SKRIPSI

ANALISIS *MOBILE FORENSICS* EKSTRAKSI *FILE* PADA APLIKASI *WHATSAPP* YANG TELAH TERHAPUS MENGGUNAKAN *FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* (NIST)

OLEH
Rahmat Kalfi
07352011057

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS KHAIRUN
TERNATE

2024

LEMBAR PENGESAHAN

ANALISIS *MOBILE FORENSICS* EKSTRAKSI FILE PADA APLIKASI *WHATSAPP* YANG TELAH TERHAPUS MENGGUNAKAN *FRAMEAWORK NATIONAL INSTITUTE OF STANDARS AND TECNOLOGY* (NIST)

Oleh
Rahmat Kafli
07352011057

Skripsi ini telah disahkan
Tanggal 21 Juni 2024

Menyetujui
Tim Penguji

Ketua Penguji

Dr. MUHAMMAD RIDHA ALBAAR, S.Kom., M.Kom.
NIP. 198504232008031001

Pembimbing I

ALFANUGRAH A. HI. USMAN, S.T., M.Kom.
NIP. 199403182019032029

Anggota Penguji

ROSIHAN S.T., M.Cs.
NIP. 197607192010121001

Pembimbing II

YASIR MUIN, S.T., M.Kom.
NIDN. 9990582796

Anggota Penguji

SAIFUL Do. ABDULLAH, S.T., M.T.
NIDN. 0018029002

Mengetahui/Menyetujui

Koordinator Program Studi
Informatika

ROSIHAN S.T., M.Cs.
NIP. 197607192010121001

Dekan Fakultas Teknik
Universitas Khairun

Ir. ENDAH HARISUN, S.T., M.T., CRP.
NIP. 197511302005011013

LEMBAR PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	:	Rahmat Kalfi
NPM	:	07352011057
Fakultas	:	Teknik
Jurusan/Program Studi	:	Informatika
Judul Skripsi	:	Analisis *Mobile Forensics* Ekstraksi File Pada Aplikasi *Whatsapp* Yang Telah Terhapus Menggunakan *Framework National Institute Of Standards And Technology* (NIST)

Dengan ini menyatakan bahwa penulis Skripsi yang telah saya buat ini merupakan hasil karya sendiri dan benar keasliannya. Apabila ternyata di kemudian hari penulis Skripsi ini merupakan hasil plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggung jawabkan sekaligus bersedia menerima sanksi aturan tata tertib Universitas Khairun.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Penulis

Rahmat Kalfi

LEMBAR PERSEMBAHAN

Pertama saya ucapkan puji syukur kehadirat Allah SWT atas segala nikmat kesehatan, hidayah dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan skripsi ini. Shalawat serta salam senantiasa penulis curahkan kepada junjungan Nabi besar Muhammad SAW beserta sahabat, keluarga dan para pengikutnya hingga akhir zaman. Skripsi ini penulis persembahkan sebagai bukti semangat dan usaha serta cinta dan kasih sayang kepada orang-orang yang sangat berharga dalam hidup penulis. Skripsi ini peulis persembahkan kepada:

1. Panutanku Ayahanda Sulaiman idris dan Ibunda Rahmi tercinta yang menjadi pintu surga bagi penulis. Yang telah mendidik dan membesarkan penulis dalam limpahan kasih sayang. Yang selalu berjuang memberikan dukungan moral, materil serta selalu melangitkan do'a untuk memperjuangkan masa depan dan kebahagiaan anak-anaknya. Terima kasih atas kasih sayang yang tiada hentinya, sehat selalu dan hiduplah lebih lama agar dunia saya tetap baik.
2. Adik-adik tercinta Sukmawati, Abudzal Algifahri, dan M. Zaki Zatmika sumber penyemangat penulis untuk terus berjuang dan bahagia.Terima kasih atas semangat, do'a dan cinta yang selalu diberikan kepada penulis. Tumbuhlah menjadi versi paling hebat, adik-adikku.

MOTTO:

"Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya"

(QS. Al-Baqarah:286)

"Setetes keringat orang tuaku, seribu langkahku untuk maju"

KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah *Subhanahu wata'ala* yang telah melimpahkan rahmat, taufik, hidayah-Nya. Sehingga penulis dapat menyusun skripsil ini dengan judul "Analisis *Mobile Forensics* Ekstraksi *File* Pada Aplikasi *Whatsapp* Yang Telah Terhapus Menggunakan *Framework* Nist", ini dapat diselesaikan untuk memenuhi salah satu persyaratan penyelesaian pendidikan sarjana Informatika Strata Satu (S1) pada Program Studi Informatika Fakultas Teknik Universitas Khairun.

Untuk menyelesaikan skripsi ini penulis sepenuhnya mendapat dukungan dari banyak pihak, oleh karena itu dengan rendah hati penulis mengucapkan terimakasih kepada:

1. Bapak Dr. Ridha Ajam, M.Hum., selaku Rektor Universitas Khairun Ternate.
2. Bapak Endah Ir. Harisun,S.T,.M.T.,CRP., selaku dekan Fakultas Teknik Universitas Khairun.
3. Bapak Rosihan, S.T., M.Cs., selaku Koordinator Program Studi Informatika Fakultas Teknik Universitas Khairun dan selaku Penguji II yang telah memberikan masukan, kritikan dan saran demi perbaikan Skripsi ini.
4. Ibu Alfanugrah A. Hi. Usman., S.T., M. Kom., sebagai Pembimbing I, terima kasih atas bimbingannya, serta dukungan dalam penyelesaian Skripsi ini.
5. Bapak Yasir Muin, S.T., M.Kom., sebagai Pembimbing II, terima kasih atas bimbingannya, serta dukungan dalam penyelesaian Skripsi ini.
6. Bapak Dr. Muhammad Ridha Albaar, S.Kom., M.Kom., Selaku Penguji I yang telah memberikan masukan, kritikan dan saran demi perbaikan Skripsi ini.
7. Bapak Saiful Do. Abdullah, S.T., M.T., Selaku penasehat akademik dan selaku Penguji III yang telah memberikan masukan, kritikan dan saran demi perbaikan Skripsi ini.
8. Kepada Kedua orang tua yang senantiasa memberikan dukungan dan kasih sayang yang senantiasa dilimpahkan kepada penulis hingga saat ini.
9. Kepada Wilda rezki Akhirunisa yang telah memberi dukungan serta *support* kepada penulis untuk menyelesaikan Skripsi ini.
10. Kepada *Circle Pejuang S.Kom* yang selalu memberi semangat agar penyusunan skripsi ini cepat selesai.

11. Kepada *Circle Bismillah Desember* yang selalu memberi semangat agar penyusunan skripsi ini cepat selesai.
12. Sahabat seperjuangan yang selalu memberikan saran kepada penulis agar dapat mengerjakan laporan skripsi dengan baik.

Akhir kata, dengan penuh kesadaran diri dan segala kerendahan hati penulis menyadari hanya Allah yang memiliki segala kesempurnaan, sehingga masih banyak lagi rahasia-Nya yang belum tergali dan penulis ketahui. Semoga Allah *Subhanahu wata'ala* selalu memberikan yang terbaik kepada semua pihak yang selalu membantu penulis. Aamiin.

Ternate, 21 Juni 2024

Penulis

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

ABSTRAK

ANALISIS *MOBILE FORENSICS* EKSTRAKSI *FILE* PADA APLIKASI *WHATSAPP* YANG TELAH TERHAPUS MENGGUNAKAN *FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* (NIST)

Rahmat kalfi[1], Alfanugrah A. Hi. Usman., S.T., M. Kom.[2], Yasir Muin, S.T.,M.Kom.[3]
program Studi Informatika, Fakultas Teknik, Universitas Khairun
Jl.Jati Metro, Kota Ternate
E-mail : rahmatkalfi18@gmail.com[1],Nugrahalfa@gmail.com[2],yasirmuin@unkhair.ac.id[3]

Pemanfaatan teknologi di era digital yang berkembang pesat menjadikan aplikasi pesan instan seperti *Whatsapp* sebagai bagian integral dari kehidupan sehari-hari, tetapi juga berpotensi disalahgunakan untuk tindak kejahatan siber. Penelitian ini bertujuan untuk menganalisis dan mengekstraksi data yang telah terhapus pada aplikasi *Whatsapp* menggunakan *framework National Institute of Standards and Technology* (NIST). Studi ini dilakukan dengan menggunakan *smartphone* Oppo A37f dan iPhone 7 Plus serta berbagai alat forensik seperti *Android Debug Bridge* (ADB), *Mobile*dit *Forensics*, dan FTK Imager. Hasil penelitian menunjukkan bahwa pada perangkat *Android*, seluruh bukti berhasil ditemukan melalui metode akuisisi menggunakan ADB dan analisis lebih lanjut dengan *Tools Autopsy*, sementara pada perangkat iPhone, akuisisi data hanya mampu menemukan data logis tanpa data yang telah dihapus sepenuhnya karena keterbatasan *Tools* yang digunakan. Penelitian ini menyoroti pentingnya pemilihan alat dan metode yang tepat dalam proses ekstraksi data forensik, terutama mengingat perbedaan keamanan antara sistem operasi *Android* dan iOS, dan menyimpulkan bahwa *framework* NIST efektif untuk analisis forensik pada perangkat *Android*, namun memerlukan pendekatan berbeda untuk perangkat iOS.

Kata kunci *:* *Mobile Forensics*, NIST *Framework*, Forensik aplikasi *Whatsapp*, *Recovery Deleted Messages*

ABSTRACT

MOBILE FORENSICS ANALYSIS OF FILE EXTRACTION ON DELETED WHATSAPP APPLICATIONS USING THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) FRAMEWORK

Rahmat kalfi[1], Alfanugrah A. Hi. Usman., S.T., M. Kom.[2], Yasir Muin, S.T.,M.Kom.[3]
Informatics Study Program, Faculty of Engineering, Khairun University
Jl.Jati Metro, Ternate City
E-mail : rahmatkalfi18@gmail.com[1],Nugrahalfa@gmail.com[2],yasirmuin@unkhair.ac.id[3]

The use of technology in the rapidly developing digital era makes instant messaging applications such as Whatsapp an integral part of everyday life, but also has the potential to be misused for cybercrime. This study aims to analyze and extract deleted data on the Whatsapp application using the National Institute of Standards and Technology (NIST) framework. This study was conducted using Oppo A37f and iPhone 7 Plus smartphones and various forensic tools such as Android Debug Bridge (ADB), Mobiledit Forensics, and FTK Imager. The results of the study show that on Android devices, all evidence was successfully found through the acquisition method using ADB and further analysis with Autopsy Tools, while on iPhone devices, data acquisition was only able to find logical data without data that had been completely deleted due to the limitations of the Tools used. This study highlights the importance of choosing the right tools and methods in the forensic data extraction process, especially considering the security differences between the Android and iOS operating systems, and concludes that the NIST framework is effective for forensic analysis on Android devices, but requires a different approach for iOS devices.

Keywords: Mobile Forensics, NIST Framework, Whatsapp application forensics, Recovery Deleted Messages

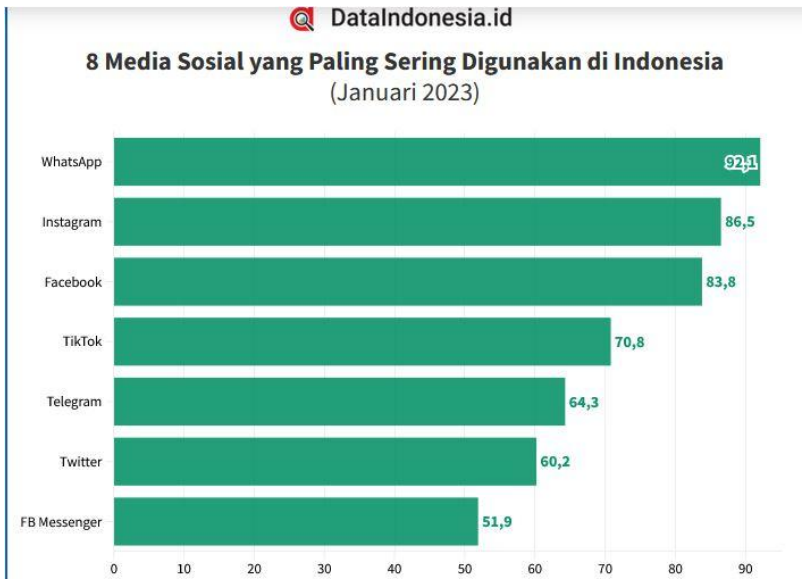
BAB I

PENDAHULUAN

1.1. Latar Belakang

Pemanfaatan teknologi di era digital yang berkembang pesat, aplikasi pesan instan telah menjadi bagian integral dari kehidupan sehari-hari, mengubah cara orang berkomunikasi dan berbagi informasi. Salah satu aplikasi paling populer adalah *Whatsapp*, yang digunakan oleh miliaran orang di seluruh dunia. *Whatsapp* bukan hanya platform komunikasi, tetapi juga berfungsi sebagai wadah penyimpanan data pribadi, foto, video, dan dokumen yang memiliki nilai penting bagi penggunanya (Zuhri , 2022).

Pengguna *smartphone* tidak terlepas dari penggunaan aplikasi *whatsapp*. *Whatsapp* sebagai salah satu pesan instan memiliki banyak pengguna dan pemakaiannya cukup tinggi di kalangan masyarakat. sebagaimana yang ditunjukan pada gambar 1.1 berikut.



Gambar 1.1. Data Pengguna Media Sosial (Dataindonesia.id 2023)

Aplikasi *whatsapp* banyak digunakan untuk kepentingan bersosialisasi maupun sebagai media penyampai pesan baik individu maupun kelompok. Para pengguna tentu

saja memiliki motif tertentu dalam menggunakan *whatsapp*, baik itu digunakan sebagai kepentingan pribadi maupun kepentingan kelompok (Hatta, 2022.). Pemanfaatan *Whatsapp* juga dapat disalah gunakan sebagai tindak kejahatan siber seperti penyebaran informasi palsu, pencurian identitas, dan penyelundupan data pribadi (Sari , 2023), sebagaimana yang ditunjukkan pada data e-MP Robinopsnal Bareskrim Polri menunjukan kepolisian menangani sebanyak 8.831 kasus cyber crime sejak 1 januari hingga 22 desember 2022 (Pusiknas, 2023). Dalam melakukan tindakan *cybercrime* pada pesan instan *whatsapp*, pelaku dapat menyembunyikan jejak kejahatan dengan menghapus bukti digital dari perangkat elektronik untuk menghilangkan jejak digita. Bukti digital sangat berperan penting dalam mengungkapkan kasus kejahatan siber (Riadi, 2019)

Mobile Forensik merupakan salah satu cabang dari digital forensik yang dilakukan untuk menemukan dan menganalisis barang bukti digital terkait dengan kasus *cybercrime* agar dapat dipertanggungjawabkan secara hukum. Barang bukti elektronik merupakan barang bukti elektronik yang dikenali secara fisik seperti perangkat komputer, *smartphone* maupun media penyimpanan. Sedangkan bukti digital merupakan hasil ekstrak atau *recovery* dari bukti elektronik seperti akun ID, kontak, text percakapan, dokumen, *file* multimedia (suara / gambar / video), atau *file* log (Yudhana, 2020).

Penerapan ilmu *Mobile* forensik dapat mengidentifikasi, menganalisis, dan mengekstraksi data berupa barang bukti digital pada aplikasi pesan instan *whatsapp* yang telah terhapus. terdapat empat tahapan pembuktian bukti digital yaitu Pengumpulan barang bukti, Pemeriksaan bukti digital, Analisis, dan yang terakhir adalah Pelaporan (Riadi, 2019). Dalam penanganan bukti digital diperlukannya metode atau *framework* sebagai sebuah teknik dalam menemukan bukti digital, *Framework National Institue Of Standards and Teknology (NIST)* merupakan salah satu *framework* yang digunakan dalam

bidang forensik yang sudah memiliki alur yang sistematis dan memiliki standar-standar oprasional dalam pengelolaan barang bukti untuk menjaga integritas dari barang bukti digital.

Berdasarkan latar belakang di atas, penelitian bertujuan untuk bagaimana melakukan analisis ekstraksi data yang telah terhapus pada aplikasi *whatsapp* menggunakan *framework National Institute of Standards and Technology* (NIST) . Penelitian ini dapat sebagai acuan referensi untuk penyelidikan lain, membahas tentang *Mobile* forensik dalam membantu penyidik memperoleh barang bukti, dan sebagai pengetahuan dalam memahami proses ekstraksi data sesuai dengan kaidah forensik.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah di atas, merumuskan masalah bagaimana melakukan analisis *Mobile* forensik pada aplikasi *whatsapp* dalam proses ekstraksi *file* pada *whatsapp* yang telah terhapus menggunakan *framework National Institute of Standards and Technology (*NIST).

1.3. Batasan Masalah

Adapun batasan masalah yang ada dalam penelitian ini dibatasi beberapa masalah sebagai berikut:

1. Penelitian ini hanya akan berfokus pada proses pengambilan data yang telah terhapus pada *smartphone* menggunakan *Tools Mobiledit Forensisc* .
2. Penelitian ini hanya berfokus data- data yang terdapat pada penyimpanan internal aplikasi *whatsapp* di *smartphone*.
3. Pengembalian barang bukti digital hanya berupa percakapan , foto/gambar , dan menampilkan daftar kontak pengguna *whatsapp*.

4. *Framework* yang digunakan adalah *National Institute of Standards and Technology* (NIST).
5. *Smarpohe* yang digunakan yaitu 1 buah *smartphone iphone* 7 plus dan 1 buah *smartphone* oppo 37f.

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah diatas, penelitian ini bertujuan mengetahui hasil dari analisis *Mobile* forensik pada ekstraksi *file* yang telah terhapus pada aplikasi *whatsapp* menggunakan *framework National Institute of Standards and Technology (*NIST).

1.5. Manfaat Penelitian

Penelitian ini memiliki beberapa manfaat sebagai berikut:

1. Penelitian ini dapat membantu dan memahami tentang proses penanganan sebuah barang bukti dalam digital forensik.
2. penelitian ini juga dapat sebagai rujukan penelitian penelitian selanjutnya yang saling berkaitan.
3. penelitian ini juga dapat membantu dalam penanganan kehilangan data yang terhapus pada *smartphone* tanpa disengaja.

1.6. Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan untuk kasus yang akan dipecah.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang teori-teori yang akan digunakan untuk penelitian rekomendasi.

BAB III METODE PENELITIAN

Bab ini menjelaskan langkah-langkah metode penelitian untuk rekomendasi dalam pemecahan masalah.

BAB IV HASIL PEMBAHASAN

Bab ini membahas tentang hasil dari peneritian yang telah dilakukan

BAB V PENUTUP

Memuat kesimpulan dari hasil penelitian yang telah dilakukan, dan saran untuk penelitian selanjutnya mengenai topik terkait.

