Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android Menggunakan metode NIST

Feryan Lutfie Nafila

17917207

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Digital Forensik

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2022

Lembar Pengesahan Pembimbing

Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android Menggunakan metode NIST

Feryan Lutfie Nafila

17917207

Yogyakarta, September, 2021

Pembimbing 1	Pembimbing 2
Dr. Ir. Bambang Sugiantoro, S.SI., MT.	Dr. Yudi Prayudi, S.Si., M.Kom.

Lembar Pengesahan Penguji

Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android Menggunakan metode NIST

Feryan Lutfie Nafila

17917207

Yogyakarta, Februari, 2022

Tim Penguji,

Dr. Ir. Bambang Sugiantoro, S.SI., MT.
Ketua

Dr. Yudi Prayudi, S.Si., M.Kom.
Anggota I

Dr. Imam Riadi, S.Pd., M.Kom.
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android Menggunakan metode NIST

Aplikasi pesan singkat saat ini sudah menjadi bagian yang melekat pada masyarakat saat ini, kemudahan dalam berkomunikasi serta berbagai fitur yang disediakan oleh aplikasi pesan singkat berbasis online ini menjadi daya tarik tersendiri. Selain fitur, keamanan dan privasi hal yang penting bagi pengguna. Keamanan dan privasi ini menjadi penting karena beberapa pengguna aplikasi ini menjadi khawatir dengan data pesan yang mereka kirimkan akan disalahgunakan oleh perusahaan penyedia aplikasi pesan tersebut. Kekhawatiran ini semakin tinggi setelah aturan baru yang dikeluarkan oleh sebuah perusahaan aplikasi pesan singkat popular dimana data dari aplikasi pesan akan dihubungkan dengan aplikasi lain untuk keperluan bisnis perusahaan, Beberapa pengguna messenger populer merasa khawatir akan privasi mereka dan memilih untuk beralih ke aplikasi pesan online lain yang dirasa lebih aman dan menawarkan privasi. Salah satu aplikasi yang menjadi pilihan adalah Signal Messenger. Aplikasi pesan singkat ini dianggap lebih aman dalam menjaga privasi. Hal ini menjadi perhatian dimana aplikasi yang dianggap lebih menawarkan privasi ini bisa menjadi sarana untuk melakukan tindak kejahatan. Dengan mempertimbangkan hal tersebut, makan karya penelitian difokuskan untuk melakukan pengujian dan analisa forensik terhadap aplikasi Signal Messenger berbasis android. Pengujian akan dilakukan pada perangkat smartphone SMA530F dan Redmi Note 4. Skenario yang akan dilakukan dengan pemasangan aplikasi Signal Messenger pada setiap smartphone, kemudian dilakukan komunikasi chat antara kedua smartphone tersebut seperti mengirim pesan teks, gambar, dan video. Dari aktivitas tersebut dilakukan tahap mobile forensik menggunakan metode NIST. Metode ini dipilih karena tahap-tahap dalam melakukan akuisisi dan proses analisa untuk mendapatkan bukti digital lebih mudah diterapkan. Hasil pengujian diharapkan bisa menjadi referensi pihak berwenang maupun pihak terkait apabila terdapat suatu kasus dengan menggunakan aplikasi Signal Messenger. Dan diharapkan dengan adanya penelitian ini bisa menambah kepustakaan dibidang ilmu digital forensik khususnya mobile forensik.

Kata kunci

Mobile forensik, Signal Messenger, Android, Smartphone.

Abstract

Digital Artifact Analysis Signal Messenger Aplication on Android Using NIST Method

Message applications have now become a part of today's society. Beside from features, security and privacy are important things for users. Security and privacy are important because some users of this application are worried if the message their send will misused by the company. This concern is heightened after a new rule issued by a popular instant messaging application company where data from the messaging application will be linked to other applications for business purposes, some popular messenger users are worried about their privacy choosing to switch to other messaging applications that are considered more secure and offers privacy. One of the applications of choice is Signal Messenger becouse this application is more secure in maintaining privacy. This is a concern if applications that offer more privacy become a means to commit crimes. Consider that, the research work will focused on conducting forensic testing and analysis of the Android-based Signal Messenger application. The test will carried out on SMA530F and RedmiNote 4 smartphone devices. The scenario that will applied is by installing the Signal Messenger application on each smartphone, then communication between the two smartphones is such as sending text messages, images, and videos. From these activities, the mobile forensics stage using the NIST. Metode ini dipilih karena tahap-tahap dalam melakukan akuisisi dan proses analisa untuk mendapatkan bukti digital lebih mudah diterapkan. This method has been choosen because it easy to apply for acquisition dan for analys process to get digital evidence. The test results will be expect for a reference for the authorities and related parties if there is a case using the Signal Messenger application and it is hoped that this research can add to the literature in the field of digital forensics, especially mobile forensics.

Keywords

Mobile forensic, Signal Messenger, Android.

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Februari, 2022

Feryan Lutfie Naflla, S.Kom.

Halaman Kontribusi

Kontribusi dari pihak terkait dalam penyelesaian penulisan tesis ini:

1. Bapak Dr. Bambang Sugiantoro, MT selaku Pembimbing I, Bapak Yudi Prayudi, S. Si., M. Kom selaku pembimbing II dan Bapak Dr. Imam Riadi, S.Pd., M.Kom. selaku dosen penguji yang telah memberikan arahan serta bimbingan sehingga penulisan tesis ini dapat terselesaikan dengan baik
2. Ibu dan Bapak yang selalu memberi dukungan dalam setiap tahap penulisan tesis ini.
3. Mbak Asti yang turut memberi motivasi dalam proses pembuatan tesis ini.

Halaman Persembahan

Alhamdulillahirobbil'alamin.

Karya ini saya persembahkan kepada kedua orang tua saya. Ibu saya Cucu Purwanti dan Ayah saya Aris Taryana, yang selalu memberi dukungan dan tidak pernah menyerah untuk selalu mensupport saya bahkan disaat paling akhir. Untuk keluarga dan teman-teman yang selalu memberikan dukungan, terimakasih atas kerja keras dan waktu yang telah dicurahkan untuk membantu, memotivasi, dan selalu memberi dukungan.

Kata Pengantar

Penulis ucapkan rasa syukur kepada ALLAH SWT yang selalu memberikan rahmat sehat dan keselamatan sehingga saya dapat menyelesaikan tugas tesis dengan judul: "ANALISIS DIGITAL ARTIFAK APLIKASI SIGNAL MESSENGER PADA SISTEM OPERASI ANDROID MENGGUNAKAN METODE NIST" sebagai persyaratan untuk mencapai gelar Magister Teknik Informatika pada program Pasca Sarjana Universitas Islam Indonesia. Pada kesempatan ini saya haturkan ucapan terima kasih yang tak terhingga kepada Ibu Cucu Purwanti, Bapak Aris Taryana, Keluarga serta Teman-teman saya yang selalu memberikan dukungan dan doa. Di samping itu, secara khusus penulis ucapkan terima kasih yang sebesar- besarnya

kepada:

1. Bapak Yudi Prayudi, S.Si., M.Kom, selaku Ketua PUSFID Fakultas Teknologi Industri Universitas Islam Indonesia Yogyakarta sekaligus Pembimbing yang telah dengan sabar membimbing saya.
2. Bapak Dr. Bambang Sugiantoro, MT, sekalu Pembimbing, terimakasih atas arahan dan bimbingannya.
3. Bapak Dr. Imam Riadi, M. Kom selaku dosen penguji, terima kasih atas segala bantuan dan masukan sehingga tulisan ini bisa tersusun dengan baik.
4. Seluruh Dosen dan Staff Universitas Islam Indonesia Yogyakarta khususnya Fakultas Teknologi Industri.
5. Teman-teman mahasiswa Digital Forensik angkatan 2017, khususnya kepada sahabat saya Rifqi, Tommy, dan Ira atas segala dukungan.
6. Semua pihak yang telah membantu penulis selama penyusunan karya ini baik secara langsung maupun tidak langsung.

Semoga Allah SWT senantiasa memberikan rahmat serta anugerah-Nya yang berlimpah kepada kita semua, penulis menyadari bahwa dalam penulisan karya ini masih terdapat banyak sekali kekurangan, oleh karena itu semua saran dan kritik dari pembaca selanjutnya diharapkan, Akhirnya harapan penulis adalah semoga penulisan tesis ini dapat bermanfaat dalam bidang ilmu pengetahuan kedepannya.

Daftar Isi

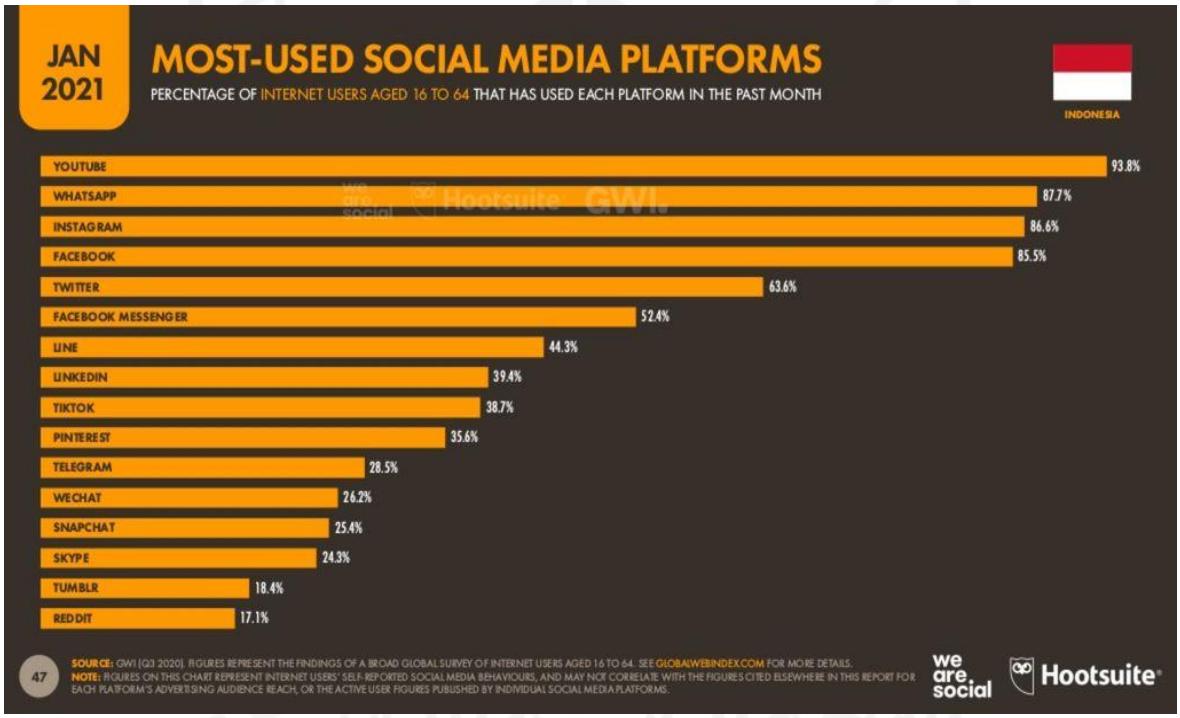
Daftar Tabel

Daftar Gambar

BAB 1
Pendahuluan

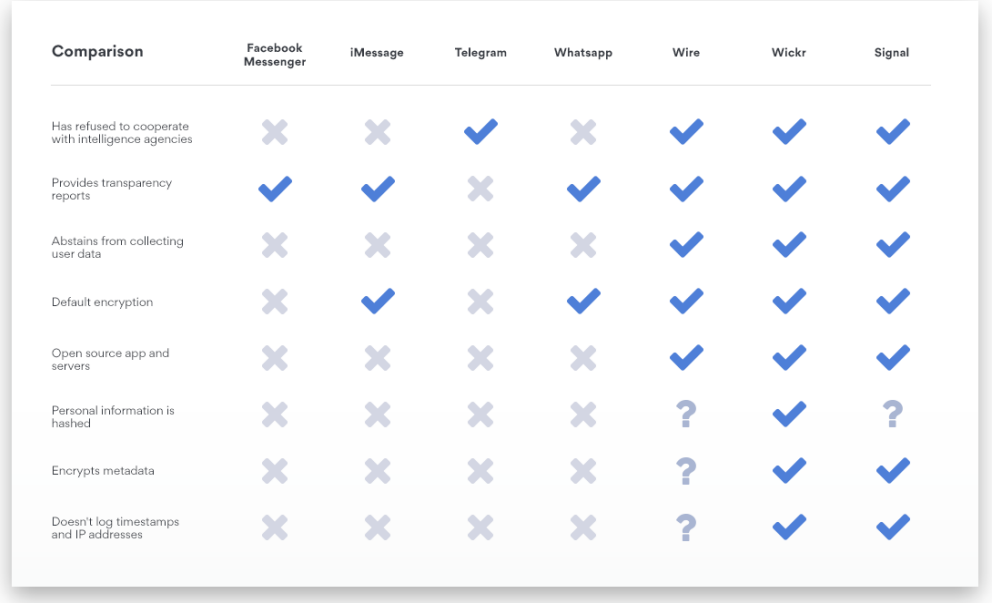
1.1 Latar Beakang

Penggunaan aplikasi pesan singkat berbasis online saat ini sudah menjadi salah satu kegiatan sehari-hari, selain menawarkan kemudahan dalam berkomunikasi berbagai fitur yang disediakan oleh beragam aplikasi pesan singkat online menjadi daya tarik aplikasi ini. Dari beberapa aplikasi media sosial yang popular di Indonesia, khususnya messenger aplikasi Whatsapp menempati posisi teratas pengguna di Indonesia.



