Analisis Keamanan Komunikasi Aplikasi *WAVE Mobile Communicator* pada Ponsel *Hybrid* dan Ponsel Konvensional Dengan Pendekatan Digital Forensik Berbasis SNI ISO 27037

Nur Uswatun Hasanah
21917015

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Magister Informatika (Forensika Digital)
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2025

Lembar Pengesahan Pembimbing

Analisa Keamanan Komunikasi Aplikasi WAVE Mobile Communicator pada Ponsel *Hybrid* dan Ponsel Konvensional Dengan Pendekatan Digital Forensik Berbasis SNI ISO 27037

Nur Uswatun Hasanah 21917015

Yogyakarta, **18** Februari 2025

Pembimbing

Dr. Ahmad Luthfi, S.Kom., M.Kom.

Lembar Pengesahan Penguji

Analisa Keamanan Komunikasi Aplikasi WAVE Mobile Communicator pada Ponsel Hybrid dan Ponsel Konvensional Dengan Pendekatan Digital Forensik Berbasis SNI ISO 27037

Nur Uswatun Hasanah 21917015

Yogyakarta, **18** Februari 2025

Tim Penguji,

Dr. Ahmad Luthfi, S.Kom., M.Kom.
Ketua

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

Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D.
Anggota II

Mengetahui,
Ketua Program Studi Informatika
Program Magister Universitas Islam Indonesia

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Analisis Keamanan Komunikasi Aplikasi *WAVE Mobile Communicator* pada Ponsel *Hybrid* dan Ponsel Konvensional Dengan Pendekatan Digital Forensik Berbasis SNI ISO 27037

Keamanan komunikasi dalam lingkungan militer memainkan peran krusial dalam melindungi kerahasiaan informasi strategis. Dalam konteks ini, ponsel menjadi alat utama untuk pertukaran informasi terutama untuk TNI, dengan Aplikasi WAVE Mobile Communicator yang menjadi salah satu platform komunikasi yang digunakan. Dengan pertumbuhan ancaman siber yang terus berkembang, penting untuk membandingkan keamanan aplikasi ini pada dua jenis perangkat yang umum digunakan: ponsel hybrid dan ponsel konvensional. Ponsel hybrid, seperti Motorola LEX L11a yang digunakan oleh Tentara Nasional Indonesia (TNI), memiliki kemampuan untuk menggunakan beberapa jenis teknologi komunikasi, sementara ponsel konvensional hanya terbatas pada satu jenis teknologi. Penelitian ini bertujuan untuk menganalisis dan membandingkan keamanan Aplikasi WAVE Mobile Communicator pada kedua jenis perangkat tersebut menggunakan pendekatan digital forensik. Melalui pendekatan digital forensik yang didasarkan pada prinsip-prinsip keamanan komunikasi militer dan standar industri, penelitian ini akan mengeksplorasi kelemahan potensial dan tingkat kerentanan pada aplikasi tersebut. Metodologi ini mencakup akuisisi data forensik dari kedua jenis perangkat, analisis struktur aplikasi, serta identifikasi dan evaluasi potensi kerentanan keamanan. Penelitian ini juga akan memperhatikan kendala teknis yang mungkin mempengaruhi keamanan aplikasi pada masing-masing jenis perangkat. Hasil dari penelitian ini diharapkan memberikan pemahaman yang lebih baik tentang perbandingan keamanan Aplikasi WAVE Mobile Communicator pada ponsel hybrid dan konvensional, serta mengidentifikasi area di mana satu jenis perangkat mungkin memiliki keunggulan keamanan dibandingkan dengan yang lain. Informasi ini akan bermanfaat dalam pengembangan strategi keamanan komunikasi militer yang lebih efektif dan responsif terhadap ancaman siber yang terus berkembang.

Kata kunci

WAVE Mobile Communicator, ponsel *hybrid*, forensika digital, SNI ISO 27037, Tentara Nasional Indonesia (TNI).

Abstract

Analysis of Communication Security on WAVE Mobile Communicator Application on Motorola LEX L11a Hybrid Mobile Phone with and Conventional Phones Digital Forensic Based on SNI ISO 27037

Security of communication in the military environment plays a crucial role in safeguarding the confidentiality of strategic information. In this context, mobile phones have become a primary tool for information exchange, particularly for the Indonesian National Armed Forces (TNI), with the WAVE Mobile Communicator application being one of the communication platforms used. With the ever-growing cyber threats, it is essential to compare the security of this application on two commonly used device types: hybrid phones and conventional phones. Hybrid phones, such as the Motorola LEX L11a used by the TNI, have the ability to utilize multiple types of communication technologies, while conventional phones are limited to a single type. This research aims to conduct a comparative analysis of the security of the WAVE Mobile Communicator application on hybrid and conventional phones using a digital forensics approach. By employing a digital forensics methodology grounded in military communication security principles and industry standards, the study will explore potential vulnerabilities and susceptibility levels within the application. The methodology will encompass forensic data acquisition from both device types, application structure analysis, and identification and evaluation of potential security vulnerabilities. Additionally, the research will consider technical constraints that may impact application security on each device type. The anticipated outcomes of this research include a comprehensive understanding of the comparative security of the WAVE Mobile Communicator application on hybrid and conventional phones, along with the identification of areas where one device type may possess a security advantage over the other. This information will prove valuable in developing more effective and responsive military communication security strategies against evolving cyber threats.

Keywords

WAVE Mobile Communicator, hybrid mobile phone, digital forensics, SNI ISO 27037, Indonesian National Army (TNI).

Pernyataan Keaslian Tulisan

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

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

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

Yogyakarta, 18 Februari 2025

Nur Uswatun Hasanah, S.Kom.

6

Daftar Publikasi

Hasanah, N. U., & Luthfi, A. (2024). Analisa Hasil Akuisisi pada Ponsel Berbasis Hybrid. Jurnal Jepin, DOI https://doi.org/1026418/jp.v11i1.90935

Kontributor	Jenis Kontribusi
Nur Uswatun Hasanah	Mendesain eksperimen (60%) Menulis paper (80%)
Ahmad Luthfi	Mendesain eksperimen (40%) Menulis dan mengedit paper (20%)

Halaman Kontribusi

Pada bagian ini penulis ingin mengucapkan terima kasih kepada TNI yang telah memberikan kesempatan dalam menganalisa salah satu perangkat komunikasi. Analisis ini dilakukan untuk menambah pengetahuan penulis dan penulis berharap hasil penelitian ini dapat digunakan sebagai acuan TNI dalam melakukan pengadaan alat komunikasi selanjutnya.

Kedua penulis berterima kasih kepada Magister Informatika UII khususnya PUSFID yang telah dilengkapi dengan berbagai fasilitas yang memadai dan ketersediaan tools lengkap sangat membantu dalam proses penyelesaian tugas akhir ini.

Halaman Persembahan

Puji syukur penulis panjatkan kehadirat Allah SWT yang berkat rahmat dan hidayahnya penulis diberikan kesehatan dan kekuatan untuk menyelesaikan tesis ini sebagai salah satu syarat untuk mendapatkan gelar kemagisteran. Tidak mudah untuk menyelesaikan tesis ini, banyak rintangan yang penulis hadapi. Walaupun jauh dari kata sempurna, namun penulis bangga telah mencapai pada titik ini, yang akhirnya tesis ini bisa selesai meskipun membutuhkan waktu yang lebih lama dari waktu yang telah ditentukan.

Orang tua saya selalu mengatakan kepada saya untuk menyelesaikan apapun yang kita mulai. Seberat apapun rintangannya, Alhamdulillah penulis tetap bisa menyelesaikan tesis ini. Pada kesempatan ini penulis akan mempersembahkan tulisan ini untuk orang - orang yang banyak berperan bagi keberhasilan tulisan ini baik peran secara akademisi, moral, maupun finansial. Tesis ini saya persembahkan untuk :

1. Orang tua penulis, Bapak Indratmoko dan Ibu Rina Tri Susilowati yang telah memberikan dorongan baik secara moril maupun finansial selama berlangsungnya pendidikan Magister ini.
2. Suami penulis, Muhammad Ikhsan Surachman, S.T. yang telah memberikan dukungan moril dan finansial serta menjaga kekondusifan selama proses pembuatan tesis ini.
3. Dosen pembimbing, Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom. yang dengan sabar dan bijak membimbing setiap proses pembuatan tesis ini dan selalu memberikan kemudahan bagi penulis dalam mendapatkan informasi.
4. Bapak Dr. Yudi Prayudi, S.Si., M.Kom. yang memberikan dorongan kepada penulis dalam mengambil perkuliahan magister sehingga penulis dapat melanjutkan pendidikan magister meskipun dilakukan secara *hybrid* selama pandemi covid 2021.
5. Seluruh rekan - rekan Magister Informatika yang telah menjalani proses perkuliahan bersama terutama Amru Rizal, S.Kom. , rekan yang selalu bertukar pikiran dengan penulis selama pembuatan tesis ini.
6. Rekan kerja penulis, staf Personalia yang selalu memberikan dukungan moril saat penulis harus menyelesaikan tesis ini.
7. Sahabat di rantau, teh Ike yang selalu menghibur dalam setiap situasi.
8. Seluruh pihak yang terlibat dalam pembuatan tesis ini baik yang secara langsung maupun yang tidak langsung yang penulis tidak bisa sebutkan satu persatu.

Kata Pengantar

Puji syukur yang sedalam-dalamnya penulis panjatkan kehadirat Tuhan Yang Maha Esa atas segala berkat dan limpahan rahmat-Nya sehingga penulis dapat menyelesaikan proposal penelitian tesis dengan judul "**Analisis Keamanan Komunikasi Aplikasi WAVE Mobile Communicator pada Ponsel Hybrid dan Ponsel Konvensional Dengan Pendekatan Digital Forensik Berbasis SNI ISO 27037** "

Tujuan dari penulisan tesis ini adalah untuk memenuhi syarat dalam mencapai derajat Magister Manajemen pada Program Studi Magister Informatika Universitas Islam Indonesia. Di dalam proses penulisan tesis ini, penulis banyak mendapatkan bimbingan dan dukungan dari berbagai pihak sehingga penulisan tesis ini dapat terselesaikan tepat waktu.

Tulisan ini jauh dari kesempurnaan, penulis harap suatu saat nanti ada yang menyempurnakan penelitian ini dan penulis berharap bahwa tulisan ini dapat bermanfaat bagi dunia pendidikan di Indonesia.

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

BPM : Business Process Management

BPMS : Business Process Management System

CFC : Control Flow Complexity

EDL : Experience Driven Learning

MCDM : Multi-Criteria Decision-Making

SAW : Simple Additive Weighting

WP : Weighted Product

XES : eXtensible Event Stream

API : Antarmuka Pemrograman Aplikasi

BTS : Base Transceiver Station (Stasiun Pemancar)

C&C : Command & Control Server

CIFS : Common Internet File System

GSM : Global System for Mobile Communication

GPS : Global Positioning System

HDD : Hardisk

HT : Handy Talky

Hybrid Cloud : Gabungan dari layanan public cloud dan layanan private cloud yang memiliki fungsi beragam bagi perusahaan atau bisnis

IKEV2 : Internet Key Exchange versi 2

ioS : iPhone Operating System

IoT : Internet of Things

ISPS : The International Ship and Port Facility Security Code

IT : Information and Technology

LTE : Long Term Evolution

MIL-STD-810G: Serangkaian standar uji yang dirancang oleh Departemen Pertahanan Amerika Serikat (DOD)

MobSF : Mobile Security Framework

NFS : Network File System

NIJ : National Institute of Justice

Public Cloud : Sebuah Cloud Computing yang dishare melalui internet dan menuju ke perusahaan atau organisasi

PTT : Push-to-Talk

Qos : Quality of Security

SAP : System Analysis and Product in Data Processing

SNI : Standar Nasional Indonesia

SSD : Solid State Drive

TNI : Tentara Nasional Indonesia

TRIM SSD : Membersihkan dan mengorganisasikan SSD, sehingga menjadikannya lebih efisien serta memperpanjang masa pakainya

USB : Universal Serial Bus

VPN : Virtual Private Network

WAVE : Waskita Application Vendor Excellence

Wifi : Wireless Fidelity

BAB 1

Pendahuluan

1.1 Pendahuluan.

Dalam dunia militer, komunikasi bukan hanya menyampaikan informasi dari satu prajurit ke prajurit lainya, keamanan komunikasi memiliki peran fundamental dalam menjaga kerahasiaan informasi strategis. Hasil dari sebuah misi tergantung tergantung dari seberapa cepat, akurat, dan amannya informasi yang diterima. Oleh sebab itu, sistem komunikasi yang terenkripsi, prosedur autentikasi berlapis, serta pelatihan personel yang berkelanjutan merupakan hal yang sangat penting bagi militer untuk memastikan tidak ada celah yang bisa dimanfaatkan oleh pihak lawan. Setiap sandi, sinyal radio, hingga pesan teks harus diperlakukan dengan tingkat kerahasiaan tinggi. Oleh karna itu, Tentara Nasional Indonesia (TNI) dan Kepolisian Republik Indonesia (POLRI) menggunakan sebuah ponsel *hybrid* Motorola LEX L11a. Perangkat ini menjadi salah satu sarana pertukaran informasi, menjadi landasan bagi koordinasi taktis dan strategis dalam pelaksanaan tugas militer dan kepolisian. Dalam era yang semakin kompleks, di mana ancaman siber mengintensif, keamanan aplikasi ini mendapatkan urgensi yang meningkat untuk mencegah potensi risiko dan memastikan keberlanjutan operasional yang aman. Studi oleh Johnson menegaskan bahwa keamanan komunikasi menjadi kunci dalam menjaga integritas operasional dan strategis militer (Johnson,2019).

Dalam operasi militer modern, komunikasi yang efektif dan aman adalah kunci keberhasilan. Motorola LEX L11 hadir sebagai solusi canggih yang menggabungkan teknologi LTE dengan standar militer, memastikan komunikasi yang handal di medan tempur. Ponsel *hybrid* Motorola LEX L11a merupakan perangkat yang umum digunakan oleh personel TNI dan POLRI. Dilengkapi dengan Wave mobile comunicator, ponsel ini menjadi salah satu tulang punggung dalam sistem komunikasi militer dan kepolisian. Oleh karena itu, keberlanjutan dan keamanan penggunaan aplikasi ini menjadi faktor yang sangat penting bagi efektivitas dan keberhasilan tugas-tugas strategis TNI dan POLRI.

Aplikasi WAVE Mobile Communicator memainkan peran sentral dalam menjaga kerahasiaan informasi strategis dan memastikan kelancaran operasi lapangan. Namun, dengan kemajuan ancaman siber yang terus berkembang, perhatian terhadap keamanan aplikasi ini semakin meningkat. Oleh karena itu, penting untuk menganalisis dan memahami perbedaan keamanan antara aplikasi ini saat diimplementasikan pada kedua jenis perangkat.

Meskipun kedua teknologi ini memiliki potensi besar dalam mendukung operasi militer, penelitian forensik yang mendalam terhadap keduanya masih sangat terbatas. Sebagai contoh, studi oleh (Kouwen, Scanlon, & Raymond Choo, 2018) menyoroti pentingnya penyelidikan forensik terhadap peralatan komunikasi radio dua arah, namun penelitian tersebut belum membahas perangkat seperti LEX L11 dan aplikasi WAVE Mobile Communicator.

Dalam era digital dan ancaman siber yang terus berkembang, perangkat komunikasi militer seperti Motorola LEX L11 dan aplikasi WAVE Mobile Communicator menjadi tulang punggung komunikasi misi-kritis. Namun, hingga saat ini, belum terdapat penelitian forensik digital yang secara spesifik mengevaluasi bagaimana kedua sistem ini menyimpan, melindungi, dan merekam data penting. Kurangnya literatur ilmiah ini menunjukkan adanya kesenjangan pengetahuan yang cukup signifikan di bidang keamanan komunikasi dan investigasi forensik digital militer.

Perangkat Motorola LEX L11 merupakan alat komunikasi LTE yang dirancang khusus untuk kebutuhan militer dan penegakan hukum. Dilengkapi dengan fitur keamanan tingkat tinggi seperti enkripsi AES-256 dan sertifikasi FIPS 140-2 Level 3, perangkat ini mendukung operasional di lingkungan ekstrem dan aman dari manipulasi pihak ketiga (Motorola Solutions, 2023). Begitu pula, aplikasi WAVE Mobile Communicator yang memungkinkan komunikasi lintas perangkat berbasis push-to-talk over LTE (PoC), telah banyak digunakan dalam organisasi militer untuk menghubungkan pengguna dari jaringan berbeda secara aman dan real-time.

Namun, sejauh ini belum ditemukan penelitian akademik yang mengkaji bagaimana jejak digital (digital artefacts) dari perangkat ini dapat diekstraksi dan dianalisis secara forensik. Padahal, keberadaan data forensik sangat penting dalam proses investigasi insiden, pelanggaran keamanan, atau sebagai alat bukti hukum dalam sistem pertahanan.

Penelitian-penelitian sebelumnya sudah pernah membahas terkait keamanan aplikasi pada ponsel konvensional (Wirara., 2020). Beberapa klasifikasi pembahasannya adalah pada aspek teknologi dan keamanan aplikasi seperti whatsapp, skype, facebook messenger, imessenger. Namun, belum ada penelitian yang khusus membahas tingkat keamanan aplikasi WAVE khususnya yang digunakan oleh institusi TNI/POLRI sebagai aplikasi utama dalam komunikasi pada saat operasi militer. Disamping itu, penelitian-penelitian sebelumnya juga belum pernah membahas studi eksperimen untuk akuisisi perangkat communicator dengan menggunakan aplikasi WAVE.

Quick dan Choo (2018) menegaskan bahwa kesiapan forensik merupakan bagian penting dari sistem keamanan, dan seluruh perangkat komunikasi, termasuk perangkat misi-kritis, harus dapat menyediakan bukti digital yang valid dan terverifikasi dalam kondisi darurat. Mereka menyatakan bahwa "tanpa kesiapan forensik yang memadai, institusi akan kesulitan menanggapi insiden keamanan secara efektif dan tepat waktu" (Quick & Choo, 2018, p. 15).