BAB II

TINJAUAN PUSTAKA

2.1. Penelitian Terkait

Penelitian terkait merupakan penelitian terdahulu yang berkaitan dengan penelitian yang sedang diteliti, untuk mengetahui perbedaan penelitian terkait dengan penelitian yang akan dilakukan dapat dilihat pada tabel 2.1.

Tabel 2. 1 Penelitian Terkait

No	Penulis	Judul penelitian	Hasil penelitian
1.	Imam Riadi, Sunardi, Sahiruddin, 2019	Analisis Forensik *Recovery* pada *Smartphone Android* Menggunakan *Metode National Institute Of Justice* (NIJ)	Hasil yang didapatkan dari proses penelitian mengenai analisis forensik *recovery* pada *smartphone android* menggunakan *metode national institute of justice* (NIJ), memberikan kesimpulan sebagai berikut : 1. Data yang telah dihapus pada perangkat *smartphone android* masih dapat dikembalikan menggunakan *Tools* Wondershare dan Bekasoft. 2. *Tools* forensik yang digunakan tidak cukup baik untuk mengembalikan data gambar, video dan *file* dokumen. Wondershare dan Belkasoft dapat mengembalikan data yang telah dihapus berupa data kontak, log panggilan, dan pesan, sedangkan *Tools Mobile*dit hanya dapat menampilkan data pada perangkat *smartphone* tetapi tidak dapat mengembalikan data yang terhapus (Riadi, 2019).
2	Nasirudin, Sunardi, Imam Riadi, 2020	Analisis Forensik *Smartphone Android* Menggunakan Metode NIST dan *Tools Mobile*dit *Forensic Express*	Hasil *Forensic smartphone* berbasis *android* merek samsung galaxy A8 dihasilkan beberapa dari target yang diinginkan guna dianalisa dandikembangkan untuk mendapatkan bukti digital dengan metode *National Institute of Standard and Technology* dan menggunakan *Tools Mobile*dit. *Forensic* Express dan dianalisa secara manual sehingga hasil yang didapat belumterpenuhi,

			ke depannya penulis akanmengembangkan cara menganalisa agar terdapathasil bukti digital yang diharapkan guna kepentingan penyidikan kasus kejahatan digital (Nasirudin , 2020)
3.	Novi Saputri, Rini Indrayani, 2022	Analisis Data Forensik Investigasi Kasus Peredaran Narkoba Pada *Smartphone* Berbasis *Android*	Bukti *Whatsapp* yang didapat melalui akses *rooting* lebih lengkap dan komprehensif terhadap bukti yang didapat, berbeda dengan proses tanpa *rooting* data yang dihasilkan hanya sebagian kecil saja, dengan demikian dikarenakan kasus-kasus yang dipelajari dengan proses tanpa *root* dan akses *root* mempunyai tujuan yang sama untuk saling melengkapi kekurangan dalam memperoleh bukti digital. Berdasarkan dari hasil pengujian yang dilakukan dapat disimpulkan bahwa Magnet AXIOM merupakan alat forensik yang direkomendasikan dalam penelitian ini (Saputri, 2022).
4.	Riya Maja*list*a, Tata Sutabri, 2023	Analisis Pencarian Data *Smartphone* Menggunakan NIST Untuk Penyelidikan Digital Forensik	Aktivitas siber merupakan aktivitas virtual yang dampaknya nyata, walaupun buktinya berupa elektronik. Oleh karena itu, target pelaku haruslah orang yang benar-benar melakukan pelanggaran hukum. Berdasarkan kasus yang disimulasikan, ada dua aspek hukum yang harus diperhatikan, yang pertama adalah kejahatan malware menurut hukum positif Indonesia yaitu Pasal 34 UU ITE, di gunakan untuk menyalah gunakan perangkat keras atau perangkat lunak. Untuk kasus kedua, yaitu hilangnya barang bukti, berlaku Pasal 282 KUHP. Dengan menggunakan metode dalam, penelitian ini, dapat disimpulkan bahwa data dapat dicari berdasarkan asumsi data dan analisis data,sehingga data dapat ditemukan dalam sistem meskipun data tersebut dihapus atau disembunyikan. Analisis pencarian data pada *smartphone* ini dapat di jadikan bahan pendukung untuk penyelidikan digital forensik, bahkan dapat menjadi bukti dari kejahatan yang terjadi di dunia maya (Maja*list*a, 2023).

5.	Mulia Fitriana, 2019	Penerapan Metode *National Institute Of Standards And Technology* (Nist) Dalam Analisis *Forensic* Digital Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku	Berdasarkan permasalahan yang telah dijabarkan sebelumnya, maka dapat ditarik kesimpulan sebagai berikut: Dengan menerapkan metode *National Institute of Standards and Technology* (NIST) maka akan mempermudah peneliti dalam menemukan barang bukti kejahatan digital pada *smartphone* yang dapat dijadikan barang bukti tindak pidana dengan mengikuti tah demi tahap yang terdapat dalam metode *National Institute of Standards and Technology* (NIST). *Tools*s forensik yang digunakan untuk menemukan barang bukti digital pada perangkat pelaku adalah *Kingroot* (*Tools*s untuk melakukan *Rooting* pada *smartphone*), CWM (ClockworkMod) *Recovery* (*File* CWM yang akan diinstall), Flashify (untuk menginstall CWM), AccessData FTK Imager (melakukan *imaging* data), *Whatsapp Viewer* (mendeskripsikan *database Whatsapp* yang terenkripsi dan membuka *database Whatsapp* yang sudah terenkripsi), DB Browser for SQLite (membuka folder wa.db untuk melihat daftar kontak ponsel). Berdasarkan kasus yang disimulasikan maka aspek hukum yang akan dikenai ada dua, yang pertama adalah aspek hukum untuk kasus pornografi dikenai 64 Undang-undang pasal 27 ayat (1) UU ITE. Kasus yang kedua yaitu penghilangan barang bukti akan dikenai pasal 282 KUHP. Berdasarkan kasus yang disimulasikan dan terjadi penghilangan barang bukti maka menurut ahli hukum undang-undang yang telah disebutkan diatas sudah sesuai dengan kasus tersebut (Fitriana, 2020).

Penelitian dengan judul "Analisis *Mobile Forensics* Ekstraksi *File* Pada Aplikasi *Whatsapp* Yang Telah Terhapus Menggunakan *Framework National Institue Of Standards and Teknology (NIST)* " membahas tentang menganalisa proses *Mobile* forensik ekstraksi *file* yang telah terhapus pada aplikasi *whatsapp* memanfaatkan *framework* NIST.

Penelitian ini menggunakan skenario sebagai hasil simulasi untuk mengatahui hasil dari proses ekstraksi tersebut. Penelitian ini dapat dijadikan referensi untuk penyelidikan lain, membahas tentang *Mobile* forensik dalam mempantu penyidik menemukan barang bukti digital, dan sebagai pengatahuan dalam memahami proses ekstraksi data sesuai kaida forensik.

2.2. *Digital Forensics*

Digital Forensics merupakan penerapan ilmu pengetahuan untuk memulihkan bukti *digita*l dari suatu perangkat baik itu komputer maupun *smartphone* dengan metode tertentu yang bertujuan untuk mengumpulkan data yang dapat diterima oleh pengadilan sebagai salah satu pembuktian. Semua fakta atau data yang terbaca dan berhasil didapatkan oleh pakar komputer forensik harus terjaga kondisinya, sehingga dapat dibuktikan bahwa data tersebut memang benar adanya dan tidak mengalami perubahan, baik disengaja maupun tidak (Fitriana, 2020).

Dalam hal ini ada hal- hal yang perlu di perhatikan seperti *Standar Operasional Prosedur* (SOP). Standar yang digunakan oleh Indonesia dalam penanganan kasus digital forensik mencakup beberapa tahapan penting mulai dari identifikasi, pengumpulan, pengamanan, analisis, hingga pelaporan bukti digital. Ada beberapa SOP yang digunakan diantaranya.

1. Perkap No. 17 Tahun 2011 tentang Tata Cara Penanganan Barang Bukti di Lingkungan Kepolisian Negara Republik Indonesia.
2. SNI ISO/IEC 27037:2014: Pedoman untuk identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital.
3. ISO/IEC 17025: Standar untuk laboratorium forensik.

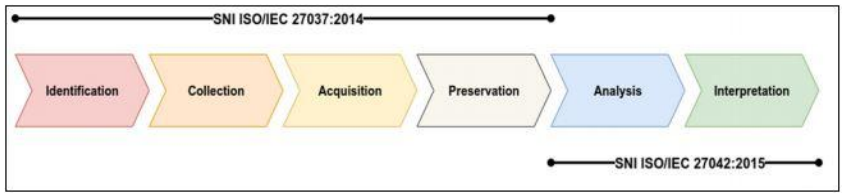
Adapun *Standar Operating Procedure* (SOP) yang disusun oleh Pusat

Laboratorium Forensik Polisi RI dalam menangani barang bukti digital antara satu kategori dengan kategori lainnya memiliki kesamaan atau memiliki tahapan yang sama. Terdapat 15 SOP dalam menangani setiap barang bukti elektronik dan/atau barang bukti digital diantaranya.

1. SOP 1 tentang prosedur analisa forensik digital.
2. SOP 2 tantang komitmen jam kerja.
3. SOP 3 tentang pelaporan forensik digital.
4. SOP 4 tentang menerima barang bukti elektronik dan/atau digital.
5. SOP 5 tentang penyerahan kembali barang bukti elektronik dan/atau digital.
6. SOP 6 tentang triage forensik (penanganan awal barang bukti komputer di TKP).
7. SOP 7 tentang akuisisi langsung.
8. SOP 8 tentang akuisisi harddisk, flashdisk dan memory card.
9. SOP 9 tentang analisa harddisk, flashdisk dan memory card.
10. SOP 10 tentang akuisisi ponsel dan simcard.
11. SOP 11 tentang analisa ponsel dan simcard.
12. SOP 12 tentang analisa forensik audio.
13. SOP 13 tentang analisa forensik video.
14. SOP 14 tentang analisa gambar digital.
15. SOP 15 tentang analisa forensik jaringan.

Beberapa negara menerapkan beberapa standardisasi pada forensik digital dalam pengungkapan suatu tindak kejahatan tetapi pada prinsipnya standardisasi satu dengan yang lainnya memiliki kemiripan. Sebagai contoh pada buku pedoman dasar digital forensik standardisasi yang digunakan adalah SNIISO/IEC 27037:2014, SNI ISO/IEC 27042:2015, dan NIST SP 80086. Untuk lebih komprehensif dalam melakukan proses

dan investi gasiforensik digital berdasar Standar Nasional Indonesia (SNI) menggunakan dua dokumen standardisasi yaitu SNI ISO/IEC 27037:2014 dan SNIISO/IEC 27042:2015. Pada SNI ISO/IEC 27037:2014 mengatur tatakelola forensik digital dari proses identifikasi, pengumpulan barang bukti elektronik, akuisisi barang bukti digital, dan preservasi. Sedangkan tatakelola forensik digital selanjutnya seperti analisis dan penyajian laporan diatur pada SNI ISO/IEC 27042:2015, tampak seperti pada Gambar 2.1.



Gambar 2.1. Kerangka SNI ISO/ICE 27037:2014(Haryadi, 2022)

Secara umum setiap standardisasi forensik digital memiliki prinsip yang harus dipegang teguh oleh tim forensik digital. Pada SNI ISO/IEC 27037:2014 telah diatur prinsip dasar forensik digital sebagai berikut (Haryadi, 2022).

1. Meminimalkan penanganan secara langsung terhadap barang bukti elektronik yang asli dan/atau barang bukti digital yang potensial.
2. Mencatat semua aktivitas.
3. Mengikuti aturan hukum yang berlaku.
4. Tim Forensik harus hati-hati dalam menangani kasus untuk menjaga nama baiknya

2.3. *Mobile Forensics*

Mobile Forensics merupakan cabang dari digital forensik, *Mobile* forensik bertujuan untuk melakukan pemulihan bukti digital atau data dari perangkat *Mobile*. Sedangkan digital forensik bertujuan untuk melakukan pemulihan bukti digital dari

perangkat digital termasuk pada perangkat *Mobile* (Fitriana, 2020).

Forensik seluler diperlukan karena layanan seluler meningkat dan jumlah pengguna meningkat. Dengan semakin populernya komputasi dan perdagangan seluler, kebutuhan akan perdagangan seluler juga meningkat. Kualitas dan kecepatan penyedia layanan seluler harus sebanding dengan transaksi seluler yang dilakukan. Tantangan transaksi seluler terletak pada banyaknya transaksi seluler yang dilakukan, terletak pada banyaknya penyedia layanan seluler dengan jaringan berkecepatan tinggi dan aman Transaksi *online* yang dilakukan menggunakan perangkat seluler harus sangat aman dan melindungi pengguna dari penyalahgunaan oleh pihak yang tidak bertanggung jawab.

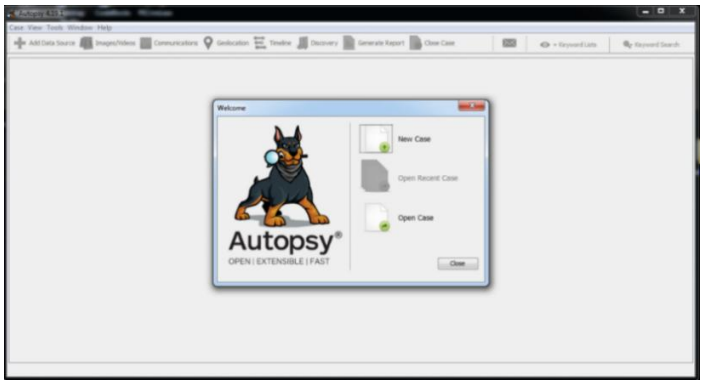
2.4. Mobiledit Forensics

Mobiledit Forensik adalah suatu *Software* yang berfungsi untuk penyelidikanatau pengambilan data pada *smartphone*. *Software* ini dapat membaca pesan, catatan panggilan, membaca SIM *card* dan lain sebagainya. Versi *lite Mobiledit* dapat didownload dari internet. Instalasi *Mobiledit* tidaklah terlampau sulit. Seperti juga *Oxygen*, *Mobiledit* membutuhkan kondisi USB *debugging mode enabled* di ponsel. Ponsel dapat terkoneksi baik menggunakan kabel langsung maupun menggunakankoneksi *wireless*. Hal ini memberikan keuntungan untuk jenis ponsel yang tidak dapat di detekesi menggunakan *Software* ini dapat diutilisasi menggunakan koneksi *wireless. Mobiledit* akan menginstal aplikasi kecil di ponsel untuk menarik data. Data yangdiekstrak dibatasi hanya *contacts*, *call list*, *messages* dan *File* (Riadi I, 2019) , dapat dilihat pada gambar 2.2 berikut ini.

Gambar 2.2. *Software Mobiledit Forensics Axiom* (Sumber : https://www.*Mobile*dit.com/*Mobile*dit-*Forensic*)

2.5. Autopsy

Autopsy adalah platform forensik digital dan antarmuka grafis ke *The Sleuth Kit* dan alat forensik digital lainnya. Ini digunakan oleh penegak hukum, militer, dan pemeriksa perusahaan untuk menyelidiki apa yang terjadi di komputer. Bahkan dapat menggunakannya untuk memulihkan foto dari kartu memori kamera. Pada dasarnya, otopsi adalah alat sumber terbuka gratis yang mendukung berbagai modul dan alat forensik digital lainnya. Dapat dilihat pada gambar 2.3 berikut ini.



Gambar 2.3 Tolls Forensik *Autopsy (Sumber: https://images.app.goo.gl/4DwB9h7yARCt6VaP6)*

Autopsy adalah perangkat lunak komputer yang menyederhanakan penerapan banyak program sumber terbuka dan plugin yang digunakan dalam *The Sleuth Kit*. antarmuka pengguna grafis menampilkan hasil pencarian forensik dari volume yang mendasarinya sehingga memudahkan penyelidik untuk menandai bagian data terkait.

Alat ini sebagian besar dikelola oleh Basis *Technology Corp*. dengan bantuan *pemrogram dari komunitas (Cybervie.com,* 2024*).*

2.6. Oxygen Forensic Detective

Oxygen Forensic adalah perangkat lunak forensik produksi *Oxygen Forensic* yang digunakan untuk keperluan ekstraksi dan analisis data dari ponsel, *smartphone* dan tablet. Penggunaan protokol berbayar yang canggih memungkinkan *Oxygen Forensic* untuk mengekstrak data lebih banyak dan menjamin pengoperasian tanpa merusak barang bukti. Perangkat lunak ini banyak digunakan oleh petugas penegak hukum, pemerintah, militer, penyelidik swasta dan spesialis forensik lainnya. (Anshori, 2021), dapat dilihat pada gambar 2.4.

Gambar 2.4. *Oxygen Forensic Detective(Sumber : https://images.app.goo.gl/hy6M2cwebBSS3FQE7)*

Oxygen Forensic Detective adalah perangkat lunak *Mobile Forensic* yang memiliki fitur ekstraksi data (data *extraction*), analisa data (data *analysis*), penampil data (data *viewer*) dan eksport data (data *export*). *Oxygen Forensic Detective* mampu mengekstraksi data dari berbagai macam perangkat, *Mobile devices (Apple IOS, android devices*, media & SIM *cards*), *drones, IOT devices* (Amazon Alexa & Google Home), cloud services (iCloud, Google, Microsoft, Samsung, Huawei, E-mail server, Facebook, Twitter, Instagram, Dropbox, *Whatsapp*, Telegram, Viber, WickrMe, etc), komputer dan

smartwatch.

2.7. *Kingroot*

Kingroot merupakan salah satu *Software* atau tools yang digunakan untuk melakukan *root*ing pada semua jenis smarthone Android. *Software* ini merupakan *Software* yang berasal dari Tiongkok yang mensupport hampir semua perangkat *smartphone* Android. Untuk melakukan *root*ing sendiri dibutuhkan beberapa persyaratan serta backup terlebih dahulu data-datapenting yang ada di *smartphone*. Beberapa model *smartphone* seperti HTC dan Sony Xperia akan membutuhkan tindakan yang lebih lanjut, karena keduamerek *smartphone* tersebut membutuhkan bootloader agar dapat melakukan proses *root*ing. Selain itu, proses *root*ing ini juga akan membatalkan garansi *smartphone* Anda. Ada beberapa persyaratan yang harus disiapkan sebelum melakukan proses *root*ing, yaitu sebagai berikut (Fitriana, 2020):

1. Baterai tidak boleh kurang dari 75%, ini untuk mengantisipasi agar *smartphone* tidak mati saat proses sedang berjalan.
2. Backup semua data-data penting yang ada di *smartphone*, termasuk kontak, pesan, dan lain-lain.
3. Pastikan *smartphone* memiliki akses internet saat melakukan proses *root*ing.

