020-04-20

[9] "What can you do with Telegram?" https://telegram.org/. 2020-05-09

[10] A. Cochereau, "A Developer's First Look At Android," *Soins. Pediatr. Pueric.*, no. 257, p. 8, 2008, [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/21180188.

[11] "Samsung Galaxy K Zoom," *Amazon.co.uk*. https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.amazon.co.uk%2FSamsung-Galaxy-SM-C115-Smartphone-Version%2Fdp%2FB00W8NYU6M&psig=AOvVaw36IfkbHkLq5h-n0ggGsykT&ust=1622015654362000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCLCf6qyt5PACFQAAAAAdAAAAABAP.