Ahmed (2021) juga menambahkan bahwa kurangnya fokus terhadap perangkat taktis dalam studi forensik "menyebabkan blind spot dalam kesiapan digital organisasi yang memiliki fungsi kritikal seperti militer atau keamanan nasional" (p. 7). Dengan belum adanya metodologi yang terdokumentasi untuk memperoleh dan memverifikasi artefak digital dari LEX L11 atau aplikasi WAVE, risiko keamanan terhadap sistem komunikasi militer tetap terbuka dan sulit ditangani secara sistematis.

Dengan demikian, dibutuhkan penelitian mendalam yang mengevaluasi aspek forensik digital dari Motorola LEX L11 dan aplikasi WAVE Mobile Communicator. Penelitian ini akan sangat penting dalam membangun model analisis forensik yang dapat digunakan oleh profesional keamanan dan penegak hukum dalam upaya mitigasi, investigasi, dan dokumentasi insiden komunikasi militer secara lebih akurat dan dapat dipertanggungjawabkan secara hukum.

Melalui pendekatan digital forensik yang terfokus pada analisis keamanan aplikasi WAVE Mobile Communicator, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam upaya memastikan keamanan dan kerahasiaan komunikasi instan di lingkungan militer dan penegak hukum. Dengan latar belakang yang terinci, diharapkan hasil penelitian ini dapat memberikan dasar yang kokoh untuk kebijakan dan tindakan lebih lanjut terkait keamanan komunikasi dalam lingkup strategis ini.

Oleh karena itu, penelitian ini memiliki dua fokus utama pekerjaan, yaitu (1) menghasilkan temuan investigasi akuisisi perangkat communicator HP Motorola Lex 11 dengan aplikasi WAVE di dalamnya, dan (2) menghasilkan perbandingan tingkat keamanan perangkat communicator hybrid dan konvensional.

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang masalah tersebut, maka dalam penelitian ini rumusan masalah yang dibahas adalah:

1. Bagaimana hasil akuisisi komunikasi aplikasi wave mobile communicator pada ponsel hybrid dan ponsel konvensional dengan pendekatan digital forensik?

2. Apakah perangkat keras Motorola LEX L11a yang digunakan TNI dan POLRI memiliki tingkat keamanan data yang lebih baik dibandingkan ponsel konvensional?

1.3 Batasan penelitian

Agar masalah yang akan dibahas tidak meluas sehingga dapat mengakibatkan ketidakjelasan pembahasan masalah maka pada penelitian ini akan dibatasi terhadap masalah yang akan diteliti, antara lain:

1. Menggunakan ponsel Motorola lex l11a.
2. Menggunakan ponsel Xiaomi Redmi Note 8.
3. Scope / ruang lingkup penelitian ini adalah perbandingan keamanan komunikasi aplikasi wave dengan metode *digital forensic*.
4. Metode digital forensik yang digunakan adalah SNI ISO 27037:2014
5. Tools yang digunakan *mobiledit* dan *cellebrite*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk melakukan analisis keamanan komunikasi pada aplikasi WAVE Mobile Communicator yang digunakan di ponsel hybrid dan ponsel Konvensional dengan menggunakan pendekatan digital forensik berbasis SNI ISO 27037. Dalam kerangka tujuan tersebut, penelitian ini berfokus untuk:

1. Menganalisis artefak yang didapatkan dari hasil akuisisi aplikasi WAVE Mobile Communicator pada Ponsel Hybrid dan Konvensional: Penelitian ini akan menilai dan menganalisis hasil akuisisi data komunikasi dari aplikasi Wave Mobile Communicator pada ponsel hybrid dan ponsel konvensional dengan pendekatan digital forensik, guna mengidentifikasi perbedaan artefak digital, tingkat keterpulihan data, serta menilai integritas dan keaslian bukti yang diperoleh sebagai dasar rekomendasi metode investigasi forensik yang efektif.
2. Mengevaluasi Pengaruh Perangkat Keras Ponsel Hybrid terhadap Keamanan Data: Penelitian ini juga akan menyelidiki dan mengevaluasi tingkat keamanan data pada perangkat keras Motorola LEX L11a yang digunakan oleh TNI dan POLRI, serta membandingkannya dengan ponsel konvensional guna menentukan sejauh mana perangkat tersebut memberikan perlindungan data yang lebih baik dalam konteks operasional dan forensik.

1.5 Manfaat Penelitian

Berikut ini merupakan manfaat yang dapat diambil dari penelitian ini:

1. Manfaat bagi akademik:

   Menyumbang pemahaman mendalam tentang keamanan aplikasi WAVE Mobile Communicator pada ponsel hybrid dan ponsel Konvensional, penelitian ini berpotensi menjadi referensi penting di lingkungan akademik. Institusi akademik, peneliti, dan mahasiswa dapat memanfaatkan temuan penelitian ini sebagai dasar untuk pengembangan kurikulum di bidang keamanan digital dan forensik.

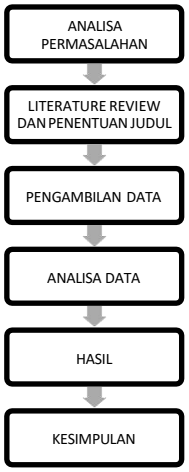
2. Manfaat bagi peneliti:

   Peneliti akan memperoleh pengalaman praktis dan meningkatkan keterampilan dalam menerapkan digital forensik berbasis SNI ISO 27037. Hasil penelitian juga akan memberikan wawasan tentang tantangan keamanan komunikasi militer menggunakan ponsel hybrid, mengembangkan pemahaman peneliti dalam domain ini.

3. Manfaat bagi investigator:

   Bagi investigator di lingkungan militer, hasil penelitian ini memberikan pemahaman yang lebih baik tentang potensi risiko dan kerentanan keamanan. Dengan demikian, investigator dapat mengambil tindakan pencegahan yang lebih efektif, meningkatkan keamanan komunikasi, dan merancang strategi perlindungan data yang lebih baik dalam menjalankan tugas operasional dan menjaga keamanan nasional.

1.6 Metodologi Penelitian



Gambar 1.1 Menjelaskan tentang alur metode penelitian.

1. Analisa Permasalahan

   Langkah awal pada tahapan penelitian ini adalah melakukan analisa permasalahan dari kejadian yang ada di lingkungan TNI AD.

2. Studi literatur dan Penentuan Judul.

   Tahapan selanjutnya dilakukan studi literatur sebagai landasan teoritis dengan mengumpulkan referensi yang relevan dengan studi penelitian dengan melalui jurnal, paper, makalah, artikel dan informasi situs website yang berfokus pada penelitian terkait selanjutny dari point of view penelitian lain ditentukan judul penelitian.

3. Pengambilan Data.

   Proses pengambilan data dilakukan dengan cara mengakuisisi perangkat Motorola Lex11 dan Xiomi Note 8 menggunakan perangkat celebrite dan mobile edit.

4. Analisa

   Melakukan analisa terhadap artefak hasil akuisisi dari perangkat motorola lex11 dan xiomi note 8 dan membandingkannya.

5. Hasil

   Hasil analisis data menjadi dasar untuk membangun keseluruhan penelitian. Disusunnya temuan, analisis keamanan, serta rekomendasi untuk perbaikan dan peningkatan keamanan aplikasi WAVE Mobile Communicator pada ponsel Motorola LEX L11a.

6. Kesimpulan.

   Menarik kesimpulan dari penelitian yang telah dilaksanakan dan melakukan memberikan saran untuk penelitian kedepannya.

1.7 Sistematika Penulisan

Penulisan yang sistematis dibuat untuk mengefektifkan proses penelitian dengan sistematika sebagai berikut:

Pendahuluan:

1. Latar Belakang: Menjelaskan pentingnya keamanan komunikasi militer melalui aplikasi WAVE Mobile Communicator pada ponsel Motorola LEX L11a dan konteks penggunaan oleh TNI dan POLRI.
2. Rumusan Masalah: Mengidentifikasi permasalahan keamanan yang perlu dianalisis, menitikberatkan pada potensi kerentanan dan risiko yang mungkin timbul.
3. Tujuan Penelitian: Merinci tujuan penelitian untuk menganalisis keamanan

aplikasi WAVE Mobile Communicator pada ponsel hybrid, dengan fokus pada pendekatan digital forensik berbasis SNI ISO 27037.

Tinjauan Pustaka:

1. Keamanan Komunikasi Militer: Mendalami teori dan konsep keamanan komunikasi dalam lingkungan militer, dengan fokus pada aplikasi dan teknologi terkini.
2. Digital Forensik dan ISO 27037: Mengulas prinsip-prinsip digital forensik dan standar ISO 27037 sebagai dasar metode analisis keamanan.

Metodologi Penelitian:

1. Desain Penelitian: Menjelaskan rancangan penelitian yang digunakan untuk menganalisis keamanan aplikasi dan ponsel hybrid.
2. Pendekatan Digital Forensik: Mendetailkan langkah-langkah implementasi pendekatan digital forensik berbasis SNI ISO 27037 dalam proses analisis.
3. Alat dan Teknik: Mengidentifikasi alat dan teknik digital forensik yang digunakan dalam pengumpulan data dan identifikasi kerentanan.

Pembahasan dan Hasil:

1. Akuisisi Data: Menyajikan hasil akuisisi data dari ponsel Motorola LEX L11a dan artefak digital yang ditemukan.
2. Analisis Keamanan: Membahas temuan dan analisis keamanan aplikasi WAVE Mobile Communicator berdasarkan data yang berhasil dikumpulkan.
3. Keterbatasan dan Kendala: Menyajikan keterbatasan penelitian, seperti kendala teknis dan potensi faktor lain yang mempengaruhi hasil.

Kesimpulan dan Saran:

1. Kesimpulan: Merangkum temuan penelitian dan jawaban terhadap rumusan masalah.
2. Saran: Memberikan saran untuk pengembangan lebih lanjut, termasuk langkah-langkah untuk memperkuat keamanan aplikasi dan ponsel hybrid dalam konteks keamanan komunikasi militer.

BAB 2

Tinjauan Pustaka

2.1 Permasalahan Umum

Dalam konteks keamanan komunikasi militer, analisis aplikasi WAVE Mobile Communicator yang digunakan pada ponsel hybrid dan konvensional menjadi sangat penting. Aplikasi ini tidak hanya menjadi sarana utama pertukaran informasi di antara personel Tenta ra Nasional Indonesia (TNI) dan Kepolisian Republik Indonesia (POLRI), tetapi juga memiliki implikasi langsung terhadap keberhasilan misi dan keselamatan personel. Oleh karena itu, pemahaman yang mendalam tentang keamanan aplikasi ini di kedua jenis perangkat menjadi krusial untuk memastikan kerahasiaan dan integritas informasi yang dipertukarkan. Perbandingan keamanan aplikasi WAVE antara ponsel hybrid dan konvensional menyoroti pentingnya memahami perbedaan dalam implementasi keamanan antara kedua jenis perangkat tersebut. Analisis harus mempertimbangkan faktor-faktor seperti tingkat enkripsi, keamanan jaringan, dan potensi kerentanan yang mungkin ada dalam setiap jenis perangkat. Dengan demikian, penelitian ini dapat memberikan wawasan yang lebih mendalam tentang kelemahan dan kelebihan keamanan masing-masing jenis perangkat.

Selain itu, analisis aplikasi WAVE pada ponsel hybrid dan konvensional dapat membantu mengidentifikasi titik lemah dalam keamanan komunikasi militer. Dengan mengeksplorasi perbedaan keamanan antara kedua jenis perangkat, penelitian ini dapat membantu dalam pengembangan strategi mitigasi risiko yang lebih efektif. Hal ini memungkinkan TNI dan POLRI untuk mengambil langkah-langkah proaktif dalam meningkatkan keamanan komunikasi mereka. Pentingnya analisis ini juga tercermin dalam upaya untuk memahami implikasi keamanan aplikasi terhadap penggunaan ponsel hybrid dan konvensional dalam operasi militer dan kepolisian. Dengan mengevaluasi potensi risiko dan keuntungan dari setiap jenis perangkat, penelitian ini dapat memberikan dasar yang kuat untuk pengambilan keputusan yang lebih baik dalam hal penggunaan teknologi oleh personel militer dan kepolisian.

Selain itu, penelitian ini juga akan memberikan pandangan yang lebih luas tentang evolusi keamanan komunikasi militer dan kepolisian dalam menghadapi ancaman siber yang terus berkembang. Dengan memahami perbedaan dalam keamanan aplikasi WAVE pada ponsel hybrid dan konvensional, penelitian ini dapat membantu mengidentifikasi tren

keamanan yang mungkin berkembang di masa depan dan memberikan panduan untuk pengembangan teknologi keamanan yang lebih baik. Dalam kerangka tujuan penelitian ini, penting untuk menekankan pentingnya analisis aplikasi WAVE Mobile Communicator dalam konteks keamanan komunikasi militer dan kepolisian. Dengan pemahaman yang lebih baik tentang kelemahan dan kekuatan keamanan aplikasi ini pada kedua jenis perangkat, TNI dan POLRI dapat meningkatkan efektivitas operasional mereka sambil meminimalkan risiko keamanan.

Terakhir, penelitian ini juga dapat memberikan kontribusi yang signifikan terhadap pengembangan kebijakan keamanan komunikasi di lingkungan militer dan kepolisian. Dengan menyediakan data yang komprehensif tentang perbedaan keamanan aplikasi WAVE pada ponsel hybrid dan konvensional, penelitian ini dapat membantu dalam merumuskan pedoman dan standar keamanan yang lebih baik untuk digunakan oleh personel TNI dan POLRI. Dengan demikian, analisis keamanan aplikasi WAVE pada ponsel hybrid dan konvensional bukan hanya menjadi tugas yang penting, tetapi juga menjadi langkah yang krusial dalam memastikan keberhasilan operasi militer dan kepolisian di era digital ini.

2.2 Penelitian sejenis

Pada bagian ini akan diulas tentang penelitian terkait penelitian yang telah dilakukan sebelumnya dengan topik analisa hasil akuisisi pada perangkat mobile maupun analisa hasil akuisisi pada aplikasi komunikasi yang ada dalam perangkat mobile tersebut.

Pada penelitian yang berjudul "Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan WhatsApp" yang lakukan oleh (Wirara, 2020) melakukan akuisisi pada aplikasi WhatsApp tanpa melakukan jailbreak. Hasilnya didapatkan file imaging database yang kemudian dianalisa lebih lanjut. Pada database tersebut didapat file gambar, teks, voice. Namun pada penelitian ini belum bisa didapatkan hasil recovery dari pesan yang terhapus.

Penelitian selanjutnya dengan judul "Identification of digital evidence facebook messenger on mobile phone with national institute of standards technology (NIST) method" . (Yudhana., 2018) memberikan gambaran bahwa akuisisi facebook messenger lebih optimal menggunakan oxygen dibandingkan menggunakan magnet axiom. Penelitian ini berhasil mendapatkan jumlah chat yang dihapus namun penelitian ini tidak dilanjutkan sampai dengan menganalisa pesan yang terhapus.

Selanjutnya pada dua penelitian selanjutnya menggunakan metode yang sama. Pada penelitian berjudul "Akuisisi Data Pada Skype Messenger Menggunakan Metode National Institute

Of Justice." (Setyawan, 2019)memberikan gambaran akuisisi dengan 2 perangkat berbeda yaitu dengan hp Evercross B75 dan Samsung J2. Didapatkan dua hasil yang berbeda. Pada Evercross B75 kita didapatkan 48% data sementara pada Samsung J2 didapatkan 100% data. Namun pada penelitian ini tidak dijelaskan faktor apa saja yang bisa mempengaruhi hal tersebut, disamping itu dalam mengambil data ponsel tidak dalam keadaan root. Berbeda dengan penelitian yang dilakukan oleh Riyadi dengan judul "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice". (Riyadi,2018).Pengambilan data pada perangkat tersebut dalam keadaan root.

Tabel 2.1 Penelitian Sejenis

No	Judul	Metode	Masalah	Kontribusi
1.	"Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan WhatsApp" (Wirara 2020)	Metode yang digunakan dalam penelitian ini adalah analisa hasil akuisisi aplikasi Whatsapp tanpa menggunakan jailbreak	Whatsapp merupakan aplikasi komunikasi yang lumrah digunakan orang sehingga beberapa kasus, aplikasi ini digunakan sebagai barang bukti. Oleh karena itu diperlukan analisa lebih lanjut terhadap hasil akuisisi untuk dijadikan sebagai barang bukti kejahatan.	Memberikan gambaran bahwa untuk mendapatkan data log yang ada di whatsapp tidak perlu mendapatkan akses khusus(dengan cara jailbreak)
2.	Identification of digital evidence facebook messenger on mobile phone with national institute of standards technology (NIST) method. (Yudhana 2018)	Metode yang digunakan adalah NIST (National Institute of Standart Technology)menggunakan Magnet Axiom dan Oxygen.	Facebook Messenger banyak digunakan sebagai sarana kejahatan. Oleh karenanya dibutuhkan data dari akuisisi facebook messenger untuk dijadikan alat bukti dipersidangan.	Memberikan gambaran bahwa akuisisi facebook messenger lebih optimal menggunakan magnet axiom dibandingkan dengan oxygen.
3.	Akuisisi Bukti Digital pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice. (Riyadi 2019)	Metode yang digunakan dalam penelitian ini adalah NIJ (National Institute of justice)dengan tahapan identification, collection, Examination, Analysis dan reporting.	tingginya pengguna instagram menjadikan peluang untuk tindak kejahatan *cyber bullying*. sehingga perlu didapatkan data ponsel untuk mengumpulkan bukti kejahatan.	akuisisi dilakukan dalam kondisi root.
4.	Akuisisi Data Pada Skype Messenger Menggunakan Metode National Institute Of	Metode yang digunakan dalam penelitian ini adalah NIJ (National Institute of justice)dengan	Tingginya pengguna aplikasi skype yang disalahgunakan sehingga dijadikan sarana untuk melakukan tindak kejahatan.	Penelitian ini diberikan gambaran akuisisi dengan 2 perangkat berbeda yaitu dengan hp Evercross 75 dan Samsung J2.