Gambar 1.1 Statistik Penggunaan Sosial Media

Namun setelah keluarnya kebijakan baru dari aplikasi Whatsapp tentang kebijakan privasi, beberapa pengguna mulai mempertimbangkan penggunakan aplikasi *messenger* lain karena merasa khawatir dengan privasi mereka seperti aplikasi messenger Signal yang lebih menawarkan privasi. Dikutip dari artikel VoI "Menurut laporan, jumlah peningkatan pengunduh *Signal* menjadi 2 juta per hari setelah sebelumnya hanya 20 ribu per hari sebagaimana yang dilansir dari *App Figures*, Selasa, 26 Januari. Menurut catatan data, pengunduh baru aplikasi *Signal* paling banyak bersumber dari Indonesia dan India."



Gambar 1.2 Perbandingan Keamanan Aplikasi Messenger

Meningkatnya penggunaan aplikasi messenger yang menawarkan keamanan dan privasi menjadi bukti kekhawatiran para pengguna aplikasi messenger terhadap privasi mereka dalam menggunakan aplikasi messenger tersebut. Di sisi lain, semakin tinggi tingkat privasi sebuah aplikasi maka semakin sedikit pula hal yang bisa dibuka atau diungkap, hal ini menjadi perhatian bila mana aplikasi yang menawarkan privasi ini dimanfaatkan oleh seseorang untuk melakukan kejahatan sehingga akan menyulitkan bagi seorang penyidik untuk menggali bukti yang terdapat pada aplikasi messenger tersebut.

Permasalahan yang akan dibahas di dalam penelitian ini adalah bagaimana sebuah proses forensik khususnya mobile forensik dalam rangka mencari jejak digital yang terdapat pada aplikasi Signal Messeger dengan menggunakan metode National Institute of Standard and Technology (NIST) sehingga jejak digital tersebut bias dijadikan barang bukti dalam sebuah kasus.

1.2 Rumusan Masalah

Dengan melihat latar belakang yang telah diuraikan diatas maka peneliti akan menjabarkan beberapa rumusan masalah sebagai berikut:

a. Bagaimana penerapan metode NIST untuk memcari bukti digital pada aplikasi messenger Signal

b. Jejak digital apa sajakah yang ditinggalkan oleh aplikasi messenger Signal setelah dilakukan aktifitas forensic

1.3 Batasan Masalah

Fokus pembahasan dalam penelitian ini adalah kejahatan melalui instant messenger dalam aplikasi Instant messenger Signal versi 5.27.13 pada perangkat Android.

1.4 Tujuan Penelitan

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah:

a. Mendapatkan data melalui proses forensik dan akusisi dari smartphone menggunakan tools forensik.
b. Mengenali dan menemukan data pada direktori Instant Messanger Signal.

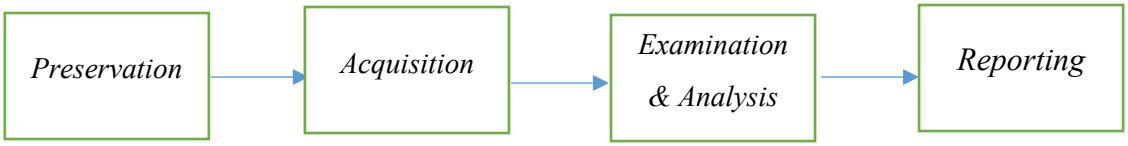
1.5 Manfaat Penelitian

Berdasarkan uraian pada latar belakang dan rumusan masalah, adapun manfaat dari penelitian ini adalah:

a. Menemukan barang bukti digital pada aplikasi messenger Signal
b. Menjadi referensi penggunaan tools yang dibutuhkan
c. Untuk menambah kepustakaan dibidang ilmu digital forensik khususnya mobile forensik.

1.6 Metodologi

Metode yang diajukan didalam penelitian ini menggunakan metode National Institute of Standard and Tecnology (NIST) sebagai dasar penelitian. Metode ini mempunyai empat tahapan proses yaitu *Preservation, Acquisition, Examination & Analysis,* dan *Reporting*.



Gambar 1.3 Alur Metode NIST

a. Preservation

   Dalam tahap ini dilakukan persiapan apa saja yang menjadi kebutuhan untuk melakukan proses analisa forensik. Seperti mempersiapkan barang bukti yang akan dianalisa, *Tools* yang akan dipakai atau diperlukan, serta alat-alat untuk melakukan dokumentasi.

b. Acquisition

   Dalam tahap ini dilakukan proses persalinan atau *imaging* terhadap ponsel pintar yang menjadi barang bukti menggunakan *tools* yang telah dipersiapkan. Tujuan dari proses persalinan ini adalah untuk melindungi keutuhan atau integrasi dari barang bukti pada saat melakukan pemeriksaan lebih lanjut terhadap barang bukti tersebut. Salinan tersebut kemudian disertai nilai hash untuk memastikan bahwa salinan ini sama dengan yang asli sesuai apa yang terdapat dalam barang bukti.

c. Examination & Analysis

   Dalam tahap ini selanjutnya proses pemeriksaan dan analisis dilakukan. Pemeriksaan diperlukan untuk mengidentifikasi keterkaitan suatu barang bukti dengan kasus yang sedang ditangani. Kemudian hasil dari pemeriksaan tersebut dikumpulkan untuk selanjutnya ditarik sebuah kesimpulan.

d. Reporting

   Setelah semua tahapan dan prosedur dijalankan dengan benar, kemudian dibuat laporan hasil.

1.7 Review Penelitian

Pada bagian ini peneliti memberikan ulasan terkait beberapa penelitian yang berhubungan dengan *Instant Messenger*. Penelitian diawali oleh (Umar et al., 2018) dimana dilakukan penelitian tentang aplikasi messenger Whatsapp. Peneliti membandingkan dan mengevaluasi alat forensik dalam menangani aplikasi tersebut. (Muhammad Kukuh Tri Haryanto, 2018) Meneliti tentang penggunaan aplikasi messenger IMO yang berpotensi untuk digunakan sebagai sarana tindak kejahatan seperti *cyber stalking, sextortion, drug trafficking*. Dimana peneliti memberikan gambaran bagaimana mengakuisisi dan analisa filefile yang bisa dijadikan bukti pada suatu kejahatan. (Praset yo Aji et al., 2018) Menyajikan studi dan teknik kemampuan tools pada aplikasi LINE messenger dengan menggabungkan metode VV dan metode forensik standar NIST. (Choi et al., 2017) menguji fitur keamanan yang terdapat pada aplikasi messenger KakaoTalk menggunakan teknik reverse engineering. Peneliti mengungkapkan prosedur pembuatan kunci dan struktur

database obrolan yang digunakan. Temuan peneliti pada prosedur pembuatan kunci menunjukkan bahwa file cadangan terenkripsi dapat bocor ke penyerang menggunakan teknik tersebut. (Fadillah et al., 2018) Penelitian ini berfokus pada layanan pembayaran melalui smartphone seperti Gopay, OVO, dan telkomsel cash. Penelitian menggunakan metode analisis forensik berdasarkan pedoman forensik perangkat mobile yang dibuat oleh National Institute of Justice (NIJ). Peneliti menguji beberapa tools sebagai bahan penelitian.

Tabel 1.1 Perbandingan Penelitian

Peneliti	**Objek Penelitian**	**Metode**	**Tools**	**Hasil Penelitian**
(Umar et al., 2018)	WhatsApp	NIST	WhatsApp Key/DB Extractor, Belkasoft Evidence (ver trial), SQLite Studio	Meneliti tentang messenger yang sangat popular yaitu whatsapp. Keamanan aplikasi whatsapp ini selalu mendapat pembaharuan untuk memastikan keamanan pada aplikasi. Teknologi keamanan yang diperkenalkan adalah teknologi enkripsi terbaru yaitu enkripsi end-to-end. Peneliti berkesperimen menggunakan metode forensik NIST untuk mengekstrak artefak whatsapp.
(Fadillah et al., 2018)	Gopay, OVO, TCash	NIJ, NIST	Forensic Autopsy	Penelitian ini berfokus pada layanan pembayaran melalui smartphone seperti Gopay, OVO, Dan telkomsel cash. Penelitian menggunakan metode analisis.
(Muhammad Kukuh Tri Haryanto, 2018)	IMO	NIST	SQLiteman, SQLite Record. Linux Santoku	Meneliti tentang penggunaan aplikasi messenger IMO yang berpotensi untuk digunakan sebagai cyber stalking, sextortion, drug trafficking. Peneliti memberikan gambaran bagaimana mengakuisisi dan analisa filefile yang bisa dijadikan bukti pada suatu kejahatan.

Tabel 1.2 Perbandingan Penelitian

(Ammar Fauzan, 2018)	LINE	NIST, validation verification (VV)	UFED Forensic Tools, MOBILedit Forensic, Oxygen Forensics	Dalam penelitian ini, peneliti menyajikan studi dan teknik kemampuan tools dan mengevaluasinya serta menggunakan aplikasi LINE messenger sebagai objek penelitiannya. Penelitian ini menggabungkan metode VV dan metode forensik standar NIST
(Choi et al., 2017)	KakaoTalk	-	UFED physical analyzer, SQLite Database browser	Penelitian ini menunjukkan betapa sulitnya melindungi data sensitif pengguna dengan teknologi perangkat lunak murni. Meskipun saat peneliti membatasi analisis keamanan pada layanan messenger KakaoTalk, Peneliti yakin jenis serangan ini juga dapat diterapkan pada aplikasi IM lainnya.
(Kaczyński, 2019)	Signal		UFED, SQLiteStudio	Penelitian ini menggunakan emulator sebagai perangkat uji coba. Versi android yang digunakan adalah 5.0.1 dan menggunakan signal versi 4.37.2. peneliti berpendapat bahwa versi signal 4.37.2 lebih rentan tentang keamanannya daripada versi sebelumnya yaitu 4.21

BAB 2
Tinjauan Pustaka

2.1 Signal Messenger

Signal Messenger adalah layanan pesan instant terenkripsi lintas platform yang dikembangkan oleh Signal Technology Foundation dan Signal Messenger LLC. Melalui aplikasi Signal Messenger pengguna dapat mengirim pesan secara individu maupun dalam sebuah grup. Pesan yang bisa dikirim meliputi pesan tekt, file, suara, gambar maupun video. Selain itu aplikasi ini juga mendukung panggilan suara dan video ke satu individu maupun dalam grup. Khusus untuk versi android. Aplikasi ini mendukung dapat berfungsi sebagai aplikasi SMS.

Signal Messenger menggunakan nomor telepon seluler standar sebagai identitas pengguna sekaligus berfungsi untuk mengamankan komunikasi antara pengguna Signal dengan dukungan *end-to-end encryption*. *End-to-end encryption* adalah metode komunikasi untuk mencegah pihak ketiga mengakses data saat suatu sistem atau perangkat berkomunikasi satu dengan yang lain. Perangkat lunak Signal dapat diunduh gratis dan merupakan perangkat lunak open-source. Aplikasi ini mendukung beberapa platform telepon seperti android, iOS dan platform desktop pada Windows, MacOS dan Linux.

Signal Foundation sebagai perusahaan pendiri Signal messenger berdiri pada Februari 2018 atas sumbangan sebesar 50 juta dollar amerika oleh Brian Acton. Menurut data statistik yang ditampilkan oleh (Singh, 2021) pada laman *techcrunch.com* jumlah pengguna Signal Messenger saat ini mencapai lebih dari 525 juta pengguna aktif bulanan.

2.2 Forensika Digital

Forensika digital dapat diartikan sebagai sebuah bidang ilmu yang mencakup proses recovery dan investigasi dari content (berupa audio, video, image maupun dokumen) yang berkaitan dengan kejahatan komputer. Digital forensik harus dilakukan sesuai dengan standar operasional untuk menjamin tidak ada terjadi perubahan terhadap media digital yang akan diforensik selama proses investigasi. (Halim, 2012) , Selain itu menurut (Halim, 2012) forensik digital adalah sebuah cabang ilmu forensik dengan penggunaan ilmu dan metode ilmiah dalam mencari dan menemukan barang bukti digital untuk merekonstruksi peristiwa kejahatan yang terjadi dengan tahapan-tahapan yang terstruktur sehingga dapat diterima dalam pengadilan untuk penegakkan hokum.

Didalam Forensik digital sendiri mempunyai beberapa sub disiplin ilmu dan turunannya. (Daniel & Daniel, 2012) menjabarkan bahwa subdisiplin ilmu dalam dunia forensik digital, di antaranya adalah.