2.8. *3uTools*

3uTools merupakan perangkat lunak berbasis *Windows* yang digunakan untuk mengelola dan menyesuaikan perangkat iOS. Hal ini membuat pengguna dapat mencadangkan atau memulihkan data. Selain itu, *Software* ini juga bisa digunakan untuk mem-*flash* dan menerapkan *jailbreak* pada iPhone, iPad, dan iPod touch Apple. dapat mem-*flash firmware* hingga memasang atau melepas aplikasi melalui perangkat ini. Sekilas fungsi aplikasi ini mirip dengan iTunes yang memungkinkanmu menjalankan

pengaturan lebih *advance* pada perangkat. Meski termasuk *third party app*, aplikasi ini punya tampilan yang ramah pengguna dan fitur canggih (Laili zain, 2023).

2.9. *National Institute of Standards and Technology* (NIST)

National Institute of Standards and Technology (NIST) merupakan Badan Nasional Standar dan Teknologi, sebuah unit dari Departemen Perdagangan Amerika Serikat. Yang dulunya dikenal sebagai *National Bureau Of Standards* – NBS (Biro Standar Nasional), sebuah nama yang diberikan dari tahun 1901 sampai 1988. NIST memiliki program aktif untuk mendorong dan membantu industri dan ilmu pengetahuan untuk mengembangkan dan menggunakan standar ini. 16 Misi dari badan ini adalah untuk membuat dan mendorong pengukuran, standar dan teknologi untuk meningkatkan produktivitas, mendukung perdagangan, dan memperbaiki kualitas hidup semua orang. Sebagai bagian dari misi ini, ilmuwan-ilmuwan dan insinyur NIST secara terus menerus mengembangkan ilmu pengukuran, yang memungkinkan rekayasa yang diperlukan oleh teknologi maju zaman sekarang. Mereka pun terlibat secara langsung di dalam pembuatan standar dan pemeriksaan yang dilakukan oleh badan-badan pemerintah. Inovasi dan kemajuan teknologi di Amerika Serikat bergantung pada keahlian dan kemampuan unik dari NIST di empat bidang utama: bioteknologi, nanoteknologi, teknologi informasi, dan manufakturing modern. NIST membuat sebuah metode yang memiliki empat tahapan dalam menyelesaikan dan penyelidikan kasus *Cyber Crime*, tahap pertama yaitu *Collection* (Pengumpulan Data), *Examination* (Pemeriksaan barang bukti), Analisis, dan yang terakhir adalah *Reporting* (Membuat laporan berdasarkan hasil analisis) (Fitriana, 2020).

Gambar 2.5. Tahapan Metode NIST (Nasirudin, 2020)

Adapun penjelasan dari gambar 2.5 adalah sebagai berikut (Nasirudin , 2020).

1. *Collection* merupakan tahapan paling awal dari framework NIST, hal-hal yang dilakukan dalam tahapan ini diantaranya koleksi, pendokumentasian, isolasi, preservasi barang bukti.
2. *Examination* merupakan bagian kedua melanjutkan dari tahapan *collection* diantaranya backup data dan *imaging system* yang mendukung format *image*.
3. *Analysis* merupakan tahapan ketiga setelah *examination* dengan menggunakan metode yang dibenarkan secara hukum dan tidak merubah teknik untuk mendapatkan sesuatu informasi yang berguna dan dapat menjawab apa yang dibutuhkan sebagai pendorong untuk melakukan pengumpulan dan pemeriksaan data.
4. *Reporting* merupakan tahapan akhir setelah 3 tahapan dilakukan guna melakukan proses pelaporan dari hasil tahapan yang meliputi penjelasan mengenai alat, dan prosedur yang dipilih, penggambaran tindakan yang dilakukan untuk memberi rekomendasi untuk perbaikian kebijakan, prosedur, akat dan aspek lainnya dalam forensik.

2.9.1. Peran dan Tanggung Jawab

Perencanaan harus membahas bagaimana personel yang ada memenuhi peran-peran ini ketika merespons dan berpartisipasi dalam penyelidikan. Serangkaian peran umum dan tanggung jawab terkait diberikan di bawah ini sebagai contoh. Mereka

termasuk Responden Pertama, Penyidik, Teknisi, Pemeriksa Forensik, Analis Forensik, dan Penjaga Bukti. Organisasi mungkin perlu memadukan peran-peran ini agar sesuai dengan metode operasi dan tingkat stafnya berdasarkan dokumen panduan dari NIST dengan no publikasi 800- 101.

1. *First Responders* adalah personel terlatih yang tiba pertama kali di lokasi kejadian, memberikan penilaian awal, dan memulai tingkat respons yang sesuai. Tanggung jawab *First Responders* adalah mengamankan lokasi kejadian, meminta dukungan yang diperlukan, dan membantu pengumpulan bukti.
2. Penyidik merencanakan dan mengelola pelestarian, perolehan, pemeriksaan, analisis, dan pelaporan barang bukti elektronik. Penyelidik Utama bertugas memastikan bahwa kegiatan di lokasi kejadian dilaksanakan dalam urutan yang benar dan pada waktu yang tepat. Penyelidik Utama mungkin bertanggung jawab untuk mengembangkan bukti, menyiapkan laporan kasus, dan memberikan pengarahan terhadap temuan dan keputusan apa pun kepada pejabat senior.
3. Teknisi melakukan tindakan atas arahan Pemimpin Investigasi. Teknisi bertanggung jawab untuk mengidentifikasi dan mengumpulkan bukti serta mendokumentasikan lokasi kejadian. Mereka adalah personel terlatih khusus yang menyita peralatan elektronik dan memperoleh gambar digital yang tersimpan dalam memori. Lebih dari satu teknisi biasanya terlibat dalam suatu insiden, karena diperlukan keterampilan dan pengetahuan yang berbeda. Keahlian yang memadai harus tersedia di lokasi kejadian untuk mengatasi semua peralatan digital yang terlibat dalam insiden tersebut.
4. Bukti Kustodian melindungi semua bukti yang dikumpulkan yang disimpan di lokasi pusat. Mereka menerima bukti yang dikumpulkan oleh Teknisi, memastikan

bukti tersebut diberi tag dengan benar, memeriksa masuk dan keluarnya bukti yang dilindungi, dan menjaga lacak balak yang ketat.

5. Pemeriksa Forensik adalah personel terlatih khusus yang mereproduksi gambar yang diperoleh dari peralatan yang disita dan memulihkan data digital.

Pemeriksa membuat informasi bukti terlihat pada perangkat. Pemeriksa juga dapat memperoleh data yang lebih sulit dipahami dengan menggunakan peralatan yang sangat khusus, rekayasa balik intensif, atau cara lain yang sesuai yang tidak tersedia bagi Teknisi Forensik. Penggunaan individu sebagai Penyidik dan Pemeriksa Forensik dalam suatu penyelidikan umumnya harus dihindari (Berkem, 2023).

2.9.2. *Standar Operasional Prosedur* (SOP)

Prosedur operasional yang dikeluarkan oleh *National Institute of Standards and Technology* (NIST) pada pedoman mobile forensik dengan no seri Publikasi Khusus NIST 800-101, berdasarkan penelian yang dilakukan oleh angkatan udara Amerika Serikat sebagai berikut .

1. Identifikasi, mengenai dan menentukan jenis kejadian.
2. Persiapan, mempersiapkan alat, teknik, surat perintah penggeledahan, otoritasi, dan persetujuan manajemen.
3. Strategi pendekatan, memaksimalkan pengumpulan bukti yang ternoda dan meminimalkan dampak terhadap korban.
4. Pelestarian, mengisolasi, mengamankan, dan melestarikan keadaan bukti fidik dan digital.
5. Koleksi, rekam pemandangan fisik dan duplikat bukti digital.
6. Pemeriksaan , mencari bukti-bukti yang berkaitan dengan dugaan kejahatan.

7. Analisis, Menentukan signifikansi, merekonstruksi bagian data, dan menarik kesimpulan berdasarkan bukti yang ditemukan. Fase Analisis dapat melalui banyak pengulangan hingga suatu teori dapat didukung.
8. Presentasi, meringkas dan memberikan penjelasan kesimpulan.
9. Bukti pengembalian, pastikan properti fisik dan digital dikembalikan ke keadaan semula.

2.9.3. Prinsip bukti

Prinsip-prinsip dasar telah diusulkan untuk menangani bukti digital. Bukti digital pada dasarnya sangatlah rapuh, terutama yang ditemukan pada telepon seluler. Isi telepon dan bukti yang terkandung di dalamnya dapat terpengaruh atau bahkan hilang kapan saja telepon tersebut dihidupkan. Bukti digital memiliki dua aspek: komponen fisik, perangkat, dan media, yang mungkin berisi data, dan data yang diambil dari sumber tersebut. Masing-masing memiliki masalah lacak balak yang terkait. Panduan Praktik yang Baik untuk Bukti Elektronik Berbasis Komputer dari *Association of Chief Police Officers* (ACPO) menyarankan empat prinsip ketika menangani bukti digital, yang dirangkum di sini:

1. Tidak ada tindakan yang dilakukan penyidik yang boleh mengubah data yang terdapat pada perangkat atau media penyimpanan digital yang selanjutnya dapat diandalkan di pengadilan.
2. Individu yang mengakses data asli harus kompeten untuk melakukannya dan memiliki kemampuan untuk menjelaskan tindakannya.
3. Jejak audit atau catatan lain dari proses yang diterapkan, yang sesuai untuk direplikasi hasilnya oleh pihak ketiga yang independen, harus dibuat dan disimpan, dengan mendokumentasikan setiap langkah investigasi secara akurat.

4. Penanggung jawab investigasi mempunyai tanggung jawab keseluruhan untuk memastikan prosedur yang disebutkan di atas dipatuhi dan mematuhi undang-undang yang berlaku.
5. Standar yang Diusulkan untuk Pertukaran Bukti Digital [IOCE] menyarankan serangkaian prinsip serupa untuk pemulihan bukti berbasis komputer yang terstandarisasi:
6. Setelah menyita bukti digital, tindakan yang diambil tidak boleh mengubah bukti tersebut.
7. Ketika seseorang perlu mengakses bukti digital asli, orang tersebut harus kompeten secara forensik.
8. Semua aktivitas yang berkaitan dengan penyitaan, akses, penyimpanan, atau pemindahan bukti digital harus didokumentasikan secara lengkap, disimpan, dan tersedia untuk ditinjau.
9. Seseorang bertanggung jawab atas semua tindakan yang diambil sehubungan dengan bukti digital selama bukti digital tersebut berada dalam kepemilikannya.
10. Setiap lembaga yang bertanggung jawab untuk menyita, mengakses, menyimpan, atau mentransfer bukti digital bertanggung jawab untuk mematuhi prinsip-prinsip ini.

Rangkaian prinsip di atas bertujuan untuk memastikan integritas dan akuntabilitas bukti digital di seluruh siklus hidup. Penanganan bukti yang tepat selalu penting agar dapat diterima dalam proses peradilan. Namun, standar yang berbeda mungkin berlaku

untuk jenis investigasi yang berbeda. Tingkat pelatihan dan keahlian yang diperlukan untuk melaksanakan tugas forensik sangat bergantung pada tingkat bukti yang diperlukan dalam kasus. Misal , menggunakan perangkat lunak forensik memerlukan tingkat keterampilan yang sederhana untuk memperoleh data aktif, dibandingkan dengan yang diperlukan .

BAB III

METODE PENELITIAN

3.1. Alat Dan bahan

Alat dan bahan yang digunakan pada penelitian kali ini terdapat pada tabel 3.1.

Tabel 3.1. Alat Penelitian

No	Nama Alat	Deskripsi/Spesifikasi	Keterangan
1.	Laptop	merk Lenovo 81HQ, Windows 10 pro 64-bit(10.0,build 19042)	Perangkat keras
2.	*smartphone android*	oppo a37f dan *iphone* 7 plus terinstal aplikasi *Whatsapp*	Perangkat keras

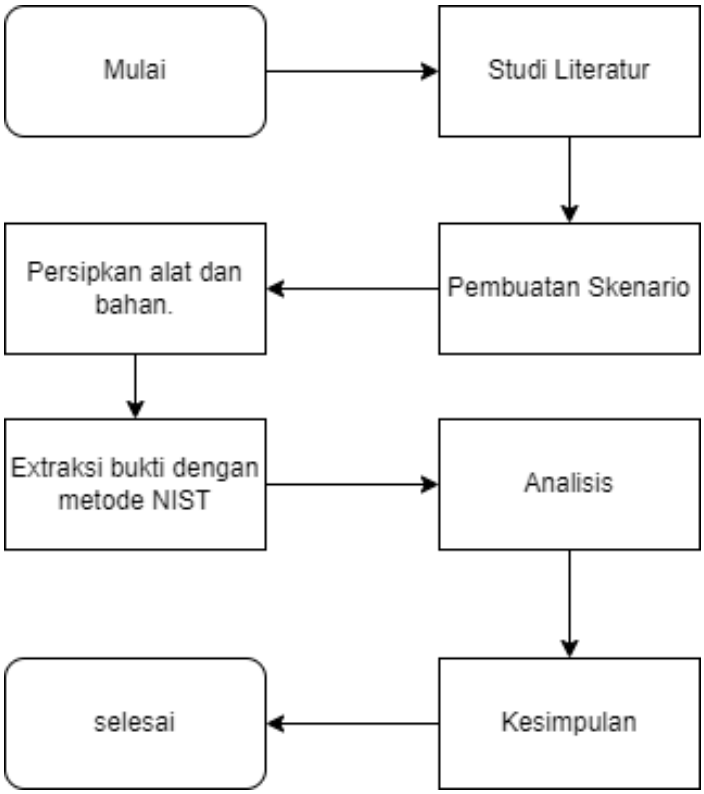
Tabel 3.2. Bahan Penelitian

No	Nama Bahan	Deskripsi/Spesifikasi	Keterangan
1.	*Kingroot* dan *root* checker basic	Aplikasi yang digunakan untuk *root* android dan mengecek status *root* android	Perangkat lunak
2.	*E3tTools*	Aplikasi yang dugunakan untuk mengecek status jeilbreak pada iphone	Perangkat Lunak
3.	*Mobile*dit Forensik	Aplikasi yang digunakan untuk mengangkat data- data pada *smartphone android*	Perangkat lunak
4.	*Autopsy*	aplikasi yang digunakan untuk mengakuisisi/ menganalisis data yang berhasil diangkat dari *smartphone android*	Perangkat Lunak
5	*Oxygen Forensic Detectiv*	aplikasi yang digunakan untuk menganalisa hasil dari akusisis sistem *file*	Perangkat lunak

6	*Whatsapp*	Aplikasi pesan instan sebagai aplikasi ujicoba	Perangkat Lunak

3.2. Alur Penelitian

Terdapat beberapa tahapan dalam penelitian ini seperti pada gambar 3.1.



Gambar 3.1. Alur Penelitian

Berikut adalah penjelasan gambar 3.1

1. Tahap Pertama yaitu studi literatur yaitu untuk mencari referensi sebagai rujukan penelitin.Tahap kedua yaitu pembuatan Skenario penelitian. pada penelitian kali ini peneliti menggunakan scenario penyebaran foto/video sebagaimana berikut:

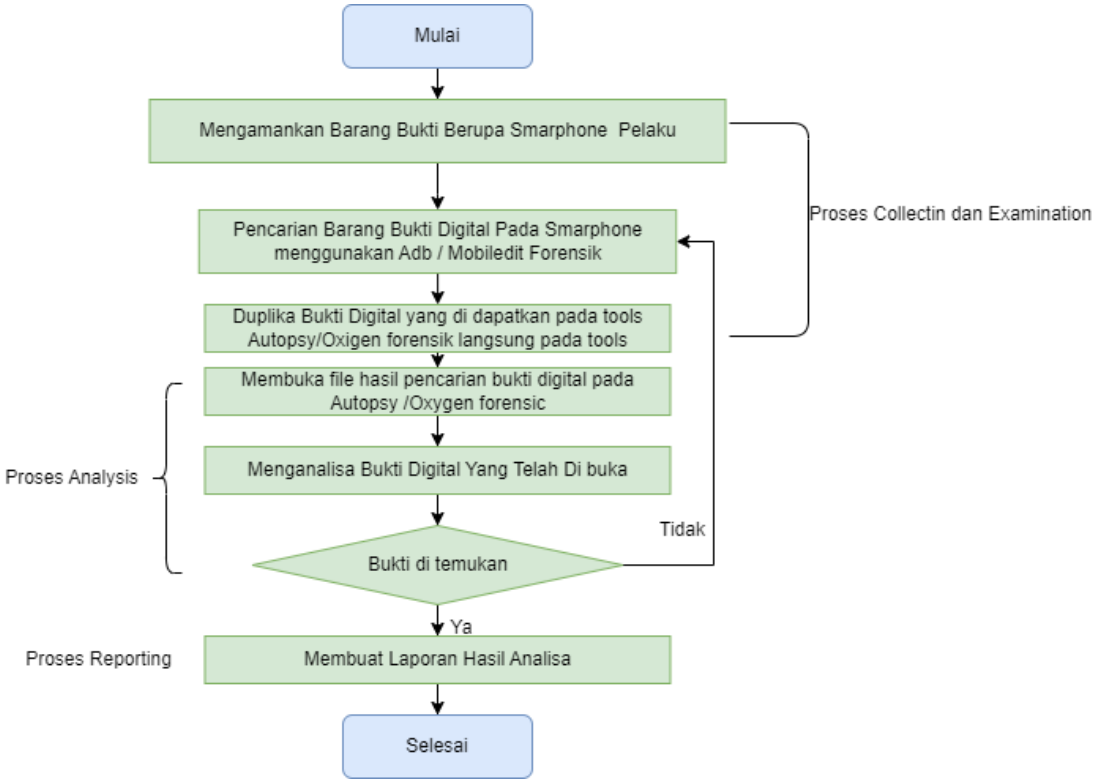
   Skenario kasus mulai dari menginstal aplikasi *whatsapp* dengan menggunakan *smartphone* oppo a37F dan *iphone* 7 Plus. setelah itu membuat akun *whatsapp* pada kedua *smartphone*, selanjutnya mengirimkan sebuah *File* ke perangkat

lainya menggunakan aplikasi *whatsapp* . *file* akan dikirim berupa sebuah gambar . setelah berhasil terkirim *file* tersebut akan dihapus untuk menghilangkan bukti jejak digital. selanjutnya masuk pada tahapan forensiknya yaitu mengekstrak *file* tersebut pada kedua *smartphone* dan dianalisis sebagai bukti digital.

2. Tahap kedua yaitu mempersiapkan alat dan bahan seperti *smartphone* dan *Tools* forensik yang akan digunakan dalam penelitian ini
3. Tahap ketiga mengimplementasikan metode NIST dalam mengekstraksi *file* pada *smartphone android,* ada beberapa tahapan dalam metode ini yaitu *Collection* (Pengumpulan Data), *Examination* (Pemeriksaan barang bukti), Analisis, dan yang terakhir adalah *Reporting* (Membuat laporan berdasarkan hasil analisis).
4. Tahap selanjutnya yaitu Analisis, menganalisa barang bukti digital hasil ekstraksi *file* yang terhapus pada pesan instan *whatsapp* untuk mengetahui apakah ekstraksi data dapat mencakup semua jenis *file*, atau terbatas pada beberapa jenis *file*, apakah ada tanda tanda aktivitas pengguna yang mencurigakan atau melibatkan kejahatan siber, apakah data yang diekstraksi konsisten dengan versi *smartphone* yang berbeda, dan apakah ada jejak penghapusan data atau upaya menyembunyikan jejak digital.
5. Tahap terakhir yaitu membuat kesimpulan dari hasil penelitian ini.