	Justice. (Setyawan 2018)	tahapan identification, collection, Examination, Analysis dan reporting.	Penelitian ini melakukan pengambilan data dengan simulasi kasus pada 2 hp berbeda.	Didapatkan dua hasil yang berbeda. Dari Evercross B75 kita didapatkan 48% data sementara pada Samsung J2 didapatkan 100% data. Namun pada penelitian ini tidak ijelaskan mengapa bisa demikian.
5.	Makalah ini memberikan gambaran fitur dan konsep sistem komunikasi nirkabel generasi kelima(5G),dengan f okus pada pemanfaatan pita frekuensi gelombang milimeter(mmWav e).	Pendekatan dan metode yang digunakan dalam memahami parameter propagasi, seperti probabilitas line-of-sight (LOS)	Paper mencoba memecahkan beberapa masalah krusial dalam implementasi jaringan 5G pada frekuensi mmWave. Hal ini mencakup pemahaman mendalam terkait probabilitas LOS, kehilangan jalur, dan kehilangan penetrasi bangunan. Oleh karena itu, penekanan pada masalah propagasi mmWave dan pemodelan saluran menjadi sorotan utama yang ingin diatasi oleh banyak badan standardisasi internasional.	Kontribusi utama dari makalah ini adalah memberikan gambaran yang komprehensif tentang konsep dan fitur Jaringan 5G Khususnya di pita frekuensi mmWave. Selain itu, paper ini menyajikan kontribusi signifikan dalam upaya pemodelan saluran, menghubungkan parameter propagasi dengan rentang frekuensi 0,5-100 GHz. Perbandingan antara berbagai badan standardisasi memberikan pemahaman yang kaya akan tantangan dan solusi dalam menghadapi masalah propagasi mmWave.
6.	Paper berjudul "Hybrid communication for Sustaining Health Social Enterprises during Covid-19 pandemi" menghadirkan Perspektif yang mendalam mengenai pendekatan komunikasi hibrida dalam konteks organisasi kewirausahaan dibidang	Permasalahan yang diangkat dalam penelitian ini sangat kontekstual dengan kondisi pandemi global Covid-19. Penelitian fokus pada bagaimana pendekatan komunikasi hibrida dapat menjadi solusi bagi organisasi kewirausahaan dibidang kesehatan dan kemanusiaan	Permasalahan yang diangkat dalam penelitian ini sangat kontekstual dengan kondisi pandemi global Covid-19. Penelitian fokus pada bagaimana pendekatan komunikasi hibrida dapat menjadi solusi bagi organisasi kewirausahaan di bidang kesehatan dan kemanusiaan dalam menghadapi tantangan yang muncul selama pandemi. Dengan merinci permasalahan ini, penelitian	Kontribusi Utama dari penelitian ini terletak pada pemahaman baru terkait dengan penerapan pendekatan komunikasi hibrida. Terlebih lagi, penelitian ini memberikan pandangan yang lebih luas tentang keberlanjutan kewirausahaan sosial di sektor kesehatan Selama masa pandemi. Dengan membawa

	kesehatan dan kemanusiaan. Meskipun istilah "hibrida"bukanlah konsep baru, penulis Memberikan pendekatan yang segar dan relevan dengan merinci penerapannya dalam mengatasi tantangan yang muncul selama pandemi Covid-19. Ulasan kritisnya mencerminkan ketajaman analisis terhadap keunikan dan kepentingan Topik ini, menambahkan pemahaman yang mendalam tentang dampak endekatan hibrida pada keberlanjutan kewirausahaan sosial di sektor kesehatan.	dalam Menghadapi tantangan yang muncul selama pandemi. Dengan merinci permasalahan ini, penelitian memberikan sumbangan konseptual dan praktisdalam upaya menjaga beberlanjutan operasional Organisasi ditengah ketidakpastian dan perubahan lingkungan ksternal yang cepat.	memberikan sumbangan konseptual dan praktis dalam upaya menjaga keberlanjutan operasional organisasi di tengah ketidakpastian dan perubahan lingkungan eksternal yang cepat.	Manfaat dalam mengatasi permasalahan yang muncul selama pandemi, terutama dalam hal fleksibilitas dan kelincahan, penelitian ini menawarkan solusi praktis dengan merinci penggunaan pendekatan Hibrida untuk meningkatkan konektivitas, pertukaran informasi, berbagi pengetahuan, dan harmonisasi hubungan kerja kewirausahaan sosial di bidang kesehatan.
7.	Paper yang berjudui Hybrid Communication for Sustaining Health Social Enterprises During Covid-19 Pandemi m emberikan gambaran luas tentang radio wave,hp dan sistem komunikasi nirkabel, dengan fokus pada pemanfaatan gelombang milimeter. Secara keseluruhan,paper menyajikan informasi yang mendalam	Penjelasan tentang metode dalam paper ini tidak secara eksplisit diuraikan. Paper cenderung lebih bersifat deskriptif dan edukatif, menjelaskan konsep dasar gelombang radio, modulasi, dan aplikasi mobile phone. Meskipun demikian, penulis menggunakan pendekatan kualitatif eksploratif untuk menjelaskan penerapan pendekatan komunikasi	Paper ini tidak menyoroti permasalahan tertentu atau gap pengetahuan yang dihadapi dalam penelitian ini. Kendati memberikan informasi yang luas, paper tidak secara tegas menyajikan pertanyaan penelitian atau permasalahan tertentu yang ingin dipecahkan, yang dapat memberikan arah dan fokus yang lebih jelas pada tulisan ini.	Kontribusi utama paper ini adalah memberikan pemahaman mendalam tentang radio wave, mobile phone, dan aplikasi komunikasi nirkabel. Selain itu, paper memberikan gambaran tentang perkembangan teknologi mobile phone dari segi penggunaan frekuensi radio, metode modulasi, hingga aplikasi yang populer. Meskipun demikian, paper kurang menekankan dampak atau implikasi dari perkembangan ini

	tentang konsep dasar radio wave, peranannya dalam komunikasi, dan perkembangan teknologi mobile phone.Namun, fokus utama terletak pada radio wave dan kurang membahas aspek teknismobile phone secara mendalam.	hibrida dalam konteks kewirausahan sosial di bidang kesehatan selama pandemi Covid-19.		dalam konteks sosial, ekonomi, atau budaya. Sebuah Analisis lebih mendalam tentang dampak teknologi ini mungkin dapat menambah nilai pada tulisan ini.

Makalah berjudul "Overview of Millimeter Wave Communications for Fifth-Generation (5G) Wireless Networks - with a focus on Propagation Models" memberikan gambaran komprehensif tentang evolusi sistem komunikasi nirkabel generasi kelima (5G) dengan penekanan pada pita frekuensi gelombang milimeter (mmWave). Dalam ulasan kritisnya, paper ini secara detail membahas hasil awal dan konsep utama yang menjadi landasan pengembangan jaringan 5G. Melibatkan banyak kelompok internasional, metode pemodelan saluran untuk aplikasi berlisensi dan tidak berlisensi dijelaskan dengan rinci, membuka wawasan mendalam terhadap parameter propagasi seperti probabilitas line-of-sight (LOS), kehilangan jalur skala besar, dan kehilangan penetrasi bangunan dalam rentang frekuensi 0,5-100 GHz. Melalui fokusnya pada pemodelan propagasi mmWave, paper ini mencoba memecahkan masalah krusial dalam implementasi jaringan 5G, menjadikannya kontribusi penting dalam upaya pemahaman dan pengembangan teknologi komunikasi nirkabel masa depan.

Paper berjudul "Hybrid Communication for Sustaining Health Social Enterprises During Covid-19 Pandemi" menghadirkan perspektif mendalam mengenai penerapan pendekatan komunikasi hibrida dalam konteks organisasi kewirausahaan di bidang kesehatan dan kemanusiaan. Dalam menjawab pertanyaan penelitian, penelitian ini menggunakan metode kualitatif eksploratif yang memungkinkan peneliti untuk merinci penggunaan pendekatan komunikasi hibrida oleh institusi dengan kecermatan analisis yang tinggi. Kontekstual dengan kondisi pandemi global, penelitian ini menyoroti permasalahan aktual organisasi selama pandemi dan fokus pada bagaimana pendekatan komunikasi hibrida dapat menjadi solusi dalam menjaga keberlanjutan kewirausahaan sosial di sektor kesehatan. Kontribusi utamanya terletak pada pemahaman baru terkait penerapan pendekatan

komunikasi hibrida dan pandangan yang lebih luas tentang keberlanjutan kewirausahaan sosial di sektor kesehatan selama masa pandemi, memberikan solusi praktis

yang signifikan bagi organisasi untuk meningkatkan konektivitas, pertukaran informasi, berbagi pengetahuan, dan harmonisasi hubungan kerja.

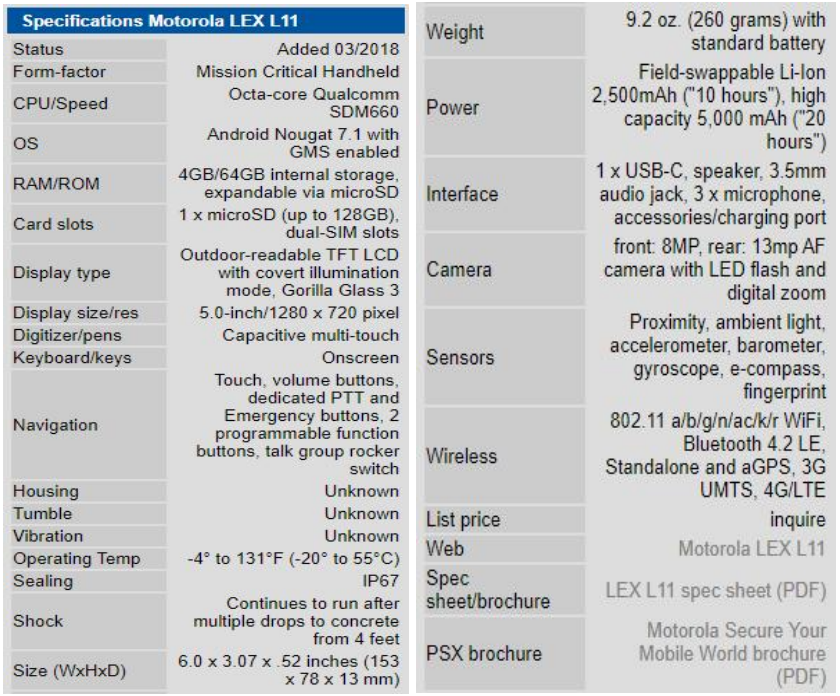
Paper berjudul "Radio wave communication system and mobile phone" memberikan gambaran menyeluruh tentang gelombang radio dan pemanfaatannya dalam komunikasi nirkabel, khususnya pada teknologi mobile phone. Dengan membahas dasar-dasar gelombang radio, metode modulasi, dan aplikasi mobile phone, paper ini menguraikan bagaimana radio wave digunakan dalam komunikasi, baik yang terjadi secara alami maupun yang dihasilkan secara buatan. Meskipun memberikan penjelasan yang komprehensif tentang bagaimana mobile phone mengoperasikan komunikasinya melalui gelombang radio, paper cenderung bersifat deskriptif dan kurang menyoroti aspek metode penelitian atau pertanyaan penelitian tertentu. Meski begitu, papernya memberikan pemahaman yang baik tentang peran gelombang radio dalam perkembangan teknologi komunikasi nirkabel.Dari beberapa penelitian terdahulu banyak yang meneliti mengenai akuisisi aplikasi pada perangkat hp android dan hasil yang ditemukan cukup beragam. Namun belum ada yang meneliti terkait aplikasi wave mobile communicator yang biasa yang terpasang pada hp hybrid, khususnya hp Motorola Lex 11.

2.3 Motorola LEX L11a

Gambar 2.1 Device Motorola LEX L11a
(sumber : www.motorolasolutions.com)

Motorola LEX 11 adalah perangkat komunikasi canggih yang dirancang khusus untuk mendukung tugas dan kebutuhan komunikasi pihak penegak hukum dan keamanan, seperti petugas polisi, penegak hukum, dan petugas keamanan (Riadi et al., 2018). Perangkat ini merupakan salah satu produk dari Motorola Solutions, yang telah lama dikenal sebagai pemimpin dalam industri komunikasi profesional.

Berikut adalah gambar dari spesifikasi Ponsel Motorola LEX 11 :



Specifications Motorola LEX L11	
Status	Added 03/2018
Form-factor	Mission Critical Handheld
CPU/Speed	Octa-core Qualcomm SDM660
OS	Android Nougat 7.1 with GMS enabled
RAM/ROM	4GB/64GB internal storage, expandable via microSD
Card slots	1 x microSD (up to 128GB), dual-SIM slots
Display type	Outdoor-readable TFT LCD with covert illumination mode, Gorilla Glass 3
Display size/res	5.0-inch/1280 x 720 pixel
Digitizer/pens	Capacitive multi-touch
Keyboard/keys	Onscreen
Navigation	Touch, volume buttons, dedicated PTT and Emergency buttons, 2 programmable function buttons, talk group rocker switch
Housing	Unknown
Tumble	Unknown
Vibration	Unknown
Operating Temp	-4° to 131°F (-20° to 55°C)
Sealing	IP67
Shock	Continues to run after multiple drops to concrete from 4 feet
Size (WxHxD)	6.0 x 3.07 x .52 inches (153 x 78 x 13 mm)
Weight	9.2 oz. (260 grams) with standard battery
Power	Field-swappable Li-Ion 2,500mAh ("10 hours"), high capacity 5,000 mAh ("20 hours")
Interface	1 x USB-C, speaker, 3.5mm audio jack, 3 x microphone, accessories/charging port
Camera	front: 8MP, rear: 13mp AF camera with LED flash and digital zoom
Sensors	Proximity, ambient light, accelerometer, barometer, gyroscope, e-compass, fingerprint
Wireless	802.11 a/b/g/n/ac/k/r WiFi, Bluetooth 4.2 LE, Standalone and aGPS, 3G UMTS, 4G/LTE
List price	inquire
Web	Motorola LEX L11
Spec sheet/brochure	LEX L11 spec sheet (PDF)
PSX brochure	Motorola Secure Your Mobile World brochure (PDF)

Gambar 2.2 Spesifikasi Ponsel Motorola LEX 11

(sumber : www.motorolasolutions.com)

Motorola LEX 11 dirancang dengan fitur-fitur khusus untuk memenuhi kebutuhan dan tuntutan operasional pihak penegak hukum dan keamanan. Perangkat ini dilengkapi dengan teknologi komunikasi tingkat tinggi, termasuk jaringan LTE dan fitur Push-to-Talk (PTT) yang memungkinkan pengguna berkomunikasi secara instan dan efisien. Dengan menggunakan teknologi broadband, LEX 11 juga mendukung transfer data yang cepat dan handal, memberikan akses real-time ke informasi penting yang dibutuhkan dalam tugas-tugas penegakan hukum (Haryadi & Supriyono, 2017).

Fitur keselamatan dan keamanan menjadi fokus utama dalam desain Motorola LEX 11. Perangkat ini dilengkapi dengan tombol darurat yang dapat dengan cepat memicu panggilan darurat ke pusat komando, memberikan akses cepat ke bantuan dalam situasi darurat atau bahaya. Selain itu, LEX 11 juga dilengkapi dengan fitur geolokasi dan pelacakan GPS yang memungkinkan pemantauan posisi petugas di lapangan, memastikan keamanan mereka dan memfasilitasi tindakan penanggulangan yang cepat dan tepat.

Daya tahan dan ketahanan adalah hal lain yang diperhatikan dalam perangkat ini. Motorola LEX 11 dirancang untuk tahan terhadap kondisi lingkungan yang ekstrem dan sesuai dengan standar MIL-STD-810G (Riadi, 2021). Ini berarti perangkat ini tahan terhadap guncangan, goncangan, kelembaban, dan suhu ekstrem, menjadikannya cocok untuk

digunakan dalam berbagai situasi dan lingkungan, termasuk operasi di lapangan yang keras. Desain Motorola LEX 11 juga memperhatikan kenyamanan dan kepraktisan bagi pengguna. Perangkat ini memiliki bodi yang ringkas dan ergonomis, sehingga mudah dipegang dan dioperasikan oleh petugas yang sedang berada di lapangan. Layarnya yang cukup besar dan intuitif memungkinkan pengguna untuk melihat informasi dengan jelas dan cepat beradaptasi dengan antarmuka yang mudah digunakan.

Motorola LEX 11 juga menyediakan konektivitas yang luas dan fleksibel. Selain menggunakan jaringan broadband, perangkat ini juga mendukung konektivitas Wifi dan Bluetooth, memungkinkan integrasi dengan perangkat lain seperti headset, printer, atau alat elektronik lainnya. Konektivitas yang luas ini memberikan fleksibilitas tambahan dalam berkomunikasi dan bekerja di lapangan.

Dalam dunia yang semakin terhubung dan kompleks, Motorola LEX 11 menjadi alat komunikasi yang kuat dan andal bagi pihak penegak hukum dan keamanan. Dengan fitur-fitur khusus yang menekankan keamanan, daya tahan, dan kenyamanan, perangkat ini dapat memastikan pengguna dapat berkomunikasi dengan efisien, merespons situasi darurat dengan cepat, dan menjalankan tugas-tugas penegakan hukum dengan lebih efektif. Sebagai salah satu solusi komunikasi terdepan dari Motorola Solutions, LEX 11 menjadi alat yang tak ternilai dalam meningkatkan produktivitas dan keselamatan para petugas di lapangan.