1. Computer Forensics
2. Mobile Forensics
3. GPS Forensics
4. Media Device Forensics
5. Social Media Forensics
6. Digital Video and Photo Forensics
7. Digital Camera Forensics
8. Digital Audio Forensics
9. Multiplayer Game Forensics
10. Game Console Forensics

Namun dalam subdisiplin ilmu komputer forensik, juga terdapat banyak turunan subdivisi ilmu dalam forensik digital lainnya. Yang mana setiap subdisiplin membutuhkan teknik dan metode yang berbeda dalam pencarian barang bukti digitalnya.

2.3 Mobile Forensik

Mobile forensik adalah salah satu cabang keilmuan dari forensik digital yang memulihkan bukti digital atau data dari mobile phone dibawah kondisi forensik suara dengan metode yang dapat di pertanggungjawabkan (Harrill & Mislan, 2007).

Forensik digital sangat berkembang pesat dengan peningkatan pada perangkat mobile. Penyelidikan forensik perangkat mobile pada umumnya di mulai dengan nomor telepon yang dihubungi, menjawab telepon di terima atau tidak, nomor telepon yang di simpan dan pesan teks yang dikirim diterima maupun yang dihapus. Kemampuan handphone atau smartphone meningkatkan kinerja, kapasitas penyimpanan dan kemampuan multimedia mengubah handphone atau smartphone menjadi penampung data yang dapat menyimpan berbagai informasi (Punja & Mislan, 2008).

Dari sudut pandang forensik digital dalam hal ini melakukan investigasi pada perangkat mobile dapat memberikan banyak barang bukti tentang pengguna dan kemampuan lain terkait pemulihan informasi tambahan sebagai barang bukti. (Ayers et al., 2007) berpendapat bahwa mobile forensik merupakan ilmu atau keahlian dalam proses dan mengelola barang bukti digital yang berasal dari mobile devices, handphone/cell-phone, tablets dan berbagai istilah serta varian sejenis lainnya dengan metode yang dapat dipertanggung jawabkan. Pada prinsipnya mobile forensik memiliki kesamaan metode

dengan digital forensik yang sudah ada, hanya saja kita mengubah point of view dari target bukti digital yang biasanya terdapat pada perangkat komputer desktop atau notebook kemudian beralih pada perangkat telepon bergerak atau mobile devices perbedaan yang sangat besar terdapat pada sisi teknis pelaksaannya.

Mobile forensik merupakan respon digital forensik terhadap perkembangan teknologi informasi yang telah mengevolusi perangkat komputer tradisional menjadi komputer tablet dan dunia telekomunikasi yang telah mengaplikasikan komputer dengan sangat baik sehingga menjadi smartphone. Sehingga ketergantungan manusia terhadap perangkat telekomunikasi saat ini sangatlah besar hampir semua tugas sederhana dari prinsip kerja komputer telah dapat diaplikasikan.

Kemajuan teknologi ini juga mempengaruhi perubahan gaya hidup dan cara bersosialisasi masyarakat modern saat ini yang mau tidak mau juga banyak melibatkan teknologi ini dalam setiap aktivitas manusia baik itu positif dan negatif termasuk diantaranya aktivitas yang berhubungan dengan kejahatan. Banyak modus operandi yang terjadi dengan melibatkan perangkat telekomuniasi bergerak bahkan popularitas smartphone juga menjadi ladang baru yang sangat menarik bagi hacker dalam kejahatan dunia maya.

Sejak pertama mobile devices mulai dihadirkan dalam persidangan dan menjadi barang bukti hukum yang sah dengan teknologi yang sangat jauh tertinggal dari smartphone saat ini, tantangan yang dihadapi oleh *investigator digital forensics* semakin hari semakin kompleks dikarenakan teknologi yang mengikutinya juga semakin lama semakin berkembang.

Perbedaan mobile device tentu berbeda juga karakteristik dari hardwarenya, berbeda juga arsitektur dari sistem operasinya dan berbeda teknologi celullarnya. Butuh keahlian yang khusus dan proses belajar yang cukup mendalam untuk dapat menjadi ahli dibidang ini. Seorang Seorang ahli mobile forensik harus mengerti dan paham mengenai apa itu mobilephone dan berbagai jenisnya, apa saja sistem operasi yang terdapat dalam mobile phone tersebut, mengerti bagaimana mobile forensik itu dilakukan serta prosesnya, tahu apa saja tools software, hardware yang harus digunakan pada masing-masing jenis dari mobile phone dan sistem operasinya.

Untuk mencakup semua ilmu pengetahuan yang diperlukan ini, seorang ahli mobile forensik harus peka terhadap perkembangan teknologi dari mobile phone. Banyak hal yang dapat dilakukan dengan menggunakan mobile devices saat ini, kemajuan teknologi seakan membuat komputer dalam genggaman kita. Berbagai potensi manfaat dari mobile devices baik itu buruk maupun positif seiring mengikuti para penggunanya. Menurut (Al-Azhar &

Muhammah, 2012) Terkait dengan bahasan mobile forensik, maka potensi kejahatan yang bisa dilakukan dengan menggunakan sebuah mobile devices, beberapa diantaranya adalah sebagai berikut.

2.4 Bukti Digital

Tujuan utama dari mobile forensik adalah mencari dan menggali berbagai informasi yang terkandung dalam mobile devices yang berpotensi sebagai alat bukti digital untuk kemudian dianalisa dan diolah agar dapat dihadirkan ke tengah persidangan sebagai alat bukti yang sah tanpa mengurangi kaedah dari aturan dan metode digital forensik sehingga hasilnya dapat dipertanggung jawabkan.

(Casey, 2011) bukti digital didefinisikan sebagai data yang disimpan atau dikirimkan menggunakan komputer yang digunakan untuk mendukung atau menyangkal teori tentang bagaimana suatu pelanggaran terjadi atau elemen-elemen penting dari pelanggaran tersebut. Data yang dimaksud kombinasi dasar dari angka-angka yang merepresentasikan dari berbagai jenis informasi seperti teks, gambar, audio, dan video.

Bukti digital menurut (Hsieh, 2019a) dalam presentasinya yang berjudul *Digital Evidence and Computer Forensics*, bukti digital merupakan Informasi dari nilai pembuktian yang disimpan atau ditransmisikan dalam bentuk biner dan dapat diandalkan di pengadilan.

(Hsieh, 2019b) dalam jurnalnya yang berjudul *Introduction to Forensic Science and Criminalistics* membagi bukti digital ke dalam dua kategori menurut sumber pembuatannya yaitu user-created, computer-created, offenders computer. Dari ketiga kategori tersebut dijabarkan hal hal yang bisa dijadikan sebagai barang bukti

- *User-Created*
    - Teks (dokumen, *e-mail*, pesan)
    - Database
    - Gambar dan Foto
    - Video dan Audio
    - Halaman Web
- *Computer-Created*
    - *Logs*
    - Metadata
    - *Browser cache*, riwayat, *cookies*
    - File *printer spool*
    - File *backup* dan *registry*

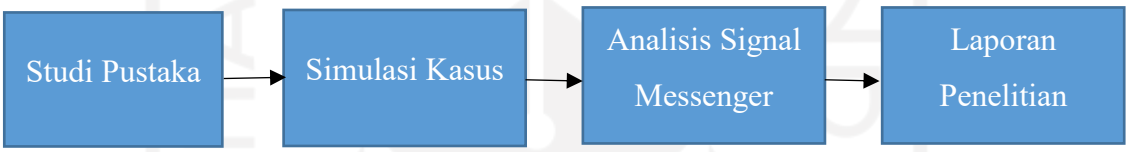
Banyaknya informasi yang bisa didapat dan besarnya potensi yang dimiliki oleh informasi tersebut dalam sebuah pengungkapan kasus menjadikan mobile forensik salah satu elemen yang penting didalam digital forensik saat ini.

BAB 3

Metode Penelitan

Metode penelitian adalah suatu cara ilmiah atau teknik yang digunakan demi memperoleh data mengenai suatu objek dari penelitan yang memiliki tujuan untuk memecahkan suatu permasalahan. Menurut Subagyo yang dikutip dalam Syamsul Bahry dan Fakhry Zamzam (2015:3). Metode Penelitian adalah suatu cara atau jalan untuk mendapatkan kembali pemecahan terhadap segala permasalahan yang diajukan.

Dalam penelitian ini langkah-langkah yang digunakan [emecahan terkait dengan permasalahan terhadap aplikasi Signal Messenger diilustrasikan kedalam gambar sebagai berikut:



Gambar 3.1 Langkah Penelitian

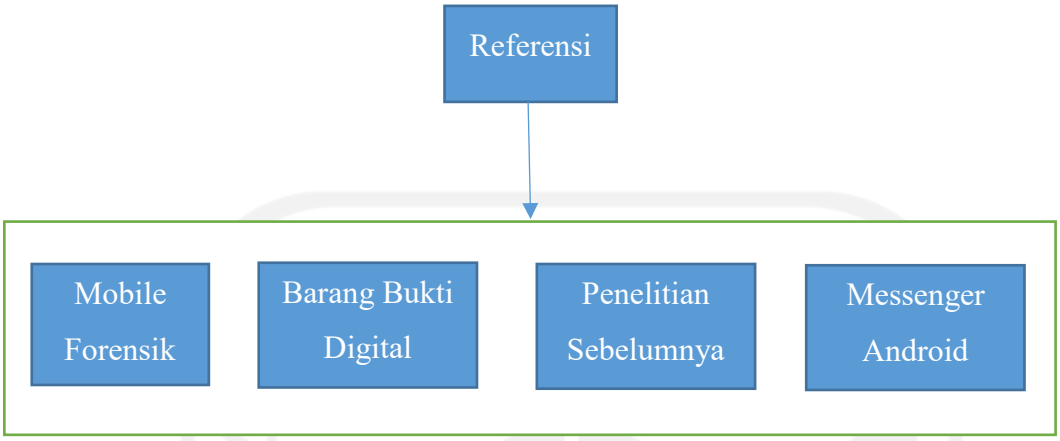
Pada langkah penelian tersebut yang dilakukan pertama adalah dengan melakukan studi pustaka melalui literature-literatur yang terkait dengan tema penelitian. Langkah kedua adalah dengan membuat sebuah simulasi kasus yang sebagai objek penelitian. Tahap selanjutnya adalah melakukan analisis aplikasi Signal Messenger berdasarkan simulasi kasus yang sudah disiapkan. Langkah terkahir adalah membuat laporan hasil dari penelitian yang telah dilakukan

3.1 Studi Pustaka

Studi pustaka merupakan teknik pengumpulan data dan informasi dengan menelaah sumber-sumber tertulis seperti jurnal ilmiah, literature, buku referensi, karangan ilmiah, serta sumber-sumber lain yang terpercaya baik dalam bentuk tulisan maupun dalam format digital yang relevan dengan objek yang diteliti. Menurut (Sarwono, 2006) dalam bukunya Metode Penelitian Kuantitatif dan Kualitatif studi pustaka adalah mempelajari berbagai referensi serta hasil peneltian sebelumnya yang sejenis yang berguna untuk mendapatkan landasan teori mengenai masalah yang akan ditelti.

Studi pustaka diperlukan untuk mengetahui permasalahan yang dihadapi oleh penelitian sejenis untuk dijadikan sebagai landasan untuk memecahkan permasalahan peneliti serta untuk menghindari pengulangan sebuah penelitian. Untuk itu peneliti

membatasi pencarian Referensi studi pustaka dengan menggunakan beberapa kata kunci yang relevan dengan objek yang sedang diteliti seperti pada gambar berikut:



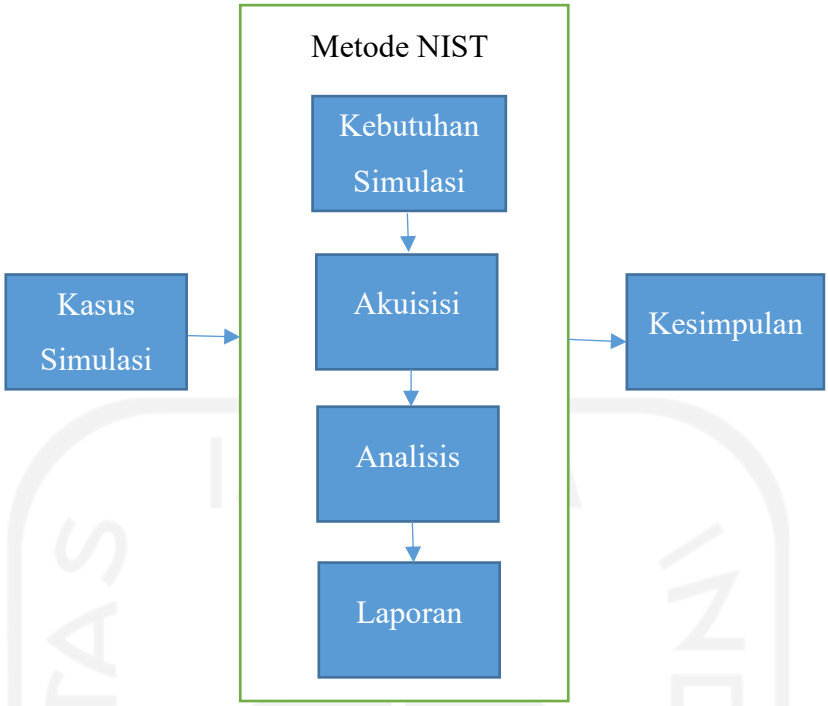
Gambar 3.2 Langkah Studi Pustaka

Pengumpulan bahan referensi sebagai landasan teori pemecahan masalah dilakukan dengan mencari pada buku, jurnal, artikel, maupun website yang bisa dipercaya yang berkaitan dengan objek yang sedang diteliti.