3.3. Metode Penelitian

Penelitian ini menggunakan *Framework National Institute of Standards and Technology* (NIST) dimana ada terdapat 4 tahapan yaitu *Collection* (Pengumpulan Data), *Examination* (Pemeriksaan barang bukti), Analisis, dan yang terakhir adalah *Reporting* (Membuat laporan berdasarkan hasil analisis). Berikut prosesnya pada gambar 3.2.



Gambar 3.2. Proses Pengangkatan Data

3.3.1. *Collection* (Pengumpulan Data)

Tahap *collection* atau tahap pengumpulan merupakan aktivitas atau proses pengumpulan data-data untuk pencarian barang bukti kejahatan digital. Pada tahap ini dimana *smartphone* sebagai barang bukti diamankan untuk dilakukan proses analisis *Mobile* forensik, proses ini dengan mengangkat segala data yang terdapat pada *smartphone* menggunakan *Tools Mobile*dit dan Magnet AXIOM untuk mengangkat barang bukti digital berupa bukti *Chat*,foto, dan video yang terdapat pada *smartphone android*.

3.3.2. *Examination* (Pemeriksaan)

Tahap *examination* atau tahap pemeriksaan ini merupakan tahap pemeriksaan data yang telah dikumpulkan pada tahap *collection* dan mem – *backup* data yang didapatkan

untuk menghindari kerusakan data tersebut, serta memastikan bahwa data yang didapatkan berupa *file* tersebut sesuai dengan yang didapatkan pada tempat kejadian digital.

3.3.3. *Analysis* (Analisis)

Tahap *analysis* atau tahap meneliti ini dilakukan setelah mendapatkan *file* atau data digital yang diinginkan dari proses pemeriksaan sebelumnya, data tersebut di analisis secara detail dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut, dimana yang dianalisis adalah data yang didapatkan seperti foto, video dan *Chat* wa yang kemudian digunakan sebagar barang bukti digital yang dapat dipertanggungjawabkan secara ilmiah dan hukum.

3.3.4. *Reporting* (Laporan)

Tahap *Reporting* atau pelaporan dilakukan setelah proses pemeriksaan dan analisis dilakukan kemudian diperole barang bukti digital. Selanjutnya pada tahap ini dilakukan pelaporan hasil analisis yaitu penggambaran tindakan atau kejahatan yang dilakukan, tols, dan metode yang digunakan.

3.4. Metode Pengumpulan Data

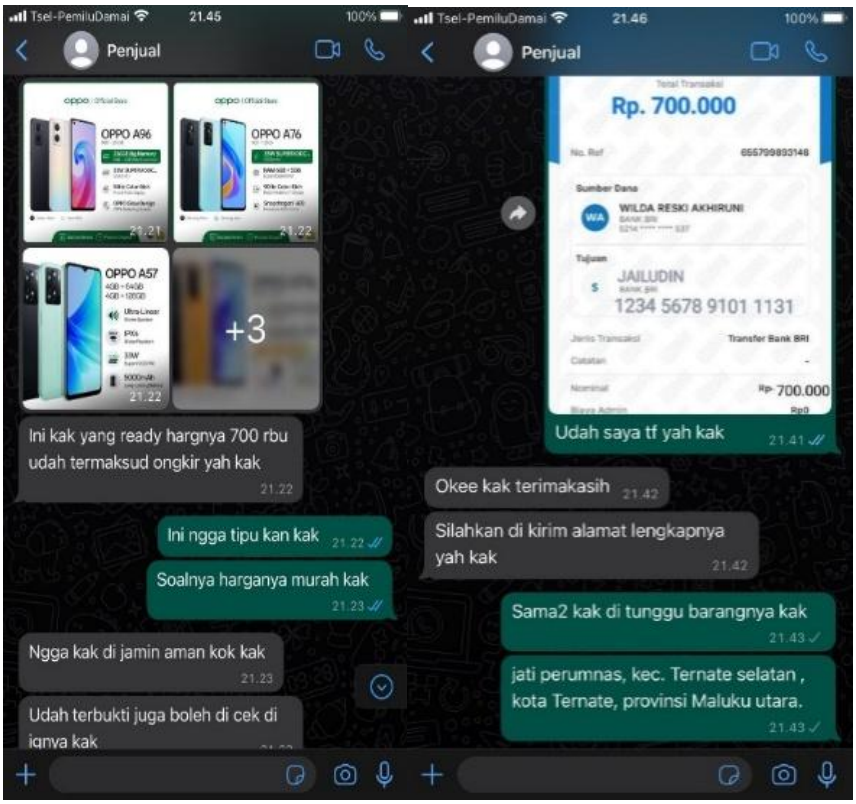
Pada penelitian ini metode pengumpulan data menggunakan *Physical Acquisition. Physical Acquisition* adalah salah satu metode dalam forensik digital yang digunakan untuk mendapatkan salinan fisik dari perangkat keras (*hardware*) suatu perangkat, seperti *smartphone*, *tablet*, atau komputer. Metode ini memungkinkan pemeriksa untuk mendapatkan salinan *bit-by-bit* dari seluruh media penyimpanan perangkat, termasuk data yang mungkin dihapus atau tidak terjangkau oleh metode ekstraksi logis.

BAB IV

HASIL DAN PEMBAHASAN

4.1. Penerapan Skenario

Simulasi penelitian ini yaitu mengsimulasikan sebuah percakapan pada aplikasi instan *whatsapp* yang mengandung unsur kejahatan pada percakapan tersebut, lalu menghapus percakapan tersebut sebagai tindakan penghilangan barang bukti digital. Berdasarkar simulasi contoh kasus di atas peneliti melakukan langka- langka forensik untuk mendapatkan barang bukti digital. Peneliti melakukan tahapan penelitian dengan menggunakan *framework* NIST yaitu *collection, examination, analysis, roporting.* simulasi percakapan pada aplikasi *whatsapp* yang telah diskenariokan terlihat pada gambar 4.1. dan 4.2.



Gambar 4.1. *Scenario* percakapan *iphone 7 plus*

Gambar 4.2. Scenario percakapan *android oppo* A37f

4.2. Extraksi file

Tahapan extraksi *file* yaitu tahapan dalam mengimplementasikan *framework National Institue Of Standart And Tecnology* (NIST).

4.2.1. *Collection* (Pengumpulan)

Pada tahap ini dimana pengumpulan barang bukti, pada penelitian ini menggunakan 2 buah unit *smartphone* yang di gunakan sebagai barang bukti yang telah diskenariokan terlihat pada gambar 4.3. Gambar hp.

Gambar 4.3. *Smartphone oppo A37f* dan *Iphone 7 Plus*

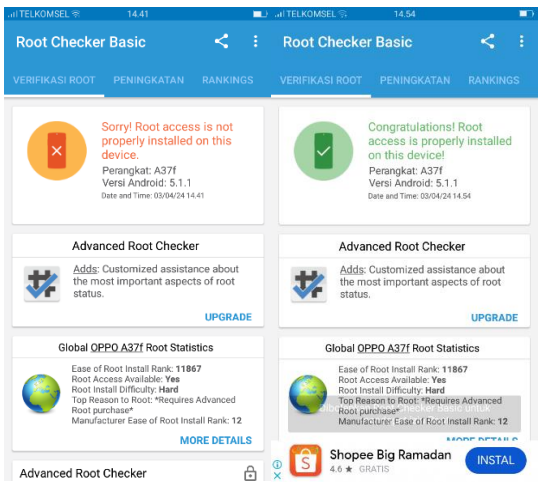
Barang bukti yang digunakan berupa 2 buah *smartphone* dengan spesifikasi yang berbeda. Berikut spesifikasi dari *smartphone* dapat dilihat pada tabel 4.1.

Tabel 4.1 Spesifikasi *Smartphone*

Nama Perengkat	*Oppo A37f*	**Iphone 7 Plus**
Versi	5.1.1	15.8
Processor/CPU	QualcommMSM8916Quad core	Apple A10
Ram/Penyimpanan	2,0 GB/16 GB	256 GB
Nomor bentukan/ Nomor Model	A3fEX_11_160614	MN502X/A

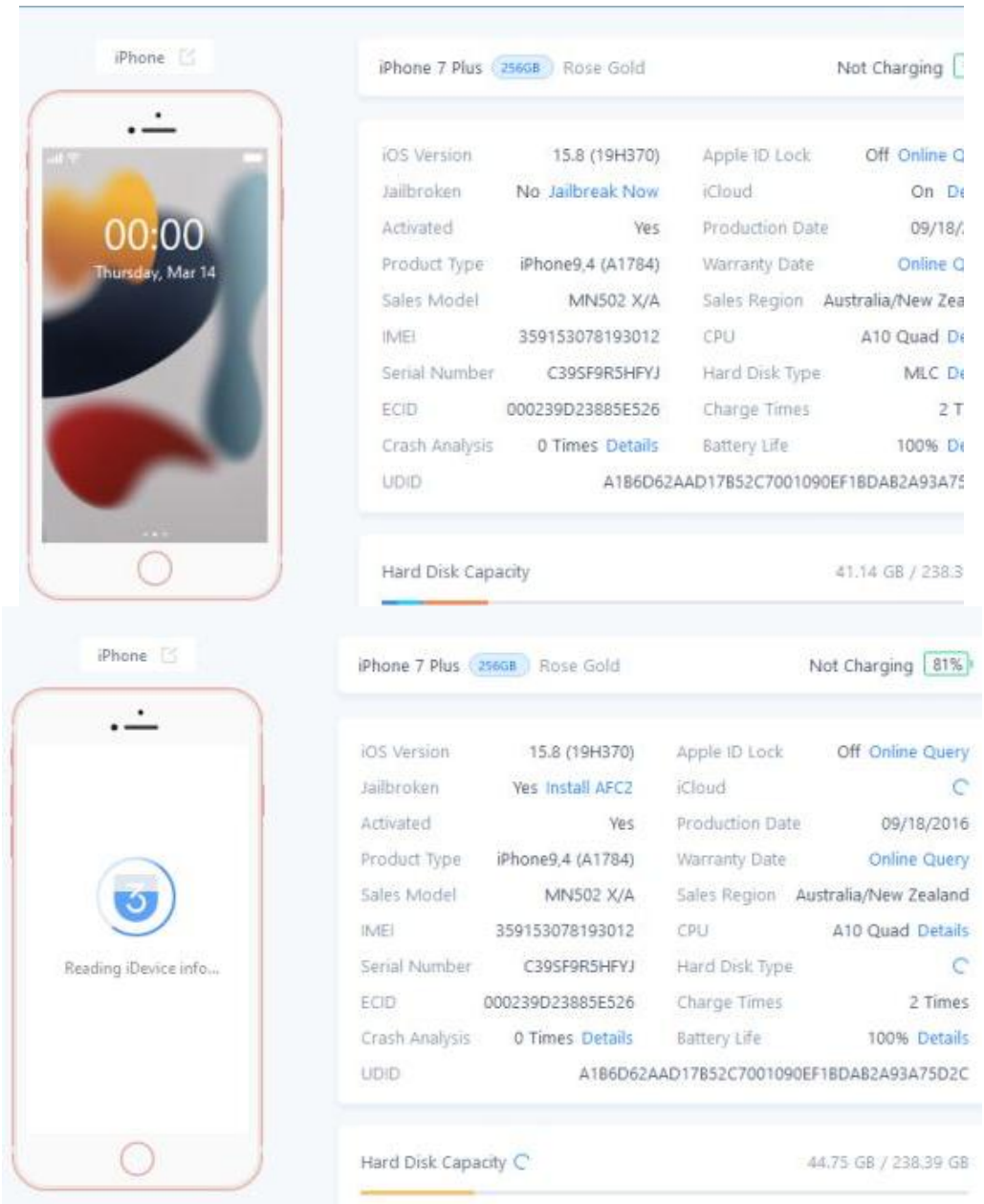
1. *Rooting*

Pada tahap *collection* kita awali dengan proses *rooting* pada *smartphone* dan *jailbreak* pada *iphone* untuk mendapatkan akses lebih kedalam sistem *smartphone*. Pada penelitian ini data yang akan di angkat berupa data yang sudah terhapus sehingga membutuhkan akses *rooting* untuk memaksimalkan analisis tentang data tersebut. Aplikasi *Kingroot* dapat digunakan proses *rooting* pada *smartphone android*. Berikut status *root android* sebelum dan sesudan di *root* menggunakan *Kingroot* dan di cek status menggunakan *root checker basic* dapat di lihat pada gambar 4.4.



Gambar 4.4. *Android* sesudah dan sebelum di*root*

Sedangkan pada *iphone* yaitu dilakukan proses *jailbreak,* fungsi dari *jailbreak* sendiri sama seperti *root* pada *android*, berikut tampilan *iphone* sesuda dan sebelum di*jailbreak* dengan bantuan *Tools 3uToolss* pada gambar 4.5.

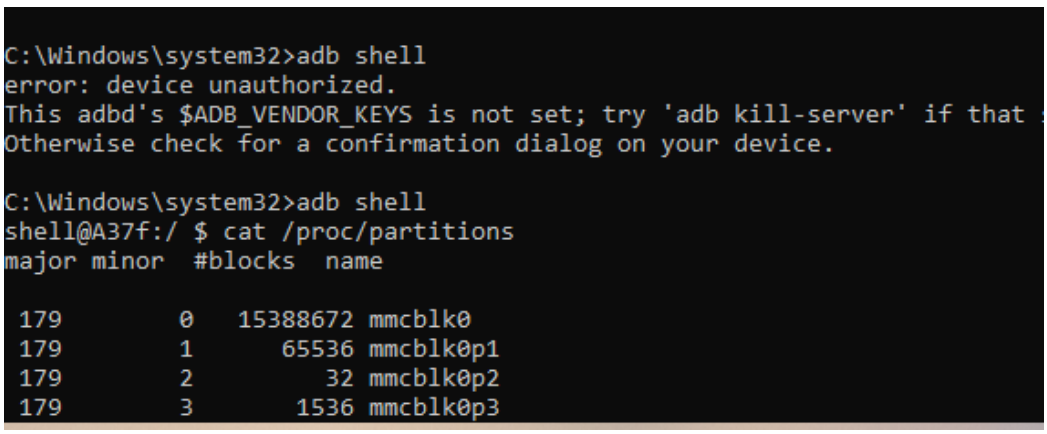


Gambar 4.5. *Iphone* sebelum dan sesudah di *jailbreak*

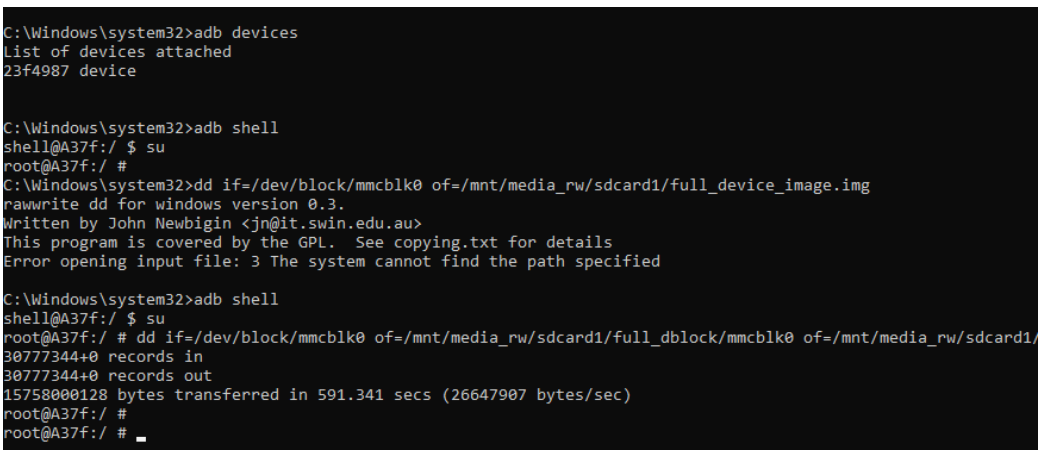
2. *Imaging*

Proses *imaging* atau sering dikenal dengan *disk cloning* adalah proses atau teknik

menyalin langsung dari sektor perangkat penyimpanan fisik (*physical storage device)* / media penyimpanan dari perangkat berupa semua *file* secara *bitstream image* yaitu menyalin data *bit –by- bit* dan mengambil *sector -by- sector* yang terdapat pada *disk block* dan menghasilkan berupa *file image / disk image*. Pada proses ini menggunakan tolls *Android Debud Bridge* (ADB) pada gambar 4.6 mencari penyimpanan android sedangkan 4.7 proses imagin pada seluru file pada android

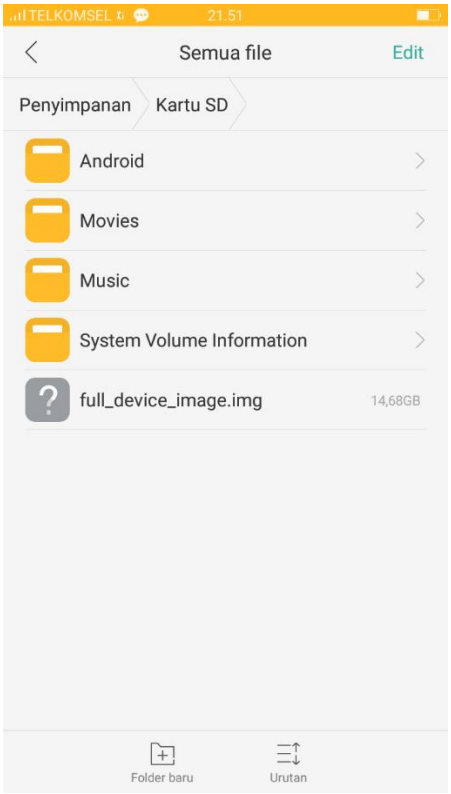


Gambar 4.6. proses pencarian penyimpanan *android*



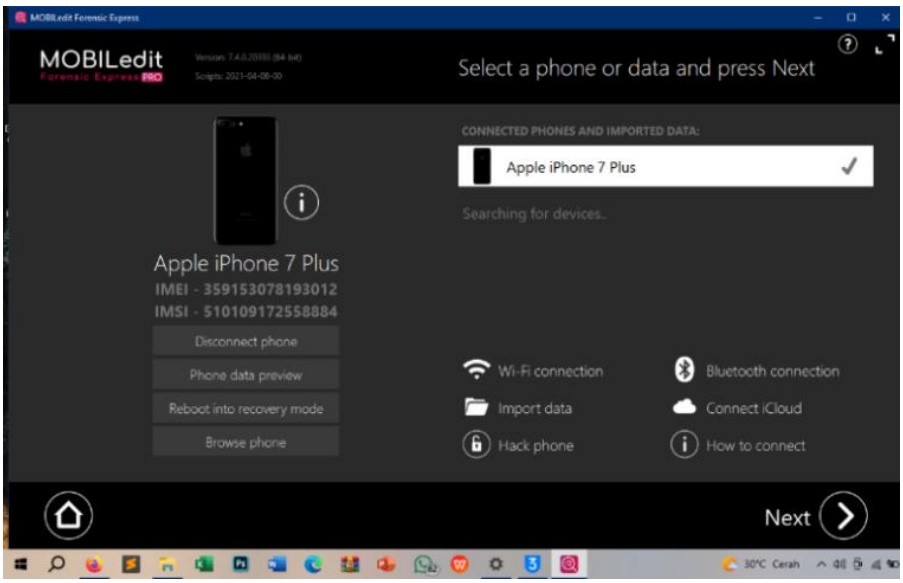
Gambar 4.7. Proses *Imaging* menggunakan ADB pada *Android*

Setelah proses di atas mendapatkan *file* dengan nama full_device_image .img yang tersimpan pada penyimpanan internal hp, dapat dilihat pada gambar 4.8.