2.4 Xiaomi Redmi Note 8

Produk Xiaomi menjadi salah satu ponsel konvensional yang telah banyak digunakan dan diperjual belikan di pasaran, khususnya Xiaomi spesifikasi Redmi Note 8 menjadi smartphone mid-range yang menawarkan spesifikasi cukup mumpuni dengan harga yang terjangkau. Ponsel ini menawarkan spesifikasi yang menarik seperti layar besar, baterai tahan lama, cukup sebagai alat komunikasi hingga penggunaan fitur lainnya. Xiaomi menghadirkan *smartphone* dengan spesifikasi yang lebih tinggi dibandingkan pesaingnya di harga yang sama. seperti penggunaan prosesor flagship, RAM besar, dan baterai tahan lama. Xiaomi juga memberikan dukungan jaringan yang luas, *smartphone* Xiaomi umumnya mendukung berbagai jaringan seluler, sehingga pengguna tidak perlu khawatir dengan masalah kompatibilitas.

Ponsel Konvensional seperti pada Xiaomi Redmi Note 8 dapat memberikan berbagai fitur yang mendukung untuk digunakan pada bidang militer, tetapi penggunaan Ponsel Konvensional juga memiliki beberapa kerentanan yang perlu dipertimbangkan karena mudahnya perangkat untuk terhubung memungkinkan terjadinya Serangan Cyber seperti

sniffing attack atau pengintaian, terutama pada perangkat yang digunakan sebagai operasional bidang militer menjadi salah satu sasaran pengintaian hingga tindakan untuk menyadap dan menangkap data yang ditransmisikan antara ponsel dan jaringan.

Ancaman lainnya pada Xiaomi Redmi Note 8 adanya BlueBorne hingga Spectre dan Meltdown. BlueBorne menjadi kerentanan keamanan yang ditemukan pada tahun 2017 dan berdampak pada implementasi Bluetooth di berbagai sistem operasi, termasuk Android, iOS**.** BlueBorne berbahaya karena tidak memerlukan interaksi pengguna untuk dieksploitasi. Artinya, pihak yang tidak bertanggungjawab dapat menyusup ke perangkat pengguna melalui Bluetooth tanpa perangkat tersebut dipasangkan (paired) atau bahkan dalam keadaan "discoverable" (dapat dilihat). Kerentanan ini memungkinkan penyerang untuk mencuri data sensitif dari perangkat, seperti kata sandi, nomor kartu kredit, dan foto. Selain BlueBorne kerentanan yang dapat menyerang ponsel konvensional ini adalah Spectre dan Meltdown yang memengaruhi banyak prosesor modern, termasuk Qualcomm Snapdragon 665 yang digunakan pada Xiaomi Redmi Note 8. Kerentanan Spectre dan Meltdown adalah ancaman keamanan serius yang dapat memengaruhi banyak perangkat, termasuk Xiaomi Redmi Note 8. Xiaomi Redmi Note 8 menerima pembaruan keamanan berkala dari Xiaomi, termasuk patch untuk kerentanan Android dan MIUI. Meskipun Xiaomi telah mengeluarkan patch untuk mengatasi kerentanan Spectre dan Meltdown, tidak ada jaminan bahwa patch tersebut akan sepenuhnya melindungi perangkat pengguna dari semua risiko keamanan.

Perangkat konvensional juga sangat bergantung pada jaringan seluler dan internet untuk beroperasi, sedangkan lokasi bidang militer biasanya terletak di pelosok atau tempat yang sulit dijangkau, Jaringan seluler mungkin tidak tersedia di semua wilayah, terutama di medan perang atau daerah terpencil. Gangguan jaringan atau kurangnya akses internet dapat menghambat komunikasi, koordinasi, dan akses informasi penting. Komunikasi melalui jaringan seluler juga dapat disadap oleh pihak yang tidak berwenang dengan berbagai media dan cara seperti membuat jaringan Wifi palsu atau mengalihkan perangkat ke jaringan jahat yang terlihat sah. Saat terhubung ke jaringan ini, penyerang dapat mencegat komunikasi antara smartphone dan internet.

2.5 Wave Mobile Communicator

Gambar 2.3 Aplikasi *WAVE Mobile Communicator*

(sumber : https://www.slideshare.net/GregParker50/wave-oncloud-customerpresentation6717#7)

WAVE Mobile Communicator adalah aplikasi komunikasi inovatif yang dikembangkan oleh Motorola Solutions (Rafique & Khan, 2013). Aplikasi ini dirancang untuk mendukung komunikasi dalam tim dan organisasi dengan memungkinkan pengguna untuk berkomunikasi secara instan melalui berbagai platform, termasuk perangkat seluler, radio dua arah, dan komputer. *WAVE Mobile Communicator* memungkinkan pengguna untuk berkomunikasi lintas platform, yang memfasilitasi integrasi dan kolaborasi yang efisien antara perangkat seluler, radio dua arah, dan komputer. Pengguna dapat berkomunikasi dengan mudah melalui aplikasi ini tanpa harus beralih antara berbagai perangkat. Fitur lintas platform ini meningkatkan efisiensi dan mengurangi gangguan dalam komunikasi tim.

Aplikasi ini mendukung layanan Push-to-Talk (PTT) yang canggih, yang memungkinkan komunikasi instan seperti walkie-talkie melalui perangkat seluler dan komputer. Pengguna dapat mengakses saluran PTT atau grup dengan cepat dan berbicara secara real-time, serupa dengan komunikasi radio dua arah. Dengan PTT yang didukung oleh aplikasi, pengguna dapat berkomunikasi dengan lebih fleksibel tanpa bergantung pada perangkat khusus. WAVE Mobile Communicator menawarkan komunikasi suara berkualitas tinggi, yang memastikan pesan yang disampaikan jelas dan mudah dipahami oleh seluruh tim. Kualitas suara yang baik penting dalam situasi darurat dan operasi lapangan, di mana informasi yang tepat dan cepat harus tersampaikan tanpa gangguan.

Keamanan adalah fokus utama dari WAVE Mobile Communicator (Sirojjam et al., 2021). Aplikasi ini menyediakan enkripsi yang kuat untuk melindungi percakapan dan data

yang sensitif. Pengguna dapat dengan tenang berkomunikasi tanpa khawatir informasi yang mereka berikan akan jatuh ke tangan yang salah. WAVE Mobile Communicator memiliki antarmuka yang intuitif dan mudah digunakan. Pengguna dapat dengan cepat beradaptasi dengan aplikasi dan mengakses fungsi-fungsi kunci dengan mudah. Kemudahan penggunaan ini penting dalam situasi di mana respons cepat diperlukan, sehingga pengguna dapat fokus pada tugas utama mereka tanpa harus menghadapi kendala teknis. Aplikasi ini juga mendukung berbagai perangkat seluler, termasuk Android dan iOS, serta komputer dengan sistem operasi Windows atau Mac OS. Fleksibilitas ini memungkinkan pengguna untuk berkomunikasi dengan perangkat yang paling sesuai dengan kebutuhan mereka dan memastikan kolaborasi yang optimal dalam tim atau organisasi.

2.6 Akuisisi Digital Forensik

Digital Forensic Acquisition, atau akuisisi forensik digital, adalah proses pengumpulan dan perolehan data elektronik dari berbagai perangkat dan media digital. Proses ini merupakan langkah awal dalam investigasi forensik digital, di mana data diambil untuk tujuan analisis dan penyelidikan terhadap aktivitas yang mencurigakan atau kejahatan yang terjadi di dunia digital. Digital Forensic Acquisition berfokus pada pengumpulan data dari berbagai perangkat dan media digital, termasuk komputer, laptop, smartphone, tablet, server, dan media penyimpanan lainnya seperti hard drive eksternal atau USB drive. Proses akuisisi dilakukan dengan hati-hati dan harus mematuhi prinsip integritas, yaitu memastikan bahwa data tidak berubah selama prosesnya untuk memastikan keaslian dan keabsahan hasil analisis nantinya.

Pengambilan data forensik digital dapat dilakukan dengan berbagai metode, termasuk tetapi tidak terbatas pada:

a. Kloning hard drive: Membuat salinan identik dari hard drive yang menjadi target akuisisi untuk menghindari kerusakan atau perubahan data asli.
b. Image File: Membuat file gambar (image file) dari media digital, seperti hard drive atau memori, yang kemudian dapat dianalisis tanpa merusak data asli.
c. Network Forensics: Mengumpulkan data dari jaringan atau lalu lintas data untuk mengidentifikasi aktivitas yang mencurigakan atau melacak serangan siber.

Digital Forensic Acquisition dilakukan oleh para ahli forensik digital yang memiliki pengetahuan mendalam tentang teknik dan metodologi pengumpulan data yang akurat dan sah secara hukum (Hariyadi, Dedy;Yunia Pasa, 2018). Mereka juga harus memahami berbagai perangkat keras dan perangkat lunak, serta memahami tentang berbagai sistem operasi dan

platform yang berbeda. Salah satu tantangan dalam Digital Forensic Acquisition adalah adanya enkripsi dan perlindungan data yang semakin ketat di berbagai perangkat dan sistem. Ahli forensik digital harus memiliki kemampuan untuk mengatasi perlindungan ini dan dapat mengakses data yang terenkripsi untuk analisis lebih lanjut. Keakuratan dan keabsahan hasil akuisisi sangat penting dalam proses investigasi forensik digital. Karena itu, selama proses akuisisi, harus ada dokumentasi yang akurat dan lengkap tentang langkah-langkah yang diambil, alat yang digunakan, dan bagaimana data diambil. Hal ini penting dalam kasus hukum dan persidangan untuk memastikan bukti yang diperoleh dianggap sah dan dapat diterima sebagai bukti yang kuat di pengadilan. Dalam era dimana teknologi semakin maju dan data elektronik semakin berlimpah, Digital Forensic Acquisition menjadi kunci dalam mengungkap kebenaran di dunia digital dan mengejar pelaku kejahatan digital. Dengan penggunaan metodologi yang tepat, alat yang canggih, dan pemahaman mendalam tentang teknologi, ahli forensik digital dapat secara akurat mengumpulkan dan menganalisis data elektronik untuk mengungkap kebenaran dan menghadirkan bukti yang sah dalam proses peradilan.

2.7. ISO 27037:2014

ISO 27037 adalah suatu standart internasional yang menjadi landasan yang kritis dalam pengaturan proses akuisisi data forensik digital. Standar ini fokus kepada penanganan barang bukti digital, khususnya pada klausul 7.1.3, yaitu mengenai akuisisi data langsung dari sistem yang berjalan atau live forensic.

Proses akuisisi live forensic merupakan teknik forensik yang dilakukan pada sistem yang sedang berjalan, memanfaatkan sumber daya langsung tanpa menghentikan operasi sistem atau perangkat lunak. Klausul 7.1.3 ISO 27037 memberikan dasar untuk proses ini dan menekankan pentingnya memastikan data yang diakuisisi dapat diandalkan dan sesuai dengan kebutuhan investigasi.

Dalam konteks penelitian keamanan aplikasi WAVE Mobile Communicator pada ponsel hybrid Motorola LEX L11a, akuisisi live forensic menjadi krusial. Proses ini memungkinkan analisis langsung terhadap data dan artefak aplikasi tersebut. ISO 27037 memberikan kerangka kerja yang relevan untuk memastikan keamanan dalam akuisisi data, terutama ketika berhadapan dengan aplikasi yang memiliki tingkat keamanan tinggi.

Klausul 7.1.3 ISO 27037 merinci langkah-langkah proses akuisisi yang harus diikuti, mulai dari perencanaan hingga identifikasi sumber daya dan penerapan metode yang sesuai. Dalam penelitian ini, langkah-langkah ini diaplikasikan pada ponsel hybrid Motorola LEX

L11a untuk memastikan keamanan komunikasi melalui aplikasi WAVE Mobile Communicator.

Penggunaan ponsel Motorola LEX L11a oleh Tentara Nasional Indonesia (TNI) menambah dimensi kepentingan keberlanjutan operasi militer dan keamanan nasional. Klausul 7.1.3 ISO 27037 menjadi kunci dalam memastikan akuisisi data dilakukan tanpa menghentikan operasi ponsel, sangat relevan dalam konteks pertukaran informasi strategis melalui WAVE Mobile Communicator.

Penelitian ini mencakup penerapan klausul 7.1.3 ISO 27037 sebagai bagian integral dari metodologi akuisisi live forensic. Langkah-langkah melibatkan identifikasi artefak digital, pemantauan data lalu lintas, dan akuisisi langsung dari sistem yang berjalan. Penerapan standar ini memberikan dasar yang kokoh untuk analisis keamanan aplikasi WAVE Mobile Communicator pada ponsel Motorola LEX L11a.

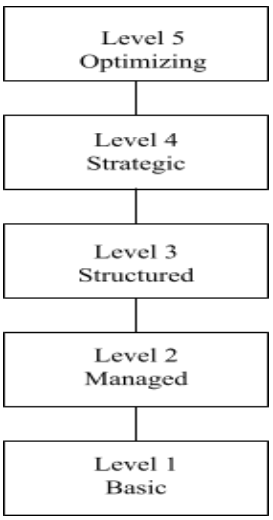
2.8. Live Akuisisi Digital Forensik

Proses Akuisisi yang dilakukan pada penelitian ini bertujuan untuk mendapatkan salinan data yang lengkap dan akurat dari perangkat Hybrid maupun Konvensional yang menyala, untuk menjaga integritas data dan memastikan admissibility-nya dalam proses investigasi. Proses akuisisi mengacu pada Klausul 7.1.3 dari SNI ISO 27037:2014, berjudul "Akuisisi dan Analisis Data Forensik", pada klausul tersebut menetapkan persyaratan untuk memastikan proses akuisisi dan analisis data forensik yang aman, terpercaya, dan teraudit.

Live akuisisi memiliki keunggulan signifikan dibandingkan metode forensik yang melibatkan pengambilan data dari perangkat statis, metode Live Akuisisi mengambil data volatile yang dapat menangkap aktivitas jaringan secara realtime, menangkap isi memori volatile yang menyimpan data yang tidak disimpan di hard drive. Proses Live akuisisi juga meminimalkan gangguan dengan dapat mengumpulkan bukti tanpa mematikan sistem, dan mencegah kehilangan data yang mungkin terjadi saat sistem mati. Proses Live Akuisisi juga dapat meningkatkan kemampuan investigasi karena pengumpulan bukti yang komprehensif dan tepat waktu.

Prosedur Live Akuisisi yang dijalankan dengan serangkaian proses dari membuat prosedur tertulis yang mencakup langkah seperti identifikasi dan klasifikasi data forensik yang relevan, pemilihan metode Live Akuisisi atau *tools* seperti Mobiledit dan Cellebrite UFED yang dipilih pada penelitian ini dan akan membantu proses akuisisi, hasil akuisisi akan didokumentasikan untuk dapat dilakukan analisis terhadap data yang diakuisisi. Prosedur Live Akuisisi juga meliputi penanganan dan penyimpanan data forensik yang aman.

2.9. Tingkat keamanan pada perangkat mobile



Gambar 2.4. Level keamanan mobile

(sumber : https://integracon.com/5-levels-of-mobile-security/)

Level Keamanan pada perangkat mobile mengacu pada tingkatan perlindungan yang diterapkan untuk melindungi perangkat mobile dari berbagai ancaman dan risiko keamanan. Seperti yang digambarkan pada gambar 2.4. menurut Gartner (integracon, 2016), level keamanan pada perangkat mobile terbagi menjadi 5, yaitu :

1. Level 1 atau level dasar. Pada level ini perangkat mobile memiliki keamanan yang sangat terbatas yang dilakukan oleh pengguna perangkat seperti penggunaan pin atau pola sebagai penguncian layar dan tidak ada enkripsi data. Pengamanan pada tingkat ini memiliki resiko keamanan sangat rentan terhadap ancaman seperti pencurian perangkat, akses tidak sah, dan malware sederhana.
2. level 2 atau level managed. Perangkat mobile dikelola dan diawasi dengan pengamanan yang lebih ketat. Kebijakan pengelolaan dan pengawasan lebih sering diterapkan, terutama pada perangkat perusahaan atau organisasi. Pada level ini pengguna melakukan pengamanan dengan pemindaian sidik jari atau wajah. Resiko keamanan level 2 cukup baik, tetapi masih dapat diakses oleh peretas dengan serangan yang lebih canggih jika kebijakan keamanan tidak diterapkan dengan benar.
3. Level 3 atau level terstruktur.Pada level ini, keamanan mobile terdiri dari berbagai lapisan perlindungan. Sistem enkripsi dan pengelolaan risiko sudah diterapkan dengan lebih ketat dan sudah menerapkan enkripsi penuh pada perangkat. pengawasan dan pelaporan aktivitas perangkat sudah terintegrasi. Level ini juga memiliki perlindungan terhadap aplikasi dan data sensitif melalui kebijakan ketat. Risiko keamanan pada level

ini lebih baik, namun masih dapat terpengaruh oleh eksploitasi yang lebih canggih atau serangan phishing.