3.2 Simulasi dan Kasus

Simulasi merupakan proses aplikasi membangun model dari sistem nyata atau usulan sistem, melakukan eksperimen dengan model tersebut untuk menjelaskan perilaku sistem. Dengan melakukan simulasi kita bisa malakukan sebuah kegiatan penelitian untuk mengevaluasi metode maupun tools yang dipakai sebelum masuk kedalam kasus yang nyata. Tujuan dari simulasi ini adalah untuk untuk pembuktian terhadap rumusan masalah dalam penelitian ini dan juga sebagai tahap pengujian terhadap metode NIST yang digunakan untuk memecahkan masalah.

NIST atau *National Institute of Standard and Technology* adalah sebuah badan yang bertugas mengembangkan standar, panduan, dan persyaratan minimum untuk menyediakan keamanan informasi yang baik bagi semua asset dan berbagai pihak yang mempunyai kompetensi pada bidang digital forensik, metode ini digunakan oleh para agen dalam pemerintahan pusat di Amerika, namun tidak menutup kemungkinan bahwa standar ini dapat digunakan oleh organisasi seperti lain akademisi, badan penyidik swasta dan lainnya. Berikut ini merupakan tahapan simulasi yang akan dilakukan oleh peneliti didalam melakakukan penelitian dan menggunakan metode NIST sebagai metode pengujiannya.



Gambar 3.3 Simulasi Penelitian

Dalam mendukung simulasi tersebut, maka dibuatkan sebuah skenario kasus yang bertujuan sebagai objek model untuk melakukan pengujian sebagai berikut:

a. Seorang penyidik kepolisian telah berhasil menangkap seorang artis yang positif menggunakan narkoba. Selain barang bukti narkoba, penyidik kepolisian juga menyita *smartphone* milik artis tersebut sebagai barang bukti. Penyitaan smartphone tersebut dilakukan penyidik untuk mengembangkan kasus untuk mencari siapa pengedar yang menjual narkotika ini kepada sang artis.
b. Penyidik pun mulai menggeledah handphone milik sang artis dengan membuka beberapa aplikasi media social untuk mencari kontak sang artis dengan pengedar.Pada saat barang bukti smartphone ditemukan dan diamankan.
c. Pada saat penyidik melakukan penggeledahan pada sebuah aplikasi pesan Signal, penyidik menemukan ada pesan mencurigakan dan percakapan terasa janggal karena seperti ada beberapa pesan yang sudah dihapus.
d. Sehingga untuk penyedilikan lebih lanjut, penyidik kepolisian membawa barang bukti tersebut ke bagian forensik untuk diteliti lebih lanjut.

Kemudian dalam mendukung kasus yang menjadi objek penelitian beberapa perangkat dibutuhkan sebagai objek penelitian. Perangkat tersebut dibagi menjadi 2 bagian yaitu perangkat keras dan perangkat lunak.

a. Perangkat Keras

Dalam melakukan penelitian ini peneliti menggunakan beberapa perangkat keras yang dibutuhkan sebagai alat yang digunakan. Perangkat keras yang dibutuhkan dirangkum didalam tabel berikut:

Tabel 3.1 Perangkat Penelitian

No.	Nama Perangkat	Spesifikasi
1	PC Desktop	Processor : Intel i5-3470 CPU @ 3.20GHz RAM : 8 GB
2	Smartphone SM A530F	Processor : Exynos 7885 2x2.2 GHz Cortex-A73 RAM : 4 GB
3	Smartphone Redmi Note 4	Processor : Snapdragon 625 2.0 GHz Cortex-A53 RAM : 3 GB

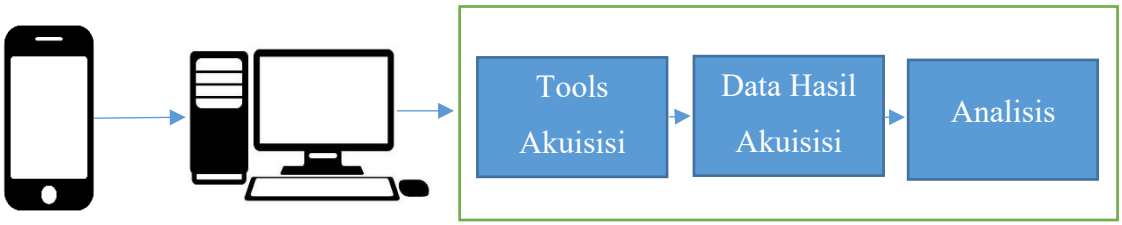
b. Perangkat Lunak

Perangkat lunak yang akan peneliti gunakan dalam melakukan penelitian adalah seperti berikut:

- MOBILedit Forensic Express 7.1
- Autopsy 4.18.0 for windows
- DB Browser for SQLite
- Magnet AXIOM 4.10
- Signal-Back
- Signalbackup-tools

3.3 Akuisisi

Akuisisi merupakan suatu proses imaging atau penggandaan berupa barang bukti seperti media penyimpanan digital untuk mendapatkan data. Akusisi diperlukan untuk kegiatan analisis data sehingga sumber data yang menjadi barang bukti utama tidak mengalami kerusakan dalam proses analisis.



Gambar 3.4 Alur Akuisisi

Seperti pada gambar 3.4 akuisisi sebuah perangkat mobile membutuhkan bantuan komputer untuk memperoleh data akuisisi. Sebuah perangkat mobile akan disambungkan kedalam komputer kemudian pada komputer menggunakan kabel data. kemudian perangkat mobile yang sudah tersambung tersebut akan terdeteksi oleh aplikasi tools untuk kemudian dilakukan proses akuisisi dan analisis.

3.4 Analisis

Analisis adalah usaha dalam mengamati sesuatu secara mendetail dengan cara menguraikan komponen pembentuknya atau menyusun sebuah komponen untuk kemudian dikaji lebih mendalam. Manurut (Latuconsina & Yunanto, 2017) analisis adalah suatu kegiatan memperhatikan, mengamati, dan memecahkan suatu masalah (mencari jalan keluar) yang dilakukan oleh seseorang.

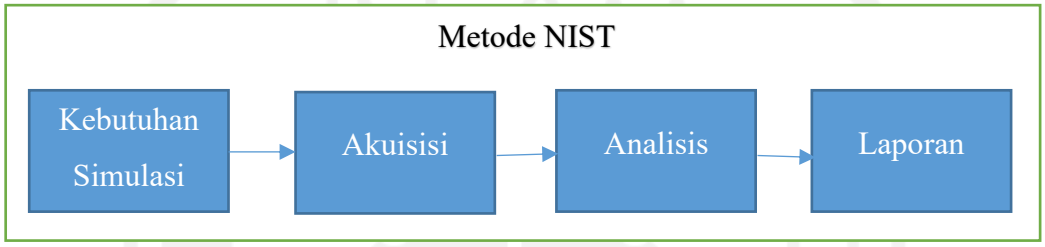
Dalam penelitian dimana menggunakan kasus sebagai objek, analisis diperlukan untuk mencari dan mengamati jejak digital yang bisa dijadikan alat bukti elektronik sebagai pengembangan dalam menyelesaikan kasus tersebut.

BAB 4

Hasil dan Pembahasan

4.1 Persiapan Simulasi

Dalam Metode NIST Proses pertama yang dilakukan adalah *preservation.* Dalam tahap ini dilakukan persiapan apa saja yang menjadi kebutuhan untuk melakukan proses analisa forensik. Seperti mempersiapkan barang bukti yang akan dianalisa, *Tools* yang akan dipakai atau diperlukan, serta alat-alat untuk melakukan dokumentasi.



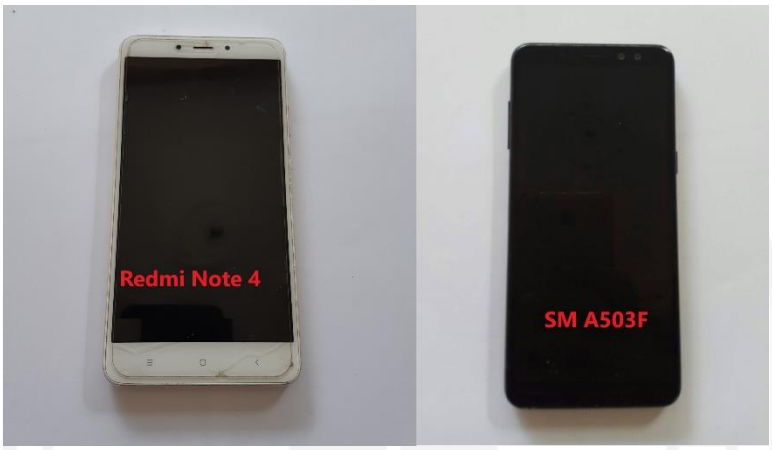
Gambar 4.1 Alur Metode NIST

Setelah semua kebutuhan terpenuhi, langkah selanjutnya adalah melakukan *Acquisition* atau Akuisisi, terdapat 3 teknik ektraksi yang bisa digunakan dalam proses pengumpulan bukti digital smartphone. Teknik – teknik tersebut adalah *physical extraction*, *logical extraction*, dan *file system extraction*. *Physical extraction* merupakan teknik ektraksi dimana perangkat tersebut akan disalin secara bit by bit pada memori yang memungkinkan file yang terhapus atau disembunyikan bisa terbaca. *Logical extraction* merupakan akuisisi bit for bit pada logical storage yang mencakup file dan direktori yang berada pada file system. Keunggulan dari akuisisi menggunakan teknik Logical extraction adalah perangkat mobile yang akan diakuisisi tidak perlu dilakukan proses *rooting*. *File System Extraction* merupakan teknik akuisisi terhadap file yang terdapat dalam memori perangkat mobile dimana dengan teknik ini memungkinkan kita untuk mendapatkan akses semua file yang ada didalam memori allocated space, termasuk gambar, video, database file, sistem file dan log.

Setelah proses akuisisi selesai, hasil dari proses akuisisi akan di analisis menggunakan software. Disini analisis bertujuan untuk mencari *digital artifact* yang terdapat pada aplikasi Signal Messenger tersebut untuk mencari file – file yang bisa dijadikan sebagai barang bukti, kemudian temuan *digital artifact* tersebut ditulis dalam bentuk laporan yang bisa digunakan penyidik untuk melengkapi berkas kasus yang sedang ditangani.

4.2 Simulasi

Dalam Penelitian ini simulasi menggunakan dua smartphone perangkat android Samsung SM A530F dan Redmi Note 4. Tampat kedua perangkat tersebut terlihat seperti gambar 4.2 berikut.



Gambar 4.2 Perangkat Simulasi

Kedua smartphone seperti pada gambar 4.2 telah terinstall aplikasi Signal Messenger dan telah saling mengirim pesan berdasarkan kasus yang disimulasikan seperti mengirim pesan teks, gambar video, dokumen, panggilan suara dan video. Kemudian tahap selanjutnya adalah melakukan proses akuisisi atau proses imaging terhadap kedua perangkat smartphone tersebut menggunakan PC.