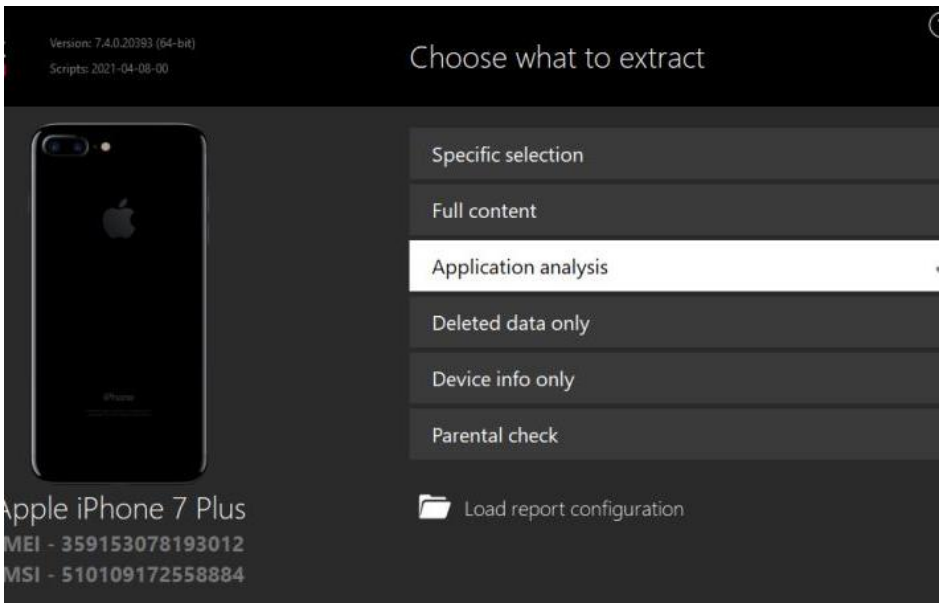
Gambar 4.8. *File* hasil *imaging android*

Sedangkan Proses *imaging* pada *iphone* Menggunakan *Tools Mobiledit forensik expres* , dapat dilihat pada gambar 4.9.

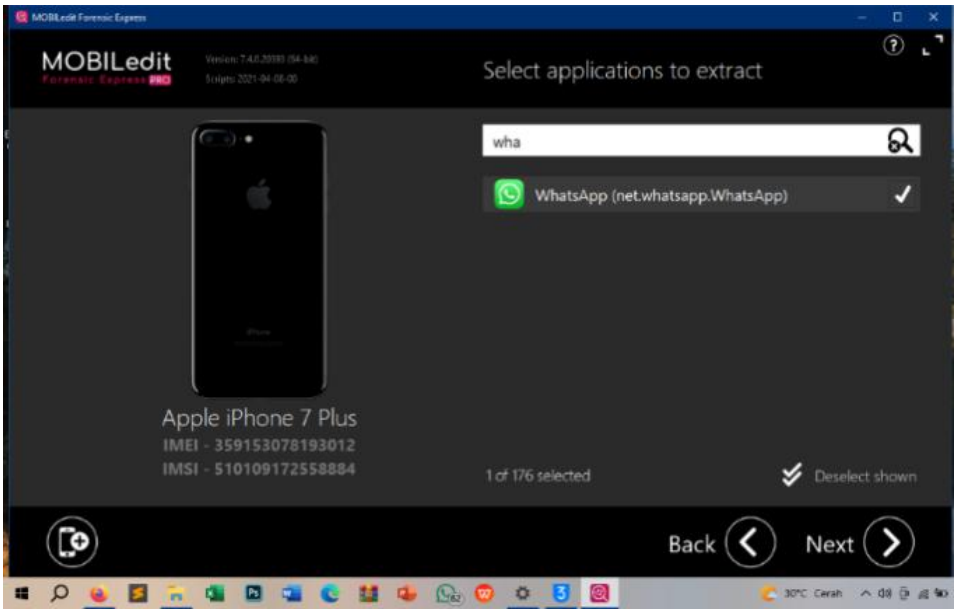


Gambar 4.9. Proses *Connecting tolls* dan perangkat

Tahap selanjutnya yaitu pemilihan data yang ingin diextrak, data yang dipilih adalah data aplikasi *whatsapp* dapat dilihat pada gambar 4.10 dan 4.11.



Gambar 4.10 Proses pemilihan extrak data

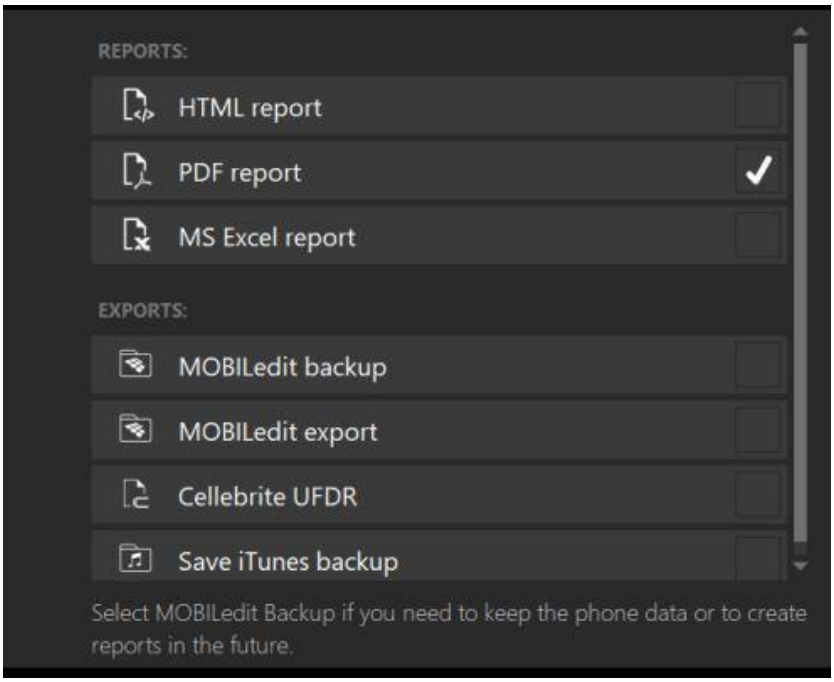


Gambar 4.11. Proses pemilihan data *whatsapp* yang akan di extrak

Tahap selanjutnya yaitu mengisi spesifikasi data kasus diatas seperti nama kasus,no kasus sampai nama penanggung jawab kasus, lebih jelas dapat dilihat pada gambar 4.12.

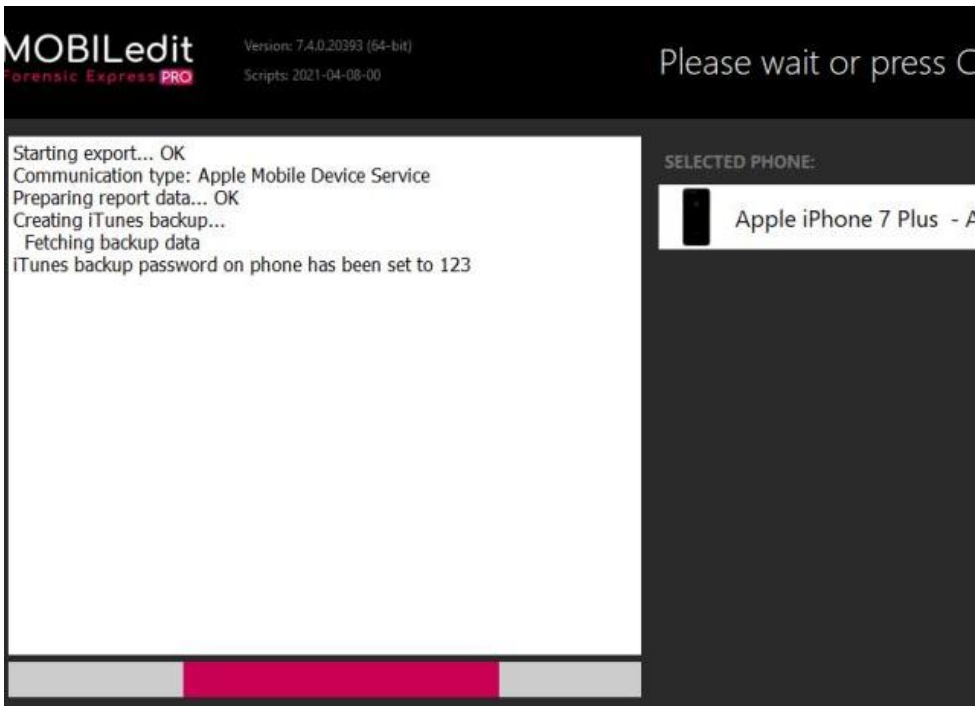
Gambar 4.12. Pengisian spesifikasi kasus

Tahap selanjutnya menentukan jenis format *output* data yang akan diextrak terlihat pada gambar 4.13.

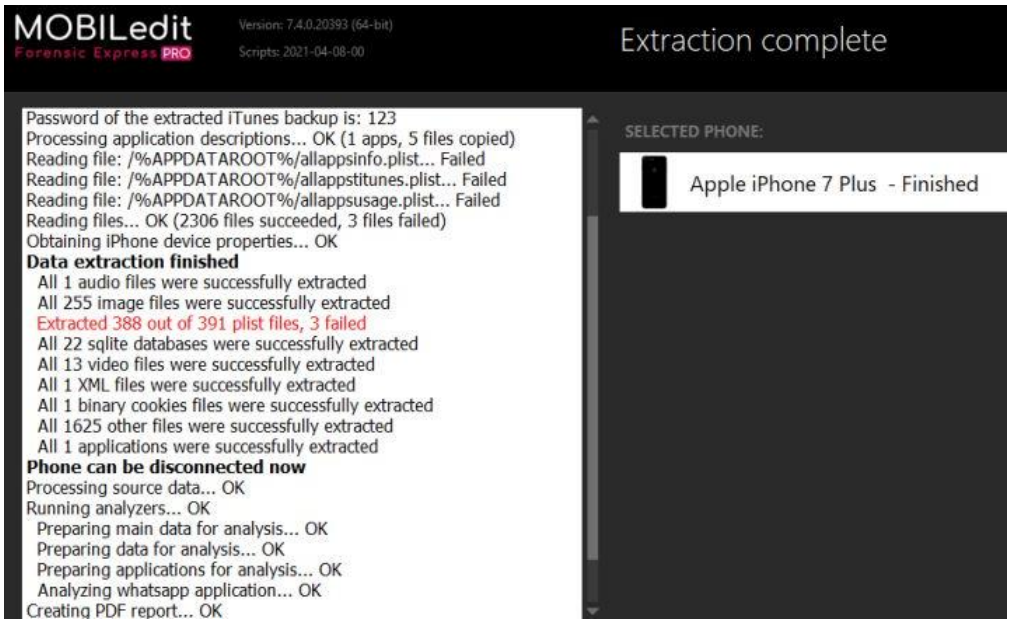


Gambar 4.13 Proses pemilihan format *Output*

Setelah beberapa tahapan diatas selanjutnya masuk pada tahap extraksi data sesuai dengan kebetuhan data seperti pada gambar 4.14 dan 4.15 tampilan proses extraksi selasai.

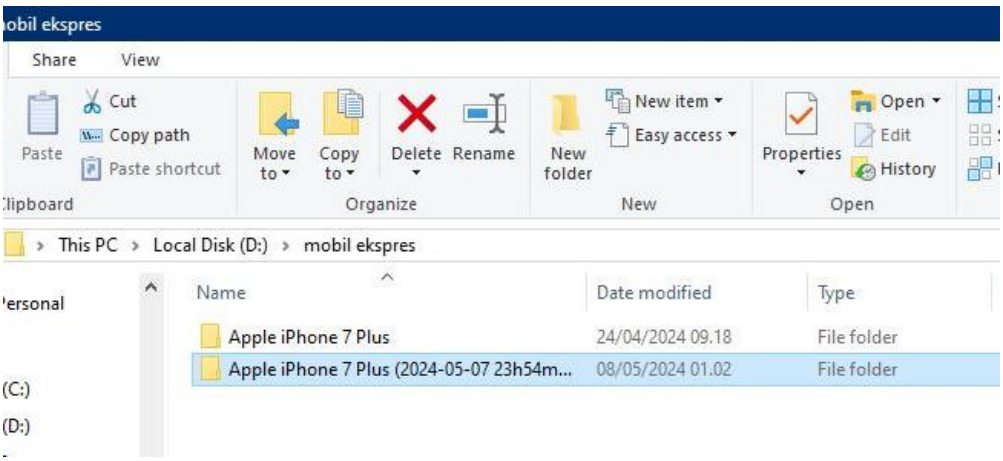


Gambar 4.14. Proses Extraksi data



Gambar 4.15. Proses extraksi Selesai

Setelah proses extraksi selesai dapat dilihat pada gambar 4.16 barikut hasil extraksi dari perangkat *iphone*.

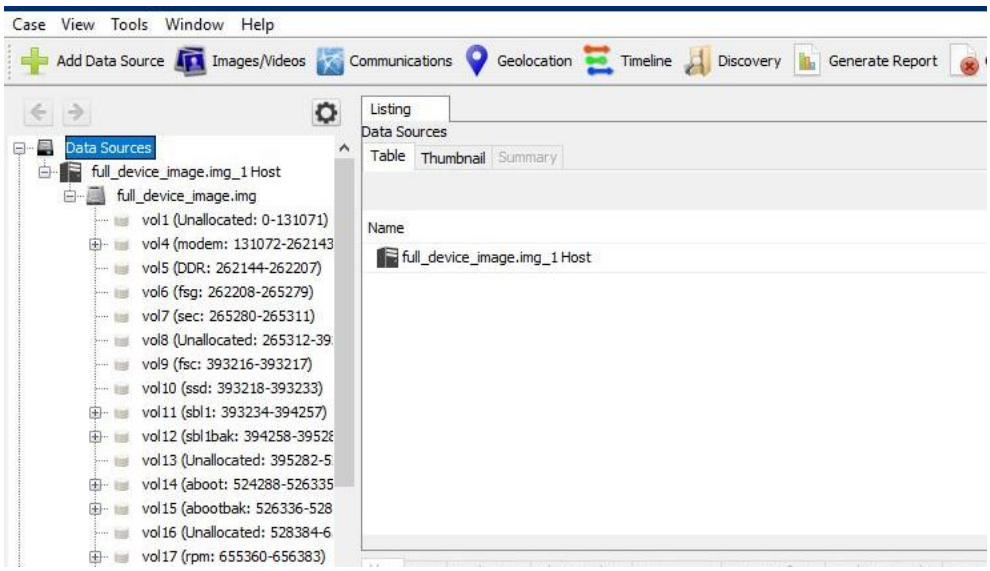


Gambar 4.16. Hasil Extraksi *Iphone*

4.2.2. Examination

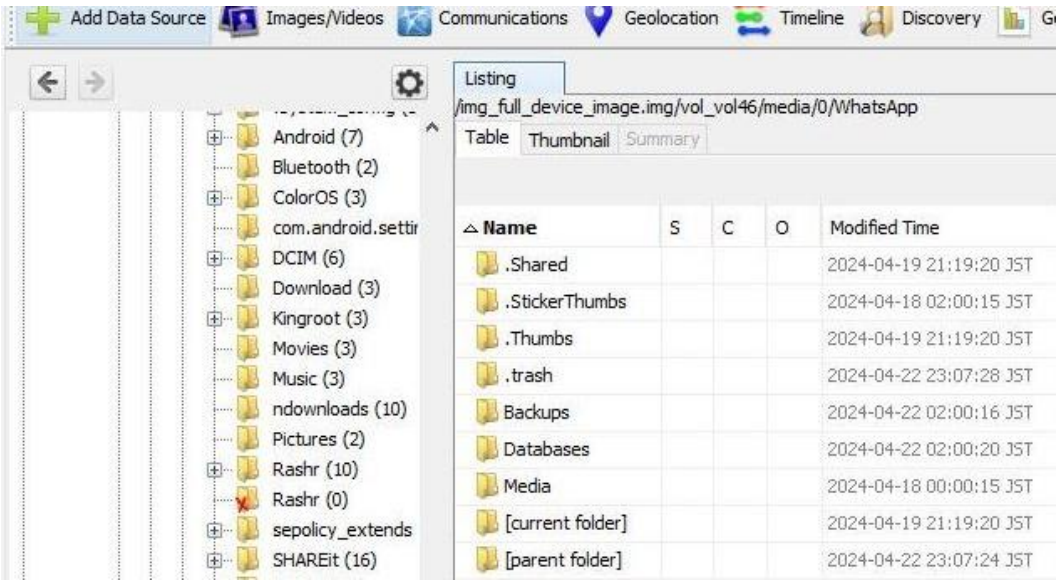
1. *Examination* pada *android*

Tahap *examination* atau tahap pemeriksaat ini menggunakan *Tools Autopsy* versi 4.0. *file* yang didapatkan pada proses *collecction* selanjutkan di *export* pada *Tools Autopsy* untuk memeriksa barang bukti seperti gambar 4.17 berikut.



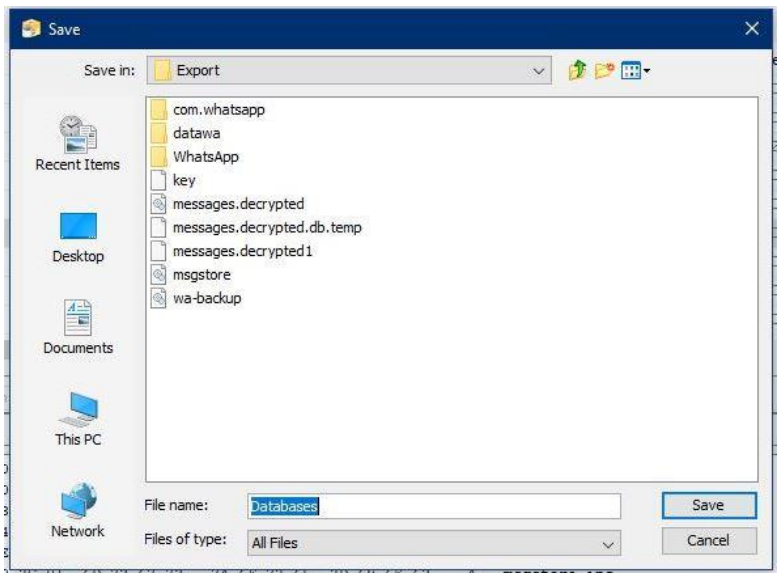
Gambar 4.17 Pemeriksaan bukti dengan *Autopsy*

Selanjutnya proses pemeriksaan dan pencarian *database whatsapp* yang akan di analisis sebagai barang bukti terdapat pada gambar 4.18.