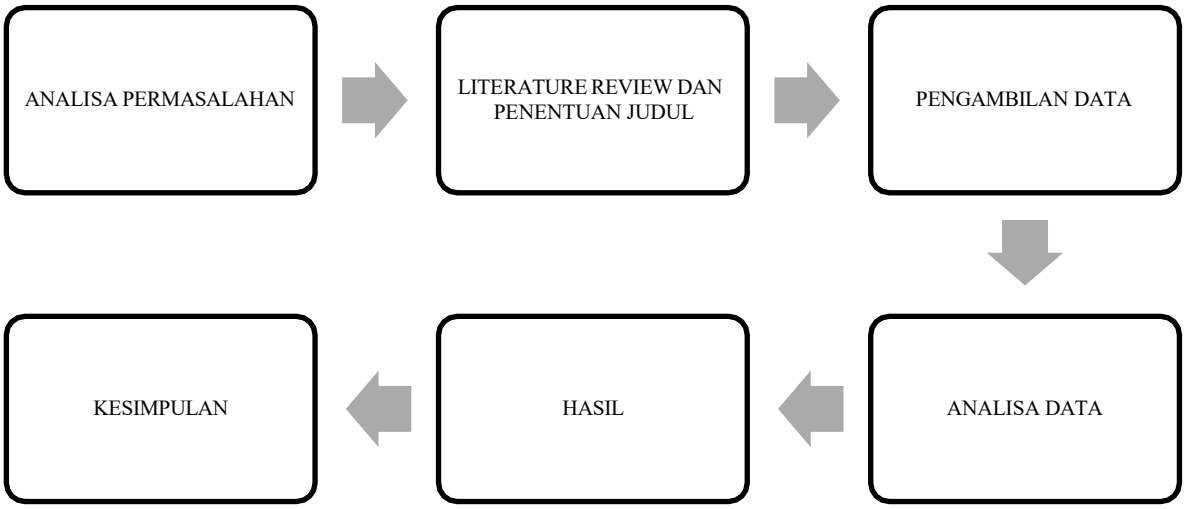
4. Level 4 atau level Strategis. Pada level ini, keamanan perangkat mobile tidak hanya terdiri dari perlindungan perangkat dan aplikasi, tetapi juga mencakup analisis risiko dan kebijakan yang sangat terorganisir untuk menghadapi ancaman yang semakin canggih. Level strategis memiliki perlindungan terhadap data diperangkat dengan enkripsi end-to-end, disamping itu pada level ini Perangkat menggunakan alat untuk mendeteksi dan merespons ancaman secara real-time. Dalam mengakses aplikasi maupun data sensitif, menggunakan otentikasi multifaktor (MFA). Level ini memiliki resiko keamanan sangat baik dan lebih tahan terhadap serangan, tetapi masih ada potensi celah jika kebijakan dan alat tidak diperbarui atau diterapkan dengan benar.
5. Level 5 atau level optimalisasi. Pada level ini, keamanan perangkat mobile dioptimalkan untuk memberikan perlindungan terbaik dan mampu beradaptasi dengan ancaman baru secara proaktif. Organisasi dan individu menerapkan teknologi dan kebijakan terkini untuk memastikan perangkat selalu aman. Optimalisasi keamanan yang terintegrasi dengan otomatisasi dan pemantauan berkelanjutan disertai dengan pembaruan keamanan yang cepat dan proaktif berdasarkan analisis ancaman terbaru. Level ini memiliki perlindungan berlapis, termasuk segmentasi data dan aplikasi untuk mengurangi potensi kerusakan. penggunaan kecerdasan buatan (AI) dan *machine learning* untuk mendeteksi ancaman dengan lebih cepat dan lebih akurat.Tingkat resiko keamanan hampir optimal, tetapi potensi risiko masih ada, terutama terhadap ancaman yang belum diketahui.

BAB 3

Metodologi

3.1. Alur Penelitian

Pembangunan alur kerja merupakan langkah krusial dalam meniti jalan penelitian analisis keamanan aplikasi WAVE Mobile Communicator pada ponsel hybrid Motorola LEX L11a. Dalam fase persiapan, perancangan alur kerja menjadi fondasi yang kokoh untuk menjalankan setiap tahapan penelitian dengan konsistensi dan ketelitian. Alur kerja ini dirancang secara cermat untuk menggambarkan tahapan akuisisi data, analisis digital forensik, hingga pembahasan hasil. Keseluruhan alur kerja ini mencakup pengembangan strategi yang komprehensif untuk memastikan bahwa seluruh aspek penelitian dapat dijalankan secara efektif dan efisien. Secara umum, penelitian ini dibangun dengan alur sebagai berikut:



Gambar 3.1 Alur Penelitian

3.1.1 Analisis Permasalahan

Sebelum menentukan judul penelitian, dilakukan analisis yang mendalam terhadap permasalahan utama yang muncul, yakni keamanan komunikasi melalui aplikasi WAVE Mobile Communicator pada ponsel hybrid Motorola LEX L11a. Perangkat ini adalah perangkat utama yang digunakan oleh TNI dan POLRI. Fokus utama analisis ini adalah pada aspek keamanan informasi dari dua sudut pandang utama, yaitu device Motorola LEX L11a dan aplikasi WAVE Mobile Communicator.

Dari segi perangkat (device), Motorola LEX L11a menjadi subjek utama karena digunakan dalam lingkungan militer oleh TNI dan POLRI. Pada tingkat perangkat, perhatian utama adalah terhadap keamanan fisik dan elektroniknya. Hal ini mencakup perlindungan terhadap akses fisik yang tidak sah ke perangkat, penggunaan teknologi enkripsi untuk

melindungi data yang tersimpan di dalamnya, serta penanganan terhadap risiko keamanan yang dapat muncul dari kerentanan perangkat keras.

Dari segi aplikasi, fokus akan tertuju pada WAVE Mobile Communicator. Pada tingkat aplikasi, analisis keamanan akan mencakup enkripsi komunikasi, validasi pengguna, manajemen otentikasi, dan deteksi potensial kerentanan keamanan pada tingkat perangkat lunak. Selain itu, pemahaman mendalam terhadap bagaimana data dikirim, disimpan, dan diakses oleh aplikasi tersebut akan menjadi fokus untuk memastikan integritas dan kerahasiaan informasi.

Penting untuk mencermati bahwa kedua aspek ini saling terkait dalam ekosistem keamanan informasi secara menyeluruh. Dalam konteks ini, analisis keamanan tidak hanya terbatas pada level perangkat keras dan aplikasi secara terpisah, tetapi juga harus mempertimbangkan cara keduanya berinteraksi untuk menjaga keamanan komunikasi secara efektif.

3.1.2 Literature review dan Menentukan Judul

Langkah pertama dalam mengeksplorasi keamanan informasi dari sisi device dan tools WAVE adalah merinci pendekatan yang spesifik, yang mencakup review literatur dari penelitian sebelumnya. Analisis literatur ini akan membantu dalam memahami metodologi dan temuan yang relevan terkait keamanan perangkat dan aplikasi serupa. Referensi dari penelitian sebelumnya dapat memberikan panduan tentang risiko keamanan yang telah diidentifikasi, teknik forensik yang efektif, dan praktik terbaik yang dapat diterapkan.

Berdasarkan analisis permasalahan, judul penelitian ditetapkan sebagai "Analisa Keamanan Komunikasi Hasil Akuisisi Aplikasi WAVE Mobile Communicator pada Ponsel Hybrid Motorola LEX L11a Dengan Pendekatan Digital Forensik Berbasis ISO 27037." Judul ini mencerminkan fokus pada aspek keamanan, pendekatan digital forensik, dan penerapan standar ISO 27037.

3.1.3 Pengambilan Data.

Pada tahap pengambilan data ini, langkah yang dilakukan adalah mengakuisisi artefak dari aplikasi WAVE dengan menggunakan metode live forensic sesuai standar ISO 27037. Proses ini melibatkan ekstraksi data secara langsung dari perangkat tanpa mengganggu operasionalnya. Artefak yang diakuisisi mencakup data riwayat komunikasi, log aktivitas, dan informasi terkait keamanan yang ada dalam WAVE. Penting untuk memastikan bahwa metode akuisisi yang digunakan sesuai dengan standar ISO 27037, yang memberikan panduan khusus untuk pengumpulan data forensik pada lingkungan digital.

Setelah artefak berhasil diakuisisi, langkah berikutnya adalah mengumpulkan data pendukung yang melibatkan data komunikasi melalui aplikasi WAVE Mobile Communicator pada ponsel Motorola LEX L11a yang digunakan oleh TNI dan POLRI. Data pendukung ini harus mencakup berbagai skenario penggunaan, termasuk pertukaran pesan, panggilan suara, dan jenis komunikasi lainnya yang mungkin terjadi dalam konteks militer. Data yang dihimpun perlu diverifikasi keabsahannya dan dijamin integritasnya agar dapat menjadi dasar yang akurat dan andal untuk analisis keamanan.

Proses ini memerlukan keterlibatan ahli forensik digital yang memiliki pemahaman mendalam tentang standar ISO 27037, metode live forensic, dan keamanan aplikasi seperti WAVE Mobile Communicator. Hasil dari langkah-langkah ini akan membentuk dasar yang kokoh untuk penelitian selanjutnya terkait analisa keamanan komunikasi pada perangkat Motorola LEX L11a dengan fokus pada aplikasi WAVE.

3.1.4 Menganalisis Data

Pada tahap analisis data untuk mendapatkan wawasan yang mendalam terkait keamanan komunikasi melalui aplikasi WAVE Mobile Communicator pada ponsel Motorola LEX L11a yang digunakan oleh TNI dan POLRI.

Pertama, tahap awal analisis data melibatkan eksplorasi terhadap berbagai artefak yang telah dikumpulkan. Ini mencakup pemahaman mendalam terhadap riwayat komunikasi, log aktivitas, dan informasi terkait keamanan yang terdapat dalam dataset. Pada tahap ini, fokus diberikan pada mengidentifikasi pola atau anomali yang mungkin menunjukkan potensi ancaman keamanan.

Kedua, dilakukan klasifikasi dan kategorisasi data untuk menyusun kerangka pemahaman yang terstruktur. Hal ini memungkinkan peneliti untuk mengorganisasi informasi menjadi kelompok-kelompok yang logis dan dapat diinterpretasikan dengan lebih baik. Misalnya, pemisahan data berdasarkan jenis ancaman atau celah keamanan yang teridentifikasi.

Selanjutnya, analisis mendalam terhadap kelemahan keamanan yang mungkin ditemukan pada aplikasi WAVE dan perangkat Motorola LEX L11a. Penggunaan pendekatan digital forensik berbasis SNI ISO 27037 menjadi landasan dalam mengevaluasi tingkat keamanan dan mendeteksi potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang.

Terakhir, hasil analisis data disusun menjadi temuan-temuan yang dapat memberikan wawasan signifikan terkait keamanan komunikasi di lingkungan TNI dan POLRI. Temuan

ini kemudian dapat dipresentasikan dalam laporan penelitian sebagai dasar untuk memberikan rekomendasi perbaikan atau langkah-langkah penguatan keamanan yang diperlukan.

Dengan menggabungkan langkah-langkah tersebut, analisis data tidak hanya memberikan gambaran yang komprehensif terhadap keamanan komunikasi pada aplikasi WAVE Mobile Communicator namun juga memberikan pemahaman mendalam terhadap kerentanan dan potensi risiko keamanan yang perlu ditanggapi secara proaktif oleh pihak berwenang.

3.1.5 Membangun Penelitian

Hasil analisis data menjadi dasar untuk membangun keseluruhan penelitian. Disusunnya temuan, analisis keamanan, serta rekomendasi untuk perbaikan dan peningkatan keamanan aplikasi WAVE Mobile Communicator pada ponsel Motorola LEX L11a. Pada tahap ini, penelitian memberikan kontribusi positif terhadap pemahaman keamanan komunikasi militer.

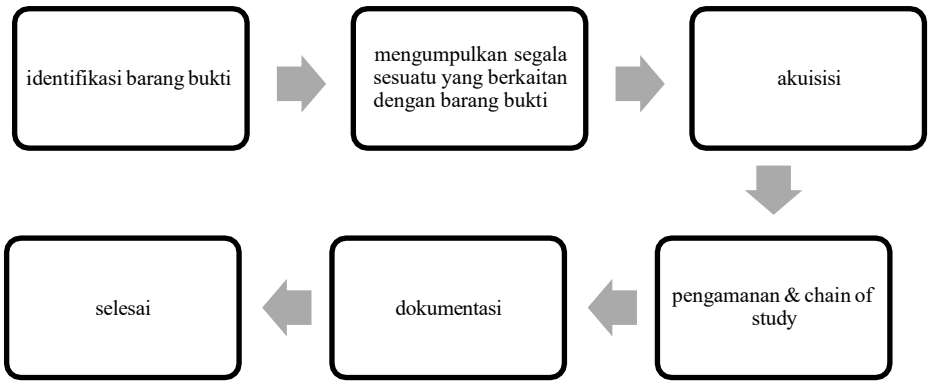
3.1.6 Membangun Kesimpulan Penelitian

Kesimpulan penelitian dihasilkan berdasarkan analisis data dan temuan yang diperoleh. Kesimpulan ini mencakup rangkuman hasil penelitian, implikasi praktis, dan arah untuk penelitian selanjutnya. Seluruh alur penelitian mengarah pada pemahaman yang mendalam terhadap keamanan aplikasi WAVE Mobile Communicator di lingkungan TNI dan POLRI.

3.2. Fase Persiapan

3.2.1 Pengembangan Alur Kerja

Dalam fase persiapan penelitian, pengembangan alur kerja menjadi langkah awal yang krusial. Berikut adalah alur kerja berdasarkan ISO/IEC 27037 Klausul 7.1.3, yang berfokus pada *"Identification of Digital Evidence"*. Klausul ini menjelaskan langkah-langkah dalam proses identifikasi bukti digital, yang merupakan bagian awal dari proses penanganan barang bukti digital secara forensik. Adapun alur proses seperti gambar 3.2 sebagai berikut:



Gambar 3.2 Alur Investigasi Forensik berdasarkan ISO 27037

Dalam tahap persiapan penelitian ini, pengembangan alur kerja menjadi aspek yang sangat penting. Alur kerja harus disusun secara cermat agar mencakup setiap tahapan yang esensial dalam analisis keamanan aplikasi WAVE Mobile Communicator pada ponsel hybrid Motorola LEX L11a. Proses ini dimulai dengan identifikasi dan pemetaan seluruh langkah yang akan dijalankan, mulai dari akuisisi data hingga tahapan analisis digital forensik. Dokumentasi yang jelas dan terinci untuk setiap tahap merupakan kunci utama, memastikan konsistensi dan akurasi selama seluruh penelitian berlangsung.

Langkah pertama dalam alur kerja adalah memastikan bahwa semua peralatan dan perangkat lunak yang diperlukan untuk akuisisi live forensic telah tersedia dan berfungsi dengan baik. Hal ini mencakup menyiapkan perangkat lunak seperti MobilEdit Forensic Express Pro dan Cellebrite UFED yang sesuai dengan standar ISO 27037. Setelah itu, proses akuisisi dilakukan dengan cermat untuk memastikan bahwa data yang diperoleh mencakup informasi yang relevan terkait keamanan aplikasi WAVE Mobile Communicator.

Selanjutnya, hasil akuisisi tersebut di imaging untuk menciptakan salinan forensik yang dapat diandalkan. Proses imaging ini harus mematuhi ketentuan ISO 27037, memastikan keberlanjutan rantai bukti digital dan integritas data yang diakuisisi. Semua langkah di dalam alur kerja ini perlu diawasi dengan ketat agar tidak ada kehilangan informasi atau potensi perubahan data selama proses akuisisi dan imaging berlangsung. Setelah berhasil mendapatkan salinan forensik, tahap analisis data digital forensik dimulai. Dalam hal ini, penggunaan alat bantu seperti Autopsy atau Forensic Toolkit dapat mendukung identifikasi potensi ancaman keamanan pada aplikasi WAVE Mobile Communicator. Hasil analisis ini kemudian diinterpretasikan dengan cermat untuk memahami implikasinya terhadap keamanan informasi yang dikomunikasikan melalui aplikasi tersebut.

Secara keseluruhan, alur kerja ini memastikan bahwa proses akuisisi live forensic

pada ponsel Motorola LEX L11a dengan menggunakan aplikasi WAVE Mobile Communicator mematuhi standar ISO 27037. Dengan demikian, penelitian dapat memberikan temuan yang akurat dan dapat diandalkan terkait keamanan komunikasi di lingkungan TNI dan POLRI.

3.2.2 Motorola LEX L11a

Pemahaman menyeluruh terhadap perangkat keras Motorola LEX L11a menjadi fokus dalam sub bab ini. Dilakukan penelitian terinci terkait spesifikasi teknis, sistem operasi yang digunakan, dan karakteristik keamanan perangkat. Identifikasi metode akses yang dapat diterapkan pada perangkat ini menjadi bagian penting untuk memastikan akuisisi data yang menyeluruh. Motorola LEX L11a adalah ponsel hybrid yang secara khusus dirancang untuk kebutuhan komunikasi di lingkungan militer dan penegakan hukum. Ponsel ini memiliki sejumlah spesifikasi teknis yang memadai untuk memenuhi tuntutan operasional di lapangan. Tabel 3.1 berikut menguraikan spesifikasi, kelebihan serta kekurangan dari Motorola LEX L11a.

Tabel 3.1 Spesifikasi Motorola LEX L11a

Spesifikasi	Kelebihan	Kekurangan
• Sistem Operasi: Menjalankan sistem operasi Android, ponsel ini memberikan fleksibilitas dalam penggunaan aplikasi yang sesuai dengan kebutuhan operasional militer dan keamanan. • Baterai: Ditenagai oleh baterai daya tinggi, memastikan ponsel dapat beroperasi dalam jangka waktu yang panjang tanpa kebutuhan pengisian daya yang konstan.	• Keamanan: Fitur keamanan tingkat tinggi untuk melindungi data sensitif dan komunikasi. • Daya Tahan Baterai: Baterai daya tinggi memastikan kelangsungan operasional dalam kondisi lapangan yang intensif.	ponsel konsumen biasa. • Harga: Harga ponsel ini mungkin lebih tinggi dibandingkan dengan ponsel konsumen sebanding, mengingat fitur-fitur keamanan dan ketahanannya.

Topologi Jaringan dari ponsel ini dirancang untuk beroperasi dalam jaringan yang andal dan aman. Topologi jaringannya dapat mencakup integrasi dengan jaringan militer dan penegakan hukum, memastikan keamanan data dan komunikasi. Koneksi nirkabel, seperti Wi-Fi dan Bluetooth, dapat digunakan untuk transfer data cepat dan efisien di lapangan. Keamanan perangkat diperkuat dengan metode otentikasi yang canggih, enkripsi data, dan kontrol akses tingkat tinggi. Fitur keamanan ini membantu melindungi informasi yang dikomunikasikan melalui aplikasi seperti WAVE Mobile Communicator dari potensi ancaman keamanan.

Pemahaman mendalam tentang perangkat keras Motorola LEX L11a ini menjadi landasan yang kokoh untuk memastikan akuisisi data yang komprehensif dan keamanan informasi yang optimal selama proses penelitian.