4.3 Akuisisi

Akuisisi atau imaging adalah proses untuk mendapatkan data. hal ini diperlukan sebagai langkah untuk melindungi data yang terdapat dalam barang bukti smartphone ketika dilalukan proses analisis. Tujuan dari proses akuisisi ini adalah untuk mendapatkan Salinan data yang terdapat pada barang bukti sehingga proses analisis bisa dilakukan pada Salinan data tersebut tanpa mengganggu data yang terdapat didalam barang bukti. dalam penelitian ini aplikasi yang digunakan bernama Magnet AXIOM dengan versi 4.10 untuk melakukan akuisisi baik physical maupun logical. Hasil dari akuisisi beserta nilai hash terlihat pada gambar/tabel berikut.

```
Relative Segment 1 Path: redmi note 4 - physical.raw
Full Segment 1 Path: C:\Users\RYAN\Documents\Tesis\Magnet File\Kasus01 - Nov 19 2021 234014\redmi note 4 - physical.raw
Segment 1 MD5 Hash: 85090C222E7EBCE790CF5C20CEB6E23E
Segment 1 SHA1 Hash: 32D880CACF4C2127A187C26E557AD9010B5F7B1D

Relative Segment 2 Path: samsung A530F physical.raw
Full Segment 2 Path: C:\Users\RYAN\Documents\Tesis\Magnet File\Kasus01 - Nov 19 2021 234014\samsung A530F physical.raw
Segment 2 MD5 Hash: B9CF2060F16475E871D946C3D3428242
Segment 2 SHA1 Hash: 600C9036FF0B15037EB276EAAB7F221C9E5944BC
```

Gambar 4.3 Laporan Akuisisi

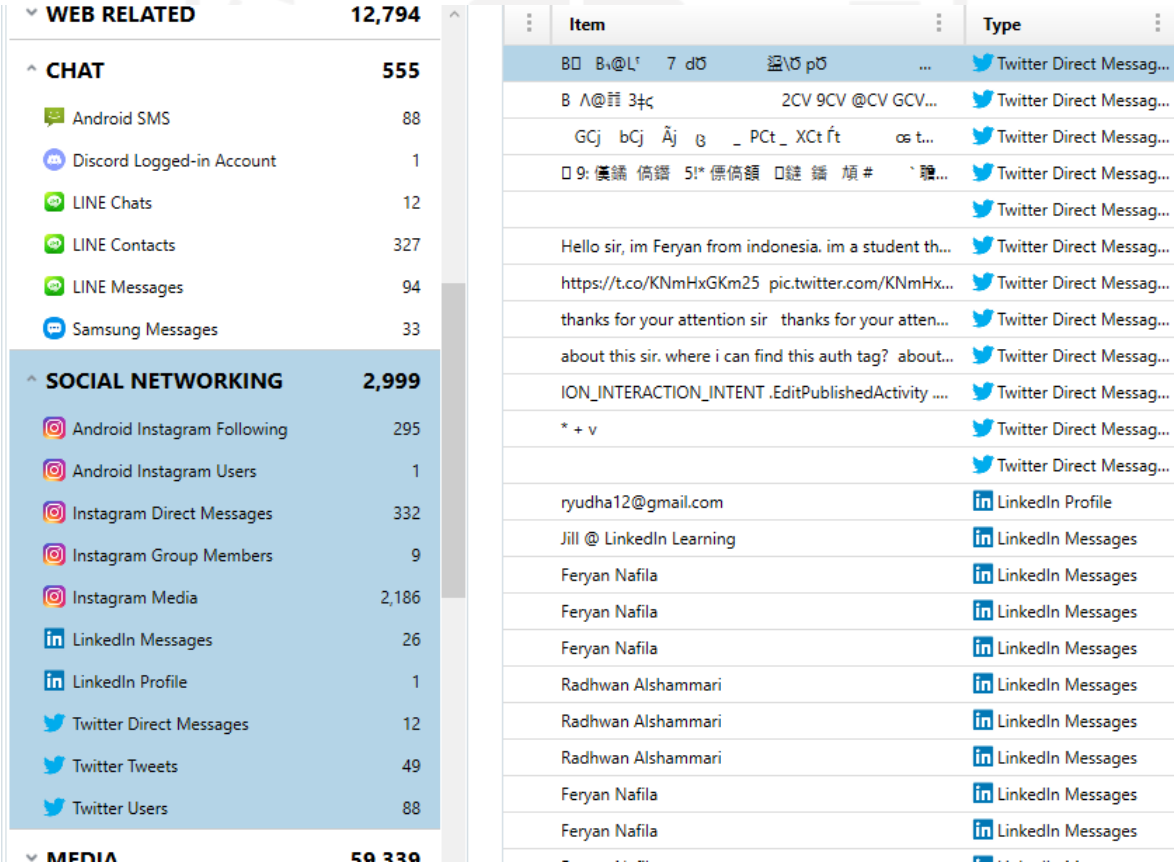
Dari hasil akuisisi seperti gambar 4.3 menggunakan Magnet AXIOM terlihat bahwa untuk proses *physical extraction* menghasilkan fire dengan format *.raw* sedangkan untuk logical menghasilkan format *.zip*

4.4 Analisis Data Akuisisi

Setelah proses akuisisi selesai penelitian berlanjut pada proses analisa terhadap file tersebut. Proses analisa ini menggunakan beberapa software untuk melakukan analisis. Hal ini bertujuan untuk mengetahui sejauh mana software tersebut bisa melakukan analisis dan sebagai pembanding kemampuan dari software tersebut.

4.4.1 Magnet AXIOM 4.10

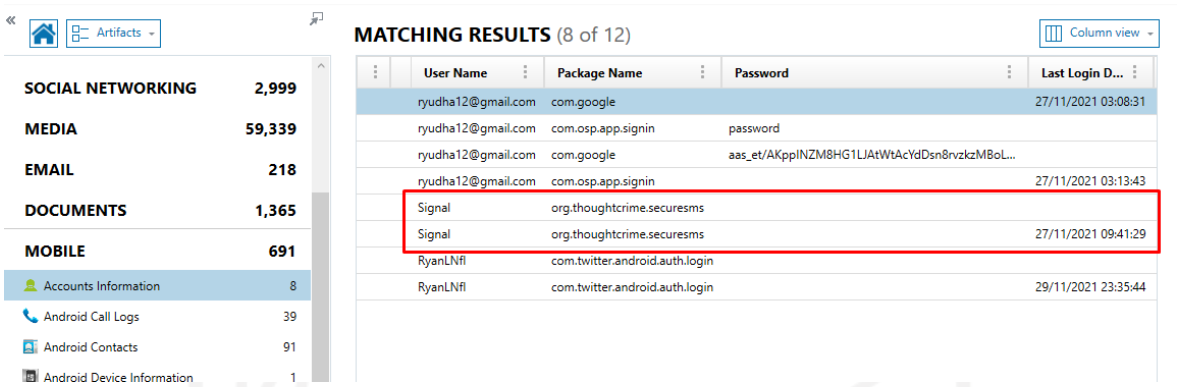
Magnet AXIOM mempunyai kemampuan untuk mengelompokkan data berdasarkan beberapa kategori. Disini dalam peneliti berfokus pada kategori *chat* dan *social networking.*



Gambar 4.4 Tampilan Chat dan Social Networking Magnet AXIOM

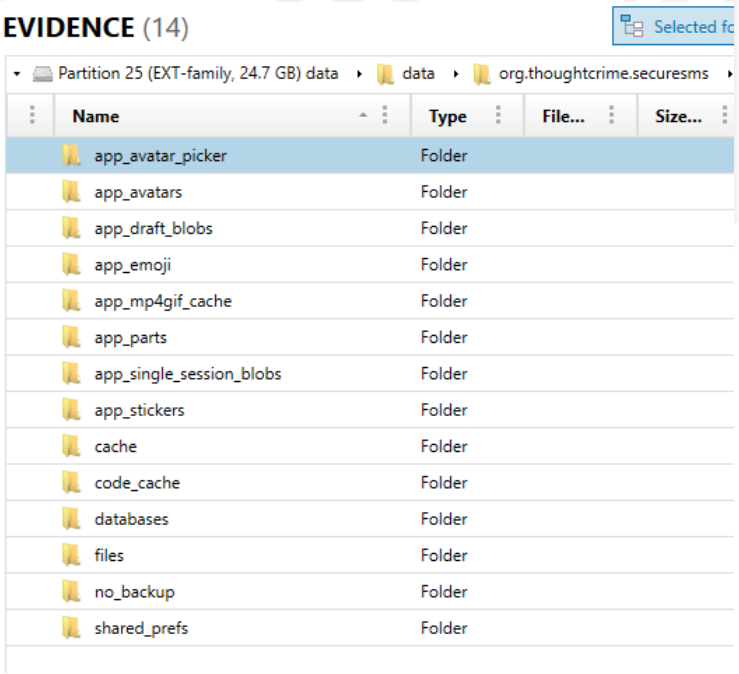
Setelah proses identifikasi file akuisisi selesai. Seperti pada gambar 4.4 beberapa data chat dan social networking ditampilkan namun tidak ada data mengenai aplikasi Signal Messenger yang bisa diindentifikasi. Hanya beberapa social media lain seperti Intagram, Line, Twitter, maupun LinkedIn yang dapat ditampilkan. Kemudian penelitian berlanjut

pada data kategori *Mobile.* Pada tab *mobile* terdapat informasi mengenai akun dengan rincian *username, package name,* dan *last login*.



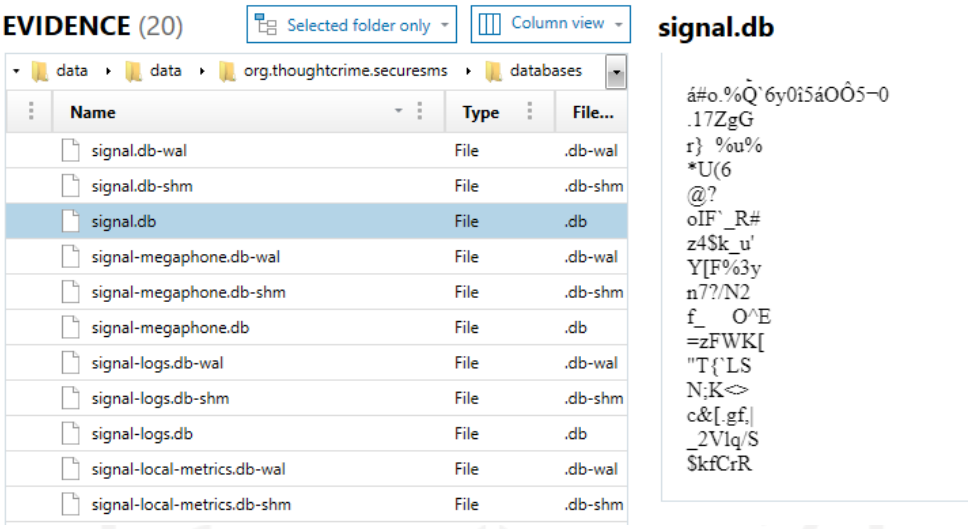
Gambar 4.5 Tampilan Mobile Magnet AXIOM

Berdasarkan gambar 4.5 diketahui informasi bahwa terdapat akun Signal Messenger, kemudian nama paket folder tempat tersimpan data dari signal messenger yaitu pada folder *org,throughtcrime.securesms* diinformasikan juga untuk terakhir aplikasi Signal Messenger ini digunakan. Setelah mengetahui folder tempat data Signal Messenger itu disimpan yaitu pada folder *org,throughtcrime.securesms* penelitian kemudian berlanjut untuk melakukan analisis pada folder tersebut. Tempat paket folder itu tersimpan yaitu pada *path:\data\data\org.thoughtcrime.securesms.* Data yang ditampilkan pada software Magnet AXIOM berisi 14 buah folder seperti pada gambar berikut:



Gambar 4.6 Folder Paket Signal Messnger

Dari data yang terlihat pada gambar 4.6 terdapat folder bernama *database*

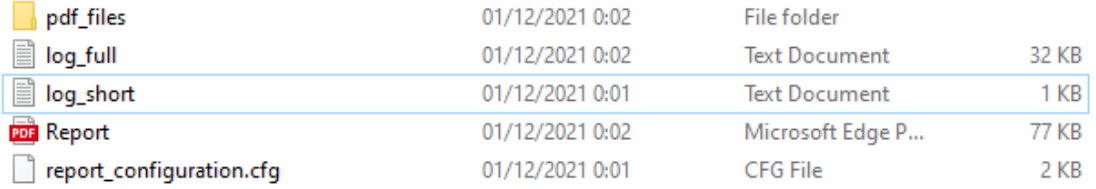


Gambar 4.7 Folder Database

Dilihat pada gambar 4.7 Magnet AXIOM tidak bisa menampilkan data dari database tersebut karena karena file signal.db tersebut dalam keadaan terenkripsi.

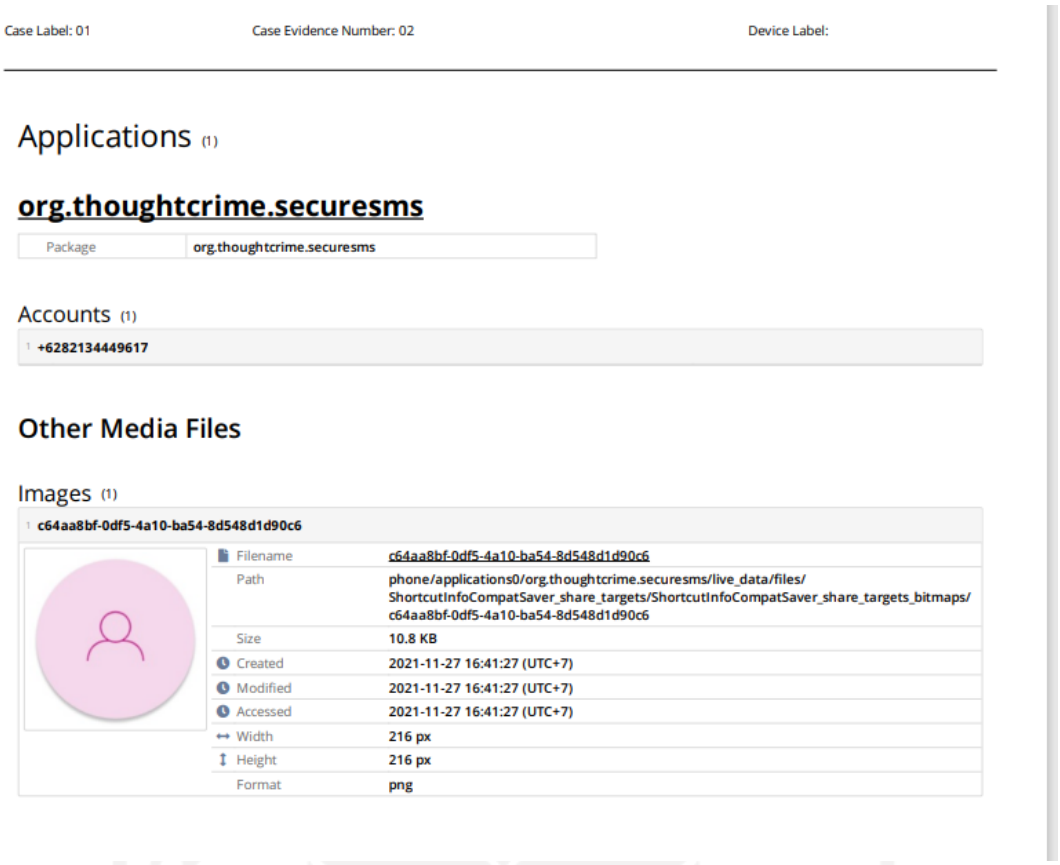
4.4.2 MobileEdit 7.1

Pada software Mobiledit Forensic peneliti menggunakan seri Express versi 7.1 analisis dimulai dengan membuka file akuisisi. Pada pilihan analisis, dikhususkan untuk menganalisis aplikasi messenger Signal. Kemudian hasil bukaan akuisisi tersebut menghasilkan file seperti berikut.