Gambar 4.18. Pemeriksaan *database whatsapp*

Berdasarkan gambar diatas *database whatsapp* terletak pada *file* full_device_image .img / vol_vol46/media/0/*Whatsapp*/*Database*. Data tersebut selanjutnya di *export* untuk dianalisis seperti gambar 4.19.

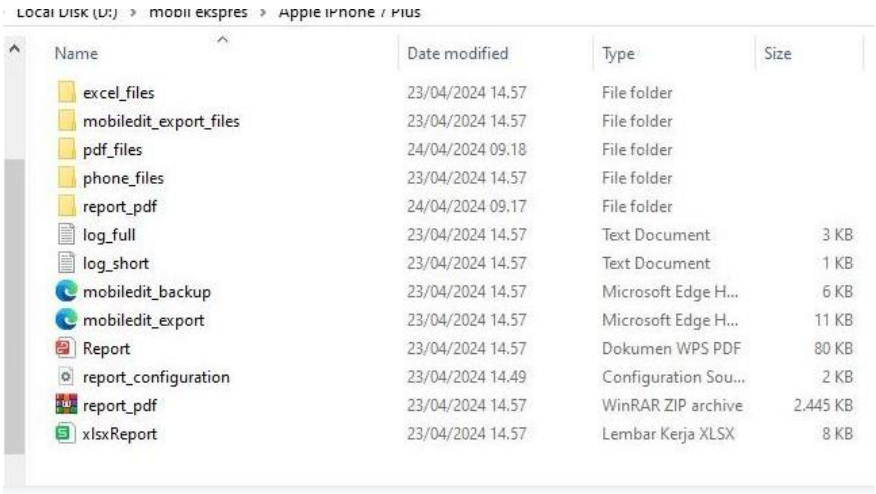


Gambar 4.19 Proses *Export* data *Whatsapp*

File yang di *export* tersimpan pada D:\forensik\evidence*Export**Whatsapp* dan data yang didapatkan siap untuk dianalisis.

2. *Examination* pada *iphone*

Proses *examination* pada *iphone* berbeda karena pada tahap ini hasil dari extraksi *iphone* tidak perlu menggunakan *Tools Autopsy*, tetapi sudah terseimpan otomatis dalam bentuk folder hasil dari extraksi data seperti pada gambar 4.20.



Gambar 4.20. Proses pemeriksaan hasil extraksi

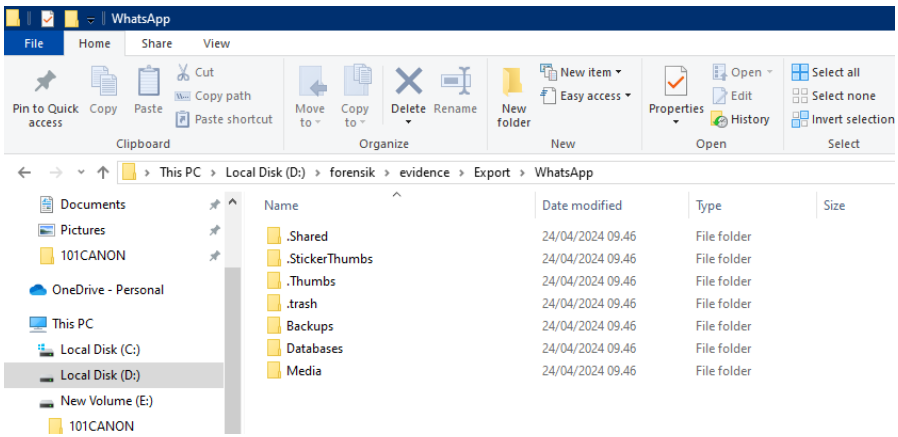
Pada folder ini terdapat *file* pdf yang mengcakup hasil laporan atau raport dalam bentuk pdf dapat dilihat pada gambar 4.21.

Gambar 4.21. Tampilan *file raport* pdf

4.2.3. Analysis

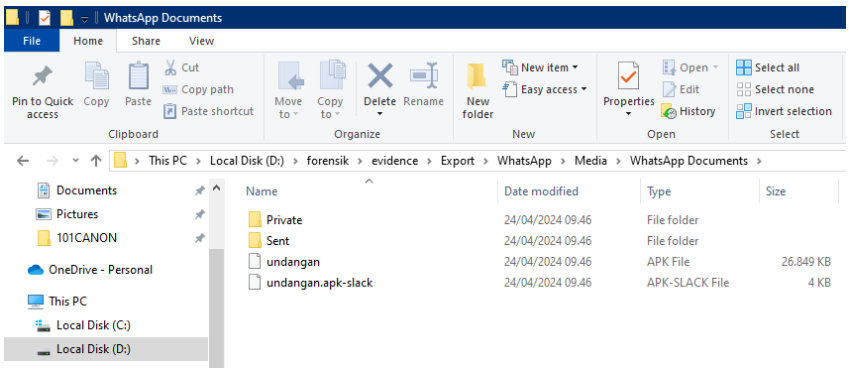
1. Analisis perangkat *android*

Pada tahapan ini *file* yang akan dianalisis sudah di *export* menggunakan *Autopsy* berupa folder *whatsapp* yang didalamnya terdapat *database whatsapp* seperti gambar 4.22.



Gambar 4.22. Isi folder *Whatsapp*

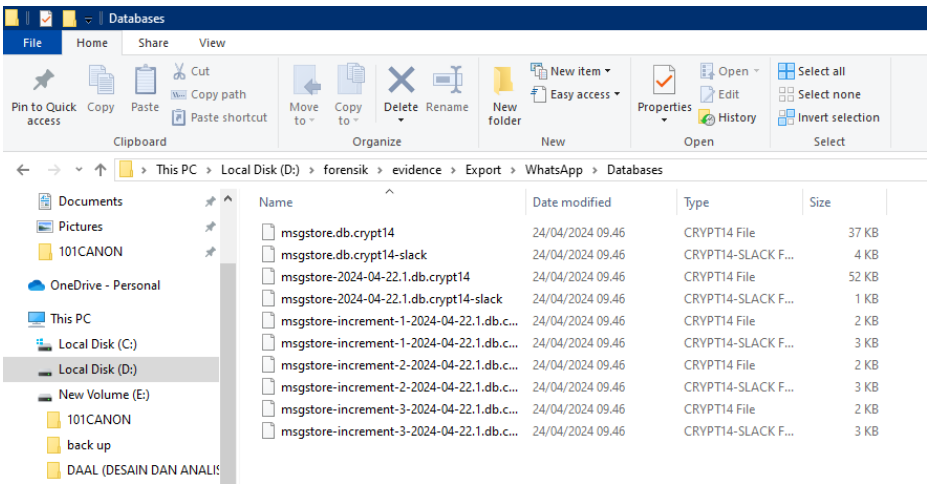
Selanjutnya menganalisi *file* yang terdapat pada folder *whatsapp*, pada folder ini ditemukan 1 *file* undangan dengan ekstensi apk, dimana *file* tersebut sesuai dengan *file* yang dikirimkan dalam skenario dapat dilihat pada gambar 4.23.



Gambar 4.23 Penemuan *file* Undangan.apk

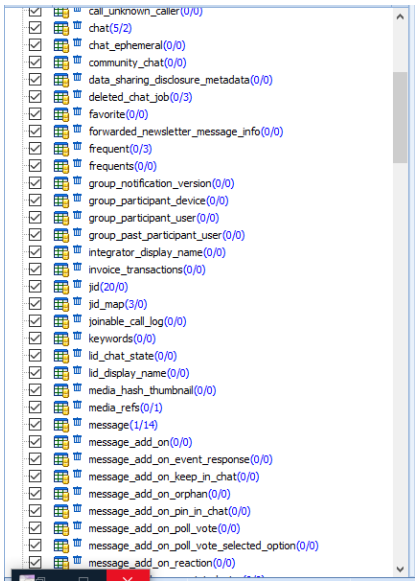
Selain itu ditemukan juga *file database whatsapp* berupa *Chat whatsapp* dengan ekstensi *crpty.14*, tetapi *file* tersebut tidak dapat langsung dibuka dan akan

dilanjutkan analisis dengan menggunakan *whatsapp viewer* untuk melihat isi percakapan tersebut, dapat dilihat pada gambar 4.24.



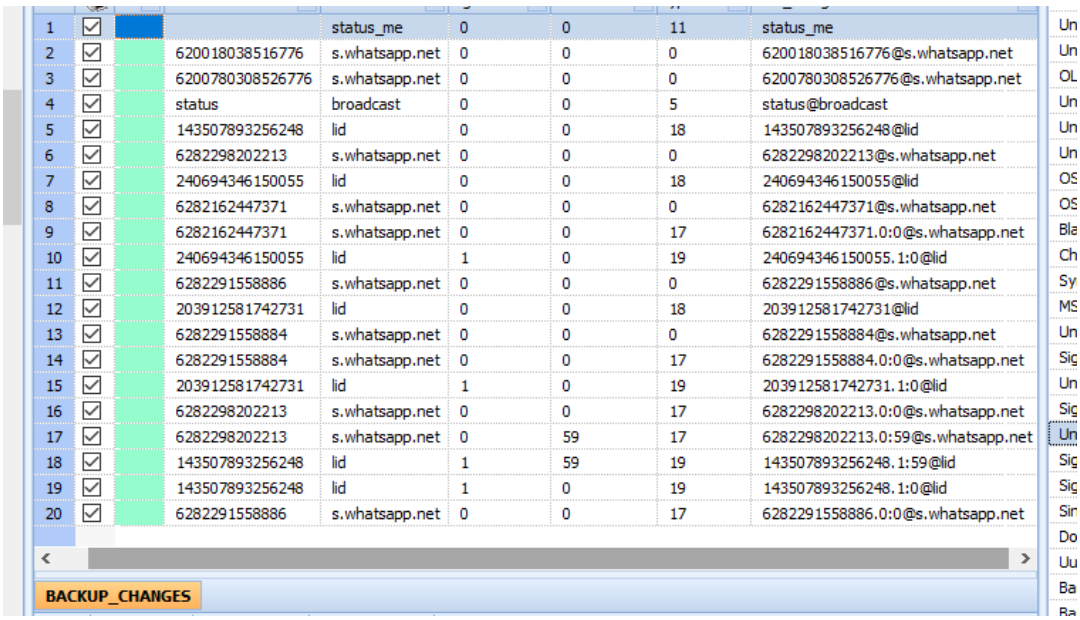
Gambar 4.24. *Database Whatsapp*

Setelah itu menganalisis *database Msgstore.db* dimana didalam *database* ini berisi informasi tentang pesan terkirim, seperti nomor kontak, isi pesan, status, cap waktu, informasi tentang *file* terlampir, dll. *File Msgstore.db* terletak di bawah jalur /data/data/com.*whatsapp*/*database*s /. Isi dari databse diatas dapat dilihat pada gambar 4.25.



Gambar 4.25. Struktur Tabel *database Msgstore.db*

Didalam tabel ini terdapat barang bukti berupa daftar nomor kontak *whatsapp* beserta statusnya yang terdapat pada tabel jid, dapat dilihat pada gambar 4.26.

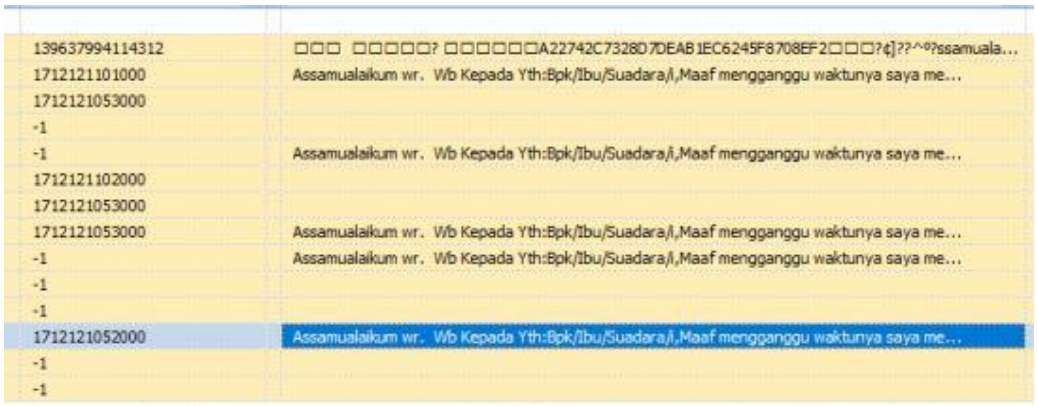


1	☑			status_me	0	0	11	status_me
2	☑		620018038516776	s.whatsapp.net	0	0	0	620018038516776@s.whatsapp.net
3	☑		6200780308526776	s.whatsapp.net	0	0	0	6200780308526776@s.whatsapp.net
4	☑		status	broadcast	0	0	5	status@broadcast
5	☑		143507893256248	lid	0	0	18	143507893256248@lid
6	☑		6282298202213	s.whatsapp.net	0	0	0	6282298202213@s.whatsapp.net
7	☑		240694346150055	lid	0	0	18	240694346150055@lid
8	☑		6282162447371	s.whatsapp.net	0	0	0	6282162447371@s.whatsapp.net
9	☑		6282162447371	s.whatsapp.net	0	0	17	6282162447371.0:0@s.whatsapp.net
10	☑		240694346150055	lid	1	0	19	240694346150055.1:0@lid
11	☑		6282291558886	s.whatsapp.net	0	0	0	6282291558886@s.whatsapp.net
12	☑		203912581742731	lid	0	0	18	203912581742731@lid
13	☑		6282291558884	s.whatsapp.net	0	0	0	6282291558884@s.whatsapp.net
14	☑		6282291558884	s.whatsapp.net	0	0	17	6282291558884.0:0@s.whatsapp.net
15	☑		203912581742731	lid	1	0	19	203912581742731.1:0@lid
16	☑		6282298202213	s.whatsapp.net	0	0	17	6282298202213.0:0@s.whatsapp.net
17	☑		6282298202213	s.whatsapp.net	0	59	17	6282298202213.0:59@s.whatsapp.net
18	☑		143507893256248	lid	1	59	19	143507893256248.1:59@lid
19	☑		143507893256248	lid	1	0	19	143507893256248.1:0@lid
20	☑		6282291558886	s.whatsapp.net	0	0	17	6282291558886.0:0@s.whatsapp.net

BACKUP_CHANGES

Gambar 4.26. Isi *database* dari tabel Jid

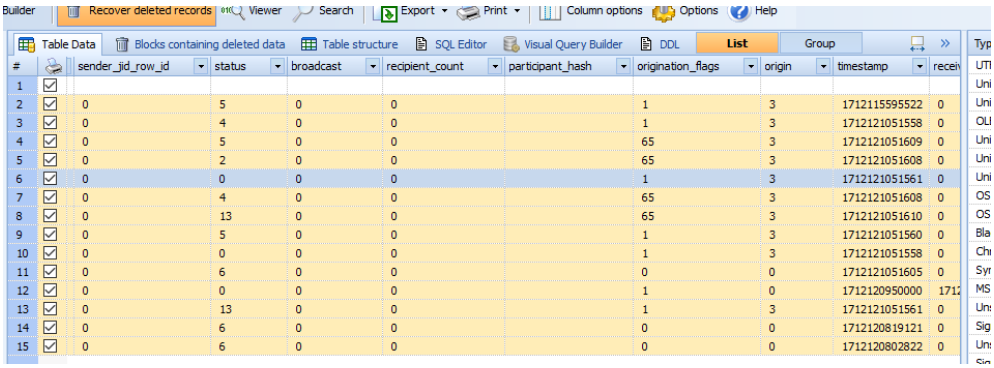
Selain itu terdapat pesan dengan status sudah terhapus didalam tabel *massege*. Tabel ini berisi informasi, seperti nomor kontak, isi pesan, status, cap waktu, dan informasi tentang *file* lampiran. Seperti pada gambar 4.27 berikut.



139637994114312	□□□ □□□□□? □□□□□□A22742C7328D7DEAB1EC6245F8708EF2□□□?¢]??^°?ssamuala...
1712121101000	Assamualaikum wr. Wb Kepada Yth:Bpk/Ibu/Suadara/i,Maaf mengganggu waktunya saya me...
1712121053000	
-1	
-1	Assamualaikum wr. Wb Kepada Yth:Bpk/Ibu/Suadara/i,Maaf mengganggu waktunya saya me...
1712121102000	
1712121053000	
1712121053000	Assamualaikum wr. Wb Kepada Yth:Bpk/Ibu/Suadara/i,Maaf mengganggu waktunya saya me...
-1	Assamualaikum wr. Wb Kepada Yth:Bpk/Ibu/Suadara/i,Maaf mengganggu waktunya saya me...
-1	
-1	
1712121052000	Assamualaikum wr. Wb Kepada Yth:Bpk/Ibu/Suadara/i,Maaf mengganggu waktunya saya me...
-1	
-1	

Gambar 4.27. Isi *database* dari tabel *massege*

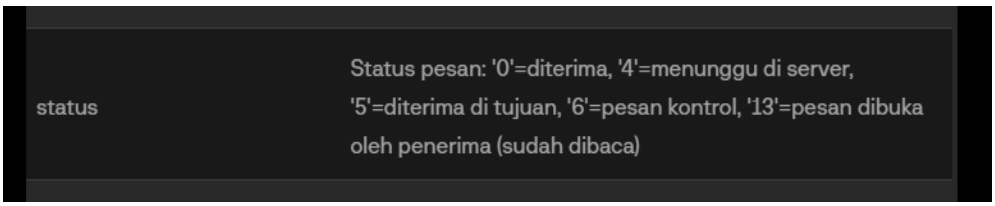
Dari tabel diatas terdapat tabel status dimana tabel tersebut menandakan pesan diterima ataupun pesan sudah terkirim dapat dilihat pada gambar 4.28 berikut.