Tabel 3.2 Spesifikasi Xiaomi Redmi Note 8

Spesifikasi	Kelebihan	Kekurangan
• Performa Snapdragon 665 cukup untuk menjalankan aplikasi sehari-hari dan game ringan. • Baterai: Ditenagai oleh baterai daya tinggi, memastikan ponsel dapat beroperasi dalam jangka waktu yang panjang tanpa kebutuhan pengisian daya yang konstan. • Kamera: Dilengkapi dengan kamera berkualitas tinggi untuk dokumentasi visual dan keperluan pengawasan.	• Harga Terjangkau: Redmi Note 8 menawarkan harga yang sangat terjangkau. • Baterai Tahan Lama: Baterai 4000mAh mampu bertahan seharian dengan penggunaan normal. • Layar Besar dan Jernih: Layar 6.3 inci dengan resolusi Full HD.	• Kontrol akses: Redmi Note 8 tidak memiliki kontrol akses yang kuat seperti perangkat khusus militer, untuk membatasi kemampuan untuk membatasi akses ke data dan aplikasi tertentu. • Keamanan: Redmi Note 8 rentan terhadap kerentanan keamanan yang umum ditemukan di platform Android .

3.2.3 *WAVE Mobile Communication*

Sub bab ini menitikberatkan pada analisis aplikasi WAVE Mobile Communicator. Pengumpulan data terkait pengaturan keamanan, protokol enkripsi yang digunakan, serta jejak digital yang dihasilkan oleh aplikasi menjadi fokus. Diperlukan pemahaman mendalam terkait fitur-fitur keamanan yang telah diimplementasikan pada aplikasi ini untuk mengidentifikasi potensi kerentanan yang mungkin terlewat.

WAVE Mobile Communication, solusi komunikasi terdepan dari Motorola Solutions, menawarkan berbagai fitur canggih untuk meningkatkan efisiensi dan konektivitas tim. Fitur-fitur ini termasuk Push-to-Talk (PTT) yang aman dan real-time, pesan teks dan multimedia, pelacakan lokasi GPS, status kehadiran anggota tim, integrasi dengan radio darat bergerak (LMR), dan dukungan untuk berbagai perangkat dan jaringan. *WAVE Mobile Communication* menggunakan arsitektur terdistribusi yang aman, dengan server WAVE dihosting di pusat data atau cloud dan klien WAVE diinstal pada perangkat pengguna. Komunikasi antara klien dan server enkripsi untuk keamanan data dan privasi.

Log komunikasi disimpan di server WAVE dan dapat diakses oleh pengguna melalui aplikasi WAVE. Log ini dapat diekspor ke format lain untuk analisis dan pelaporan, membantu tim mengoptimalkan kinerja dan meningkatkan akuntabilitas. Manfaat utama *WAVE Mobile Communication* termasuk peningkatan komunikasi dan kolaborasi tim, peningkatan efisiensi dan produktivitas, peningkatan keselamatan dan keamanan, dan pengurangan biaya komunikasi. Solusi ini digunakan oleh berbagai organisasi di berbagai industri, termasuk keamanan publik, layanan darurat, transportasi, utilitas, manufaktur, dan perhotelan. *WAVE Mobile Communication* dapat diintegrasikan dengan aplikasi lain, seperti CRM dan ERP, untuk meningkatkan konektivitas dan efisiensi data.

Informasi lebih lanjut tentang *WAVE Mobile Communication*, termasuk panduan pengguna, studi kasus, dan layanan pelatihan, tersedia di situs web Motorola Solutions. Dengan berbagai fitur canggih, arsitektur yang aman, dan fleksibilitas integrasi, *WAVE Mobile Communication* adalah pilihan ideal untuk organisasi yang ingin meningkatkan kinerja dan konektivitas tim.

3.2.4 MobilEdit Forensic Express Pro

MobilEdit Forensic Express Pro dipilih sebagai salah satu alat pendukung utama dalam analisis digital forensik. Pada sub bab ini, diuraikan langkah-langkah penggunaan perangkat lunak ini, termasuk teknik akuisisi data dan fungsionalitas analisis yang relevan. Diperlukan pemahaman menyeluruh tentang kemampuan alat ini untuk memastikan optimalitas proses analisis.

3.2.5 Cellebrite UFED

Cellebrite UFED menjadi alat tambahan yang diperlukan dalam fase akuisisi data. Sub bab ini mencakup teknis penggunaan Cellebrite UFED, termasuk proses ekstraksi data dan kemampuan alat dalam menangani perangkat Motorola LEX L11a. Pemahaman yang mendalam tentang metode ini mendukung integritas dan kelengkapan data yang akan diolah.

3.3. Proses Investigasi dengan MobilEdit

MobilEdit membantu proses ekstrak data pada perangkat Perangkat Hybrid dan Perangkat Konvensional, sehingga dapat dilakukan analisis data. MobilEdit juga memiliki beberapa fitur seperti memulihkan data yang telah dihapus dari perangkat, memecahkan kata sandi yang telah diterapkan pada perangkat, hingga mendekripsi data yang telah dienkripsi. Berikut proses investigasi yang dilakukan dalam penggunaan *tools* Mobiledit,

3.3.1. Akuisisi Perangkat

Proses akuisisi dapat dilakukan dengan menghubungkan perangkat mobile ke komputer menggunakan USB atau Wi-Fi, Proses akuisisi penelitian ini dilakukan dengan menggunakan pendekatan digital forensik dan menggunakan metode ISO 27037 dalam melakukan proses akuisisi pada perangkat menyala untuk menemukan artefak digital berupa volatile.

3.3.2. Analisis Data

Proses analisis data menggunakan *tools* MobilEdit memiliki fitur berupa tersedianya alat untuk menganalisis data ingin di ekstrak seperti viewer riwayat panggilan untuk melihat riwayat panggilan masuk, keluar dan tidak terjawab. Pada proses analisa juga didapatkan data berupa folder yang melekat pada perangkat, sehingga seluruh informasi yang ada dan terjadi menggunakan perangkat dapat diambil dan dilakukan analisa lebih lanjut, pada proses ini MobilEdit juga dapat mencari kata kunci hingga filter data.

3.3.3. Pelaporan

Dari hasil akuisisi perangkat dan Analisa dilakukan pelaporan untuk merangkum hasil akuisisi, laporan menyertakan informasi seperti Informasi perangkat (Model dan sistem operasi), data yang diekstrak (Jenis data, tanggal dan waktu akuisisi), serta Hasil temuan yang memberikan informasi relevan sesuai dengan hasil akuisisi perangkat.

3.4 Proses Investigasi dengan Cellebrite UFED

3.4.1 Akuisisi perangkat

Sama seperti penggunaan *tools* Forensik lainnya Proses akuisisi menggunakan *tools* Cellebrite UFED dapat dilakukan dengan menghubungkan perangkat mobile ke komputer menggunakan USB atau Wi-Fi dan dapat dilakukan dengan Firewire. Proses akuisisi penelitian ini dilakukan dengan menggunakan pendekatan digital forensik dan menggunakan metode ISO 27037 dalam melakukan proses akuisisi pada perangkat menyala untuk

menemukan artefak digital berupa volatile.

Metode *live acquisition* menjadi pilihan yang tepat untuk jenis perangkat maupun sistem operasi yang ada pada ponsel konvensional. Metode akuisisi dengan *live acquisition* dilakukan dengan menghubungkan ponsel konvensional ke USB yang sudah disiapkan, selain USB juga bisa melalui jaringan maupun Wi-Fi sehingga dapat mengakuisisi perangkat yang aktif maupun perangkat yang dienkripsi. UFED akan membuat salinan forensik dari perangkat dan menyimpannya sebagai file image.

3.4.2 Analisis Data

Proses analisis data menggunakan *tools* Cellebrite UFED menyediakan modul untuk melakukan analisis data yang diekstrak seperti Modul File System untuk melihat dan mengekstrak file dari perangkat, Modul iOS untuk menganalisis data dari perangkat ios dan Modul Android untuk menganalisis data dari perangkat android, hingga modul Logical untuk menganalisis data log database pada perangkat dan data rawa pada perangkat. Proses analisis dapat dilakukan lebih dalam dengan tersedianya berbagai modul dari *tools* cellebrite UFED.

3.4.3. Pelaporan

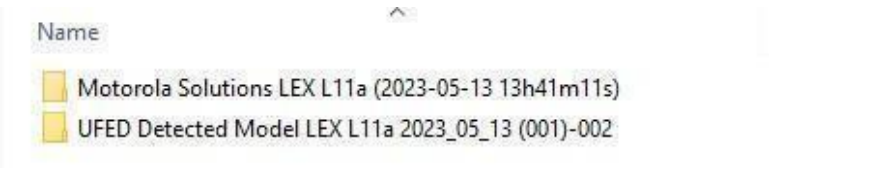
Pelaporan dari hasil akuisisi perangkat dan Analisa dilakukan pelaporan untuk merangkum hasil akuisisi, laporan pada proses investigasi dengan Cellebrite UFED dapat disajikan lebih banyak informasi karena hasil Analisa yang didapatkan berupa seperti hasil pemulihan data, pemecahan kata sandi hingga salinan forensic dari perangkat.

BAB 4

Hasil dan Pembahasan

4.1. Analisa Hasil Akuisisi Cellebrite UFED.

Proses akuisisi pada Ponsel Hybrid dilakukan dengan menghubungkan perangkat digital dengan *tools* digital forensik untuk mencari artefak digital yang dapat membantu analisa forensik digital untuk kepentingan pengadilan dan sebagainya. Aplikasi yang digunakan dalam penelitian ini adalah MOBILedit Forensic Express, versi 7.4.0.20408 (x64) dan Cellebrite UFED Product Version: 7.50.0.137 , Internal Build: 7.50.0.137 UFED. Ponsel Hybrid yang digunakan untuk penelitian ini seperti yang telah dijabarkan diatas menggunakan ponsel Motorola LEX L11a yang merupakan manufaktur dari Motorola Solutions yang menggunakan OS Android dengan IMEI : 353978090103672 dan berwarna Hitam. Setelah mengetahui spesifikasi ponsel hybrid maka dilakukan analisis dengan Pendekatan Digital Forensik yang dilakukan menggunakan dua *tools* yaitu *Mobiledit* dan *Cellebrite UFED*, dari kedua metode tersebut didapatkan file ekstraksi hasil akuisisi pada gambar berikut:

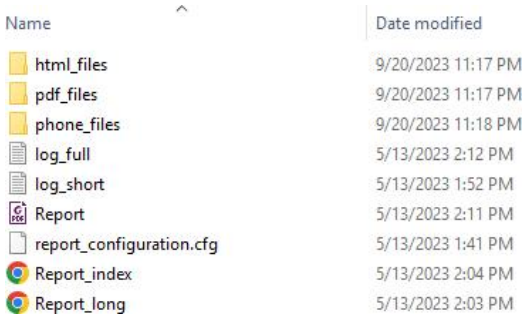


Gambar 4.1 Folder Hasil Akuisisi

Hasil akuisisi yang dilakukan bertujuan untuk mendapatkan informasi yang terekam pada Ponsel.

4.1.1 Analisa Hasil Akuisisi dengan MobilEdit

Hasil Analisa yang dilakukan dengan aplikasi MobileEdit didapatkan Ekstraksi sebagai berikut :

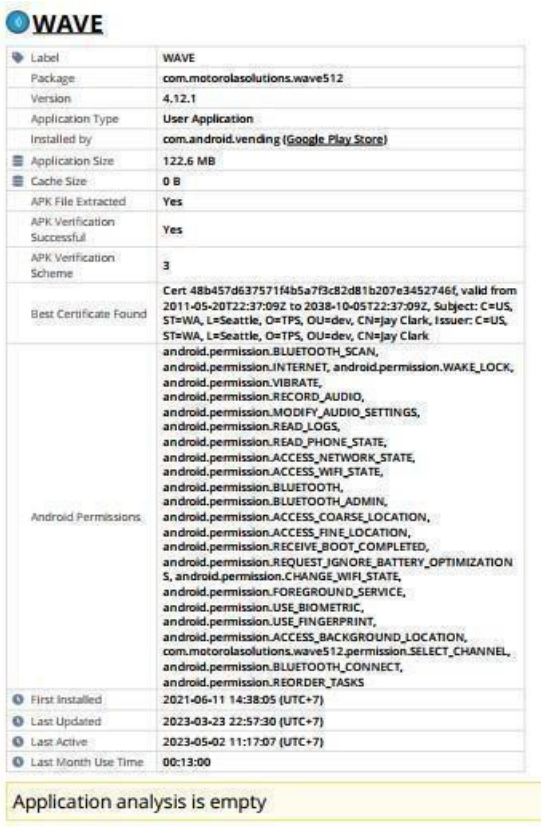


Gambar 4.2 Folder Hasil Akuisisi MobilEdit

Setelah mendapatkan hasil akuisisi dari aplikasi MobilEdit dengan menggunakan pendekatan digital forensik, peneliti melakukan analisa dari report yang di dapatkan. Dengan melakukan analisa pada file Report.pdf peneliti melakukan analisa mendalam mengenai hasil yang diperoleh aplikasi MobilEdit terhadap aplikasi Wave Mobile Communicator. Setelah melakukan analisa terhadap hasil Report.pdf, didapatkan beberapa keterangan seperti pada gambar berikut:

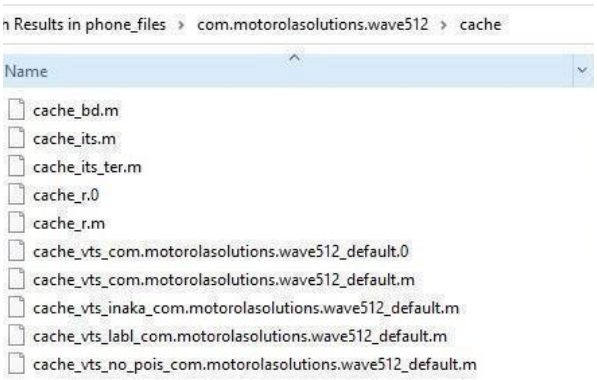
Gambar 4.3 Analisa Ponsel Hybrid MobileEdit

Dari informasi spesifikasi ponsel hybrid maka peneliti akan melakukan analisa menggunakan Wave Mobile Communicator untuk mencari artefak digital yang dapat ditemukan, hasil dari analisa dengan tools MobilEdit pada aplikasi Wave dijelaskan pada gambar berikut:



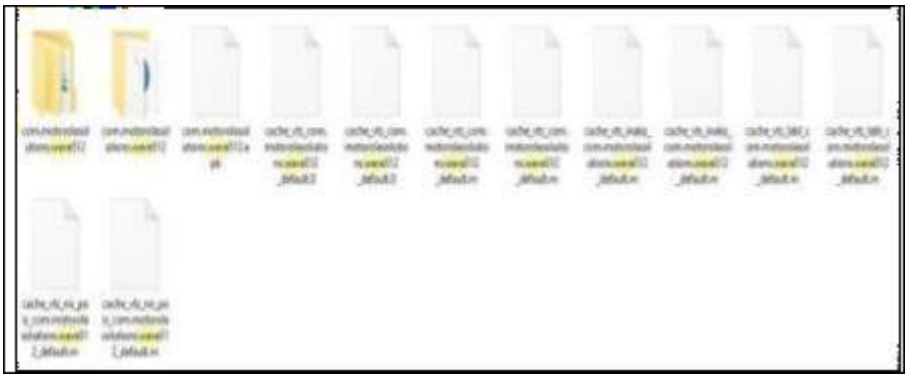
Gambar 4.4 Hasil Akuisisi Aplikasi Wave

Pada Gambar 4.4 dijelaskan bahwa aplikasi WAVE yang terdapat pada objek penelitian ini memiliki versi 4.12.1 dan diinstall dari Google Play Store dan memiliki ukuran 122.6 Mb. Aplikasi Wave ini di install pada 11 Juni 2021 dan update terakhir pada 23 Maret 2023, serta digunakan terakhir kali pada 2 Mei 2023. Namun dibawah keterangan tersebut dijelaskan bahwa aplikasi tersebut memiliki analisis yang kosong, artinya aplikasi MobilEdit tidak melakukan analisa pada aplikasi WAVE tersebut. Lalu dilakukan analisa lebih lanjut pada hasil akuisisi Report.pdf dan ditemukan beberapa informasi mengenai file yang terdapat pada ponsel Motorola LEX11 sebagai berikut:



Gambar 4.5 Analisa Aplikasi Wave

Gambar di atas menunjukkan hasil yang diperoleh oleh aplikasi *MobilEdit* dari proses akuisisi terhadap ponsel *Hybrid Motorola LEX11*. Rincian file yang ditemukan pada hasil akuisisi tersebut tidak menunjukkan adanya indikasi *Log* percakapan dari aplikasi *WAVE* yang digunakan. Untuk menemukan artefak digital yang ingin dicari, peneliti melakukan analisa mendalam kepada setiap hasil akuisisi dari *MobilEdit* termasuk folder yang dihasilkan, dan ditemukan beberapa artefak digital seperti pada gambar dibawah:

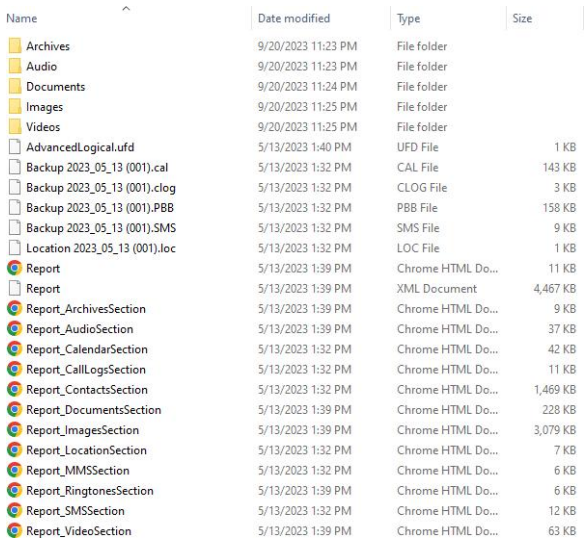


Gambar 4.6 Analisa Hasil Akuisisi Ponsel *Hybrid* MobilEdit

Pada hasil akuisisi tersebut ditemukan beberapa file hasil akuisisi, namun tidak ditemukan file yang ingin dicari, yaitu *Log* komunikasi dari aplikasi *WAVE*, untuk lebih detail mengenai hasil akuisisi tersebut peneliti melakukan analisa terhadap *cache file* yang ditemukan, *cache* yang ditemukan dijelaskan pada gambar Gambar 4.5, namun setelah melakukan analisa pada setiap *file cache* tetap tidak ditemukan adanya file log dari aplikasi *WAVE Mobile Communicator*. Maka peneliti melakukan analisa berikutnya dengan menggunakan aplikasi *Cellebrite UFED* untuk mencari artefak digital dari aplikasi *WAVE Mobile Communicator*.