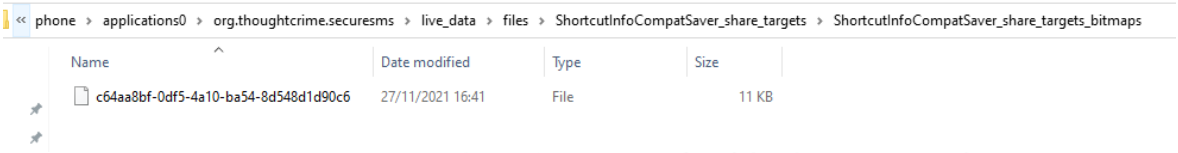
Gambar 4.8 Hasil Analisis MOBILedit

Pada gambar 4.9 terlihat file laporan *Report* dimana ketika dibaka maka report tersebut berisi data berikut ini.



Gambar 4.9 Hasil Report MOBILedit

Pada gambar terdapat informasi yang bisa didapat dengan software ini berupa nama folder data Signal Messenger, kemudian informasi akun dengan nomor akun yang digunakan yaitu *+6582134449617* selain itu juga terdapat sebuah file image yang teridentifikasi namun tidak menampilkan gambar dari file tersebut.



Gambar 4.10 File Image

Kemudian pada gambar terdapat folder *pdf.file* yang ketika dibuka hanya menampilkan 1 file seperti pada gambar 4.10 dan file ini adalah file image yang diidentifikasi pada file *Report* pada gambar 4.9.

4.4.3 Autopsy 4.18.0

Analisis dimulai dengan membuka file akuisisi, kemudian setelah proses telah selesai. Analisis pertama tertuju pada aplikasi yang terinstall pada perangkat yang diakuisisi.

Type	Value	Source(s)
Program Name	org.thoughtcrime.securesms	Android Installed Applicati
Date/Time	2021-07-24 09:30:55	Android Installed Applicati
Source File Path	/img_samsung SM-A530F Full Image - MMCBLK0.raw/vol_vol28/data/com.android.vending/databases/library.db	
Artifact ID	-9223372036854774848	

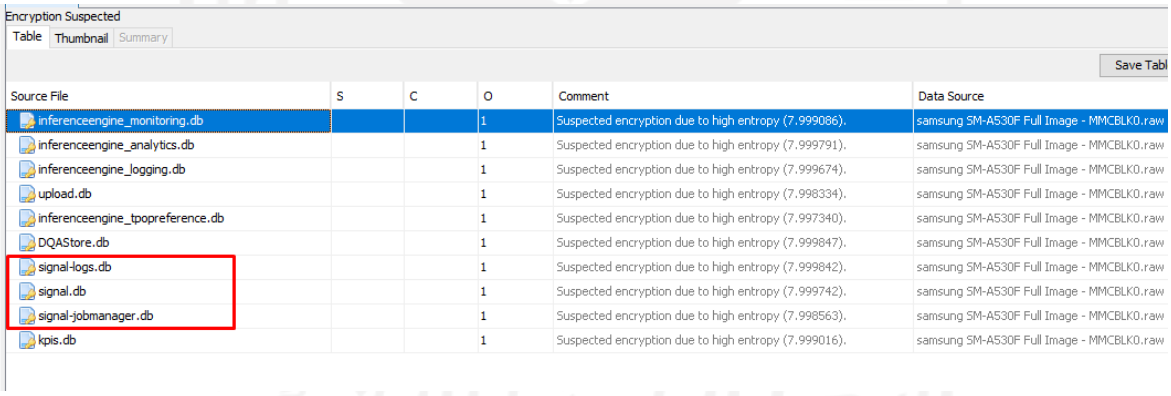
Gambar 4.11 Informasi Aplikasi Terpasang

Pada gambar 4.11 menampilkan keterangan mengenai program *org.throughcrime.*securesms terinstall bersama waktu installasi. Kemudian analisis berlanjut pada akun yang terbaca oleh software ini.

Gambar 4.12 Informasi Akun

Pada gambar 4.12 tab *Account* tidak menampilkan aplikasi Signal Messenger. Kemudian analisis dilanjutkan dengan melihat tab *Encryption Suspected* pada tab ini berisikan informasi mengenai file yang kemungkinan terenkripsi.

Pada gambar 4.13 menampilkan file *signal-logs.db, signal.db, signal-jobmanager.db* terindikasi enkripsi.



Gambar 4.13 File Terenkripsi

Kemudian hasil dari beberapa software tersebut dirangkum dalam tabel berikut.

Tabel 4.1 Perbandingan Menganalisa File Akuisisi

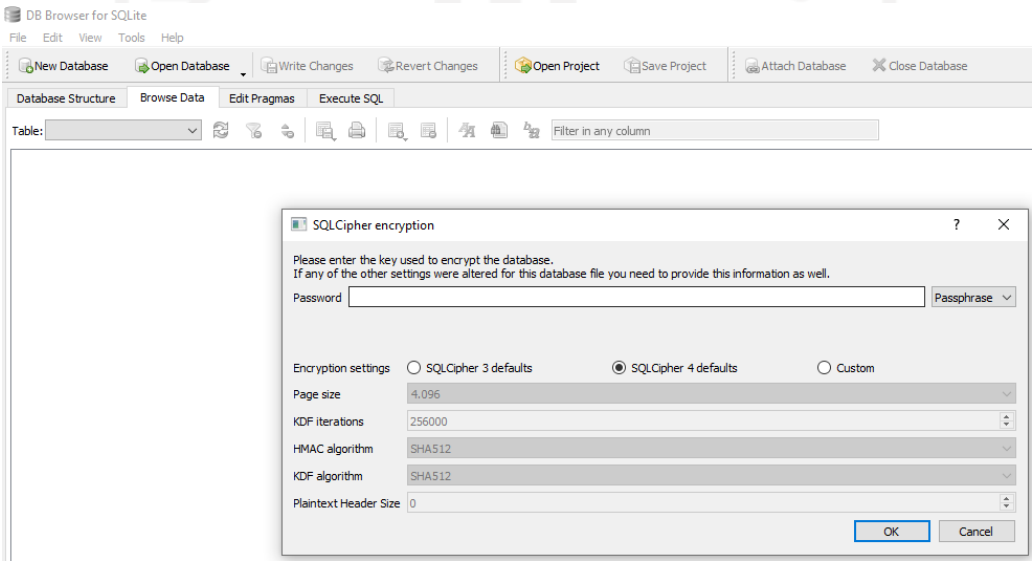
Perangkat	Software	Data informasi hasil analisis			
		Aplikasi	Akun	Database	Informasi lain
SM A530F	Magnet AXIOM	✓	✓	terenkripsi	Terdapat keterangan *last login*

Tabel 4.2 Perbandingan Menganalisa File Akuisisi

	MobileEdit Express	✓	✓	terenkripsi	Nomor akun pengguna ditampilkan
	Autopsy	✓	n/a	terenkripsi	Beberapa file Signal Messenger terdeteksi enkripsi
Redmi Note 4	Magnet AXIOM	✓	✓	terenkripsi	Terdapat keterangan *last login*
	MobileEdit Express	✓	✓	terenkripsi	Nomor akun pengguna ditampilkan
	Autopsy	✓	n/a	terenkripsi	Beberapa file Signal Messenger terdeteksi enkripsi

* n/a (not available)

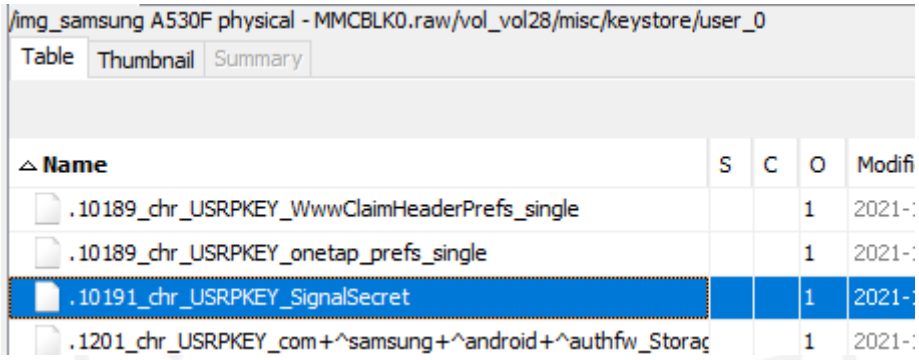
Kemudian analisis berlanjut pada database aplikasi Signal Messenger yang tersimpan pada *org.thoughtcrime.securesms* > *database* > file database tersebut kemudian diekstrak untuk dilihat isi file database tersebut.



Gambar 4.14 Database Terenkripsi

Terlihat pada gambar 4.14 software *DB browser (SQLchiper)* ketika mencoba membuka aplikasi tersebut. Kemudian muncul pesan bahwa database signal ter-encrypte

sehingga database tidak dapat dibuka dan untuk membuka database tersebut dibutuhkan sebuah kunci untuk melakukan decrypte.) kunci decrypte pada aplikasi Signal messenger terdapat pada folder keystore folder tersebut berada pada *misc/keystore/user_0.*



Gambar 4.15 Signal Key

Seperti pada gambar 4.15 terdapat file *.10191_chr_USRPKEY_SignalSecret* namun setelah dicoba dengan beberapa *tools decrypt* penulis masih belum dapat memecahkan kunci untuk melakukan decrypt pada database Signal Messenger perbedaan versi signal messenger, versi android, dan bukan menggunakan emulator menjadi perbedaan pada penelitian ini.

4.5 Analisis Data backup

Selain database untuk menyimpan data pesan, aplikasi Signal Messenger juga mempunyai fitur berupa *backup*. Bila fitur ini diaktifkan, maka aplikasi ini akan membuat sebuah backup dari database disertai kunci yang bisa digunakan untuk membuka file backup tersebut. Backup file ini bisa menjadi alternative bagi peneliti untuk melihat data yang terdapat pada Signal messenger selain data dari database. Disini peneliti akan mengunakan dua aplikasi yang berjalan pada comman propt. Dikutip dari halaman web resmi dari Sinal, file backup ini tersimpan pada */Internal Storage/Signal/Backups.*

4.5.1 Signal-Back

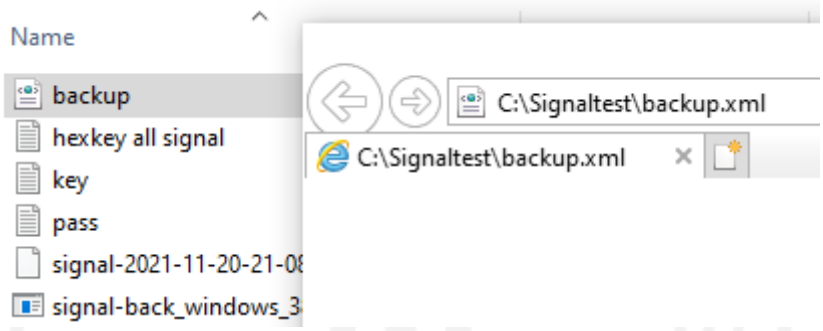
Kemudian peneliti mencoba menggunakan file decrypt bernama *Signal-back*. Dimana file *compile* ini disimpan satu folder dengan file backup. Kemudian memanggil file tersebut menggunakan command propt seperti gambar berikut ini. Disini peneliti mencoba mengangkat file yang terdapat pada file backup tersebut.

```
C:\Signaltest>signal-back_windows_386.exe format -f XML -o backup.xml signal-2021-11-20-21-08-32.backup
Password: 46447 59927 45685 52481 00426 31814
panic: runtime error: makeslice: len out of range

goroutine 1 [running]:
github.com/xeals/signal-back/types.(*BackupFile).Frame(0x11046080, 0x11de3230, 0x0, 0x0)
        /home/xeal/.local/share/go/src/github.com/xeals/signal-back/types/backup.go:94 +0xca
github.com/xeals/signal-back/cmd.XML(0x11046080, 0x5b52a0, 0x11024120, 0x3, 0x1)
        /home/xeal/.local/share/go/src/github.com/xeals/signal-back/cmd/format.go:145 +0xb6
github.com/xeals/signal-back/cmd.glob..func4(0x11030370, 0x0, 0x0)
        /home/xeal/.local/share/go/src/github.com/xeals/signal-back/cmd/format.go:67 +0x338
github.com/xeals/signal-back/vendor/github.com/urfave/cli.HandleAction(0x562a00, 0x59d1cc, 0x11030370, 0x1104ec00, 0x0)
        /home/xeal/.local/share/go/src/github.com/xeals/signal-back/vendor/github.com/urfave/cli/app.go:490 +0xa2
github.com/xeals/signal-back/vendor/github.com/urfave/cli.Command.Run(0x58fd56, 0x6, 0x0, 0x0, 0x0, 0x0, 0x0, 0x59737f,
0x1f, 0x59c592, ...)
        /home/xeal/.local/share/go/src/github.com/xeals/signal-back/vendor/github.com/urfave/cli/command.go:210 +0x8e1
github.com/xeals/signal-back/vendor/github.com/urfave/cli.(*App).Run(0x110202a0, 0x11046000, 0x7, 0x8, 0x0, 0x0)
        /home/xeal/.local/share/go/src/github.com/xeals/signal-back/vendor/github.com/urfave/cli/app.go:255 +0x58b
main.main()
        /home/xeal/.local/share/go/src/github.com/xeals/signal-back/main.go:52 +0x210
```