#	sender_jid_row_id	status	broadcast	recipient_count	participant_hash	origination_flags	origin	timestamp	receiv
1									
2	0	5	0	0		1	3	1712115595522	0
3	0	4	0	0		1	3	1712121051558	0
4	0	5	0	0		65	3	1712121051609	0
5	0	2	0	0		65	3	1712121051608	0
6	0	0	0	0		1	3	1712121051561	0
7	0	4	0	0		65	3	1712121051608	0
8	0	13	0	0		65	3	1712121051610	0
9	0	5	0	0		1	3	1712121051560	0
10	0	0	0	0		1	3	1712121051558	0
11	0	6	0	0		0	0	1712121051605	0
12	0	0	0	0		1	0	1712120950000	1712
13	0	13	0	0		1	3	1712121051561	0
14	0	6	0	0		0	0	1712120819121	0
15	0	6	0	0		0	0	1712120802822	0

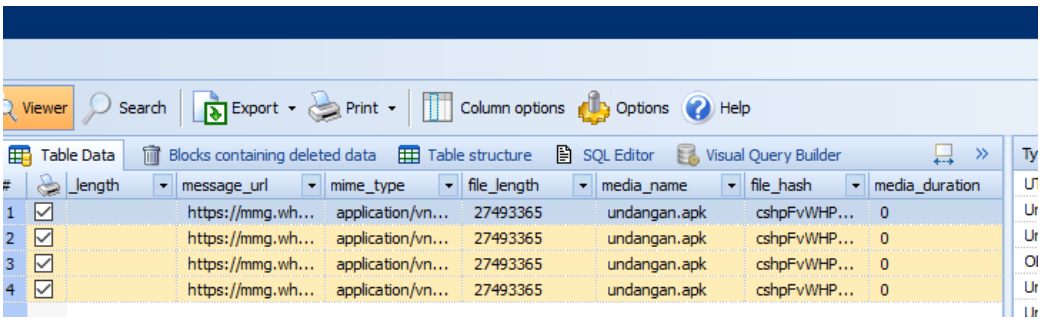
Gambar 4.28. Keterangan staus pada tabel *massege*

Keterangan status diatas berisi angka biner dimana didalam angka biner tersebut memiliki arti keterangan dari status pesan diatas dapat dilihat pada gambar 4.29 keterangan dari status pesan tersebut.



Gambar 4.29. Arti dari keterangan status tabel *massege*

Selain itu terdapat tabel *massege_media*, tabel ini berisi *media_name* yang terdaftar didalam aktifitas pengguna *whatsapp* dapat dilihat pada gambar 4.30 berikut.



#	_length	message_url	mime_type	file_length	media_name	file_hash	media_duration
1		https://mmg.wh...	application/vn...	27493365	undangan.apk	cshpFvWHP...	0
2		https://mmg.wh...	application/vn...	27493365	undangan.apk	cshpFvWHP...	0
3		https://mmg.wh...	application/vn...	27493365	undangan.apk	cshpFvWHP...	0
4		https://mmg.wh...	application/vn...	27493365	undangan.apk	cshpFvWHP...	0

Gambar 4.30. Isi dari tabel *massege _media*

2. Analisis perangkat *Iphone*.

Setelah proses *examanation* selanjutnya yaitu menganalisis hasil data yang berhasil diangkat. Berikut dapat dilihat pada gambar 4.31 analisis pada *file* pdf.

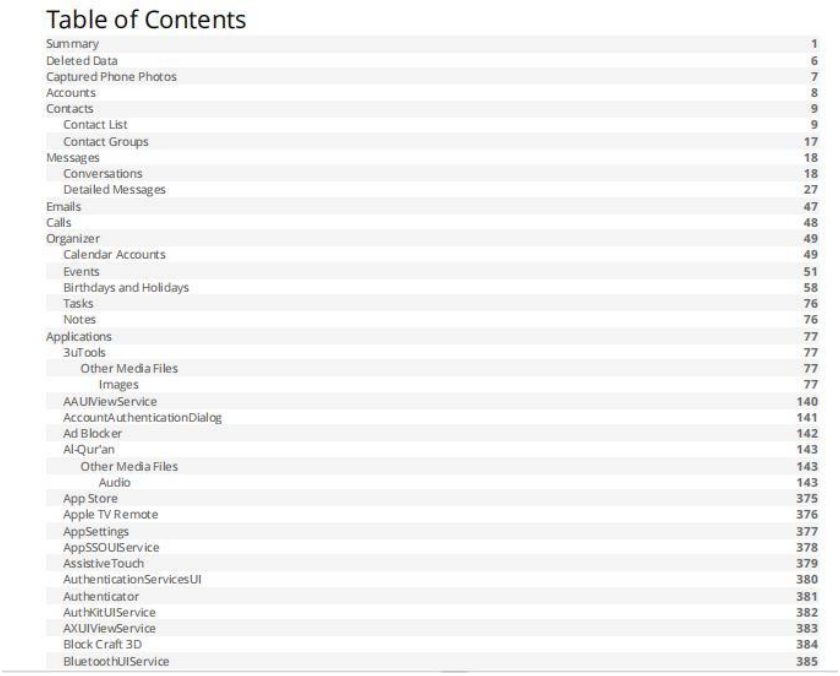
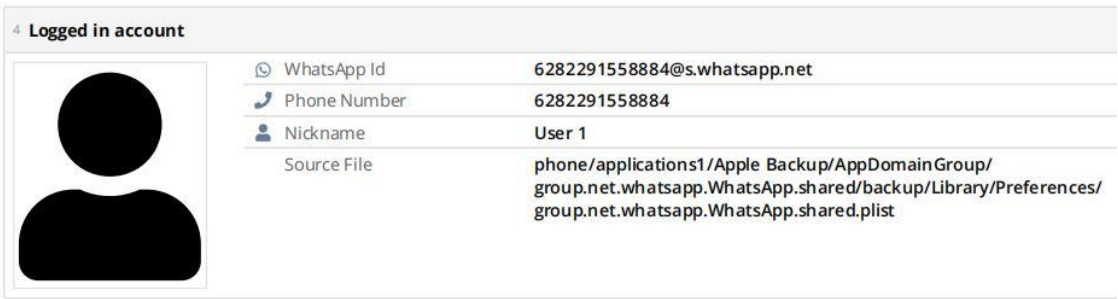


Table of Contents

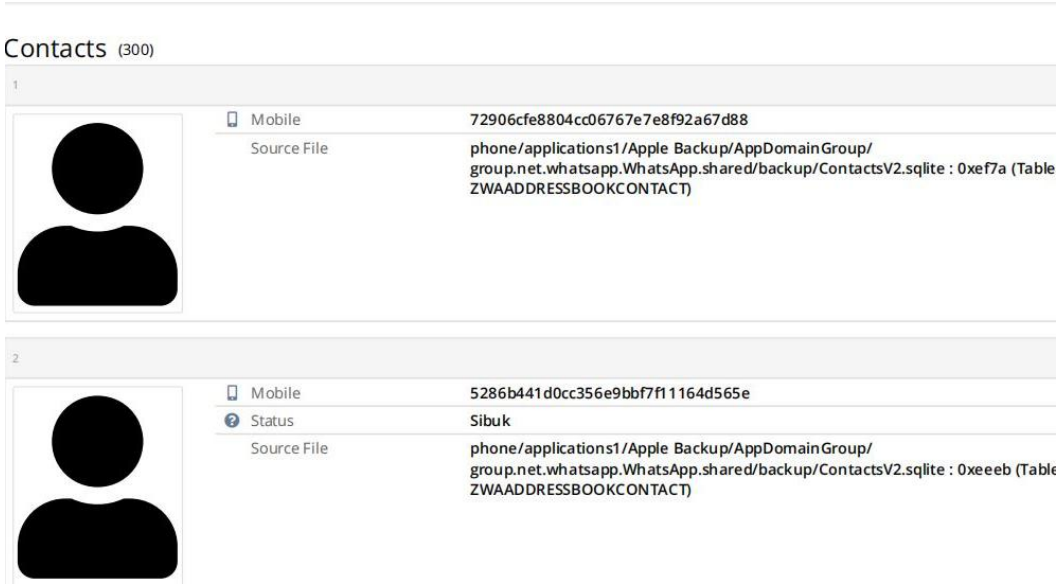
Gambar 4.31. Tabel *of content* hasil extraksi

Dari tabel diatas terdapat format data yang berhasil diextraksi seperti *accounts*, *contacts, Chat, masseges, strored media s*, selanjutnya menganalisis dari hasil extraksi di atas. Terdapat informasi mengenai akun dari pengguna *whatsapp* dapat dilihat pada gambar 4.32 berikut.



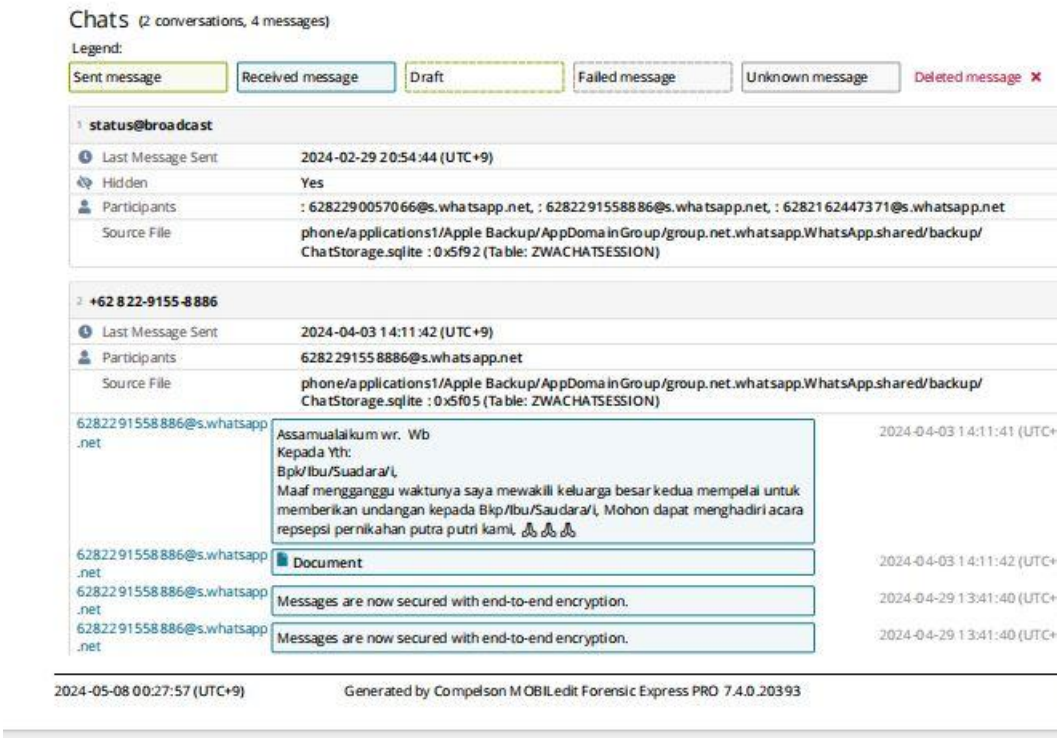
Gambar 4.32 Informasi Akun Pengguna

Selain dari itu terdapat informasi berupa kontak dari pengguna lain, beserta status akun tersebut. Terdapat 300 jumlah kontak yang berhasil diextraksi, seperti pada gambar 4.33 berikut .



Gambar 4.33. Informasi Kontak

Adapun bukti *Chat* yang didapatkan dari hasil extraksi ini beserta status pengirim dan informasi lainnya mengenai pengirim untuk lebih jelas terdapat pada gambar 4.34 berikut.



Gambar 4.34. Informasi *Chat*

4.2.4. Reporting

Setelah tahap Pengumpulan, *Examination dan Analysis* berhasil dilakukan, maka barang bukti yang berkaitan dengan aplikasi *Whatsapp* telah didapatkan. Pada tahapan ini akan membahas dan menyajikan barang bukti yang berhasil didapat yang berkaitan dengan aplikasi *Whatsapp* untuk mengungkapkan sebuah kasus kejahatan yang telah diskenariokan. Dapat dilihat pada tabel 4.2 berikut ini.

Tabil 4.2. Keterangan Barang bukti

No	Barang Bukti	Keterangan	
		Ipohne 7 Plus	Oppo A37f
1.	*Smartphone*	Ada	Ada
2	Nomor Hanphone Pengguna	Ada	Ada
3	Akun Korban	Ada	Ada
4	Percakapan	Tidak ada	Ada
5	*File*/gambar	Tidak ada	Ada

Dari tabel diatas dapat dilihat ada beberapa data yang tidak berhasil di temukan yaitu data pada perangkat *iphone* berupa data percakapan dan data gambar yang telah discenariokan, hal ini disebabkan keterbatasan dari *Tool*ss yang digunakan, *Tool*ss *Mobile*dit forensik expres hanya dapat melaukan *logic aquisesion* sehingga data yang terhapus tidak ditemukan.

4.3. Analisis

Pada tahpan ini yaitu tahapan terakhir dari proses extraksi pada *smartphone android* oppo a37f dan *iphone* 7 plus untuk lebih jelasnya sebagai berikut.

4.3.1. Smartphone Oppo A37f

Berdasarkan penelitian yang dilakukan pada perangkat *android* oppo a37f, proses extraksi berjalan sesuai yang diharapkan, dimana bukti - bukti dalam skenario berhasil ditemukan. Tetapi pada proses ini terdapat beberapa kendala didalamnya, diantarnya *database* dari perangkat ini tidak dapat di deskripsikan menggunakan *whatsapp viewer*

dikarenakan perbedaan dari versi *database* itu sendiri sehingga, untuk mengatasi hal itu peneliti menggunakan *sqlite* dari *Tools oxsigen* yang dapat membaca isi dari *database* itu sendri. *Database* yang penting untuk diteliti pada kasus *whatsapp* ini yaitu berupa *wa.db* dimana didalamnya terdapat data kontak dan *Msgstore.db*, *database* ini berisi aktifitas dari pengguna akun itu sendri, seperti percakapan. Ada beberapa temuan yang peneliti temukan berupa *Chat whatsapp* yang telah di hapus dengan otomatis hilang dari *database*, sehingga hal ini tidak memungkinkan dilakukan diluar *Tools*s forensik itu sendri, *database* yang sudah terhapus kehilangan id dari *database* itu sendri. Karena hal ini *Tools*s forensik sangat membantu untuk mengantisipasi hal hal seperti itu. Dalam extraksi pesan *whatsapp* yang telah terhapus harus menggunakan teknik *phisical aqusesion* hal ini memungkinkan untuk mendapatkan seluru *file* sistem sehingga tidak terjadinya kehilangan data, tetapi untuk mencapai hal itu diperlukannya akses *root* unt uk mendapatkan hak istimewa pada *smartphone* tersebut. Hal ini tidak berlaku pada *logic aquisesion*.

4.3.2. Smartphone Iphone 7 Plus

Berdasarkan penelitian pada *smartphone iphone* 7 plus, proses extraksi tidak menemukan semua bukti yang dibutuhkan, perangkat *iphone* telah melewati proses *jailbreak*, proses *jailbreak* ini kurang lebih sama seperti proses *root* dimana untuk mendapatkan akses istimewa di dalam perangkat tersebut tetapi hal itu tidak cukup sehingga untuk mendapatkan seluru barang bukti dengan mengangkat seluru sistem *file* memerlukan teknik *checkm8. Checkm8* merupakan ekspoitasi jeiblreak untuk perangkat ios, artinya memanfaatkan kerentanan di perangkan ios untuk memberi pengguna "*root*" untuk akses administratif *iphone*. Kebanyakan *jailbreak* mengeksploitasi kerentanan dalam sistem operasi iThing iOS. *Checkm8* berbeda, karena digolongkan sebagai eksploitasi *Boot ROM*.. Semua komputer memiliki memori hanya baca (ROM) permanen yang tidak

dapat diubah atau ditimpah. Saat Anda memboot komputer,sistem operasi tidak langsung dimuat. Sebelum hal ini terjadi, chip penyimpanan dengan ROM yang berisi instruksi sederhana untuk memuat sistem operasi sebenarnya harus terlebih dahulu mengeksekusi kodenya. Ini disebut Boot ROM. Faktanya, ini sedikit penyederhanaan yang berlebihan, karena Boot ROM biasanya memuat program tingkat rendah lainnya yang disebut bootloader, yang pada gilirannya mencari dan memuat sistem operasi. Namun untuk tujuan kita, cukup diketahui bahwa saat menghidupkan *iphone*, Boot ROM adalah hal pertama yang melakukan apa saja.

Hal yang penting untuk disadari adalah bahwa kode Boot ROM ini tertanam di dalam prosesor yang digunakan untuk memulai perangkat (sekali lagi, bahkan sebelum sistem operasi dimuat. Saat Apple merilis patch perangkat lunak untuk *jailbreak* biasa, patch tersebut memperbaiki sesuatu dalam kode sistem operasi. Namun karena checkm8 mengeksploitasi kerentanan di Boot ROM bukan merupakan bagian dari sistem operasi Apple benar-benar tidak dapat menambalnya. Satu-satunya pilihan mereka adalah melakukan penarikan besar-besaran terhadap perangkat yang terkena dampak dan secara fisik mengganti chip yang rentan.

Dalam hal ini ada beberapa *Tool*ss forensik yang mengsuport checkm8 ini seperti belkasoft eviden center dan celebrite UFED. Akan tetapi ekses untuk *Tool*ss ini terbatas sehinnga peneliti menggunakan *Tool*ss yang dapat digunakan, hal ini tidak efektif karena tolls hanya dapat melakukan logis aquisesion bukan phisical aquisesion.

4.4. Evaluasi Hasil

Dari hasil diatas bahwa dalam penangan kasus extraksi *file* pesan *whatsapp* yang telah terhapus dalam menghadirkan barang bukti digital, diperlukannya *Tools* forensik. Selain dari itu pada kasus pesan *whatsapp* yang telah terhapus teknik pengumpulan data

yang dilakukan yaitu menggunakan *physical aquisesion* atau akusisi fisik. Hal ini diperlukan karena *file* atau pesan yang terhapus tidak akan terlihat secara *logic* tetapi tidak hilang masi tersimpan di dalam *database*.

Proses akusisi atau imagin dapat menggunkan *Tools* seperti *Android* Debug Bridge (ADB), *Mobile*dit forensik, dan *Oxigen* Detektif *Forensics* dan dalam menganalisis untuk mencari barang bukti dapat menggunakan *Tools Autopsy*, FTK Imager, dan *Oxigen* Detektif *Forensics*.

Penelitian yang dilakukan pada 2 buah *smartphone android* oppo a37f dan iphone 7 plus. Bukti pada *smartphone android* berhasil ditemukan secara keseluruhan, proses imagin pada *android* menggunakan *Android* Debug Bridge (ADB), setalah *file* sistem berhasil di akusisi di lanjutkan dengan proses analisis menggunkan *Tools Autopsy*. Karena pada kasus ini yaitu *whatsapp* untuk mendapatkan seluruh barang bukti, diperlukannya *database whatsapp* untuk dianalisis lebih lanjut. Ada beberapa tabel *database whatsapp* yang penting untuk dianalisis berupa *Msgstore.db* dan wa.db. pada tabel *Msgstore.db* berisi informasi tentang pesan terkirim, seperti nomor kontak, isi pesan, status, cap waktu, informasi tentang *file* terlampir, dll. *File Msgstore.db* terletak di bawah jalur /data/data/com.*whatsapp*/*database*s / , sedangkan wa.db berisi daftar lengkap kontak pengguna *Whatsapp*, termasuk nomor telepon, nama tampilan, cap waktu, dan informasi lain yang disebutkan saat mendaftar di *Whatsapp*. *File* wa.db terletak di bawah jalur /data/data/com.*whatsapp*/*databases*/. Berbeda dengan *smartphone* iphone yang proses akusisinya menggunakan *Mobile*dit *Forensics* dan hasil akusisi didapatkan dalam bentuk

folder dan pdf, dari a*output* itu dapat dianalisis secara langsung, tetapi pada proses pencarian barang bukti di perangkat iphone tidak menemukan secara keseluruhan dikarenakan *Tools* yang digunakan hanya mengangkat data *logic* tidak dengan keseluruhan data.