4.1.2 Analisa Hasil Akuisisi dengan Cellebrite UFED

Setelah melakukan analisa hasil akuisisi ponsel *hybrid* dengan tools *MobilEdit*, peneliti melakukan analisa tambahan untuk mendukung hasil penelitian yang valid. Pada penelitian ini penulis melakukan akuisisi dengan *Cellebrite UFED* untuk mencari artefak digital pada ponsel *hybrid Motorola LEX11* pada aplikasi *WAVE Mobile Communicator* yang digunakan oleh penegak hukum dalam berkomunikasi dengan memanfaatkan satelit. Hasil akuisisi dengan menggunakan *Cellebrite* dijelaskan pada gambar berikut:



Name	Date modified	Type	Size
Archives	9/20/2023 11:23 PM	File folder	
Audio	9/20/2023 11:23 PM	File folder	
Documents	9/20/2023 11:24 PM	File folder	
Images	9/20/2023 11:25 PM	File folder	
Videos	9/20/2023 11:25 PM	File folder	
AdvancedLogical.ufd	5/13/2023 1:40 PM	UFD File	1 KB
Backup 2023_05_13 (001).cal	5/13/2023 1:32 PM	CAL File	143 KB
Backup 2023_05_13 (001).clog	5/13/2023 1:32 PM	CLOG File	3 KB
Backup 2023_05_13 (001).PBB	5/13/2023 1:32 PM	PBB File	158 KB
Backup 2023_05_13 (001).SMS	5/13/2023 1:32 PM	SMS File	9 KB
Location 2023_05_13 (001).loc	5/13/2023 1:32 PM	LOC File	1 KB
Report	5/13/2023 1:39 PM	Chrome HTML Do...	11 KB
Report	5/13/2023 1:39 PM	XML Document	4,467 KB
Report_ArchivesSection	5/13/2023 1:39 PM	Chrome HTML Do...	9 KB
Report_AudioSection	5/13/2023 1:39 PM	Chrome HTML Do...	37 KB
Report_CalendarSection	5/13/2023 1:32 PM	Chrome HTML Do...	42 KB
Report_CallLogsSection	5/13/2023 1:32 PM	Chrome HTML Do...	11 KB
Report_ContactsSection	5/13/2023 1:32 PM	Chrome HTML Do...	1,469 KB
Report_DocumentsSection	5/13/2023 1:39 PM	Chrome HTML Do...	228 KB
Report_ImagesSection	5/13/2023 1:39 PM	Chrome HTML Do...	3,079 KB
Report_LocationSection	5/13/2023 1:32 PM	Chrome HTML Do...	7 KB
Report_MMSSection	5/13/2023 1:32 PM	Chrome HTML Do...	6 KB
Report_RingtonesSection	5/13/2023 1:39 PM	Chrome HTML Do...	6 KB
Report_SMSSection	5/13/2023 1:32 PM	Chrome HTML Do...	12 KB
Report_VideoSection	5/13/2023 1:39 PM	Chrome HTML Do...	63 KB

Gambar 4.7 Hasil akuisisi ponsel *hybrid* dengan cellebrite

Hasil akuisisi dengan menggunakan *Cellebrite* menghasilkan beberapa file seperti pada Gambar 4.7 Pada file *Report.XML* tersebut, berisi informasi mengenai apa saja yang didapatkan oleh aplikasi *Cellebrite* selama proses akuisisi, maka penelitian akan berfokus pada artefak yang didapatkan dari proses akuisisi dengan *cellebrite* pada file tersebut. informasi yang didapatkan mengenai spesifikasi ponsel *hybrid* dari aplikasi *cellebrite* dijelaskan pada gambar berikut:

Selected Manufacturer:	Detected Model
Selected Model:	LEX L11a
Detected Manufacturer:	MotorolaSolutions
Detected Model:	LEX L11a
Revision:	9 PIE L11_P_R30.25.10
IMEI:	353978090103672
ICCID:	8962100019150000273
IMSI:	510101915000027
Advertising ID:	ce0c9059-3bef-4a1a-b8ae-78fcafd7c63a
Extraction start date/time:	13/05/2023 01:28:41 (GMT-5)
Extraction end date/time:	13/05/2023 01:39:26 (GMT-5)
Phone Date/Time:	13/05/2023 13:17:19 (GMT+7)
Connection Type:	USB Cable
UFED Version:	Product Version: 7.50.0.137 , Internal Build: 7.50.0.137 UFED
UFED S/N:	7018824

Note: This device is using client in order to communicate with UFED

Gambar 4.8 hasil akuisisi ponsel *hybrid* dengan cellebrite

Pada Gambar 4.8 diketahui bahwa ponsel yang terdeteksi adalah ponsel *Motorola LEX L11a* dari manufaktur *Motorola Solutions* dengan *IMEI : 353978090103672*. Dan didapatkan beberapa hasil akuisisi sebagai berikut:

#	File Name	File Size	File Date/Time	File Link
1	AUD-20221002-WA0043.opus Path: Internal shared storage/WhatsApp/Media/WhatsApp Audio/ Source: Phone SHA256: 0A20C531 EC769D1 D126C7C A39E809 53C4CE0 556BD46 0C78812 845DAC3 D0191A8	97268 Bytes	Created: 02/10/2022 15:43:49 Modified: 02/10/2022 15:43:49	AUD-20221002-WA0043.opus
2	AUD-20221002-WA0040.opus Path: Internal shared storage/WhatsApp/Media/WhatsApp Audio/ Source: Phone SHA256: E76C7F1E 744F51F 9CE8E5D 7E6B0EE EB5739D 4EF2282 101C915 CF3272E 5AC2D8B	369220 Bytes	Created: 02/10/2022 15:43:35 Modified: 02/10/2022 15:43:35	AUD-20221002-WA0040.opus
3	PTT-20230120-WA0027.opus Path: Internal shared storage/WhatsApp/Media/WhatsApp Voice Notes/202303/ Source: Phone SHA256: A3C0C300 4B87886 410845A 68C170A ACB48A1 924D216 25441D4 EE7D019 3E37D74	2609 Bytes	Created: 20/01/2023 20:20:20 Modified: 20/01/2023 20:20:20	PTT-20230120-WA0027.opus

Gambar 4.9 File Hasil Akuisisi Ponsel *Hybrid* Dengan Cellebrite

Penelitian ini berfokus pada artefak digital dari aplikasi *WAVE Mobile Communications*, maka peneliti akan berfokus pada aspek aspek yang berkaitan dengan informasi tersebut. peneliti akan mencari informasi mengenai audio yang terekam pada saat proses akuisisi ponsel *hybrid*, namun tidak ditemukannya file yang dituju yaitu *Log* komunikasi dari aplikasi *WAVE* dengan menggunakan jaringan satelit. Hasil akuisisi *file audio* dengan aplikasi *Cellebrite* dijelaskan pada gambar berikut:

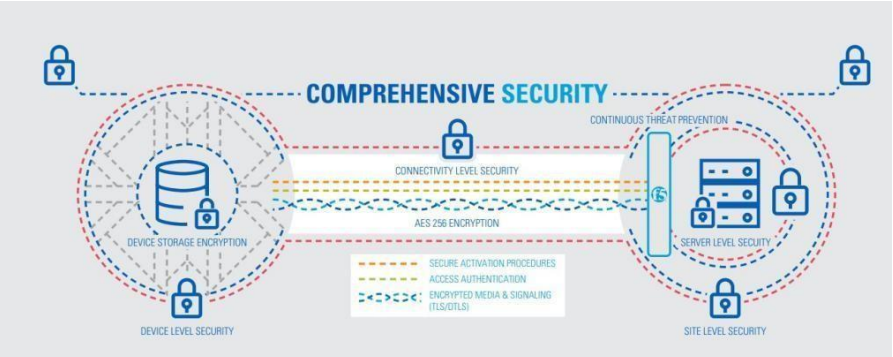
Contacts (1641)	Selected
SMS - Text Messages (14)	Selected
Calendar/Notes/Tasks (152)	Selected
Call Logs (9)	Selected
MMS - Multimedia Messages	Selected
Email Messages	Not Supported
Instant Messages	Not Supported
Browser Bookmarks	Not Supported
Browser History	Not Supported
Web Searches	Not Supported
User Dictionary	Not Supported
Location	Selected
Images (4454)	Selected
Ringtones	Selected
Audio (53)	Selected
Video (102)	Selected
Documents (357)	Selected
Archive (4)	Selected
Files	Not Selected

Gambar 4.10 Hasil Akuisisi Audio Ponsel *Hybrid* Dengan Cellebrite

Pada Gambar 4.10 dijelaskan hasil akuisisi ponsel *hybrid* pada audio untuk menemukan artefak digital pada komunikasi dengan aplikasi *WAVE*, namun pada file tersebut tidak ditemukan *file Log* hasil komunikasi dengan aplikasi *WAVE*.

4.2. Struktur Keamanan Wave Mobile Communicator.

Setelah melakukan analisa dari hasil akuisisi kedua aplikasi tersebut, tidak ditemukan artefak digital yang merupakan hasil komunikasi dengan menggunakan aplikasi *WAVE Mobile Communicator* Aplikasi MobilEdit maupun Cellebrite tidak mampu mendeteksi adanya Log komunikasi dari aplikasi Wave, *tools* hanya menemukan informasi umum mengenai aplikasi Wave, hal tersebut disebabkan karena *WAVE Mobile Communicator* menggunakan perilndungan data yang kompleks. Wave Mobile Communicator menggunakan 3GPP (3rd Generation Partnership Project) Mission Critical PTT (MCPTT) standard atau standar komunikasi yang dirancang dapat digunakan untuk dalam melakukan komunikasi suara dan data secara real-time dengan tingkat keandalan yang tinggi. Sehingga *Wave Mobile Communicator* fokus melakukan perlindungan data end to end, selama perjalanan dan perlindungan server seperti yang digambarkan sebagai berikut:



Gambar 4.11 topologi enkripsi end to end pada wave. (sumber : https://svbradiocom.se/wp-content/uploads/2023/03/wave-ptx-azure-cloud-security-v3.pdf)

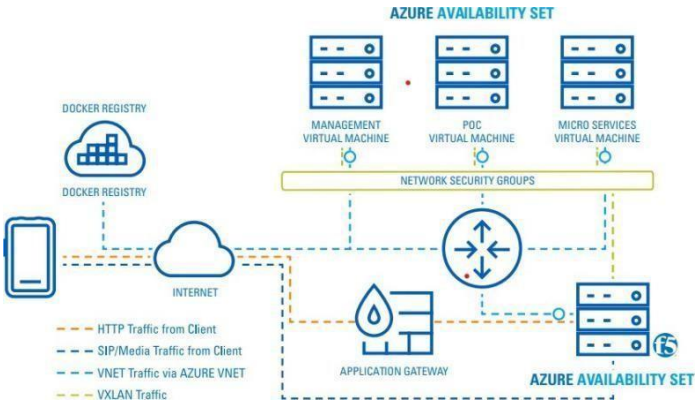
Dari segi keamanan, WAVE mengimplementasikan *Comprehensive Security* dengan pendekatan multi-lapisan untuk melindungi data di seluruh platform. Pertama, pada *Device Level Security*, data yang disimpan pada perangkat pengguna dilindungi oleh enkripsi yang kuat, memastikan bahwa informasi tetap aman meskipun perangkat tersebut jatuh ke tangan yang tidak berwenang. Selanjutnya, *Connectivity Level Security* menjamin bahwa data yang berpindah antara perangkat dan server dilindungi melalui protokol enkripsi seperti Transport Layer Security (TLS) dan Datagram Transport Layer Security (DTLS). Ini memberikan lapisan keamanan tambahan selama proses komunikasi, mencegah penyadapan dan serangan man-in-the-middle.

Di tingkat *Server Level Security*, WAVE menerapkan kontrol akses berbasis peran dan otentikasi multi-faktor. Hal ini memastikan bahwa hanya pengguna yang memiliki hak akses yang dapat berinteraksi dengan data sensitif, sehingga mengurangi risiko kebocoran informasi. Selain itu, *Site Level Security* mencakup pengamanan fisik dari pusat data yang menyimpan server, dengan penerapan sistem pengawasan CCTV, kontrol akses biometrik, dan alarm untuk mencegah akses fisik yang tidak sah.

Terakhir, WAVE juga dilengkapi dengan *Continuous Threat Prevention,* yang berfungsi untuk mendeteksi dan merespons potensi ancaman secara real-time. Dengan memanfaatkan algoritma pembelajaran mesin, sistem ini memonitor aktivitas mencurigakan dan dapat memberikan peringatan kepada administrator tentang kemungkinan pelanggaran keamanan. Tindakan mitigasi dapat dilakukan dengan cepat untuk mengurangi risiko terhadap data dan memastikan bahwa komunikasi tetap aman.

Secara keseluruhan, WAVE merupakan platform komunikasi yang mengintegrasikan kecepatan, keamanan, dan efisiensi dalam satu solusi. Dengan kemampuan untuk beradaptasi dengan kebutuhan pengguna dan situasi yang terus berubah, WAVE menjadi alat penting bagi organisasi yang memprioritaskan komunikasi yang aman dan efektif dalam situasi kritis. Dengan pendekatan yang menyeluruh terhadap keamanan data, WAVE tidak hanya memenuhi tuntutan komunikasi modern, tetapi juga menetapkan standar baru untuk interoperabilitas dan perlindungan informasi di era digital saat ini.

Sistem keamanan server yang digunakan adalah *azure cloud security* yaitu sebuah sesi sebuah sesi yang berada dalam kontainer yang dijalankan dalam virtual mechine Micrsoft Azure. Adapun topologinya sebagai berikut:



Gambar 4.12 Topologi pengamanan server (sumber : https://svbradiocom.se/wp-content/uploads/2023/03/wave-ptx-azure-cloud-security-v3.pdf)

Pada Gambar 4.12 dijelaskan pengamanan tingkat tinggi pada arsitektur WAVE, platform push-to-talk (PTT) yang dikembangkan oleh Motorola Solutions, dirancang untuk memberikan layanan komunikasi yang handal dan aman. Di dalam arsitektur ini, beberapa komponen penting bekerja sama untuk menyediakan komunikasi real-time dengan integritas dan ketersediaan yang tinggi. Dasar dari arsitektur ini adalah standar 3rd Generation Partnership Project (3GPP) yang mengatur penggunaan signaling Session Initiation Protocol (SIP) dan Real-Time Transport Protocol (RTP), yang memainkan peran penting dalam pengaturan komunikasi serta streaming media.

4.2.1 Struktur Dasar Arsitektur

Arsitektur WAVE terdiri dari berbagai elemen yang terhubung satu sama lain untuk mendukung operasional PTT. Di bagian atas arsitektur, terdapat Azure Availability Sets yang menyatukan beberapa Virtual Machine (VM) untuk memastikan ketersediaan layanan yang tinggi. Availability Sets dirancang untuk mengurangi risiko downtime dengan menempatkan VM dalam grup yang terpisah secara fisik di dalam data center. Hal ini mengurangi kemungkinan kegagalan sistem secara bersamaan, sehingga layanan tetap dapat diakses meskipun salah satu komponen mengalami masalah.

4.2.2 Penggunaan Docker dan Manajemen Kontainer

Di dalam arsitektur ini, penggunaan Docker Registry menjadi krusial untuk manajemen aplikasi. Docker memungkinkan penyimpanan dan distribusi kontainer yang berisi aplikasi dan dependensinya. Dengan memanfaatkan kontainerisasi, proses deployment menjadi lebih cepat dan efisien, serta memungkinkan pembaruan aplikasi yang lebih mudah. Kontainer-kontainer ini dapat berisi server aplikasi WAVE, yang bertanggung

jawab untuk mengelola sesi komunikasi antara pengguna.

4.2.3 Virtual Machines dan Microservices

WAVE mengimplementasikan berbagai jenis Virtual Machines (VM) yang menyokong layanan berbeda, seperti Management Virtual Machine, POC (Push-to-Talk Over Cellular) Virtual Machine, dan Micro Services Virtual Machine. Manajemen VM bertanggung jawab untuk memantau dan mengelola sumber daya dalam sistem, sedangkan POC VM berfokus pada pengelolaan saluran komunikasi. Microservices VM mendukung berbagai fungsi spesifik, memungkinkan pengembangan modular yang meningkatkan fleksibilitas dan kecepatan dalam mengadaptasi fitur baru atau perbaikan.

4.2.4. Jaringan Keamanan

Keamanan jaringan merupakan aspek penting dalam arsitektur WAVE. Network Security Groups (NSG) digunakan untuk mengatur dan mengontrol akses ke sumber daya jaringan. NSG berfungsi sebagai firewall yang membatasi lalu lintas jaringan berdasarkan aturan yang telah ditentukan. Dengan menetapkan kebijakan yang ketat, NSG membantu melindungi data yang ditransmisikan dan mencegah akses tidak sah ke sistem. Ini merupakan langkah penting dalam menjaga integritas dan kerahasiaan komunikasi.

4.2.5. Gateway Aplikasi

Di pusat arsitektur terdapat Application Gateway yang bertanggung jawab untuk mengelola lalu lintas masuk dan keluar dari aplikasi. Gateway ini mengoptimalkan permintaan dan mendistribusikan lalu lintas ke VM yang sesuai, memastikan kinerja yang optimal. Selain itu, gateway ini juga menyediakan lapisan tambahan untuk pemfilteran dan pengamanan data, termasuk kemampuan untuk mendeteksi dan memitigasi serangan DDoS (Distributed Denial of Service).