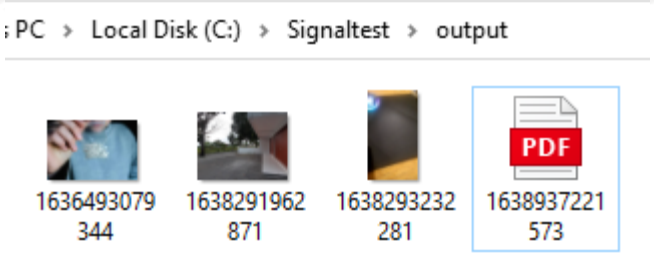
Gambar 4.16 Proses membuka file backup

Dari hasil proses decrypte seperti pada gambar 4.16 didapat file dengan format *.xml* namun ketika dibuka file xml ini tidak menampilkan data apapun dan bernilai 0KB seperti pada gambar 4.17



Gambar 4.17 Tampilan File ackup.xml

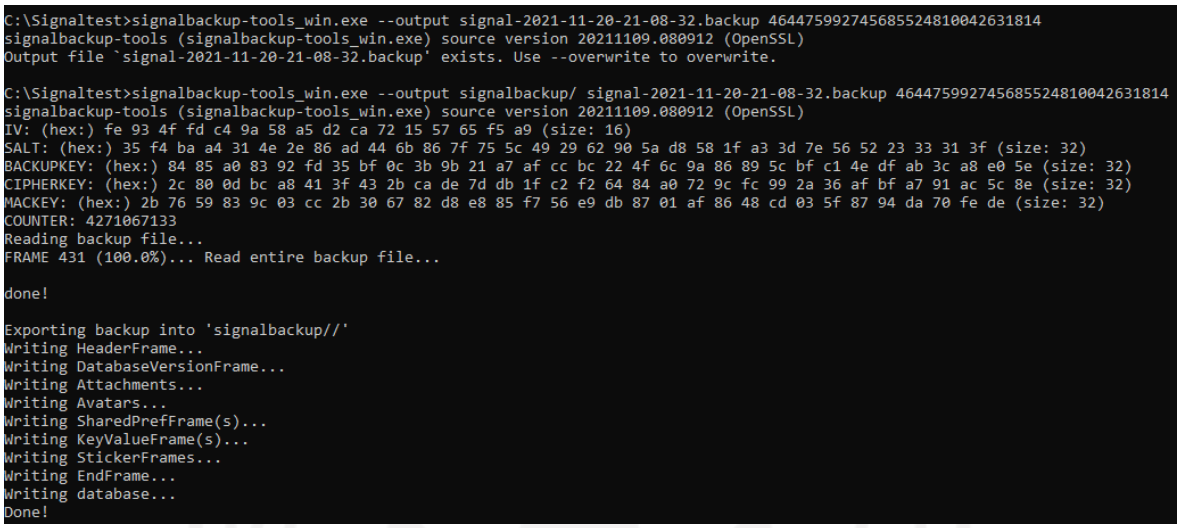
Kemudian peneliti mencoba untuk mengangkat file media dengan menggunakan perintah *signal-back_windows_386.exe extract -o output signal-2021-11-20-21-08-32.backup*. Setelah proses selesai, terdapat media gambar dan video yang berhasil diangkat seperti 4.18 berikut.



Gambar 4.18 Data Media

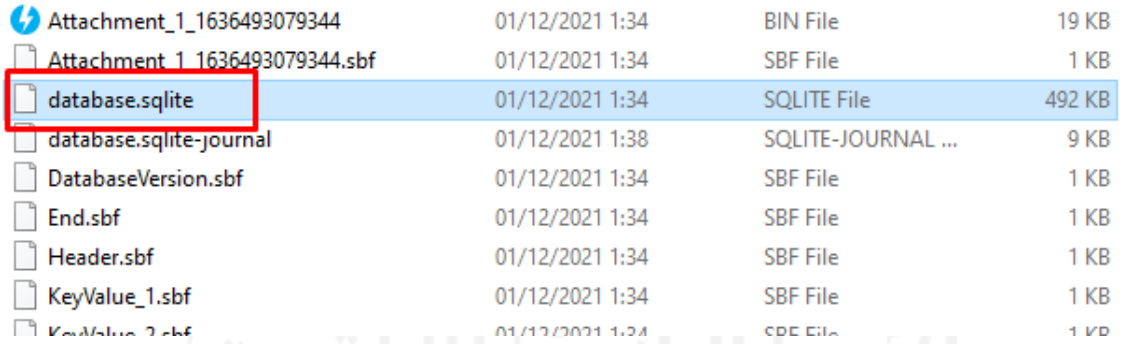
4.5.2 Signalbackup-tools

Sama dengan Signal-Back diatas, peneliti mencoba menarik data yang terdapat pada file backup signal. Disini peneliti menggunakan perintah *signalbackup-tools_win.exe --output signalbackup/ signal-2021-11-20-21-08-32.backup 464475992745685524810042631814* pada command prompt. Proses perintah ini dapat dilihat pada gambar 4.19 berikut.



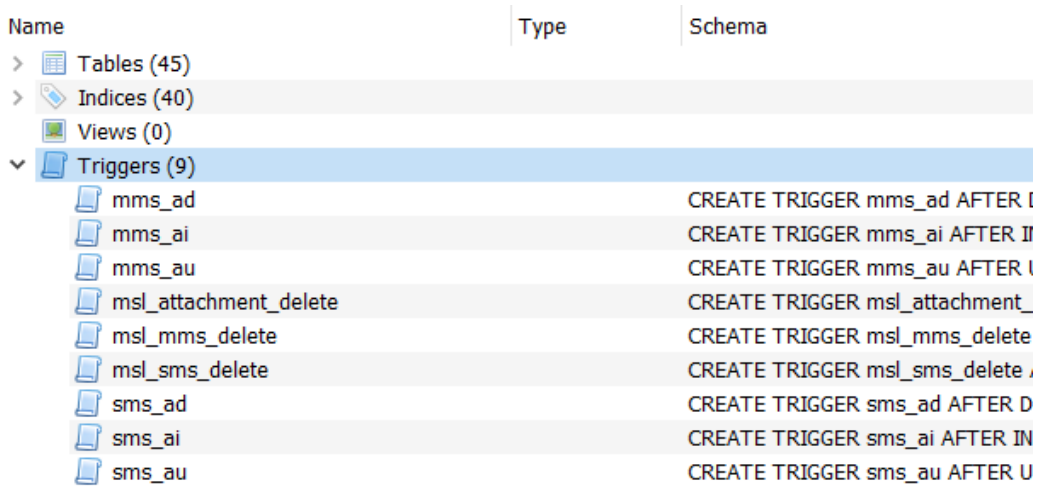
Gambar 4.19 Proses Decrypte Signalbackup-tools

Setelah proses selesai terdapat beberapa file yang bisa terangkat. Salah satunya adalah file database signal bernama *database.sqlite* seperti gambar 4.20 berikut.



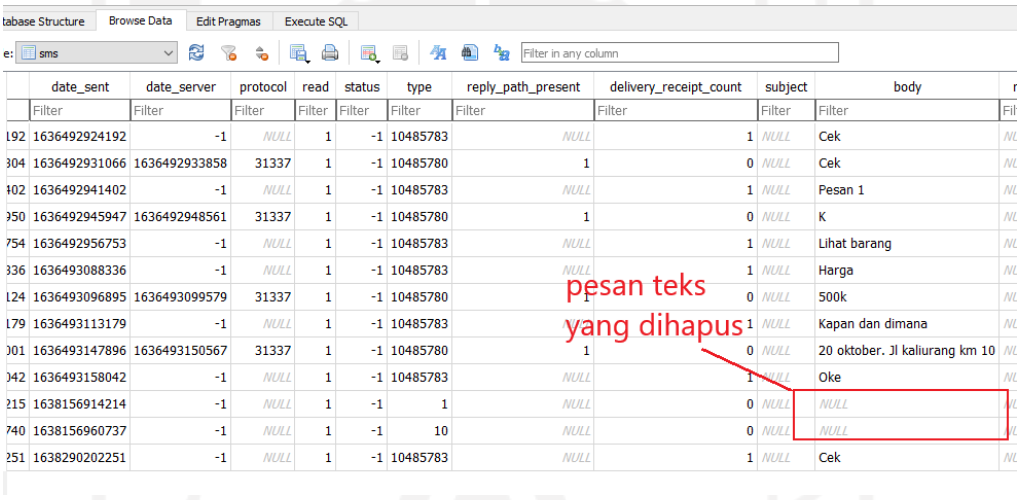
Gambar 4.20 Hasil Decrypte Data Backup

Kemudian penelitian berlanjut dengan membuka file *database.sqlite* tersebut menggunakan software *DB Browser for SQLite* dan diperlihatkan bahwa terdapat 45 tabel pada database tersebut.



Gambar 4.21 Isi File signal.db

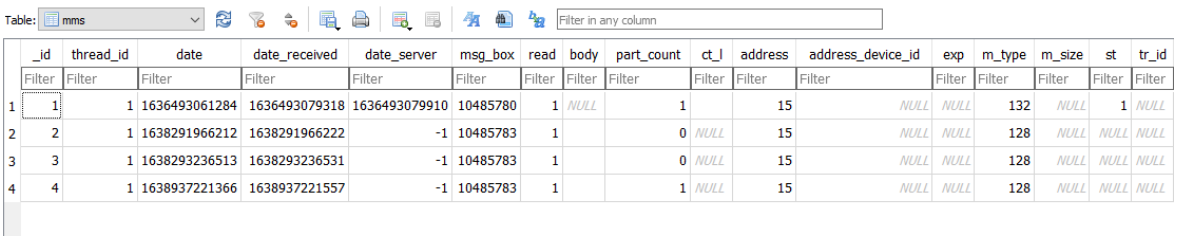
Dari database ini tersimpan beberapa data seperti pesan teks yang tersimpan pada tabel *sms* seperti pada gambar berikut.



	date_sent	date_server	protocol	read	status	type	reply_path_present	delivery_receipt_count	subject	body
192	1636492924192	-1	NULL	1	-1	10485783	NULL	1	NULL	Cek
304	1636492931066	1636492933858	31337	1	-1	10485780	1	0	NULL	Cek
402	1636492941402	-1	NULL	1	-1	10485783	NULL	1	NULL	Pesan 1
950	1636492945947	1636492948561	31337	1	-1	10485780	1	0	NULL	K
754	1636492956753	-1	NULL	1	-1	10485783	NULL	1	NULL	Lihat barang
336	1636493088336	-1	NULL	1	-1	10485783	NULL	1	NULL	Harga
124	1636493096895	1636493099579	31337	1	-1	10485780	1	0	NULL	500k
179	1636493113179	-1	NULL	1	-1	10485783	NULL	1	NULL	Kapan dan dimana
001	1636493147896	1636493150567	31337	1	-1	10485780	1	0	NULL	20 oktober. Jl kaliurang km 10
042	1636493158042	-1	NULL	1	-1	10485783	NULL	1	NULL	Oke
215	1638156914214	-1	NULL	1	-1	1	NULL	0	NULL	NULL
740	1638156960737	-1	NULL	1	-1	10	NULL	0	NULL	NULL
251	1638290202251	-1	NULL	1	-1	10485783	NULL	1	NULL	Cek