Pada proses pencarian barang bukti untuk *smartphone android* dan iphone cukup berbeda hal ini dipengaruhi *Tools* yang suport dengan perangkat. Dalam akusisi fisik juga diperlukan akses *root* untuk mendapatkan akses super user agar memiliki akses lebih diperangkat yang akan di analisis.

Berbeda dengan penelitian sebelumnya dimana hanya menggunakan 1 perangkat saja dengan versi *android*, pada penelitian ini memanfaatkan *Android* Debug Bridge (ADB), dan *Mobile*dit forensik untuk melakukakn akusisi, tetapi barang bukti yang yang dicari ditemukan terutama pada perangkat *android*.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan temuan penelitian makalah "Analisis Mobile Forensik Ekstraksi File pada Aplikasi *WhatsApp* yang Dihapus Menggunakan Kerangka *National Institute of Standards and Technology* (NIST)" oleh, dapat diambil beberapa kesimpulan sebagai berikut.

1. *Framework* NIST telah terbukti efektif untuk ekstraksi data forensik pada perangkat *Android*. Metode ini memungkinkan identifikasi dan pemulihan data *WhatsApp* yang terhapus melalui prosedur sistematis yang mencakup pengumpulan bukti digital, investigasi, analisis, dan pelaporan.
2. Terdapat perbedaan signifikan dalam kemampuan ekstraksi data antara perangkat *Android* dan *iOS*. Di perangkat *Android,* Anda dapat menggunakan alat seperti ADB dan *Autopsy* untuk mengekstrak data yang dihapus secara lebih lengkap. Sebaliknya, pada perangkat *iOS*, khususnya iPhone, alat yang tersedia hanya cocok untuk ekstraksi logis dan tidak dapat memulihkan data yang terhapus sepenuhnya.
3. Keterbatasan alat forensik yang digunakan merupakan faktor penting keberhasilan ekstraksi data. Alat seperti *Mobileedit Forensics* dan *FTK Imager* berfungsi dengan baik di perangkat *Android,* namun memiliki keterbatasan pada perangkat *iOS*. Hal ini menyoroti pentingnya memilih alat yang tepat tergantung pada jenis perangkat dan sistem operasi.
4. Proses *rooting* pada perangkat *Android* dan *jailbreak* pada perangkat *iPhone*

merupakan langkah penting untuk mengakses data tersembunyi yang lebih dalam. Jika Anda tidak mengikuti langkah-langkah ini, akses ke data Anda yang terhapus akan sangat terbatas.

5. Penelitian ini juga menyoroti perbedaan tingkat keamanan antara sistem operasi *Android* dan *iOS*. Android cenderung membuat data lebih mudah diakses dan diekstraksi, sedangkan *iOS* memiliki tingkat perlindungan data yang lebih tinggi sehingga membuat proses forensik menjadi lebih sulit.
6. Hasil penelitian ini sangat relevan bagi profesional forensik digital, penyelidik kejahatan dunia maya, dan pengambil keputusan keamanan informasi. Pengetahuan tentang metode yang efektif dan alat yang tepat dapat meningkatkan efisiensi dalam mengungkap bukti digital, terutama ketika melibatkan aplikasi pesan instan seperti *WhatsApp*.

Oleh karena itu, penelitian ini memberikan kontribusi penting pada bidang forensik seluler, terutama dalam konteks aplikasi pesan instan yang dihapus, dan disesuaikan dengan jenis perangkat dan sistem operasinya untuk mencapai hasil yang optimal.

5.2. Saran

Pada peneitian ini terdapat banyak kekurangan, untuk itu peneliti berharap masukan serta saran untuk memaksimalkan penelitian ini. Peneliti menyarankan untuk penelitian berikutnya lebih ditingkatkan metode maupun teknik forensik dalam pemecahan kasus tersebut. Dan mencoba pada versi *smartphone* yang berbeda, karena tidak semua *smartphone* memiliki teknik yang sama tergantung studi kasusunya.

DAFTAR PUSTAKA

Anshori, I., Putri, K. E., & Ghoni, U., 2021, Analisis Barang Bukti Digital Aplikasi *Facebook Messenger* Pada *Smartphone Android* Menggunakan Metode Nij. It *Journal And Development* (ITJRD), ISSN:2528-4061, Vol. 5 *Issue.2* Maret, 2021

Ayers, R., Brothers, S., & Jansen, W, (2014). *Guidelines On Cell Phone Forensics.* Nist Special Publication 800-101.

Barkem, W., Jackson S.,2023, *Digital Forensic Analysis Of Whatsapp Business Aplications On Android Smarphone Using NIST*.Jurnal Manajemen, Teknik Informatika, Dan Rekayasa Komputer, ISSN:2476-9843, Vol. 22 *Issue*.3 July, 2023.

Cybervie.com, 2024, Pada artikel ini kita akan mempelajari tentang otopsi yang merupakan alat sumber terbuka untuk forensik digital : https://cybervie.com/blog/introduction-to-*Autopsy*-an-open-source-digital-*Forensics*-tool/.

Haryadi, D, (2022), Buku Panduan Dasar Forensik Digital, Penerbit Baskara Media

Fitriana, M. (2019). Penerapan Metode *National Institute Of Standards And Technology* (Nist) Dalam Analisis *Forensic Digital* Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku, 23-84.

Harmin Hatta, & Muhammad Zia Ulhaq., 2022, Penggunaan Media Sosial *Whatsapp* Di Kalangan Mahasiswa Program Studi Desain Komunikasi Visual Universitas Negeri Makassar. Jurnal Kependidikan Media, ISSN:2964-7355, Vol. 11 *Issue.3* Oktober 2022

Isnaini, K., Ashari, H., & Kuncoro, A., 2020, Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode Nist. Jurnal Rekayasa Sistem Komputer (RESISTOR), ISSN:2598-7542, Vol. 3 *Issue*.2 Oktober 2020

Maja*list*a, R., & Sutabri, T., 2023, Analisis Pencarian Data *Smartphone* Menggunakan Nist Untuk Penyelidikan Digital Forensik. Jurnal Informatika Teknologi Dan Sains (JINTEKS), ISSN:2686-3359, Vol. 5 *Issue*.1 Februari 2023

Mustajab, R., 2023, Dataindonesia.Id. Diambil Kembali Dari *Whatsapp* Masih Menjadi Media Sosial Terfavorit Di Indonesia: Https://Dataindonesia.Id/Internet/Detail/*Whatsapp*-Masih-Menjadi-Media-Sosial-Terfavorit-Di-Indonesia

Nasirudin, Sunardi, & Riadi, I., 2020, Analisis Forensik *Smartphone Android* Menggunakan Metode Nist Dan *Tools Mobiledit Forensic Express*. Jurnal Informatika Universitas Pamulang, ISSN:2541-1004, Vol. 5 *Issue.*1 Maret 2020

Polri, P., 2023, Kejahatan Siber Di Indonesia Naik Berkali-Kali Lipat. Diambil Kembali Dari Pusat Informasi Kriminal Nasional: Https://Pusiknas.Polri.Go.Id/Detail_Artikel/Kejahatan_Siber_Di_Indonesia_Naik_Berkali-Kali_Lipat

Qibriya, M., Ambarwati, A., & Susilo, K., 2021, Analisis Forensik Digital Pada Aplikasi *Instant Messaging* Di *Smartphone* Berbasis *Android* Untuk Bukti Digital. Jurnal Teknologi Informas*i*, ISSN:2580-7927, Vol. 5 *I*ssue.2 Desember 2021

Riadi, I., Sunardi, & Sahiruddin., 2019, Analisis Forensik *Recovery* Pada *Smartphone Android* Menggunakan Metode *National Institute Of Justice* (Nij). Journals System Universitas Mulawarman, ISSN:2579-8790, Vol. 3 *Issue*.1 Juni 2019

Saputri, N., & Indrayani, R., 2022, Analisis Data Forensik Investigasi Kasus Peredaran Narkoba Pada *Smartphone* Berbasis *Android*. *Journal Of Information Technology Research*, ISSN:2776-8546, Vol. 3 *Issue*.2 Desember 2022

Sari, D., Takariani, C. S., Pangaribuan, T. R., & Simatupang, O., 2023, Relasi Sosiodemografi Terhadap Kesadaran Keamanan Dan Privasi Data Pengguna *Whatsapp* Di Provinsi Jawa Barat. Jurnal Studi Komunikasi Dan Media, ISSN:1978-5003, Vol. 27 *Issue*.1 Juni 2023

Syaharani, M. (2023, Agustus 10). Goodstats. Diambil Kembali Dari 10 Negara Pengguna *Smartphone* Terbanyak Di Dunia: Https://Goodstats.Id/Article/10-Negara-Dengan-Pengguna-*Smartphone*-Terbanyak-Di-Dunia-Indonesia-Masuk-Daftar-Fdv25

Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital *Facebook Messenger* Mengunakan Metode Nist. *It Journal Research And Development,* ISSN:2528-4053, Vol. 3 *Issue.*1 Agustus 2018

Zain , L.., 2023, Apa itu *3uTools* ? Aplikasi Multifungsi buat perangkat *IOS* : https://www.idntimes.com/tech/gadget/laili-zain-damaika-1/apa-itu-*3uTools*-1

Zuhri, A., Putra, H. R., Fazri, A., & Miftahurrahmah. (2022). Aplikasi *Instan Accessible* Di Era Komunikasi Kontemporer Tahun 2022 Bagi Mahasiswa Natives Indonesia.

Komuniti: Jurnal Komunikasi Dan Teknologi Informasi, ISSN:2087-085X, Vol. 14 *Issue*.2 September 2022

LAMPIRAN

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN SEMINAR HASIL SKRIPSI

Dengan ini dinyatakan bahwa pada

Hari / tanggal	:	JUMAT, 31 MEI 2024
Pukul	:	10:30 - 12:30
Tempat	:	RUANG SIDANG

telah berlangsung Seminar Hasil Skripsi dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

Perbaiki sesuai arahan penguji

11-06-24

Dosen Pembimbing 1,

ALFANUGRAHA, Hi. USMAN, S.T., M.Kom.
NIP. 199403182019032029

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN SEMINAR HASIL SKRIPSI

Dengan ini dinyatakan bahwa pada

Hari / tanggal	:	JUMAT, 31 MEI 2024
Pukul	:	10:30 - 12:30
Tempat	:	RUANG SIDANG

telah berlangsung Seminar Hasil Skripsi dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

- Lakukan Perbaikan sesuai yang diminta pembimbing

OK Siap ayuun
Prangat 10/6/2024

Dosen Pembimbing II,

YASIR MUIN, S.T., M.Kom.
NIDN. 9990582796

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN SEMINAR HASIL SKRIPSI

Dengan ini dinyatakan bahwa pada

Hari / tanggal	:	JUMAT, 31 MEI 2024
Pukul	:	10:30 - 12:30
Tempat	:	RUANG SIDANG

telah berlangsung Seminar Hasil Skripsi dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

Tambahkan Pembahasan yang menjelaskan terkait hasil penelitian anda dan bandingkan dengan penelitian yang lain.

Pada halaman 14 cari referensi 5 tahun terakhir

Tambahkan Abstrak

Perbaiki Sistematika Penulisan

4/6/24.

Dosen Penguji I,

Dr. MUHAMMAD RIDHA ALBAAR, S.Kom., M.Kom.
NIP. 198504232008031001

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN SEMINAR HASIL SKRIPSI

Dengan ini dinyatakan bahwa pada

Hari / tanggal	:	JUMAT, 31 MEI 2024
Pukul	:	10:30 - 12:30
Tempat	:	RUANG SIDANG

telah berlangsung Seminar Hasil Skripsi dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

- Ikuti format penulisan (terutama di BAB II tentang sumber dari teori, gambar, tabel)
- Buat running program pada saat asistensi
- harus ada analisis yang dibahas secara menyeluruh dari hasil yang diperoleh, jangan hanya setting pada tools yang digunakan
- pelajari defenisi perintah2 command line yang digunakan

Dosen Penguji II,

ROSIHAN, S.T., M.Cs.
NIP. 197607192010121001

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN SEMINAR HASIL SKRIPSI

Dengan ini dinyatakan bahwa pada

Hari / tanggal	:	JUMAT, 31 MEI 2024
Pukul	:	10:30 - 12:30
Tempat	:	RUANG SIDANG

telah berlangsung Seminar Hasil Skripsi dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

1. Buat video sebagai bukti penarapan metede yang telah dilakuka
2. Perhatikan penulisan

06-06-2024

Dosen Penguji III,

SAIFUL Do. ABDULLAH, S.T., M.T.
NIDN. 0018029002

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN UJIAN SKRIPSI/TUTUP

Dengan ini dinyatakan bahwa pada

Hari / tanggal	:	JUMAT, 21 JUNI 2024
Pukul	:	07:30 - 09:00
Tempat	:	RUANG PRODI

telah berlangsung Ujian Skripsi/Tutup dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

Perbaiki sesuai arahan penguji

Dosen Pembimbing I,

ALFANUGRAHA A. Hi. USMAN, S.T., M.Kom.
NIP. 199403182019032029

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN UJIAN SKRIPSI/TUTUP

Dengan ini dinyatakan bahwa pada

Hari / tanggal	:	JUMAT, 21 JUNI 2024
Pukul	:	07:30 - 09:00
Tempat	:	RUANG PRODI

telah berlangsung Ujian Skripsi/Tutup dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

- Perbaikan Sesuai dengan permintaan penguji

Acc ole
tgl: 18/7/24

Dosen Pembimbing II,

YASIR MUIN, S.T., M.Kom.
NIDN. 9990582796

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN UJIAN SKRIPSI/TUTUP

Dengan ini dinyatakan bahwa pada

Hari / tanggal	:	JUMAT, 21 JUNI 2024
Pukul	:	07:30 - 09:00
Tempat	:	RUANG PRODI

telah berlangsung Ujian Skripsi/Tutup dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

Citasi mininal 5 Tahun terakhir halaman 20 masih ada tahun citasi 2014

Gambar pada halaman 29,41,42 di perjelas

Kesimpulan belum menjawab batasan masalah anda

ACC

27-06-24

Dosen Penguji I,

Dr. MUHAMMAD RIDHA ALBAAR, S.Kom., M.Kom.
NIP. 198504232008031001

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN UJIAN SKRIPSI/TUTUP

Dengan ini dinyatakan bahwa pada

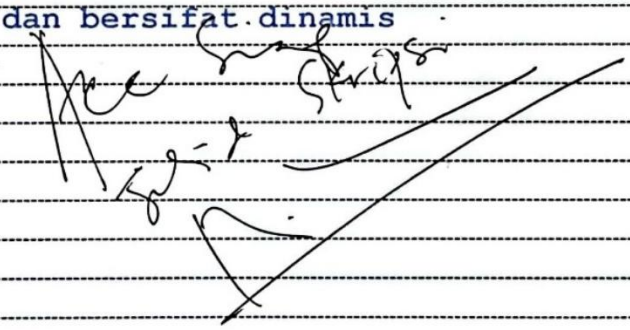
Hari / tanggal	:	JUMAT, 21 JUNI 2024
Pukul	:	07:30 - 09:00
Tempat	:	RUANG PRODI

telah berlangsung Ujian Skripsi/Tutup dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

- Ikuti format penulisan
- Jelaskan perkembangan teknologi jaringan seluler
- Belajar pembuatan program untuk menginput biodata mahasiswa memanfaatkan struktur data record dan bersifat dinamis



Dosen Penguji II,

ROSIHAN, S.T., M.Cs.
NIP. 197607192010121001

UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK
PROGRAM STUDI INFORMATIKA

DAFTAR PERBAIKAN UJIAN SKRIPSI/TUTUP

Dengan ini dinyatakan bahwa pada

Hari / tanggal	:	JUMAT, 21 JUNI 2024
Pukul	:	07:30 - 09:00
Tempat	:	RUANG PRODI

telah berlangsung Ujian Skripsi/Tutup dengan Peserta:

Nama Mahasiswa	:	RAHMAT KALFI
NPM	:	07352011057
Judul	:	ANALISIS MOBILE FORENSIC EKSTRAKSI FILE PADA APLIKASI WHATSAPP YANG TELAH TERHAPUS MENGGUNAKAN FRAMEWORK NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

dinyatakan HARUS menyelesaikan perbaikan, yaitu:

Perbaikan penulisan
Kesimpulan diperbaiki
Bahasa inggris diperhatikan

27-06-2024

Dosen Penguji III,

SAIFUL Do. ABDULLAH, S.T., M.T.
NIDN. 0018029002

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK PROGRAM STUDI INFORMATIKA
Kampus III Universitas Khairun, Kelurahan Jati Kota Ternate Selatan
http://if.unkhair.ac.id, http://unkhair.ac.id Group FB: if.unkhair

KARTU BIMBINGAN HASIL

Nama Mahasiswa : Rahmat Kalfi
NIM : 07352011057
Dosen Pembimbing I : Alfanugrah A. Hi. Usman, S.T., M.Kom.
Judul : Analisis *Mobile Forensics* Ekstraksi File Pada Aplikasi *Whatsaap* Yang Telah Terhapus Menggunakan Framework *National Institute of Standards and Technology* (NIST)

NO	Tanggal	Uraian	Paraf
1	9/05/21	TYPO/KAPITAL -	
		Penjelasan /ket di gambar 4.3	
		Tambahkan Penjelasan di reporting	
2	21/05/21	Perbaikan Paragraf pada halaman 40.	
		Untuk pada B. Inggris /B. Asing	
		Gambar 4.2 ada 2	
		Acc 24/05/21	
3	24/05/21	PPT.	

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS KHAIRUN
FAKULTAS TEKNIK PROGRAM STUDI INFORMATIKA
Kampus III Universitas Khairun, Kelurahan Jati Kota Ternate Selatan
http://if.unkhair.ac.id, http://unkhair.ac.id Group FB: if.unkhair

KARTU BIMBINGAN HASIL

Nama Mahasiswa : Rahmat Kalfi
NIM : 07352011057
Dosen Pembimbing II : Yasir Muin, S.T., M.Kom.
Judul : Analisis *Mobile Forensics* Ekstraksi File Pada Aplikasi *Whatsaap* Yang Telah Terhapus Menggunakan Framework *National Institute of Standards and Technology* (NIST)

NO	Tanggal	Uraian	Paraf
1	01/05/2024	Metode disesuaikan dengan Kasus	
2	07/05/2024	Jadwal Penelitian dihapus	
3	11/05/2024	Perbaiki alur Penelitian	
		ok siap uji.	
		Pbl 13/5/24	