Gambar 4.22 Pesan Dihapus

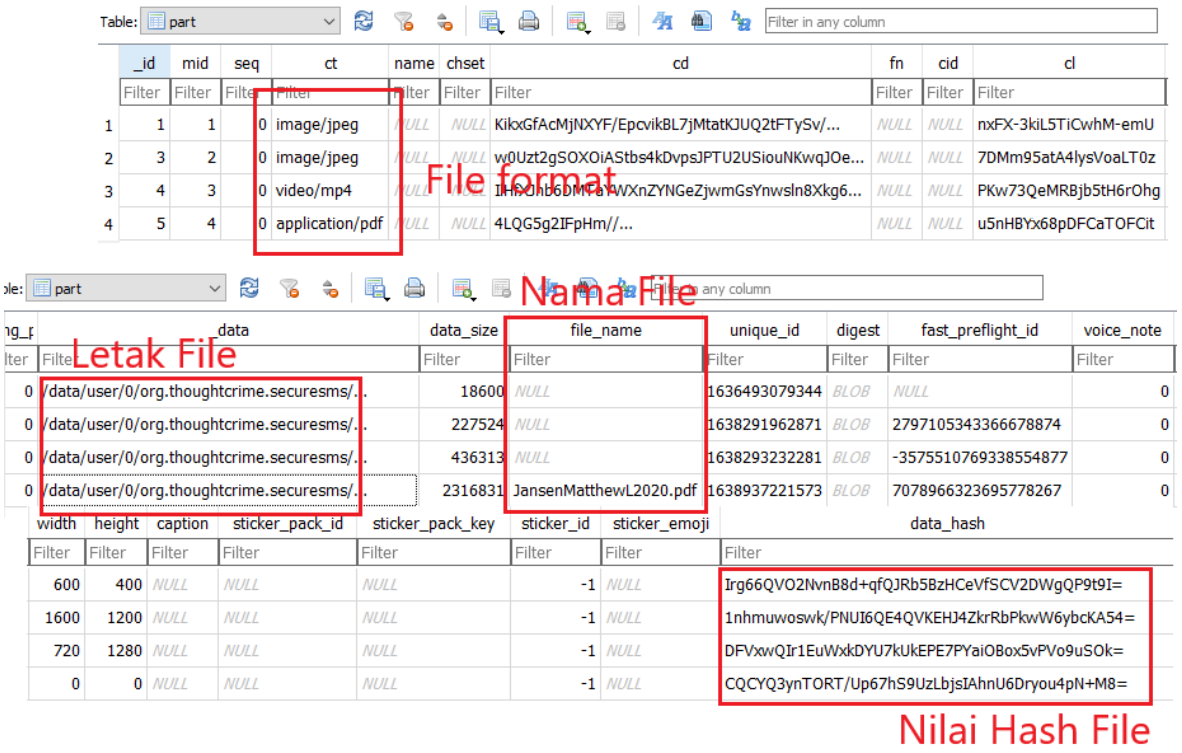
Seperti pada gambar 4.22 pada kolom body terdapat teks pesan. Kemudian untuk pesan yang telah dihapus pada tabel tertulis *NULL*. Setelah itu analisis berlanjut pada tabel *mms*.



	_id	thread_id	date	date_received	date_server	msg_box	read	body	part_count	ct_l	address	address_device_id	exp	m_type	m_size	st	tr_id
1	1	1	1636493061284	1636493079318	1636493079910	10485780	1	NULL	1		15	NULL	NULL	132	NULL	1	NULL
2	2	1	1638291966212	1638291966222	-1	10485783	1		0	NULL	15	NULL	NULL	128	NULL	NULL	NULL
3	3	1	1638293236513	1638293236531	-1	10485783	1		0	NULL	15	NULL	NULL	128	NULL	NULL	NULL
4	4	1	1638937221366	1638937221557	-1	10485783	1		1	NULL	15	NULL	NULL	128	NULL	NULL	NULL

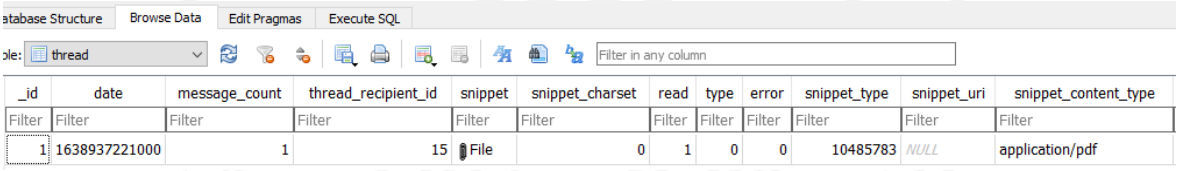
Gambar 4.23 Isi Data Tabel mms

Pada tabel mms ditemukan data pada tabel namun tidak terdapat keterangan mengenai data jenis tersebut. Kemudian analisi berlanjut pada tabel *part.*



Gambar 4.24 Isi Data Tabel Part

Seperti pada gambar tabel part menyimpan data mengenai file yang dikirim seperti gambar, video, maupun document. Pada kolom *file_name* hanya file document yang mempunyai nilai. Pada tabel part juga menyimpan data hash dari masing-masing file yang diupload. Kemudian analisis berlanjut pada tabel *thread.* Pada gambar 4.25 ini terlihat tabel *thread* menyimpan data file dokumen yang diupload. Tabel lain yang terdapat database selebihnya kosong sehingga tidak dimuat dalam tulisan ini.



Gambar 4.25 Isi Data Tabel Thread

Dari hasil analisis menggunakan *file backup* Signal Messenger semua dirangkum kedalam tabel 4.2 berikut.

Tabel 4.3 Perbandingan Analisis Data Backup

Perangkat	Software	Artifak Pada Database					
		Pesan Teks	Pesan Gambar	Pesan Video	Panggilan Suara	Panggilan Video	File Dokumen
Samsung SM A530F	Signal-Back	n/a	✓	✓	n/a	n/a	✓
	Signalbackup-tools	✓	Informasi gambar	✓	n/a	n/a	Informasi dokumen
Redmi Note 4	Signal-Back	n/a	✓	✓	n/a	n/a	✓
	Signalbackup-tools	✓	Informasi gambar	✓	n/a	n/a	Informasi dokumen

* n/a (not available)

Berdasarkan latar belakang masalah mengenai proses mencari jejak digital aplikasi Signal Messenger berbasis Android dapat dirumuskan bahwa untuk proses akuisisi tidak mengalami kendala. Software Magnet AXIOM mampu melakukan akuisisi dengan baik. Kemudian dalam proses analisis artifak hasil akuisisi, software yang digunakan tidak mampu membaca database dari aplikasi Signal Messenger karena database *signal.db* dilindungi oleh enkripsi. Namun beberapa informasi seperti nomor akun yang digunakan, kemudian beberapa informasi kapan aplikasi terakhir digunakan masih bisa ditampilkan.

Pada analisis data backup, dua software yang digunakan yaitu Signal-Back dan Signalbackup-tools mampu mengekstrak data dari file backup. Pada Signal-Back terdapat kendala ketika proses ektraksi database file *.xml* yang dihasilkan tidak menampilkan data apapun namun untuk data lain seperti gambar, video, dan file dokumen bisa ekstrak dengan baik. Pada software Signalbackup-tools database berhasil dienktrak kemudian database tersebut dianalisis menggunakan *DB Browser for SQLite* dimana beberapa artifak seperti pesan teks, gambar, video, dan file dokumen tercatat pada tabel. Disini penulis mendapat kendala dan tidak bisa menemukan data untuk panggilan suara maupun panggilan video.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Setelah dilakukan serangkaian penelitian dan analisa terhadap perangkat android Samsung SM A530F dan Redmi Note 4 terkait penelitian aplikasi Signal Messenger versi 5.27.13 dapat disimpulkan sebagai berikut:

a. Dalam penelitian ini penerapan metode NIST berjalan dengan baik. Akusisi dengan menggunakan software Magnet AXIOM 4.10 dan hasil Akuisisi terbaca dengan baik oleh software Magnet AXIOM 4.10, MobileEdit Express 7.1, dan Autopsy 4.18 namun software tersebut tidak dapat membaca database dari aplikasi Signal Messenger yang ter *decrypt* sehingga informasi mengenai pesan, media, video, file tidak dapat diperoleh.
b. Analisis *data backup* dengan menggunakan software Signal-back mampu menampilkan media yang tersimpan dalam data backup seperti gambar, video, file sedangkan untuk software Signalbackup-tools file database dapat didecrypt dan diektrak dan kemudian data pada pada database dapat ditampilkan dan menyimpan informasi seperti pesan teks, pesan gambar, pesan video serta informasi file dokumen namun tidak ditemukan data mengenai panggilan suara maupun panggilan video.

Dari beberapa software yang telah diuji beberapa digital artifak yang berhasil didapat dan kemudian bisa dijadikan sebagai barang bukti adalah data pesan teks, media gambar, media video, dan file dokumen.

5.2 Saran

Pada penelitian ini beberapa software yang digunakan seperti Magnet AXIOM 4.10, MobileEdit Express 7.1, dan Autopsy 4.18 belum mampu untuk membaca database aplikasi Signal Messenger yang terenkripsi. Kemudian software Signal-back dan Signalbackup-tools yang digunakan untuk melakukan *decrypte* pada data backup tidak mampu menampilkan panggilan suara dan panggilan video. Oleh karena itu diharapkan untuk penelitian berikutnya mampu melakukan analisis lebih lanjut dengan file akuisisi serta data backup yang dapat menampilkan informasi lebih lengkap.

Daftar Pustaka

Al-Azhar, & Muhammah, N. (2012). *Digital Forensik Panduan Praktis Investigasi Komputer*.

Ayers, R., Brothers, S., & Jansen, W. (2007). Guidelines on Cell Phone Forensics Guidelines on Mobile Device Forensics. *Archived NIST Technical Series Publication Archived Publication*, *1*. http://dx.doi.org/10.6028/NIST.SP.800-101r1http://csrc.nist.gov/groups/SNS/mobile_security/index.htmlN/A

Casey, E. (2011). *Digital Evidence and Computer Crime*. Elsevier Science.

Choi, J., Park, J., & Kim, H. (2017). Forensic analysis of the backup database file in KakaoTalk messenger. *2017 IEEE International Conference on Big Data and Smart Computing, BigComp 2017*, 156–161. https://doi.org/10.1109/BIGCOMP.2017.7881732

Daniel, L., & Daniel, L. (2012). Digital Forensics for Legal Professionals. In *Digital Forensics for Legal Professionals*. https://doi.org/10.1016/C2010-0-67122-7

Fadillah, M. N., Umar, R., & Yudhana, A. (2018). Rancangan Metode Nist Untuk Forensik Aplikasi Mobile Payment Berbasis Android. *Seminar Nasional Informatika 2018 (SemnasIF 2018)*, *2018*(November), 115–119. http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2626

Halim, S. H. S. (2012). *Panduan Praktis Dijital Forensik*.

Harrill, D. C., & Mislan, R. P. (2007). A Small Scale Digital Device Forensics ontology. *Small Scale Digital Device Forensics Journal*, *1*(1), 1–7.

Hsieh, R. J. (2019a). Digital evidence and computer forensics. *Introduction to Forensic Science and Criminalistics*, 201–221. https://doi.org/10.4324/9781315119175-9

Hsieh, R. J. (2019b). Digital evidence and computer forensics. *Introduction to Forensic Science and Criminalistics*, *December*, 201–221. https://doi.org/10.4324/9781315119175-9

Kaczyński, K. (2019). *SECURITY ANALYSIS OF SIGNAL ANDROID*. *11*, 63–70.

Latuconsina, N. M., & Yunanto, P. W. (2017). Pembuatan Bank Soal Dan Analisis Butir Soal Mata Kuliah Kriptografi Untuk Mahasiswa Program Studi Pendidikan Teknik Informatika Dan Komputer Universitas Negeri Jakarta. *PINTER : Jurnal Pendidikan Teknik Informatika Dan Komputer*, *1*(2), 142–145. https://doi.org/10.21009/pinter.1.2.7

Messenger, A. L. (2018). A Study of Mobile Forensic Tools Evaluation on. *(IJACSA) International Journal of Advanced Computer Science and Applications*, *9*(10), 201–206.

Muhammad Kukuh Tri Haryanto. (2018). *Analisa Forensics Terhadap Database Sqlite pada Aplikasi IMO Berbasis Android*. 17.

Praset yo Aji, M., Riadi, I., Fadlil, A., & Fauzan, A. (2018). Evidence Gathering and Identification of LINE Messenger on Android Device. *Messenger Using NIST Mobile Foren… Journal of Comput Er Science IJCSIS Journal of Comput Er Science*, *16*(5), 201–205. https://sites.google.com/site/ijcsis/

Sarwono, J. (2006). *Metode Penelitian Kuantitatif dan Kualitatif* (Vol. 1, Issue 2, pp. 46–51). http://www.pps.unud.ac.id/thesis/pdf_thesis/unud-1353-426991514-tesis dewa ayu.pdf

Singh, M. (2021). *Signal's Brian Acton talks about exploding growth, monetization and WhatsApp data-sharing outrage*. Https://Techcrunch.Com/. https://techcrunch.com/2021/01/12/signal-brian-acton-talks-about-exploding-growth-monetization-and-whatsapp-data-sharing-outrage/

Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile forensic tools evaluation for digital crime investigation. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(3), 949–955. https://doi.org/10.18517/ijaseit.8.3.3591