4.2.6. Protokol Komunikasi Data.

Arsitektur ini juga mengelola berbagai jenis lalu lintas yang berbeda. Misalnya, lalu lintas HTTP dari klien untuk interaksi umum, serta SIP/Media Traffic yang diperlukan untuk komunikasi suara dan video. Penggunaan VNET (Virtual Network) melalui Azure memberikan isolasi dan keamanan tambahan untuk komunikasi internal antara komponen sistem. VNET memastikan bahwa semua data yang ditransfer antar VM tetap dalam batasan yang aman, mengurangi risiko serangan luar.

4.2.7. Menggunakan VXLAN untuk Isolasi Lalu Lintas

Virtual Extensible LAN (VXLAN) digunakan dalam arsitektur ini untuk mengatasi keterbatasan VLAN tradisional dengan menyediakan lebih banyak ruang alamat dan isolasi yang lebih baik. VXLAN memungkinkan pengguna untuk membangun jaringan overlay yang lebih besar di atas infrastruktur yang ada, memberikan fleksibilitas dalam pengelolaan sumber daya dan meningkatkan keamanan data. Hal ini sangat penting dalam lingkungan cloud di mana banyak aplikasi berjalan bersamaan.

4.2.8. Keuntungan dari Arsitektur Berbasis Cloud

Dengan memanfaatkan Microsoft Azure sebagai platform cloud, WAVE dapat menawarkan skalabilitas yang tinggi. Dalam situasi permintaan puncak, seperti saat terjadi bencana atau peristiwa besar, platform ini dapat dengan cepat mengalokasikan lebih banyak sumber daya tanpa perlu infrastruktur fisik tambahan. Ini memungkinkan respon yang cepat dan efisien untuk memenuhi kebutuhan komunikasi real-time yang terus berubah.

4.2.9. Pengelolaan Data dan Keamanan Data

Data yang dikirim dan diterima dalam platform WAVE dienkripsi, menjamin bahwa informasi sensitif tetap terlindungi. Penggunaan protokol yang aman seperti RTP dan RTCP untuk streaming media memastikan bahwa data tidak hanya sampai tujuan, tetapi juga dalam kondisi yang aman dari penyadapan dan gangguan. Keamanan data adalah prioritas utama dalam desain arsitektur ini, mengingat sifat kritis dari komunikasi yang dilakukan.

4.2.10. Pemeliharaan dan Monitoring

Pemeliharaan sistem dan monitoring kinerja adalah aspek penting dari arsitektur ini. Dengan memanfaatkan alat analitik yang disediakan oleh Azure, pengelola sistem dapat secara proaktif memantau kesehatan layanan, mendeteksi anomali, dan melakukan tindakan perbaikan yang diperlukan. Kemampuan untuk memantau kinerja secara real-time meningkatkan responsifitas dan keandalan layanan.

4.2.11. Keandalan dan Redundansi

Arsitektur ini dirancang dengan fokus pada keandalan dan redundansi. Penggunaan Azure Availability Sets dan pengaturan load balancing di seluruh VM memungkinkan sistem untuk terus beroperasi meskipun ada kegagalan di salah satu komponen. Ini penting untuk memastikan bahwa layanan PTsT dapat diandalkan dalam situasi kritis di mana

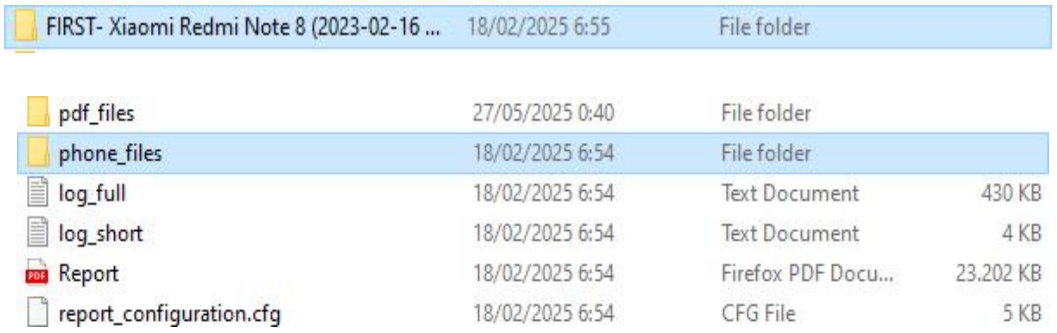
komunikasi harus tetap terjaga tanpa gangguan.

4.2.12. Kesesuaian dengan Standar Industri

Dengan mengadopsi standar 3GPP dalam desain arsitektur, WAVE menjamin bahwa platform ini tidak hanya memenuhi kebutuhan spesifik Motorola Solutions tetapi juga konsisten dengan praktik terbaik dalam industri komunikasi. Hal ini memberikan kepercayaan lebih kepada pengguna bahwa sistem ini dirancang untuk menghadapi tantangan komunikasi yang paling kompleks sekalipun.

4.3. Analisa Hasil Akuisisi Xiomi Note 8.

Proses akuisisi pada ponsel Xiomi dilakukan dengan menghubungkan perangkat digital dengan *tools* digital forensik untuk mencari artefak digital yang dapat membantu analisa forensik digital untuk kepentingan pengadilan dan sebagainya. Aplikasi yang digunakan dalam penelitian ini adalah MOBILedit Forensic Express, versi 7.4.0.20408 (x64). Ponsel konvensional yang digunakan untuk penelitian ini menggunakan ponsel Xiomi yang dengan IMEI : 863144045275213 dan berwarna Hitam. Setelah mengetahui spesifikasi Xiomi maka dilakukan analisis dengan pendekatan Digital Forensik yang dilakukan menggunakan *Mobiledit* kemudian didapatkan file ekstraksi hasil akuisisi pada gambar berikut:

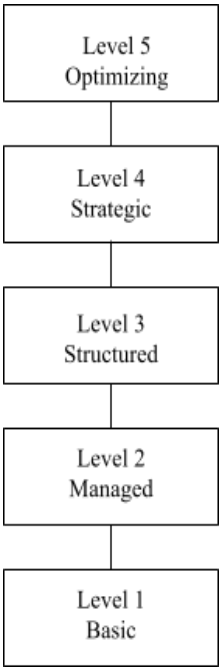


Gambar 4.11. hasil imaging xiomi note 8.

Pada gambar 4.11 terdapat metadata log

4.4. Analisa Level Keamanan

Menurut *Gartner Research,* tingkat keamanan sebuah perangkat mobile dibagi menjadi 5. Berikut ini adalah tingkat keamanan dari level tertinggi ke level terendah.



Gambar 4.1 level keamanan perangkat mobile.

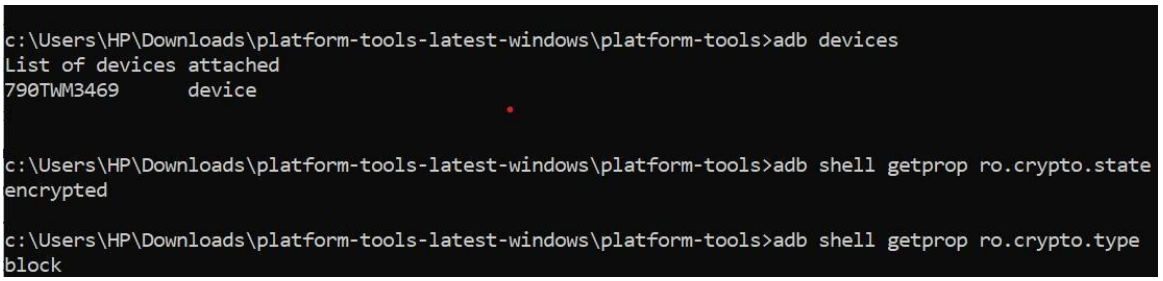
Gambar 4.1 menggambarkan level keamanan menurut Gartner research. Pada level satu, perangkat diamankan secara standart tanpa enkripsi dan root langsung diaktifkan sehingga pengguna dapat dengan mudah mengelola data yang ada pada perangkat tersebut. Selanjutnya level dua atau level *management* yaitu apabila sebuah perangkat sudah menerapkan kunci dengan password namun belum merepkan MDM (multi device management) atau perangkat dikendalikan oleh satu server besar yang mencangkup beberapa perangkat. Berbeda dengan level sebelumnya, pada level 3 keamanan yang diterapkan sebuah tinggi begitu juga pada level empat dan level lima. Semakiin tinggi level keamanan perangkat tersebut, semakin tinggi pula tingkat keamanan yang diterapkan perangkat mobile tersebut. Jika digambarkan menggunakan sebuah tabel, kriteria tersebut tercerminkan pada tabel 4.1.

Tabel 4.1. kriteria level keamanan menurut Gartner research.

Level	Karakteristik Umum	Pembuktian
Level 1	Tanpa enkripsi, lock screen lemah, root terbuka	Tidak ada FDE, root aktif, patch lawas
Level 2	Ada lock screen dan enkripsi, tanpa MDM	getprop ro.crypto.state, tidak ada MDM
Level 3	Ada FDE, patch aktif, sandbox aplikasi	Ada FDE, patch up to date, belum MDM
Level 4	MDM aktif, TEE, Verified Boot, 2FA	MDM aktif, getprop ro.boot.verifiedbootstate, biometrik
Level 5	Level 4 + sertifikasi resmi (EAL4+, FIPS 140-2) + audit ketat	Dokumen sertifikat, konfigurasi hardened OS

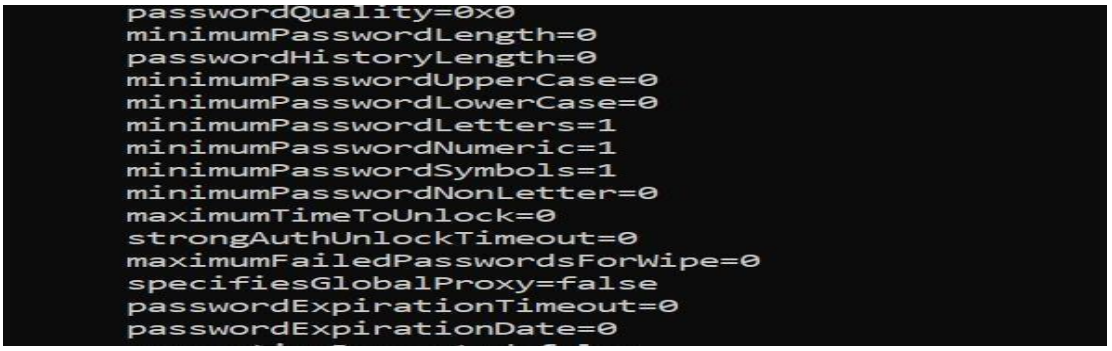
4.4.1 Motorola LEX L11 Mission Critical LTE

Dari kriteria level keamanan yang digambarkan pada tabel 4.1, penulis melakukan analisa terhadap perangkat Motorola lex11. Pada tingkat **device** security, perangkat tersebut harus memenuhi beberapa kriteria yaitu pertama, mengaktifkan *full disk* encryption seperti gambar 4.2.



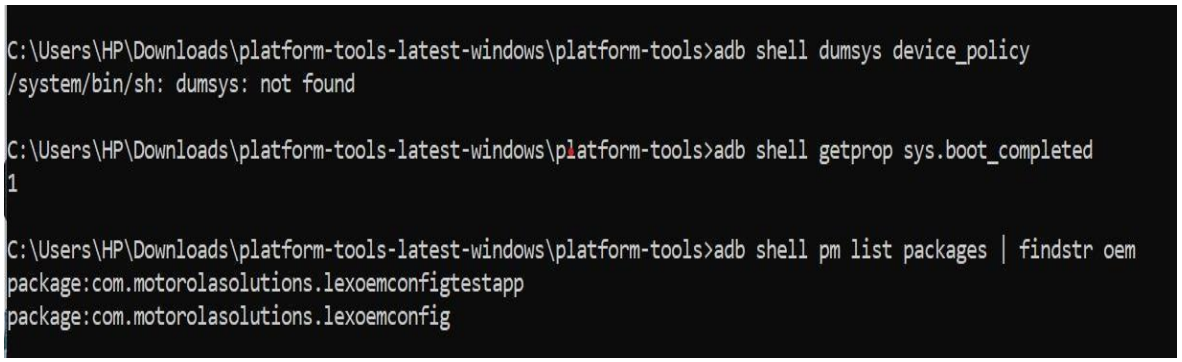
Gambar 4.2 perangkat motorola lex11 menerapkan FDE

Pada gambar 4.2 terdapat perangkat dengan nomor seri 790TWM3469, perangkat tersebut adalah motorola lex11. Kemudian dilakukan penerapan enkripsi dengan perintah *adb shell getprop ro.crypto.state* kemudian tertulis *encypted* yang berarti perangkat lex 11 menerapkan enkripsi kemudian dilanjutkan dengan mencari tahu tipe enkripsi dan tertulis disitu ***block*** yang artinya perangkat tersebut menerapkan enkripsi *FDE (full disk encryption).*



Gambar 4.3 perangkat motorola lex11 menerapkan FDE

Selain dari segi enkripsi, keamanan perangkat juga terlihat dari penerapan otentikasi multi faktor. Pada gambar 4.3 terlihat bahwa perangkat tersebut menerapkan keamanan dengan password, pola, dan biometrik namun hanya *password* saja yang diaktifkan. Apabila user salah memasukkan *password* maka data akan dihapus oleh server. Hal ini karena motorola lex11 memiliki *policy* yang dikendalikan oleh server atau *mobile device management.* wipe data dilakukan secara remote dan berkala. Apabila ada keadaan darurat, perangkat bisa diambil alih melalui server,seperti yang tercantum pada gambar 4.4.



Gambar 4.4 perangkat motorola lex11 menerapkan MDM.

Pada gambar 4.4, perintah direktori dumsys tidak ditemukan. Padahal saat dijalankan perintah *adb shell getprop sys.boot_completed* muncul angka 1 yang berarti perangkat sudah dibooting sempurna. Hal ini terjadi karena policy yang berada pada server tidak memberikan akses shell abd secara penuh, dumsys hanya bisa diakses oleh server. Pada skrip selanjutnya, terdapat informasi *package:com.motorolasolutions.lexoemconfigtestapp* membuktikan bahwa perangkat dikelola secara enterprise. Hal ini mengakibatkan user tidak dapat mengubah pengaturan perangkat. Selain itu server juga bisa melakukan kebijakan keamanan secara paksa serta memiliki kontrol penuh terhadap aplikasi dan jaringan.

Wave mobile comunikator adalah salah satu aplikasi krusial di perangkat motorola lex11. Dengan adanya hasil analisa diatas dapat disimpulkan artefak wave tidak dapat diakses ataupun di ekstrak karena kebijakan MDM diberangkat lex11 membatasi akses tersebut karena MDM dapat mengatur *data separation* dan *app containerization.* Log data yang berada pada wave mobile comuncator tidak dapat diakses via adb bahkan ketika motorola di root pun data yang berada pada aplikasi wave di enkripsi secara khusus sehingga hanya orang yang memiliki akses server saja lah yang bisa mengakses data wave. Ini membuktikan bahwa wave dikendalikan sepenuhnya oleh kebijakan MDM berbasis OEMConfig Motorola soulution. Kebijakan ini membatasi akses ADB, memproteksi data aplikasi, dan mencegah pencadangan atau penyalinan data tanpa otorisasi.

Dengan demikian dapat disimpulkan kedalam sebuah tabel yang sesuai dengan kriteria *Mobile Security Checklist* dari Gartner adalah sebagai berikut :

Tabel 4.1. Mobile Security Checklist Motorola Lex 11

Kategori	Deskripsi	Checklist
Device Security	Full disk encryption diaktifkan	√
	OS dan App diperbarui secara otomatis	√
	Otentikasi multi faktor atau biometrik digunakan	√
	Remote wipe tersedia dan diuji secara berkala	√
	Mobile device management diterapkan	√
Application Security	Aplikasi diuji dengan penetration testing	-
	Menggunakan RASP (Runtime Application Self-Protection)	√
	API hanya menerima request dari sumber terpercaya	√
	Aplikasi hanya bisa diinstal dari source resources	√
	App sandboxing diterapkan untuk membatasi akses aplikasi ke data	√
Network Security	Perangkat menggunakan VPN untuk akses data perusahaan	-
	TLS digunakan untuk semua komunikasi data	√
	Zero Trust Network Access diterapkan	√
	IDS/IPS digunakan untuk mendeteksi ancaman jaringan	√
	Penggunaan wifi publik dibatasi	√
Data Security	Data security	√
Identity & Acc ess Management	Semua akses ke aplikasi membutuhkan MFA	-
	SSO diterapkan untuk aplikasi berbasis cloud	√
	Behavioral analytics digunakan untuk mendeteksi anomali	-
	ZTP diterapkan	√
	Penghapusan akun pengguna yang tidak aktif dalam jangka waktu tertentu	√

4.4.2. Xiomi Note 8

Berdasarkan tingkat level keamanan pada perangkat mobile, berikut adalah analisis keamanan perangkat Xiomi Note 8 sesuai dengan kriteria Mobile Security Checklist dari Gartner:

Tabel 4.2 **Mobile Security Checklist Xiomi note 8**

Kategori	Deskripsi	Checklist
Device Security	Full disk encryption diaktifkan	-
	OS dan App diperbarui secara otomatis	-
	Otentikasi multi faktor atau biometrik digunakan	-
	Remote wipe tersedia dan diuji secara berkala	-
	Mobile device management diterapkan	-
Application Security	Aplikasi diuji dengan penetration testing	-
	Menggunakan RASP (Runtime Application Self-Protection)	-
	API hanya menerima request dari sumber terpercaya	√
	Aplikasi hanya bisa diinstal dari source resources	√
	App sandboxing diterapkan untuk membatasi akses aplikasi ke data	-
Network Security	Perangkat menggunakan VPN untuk akses data perusahaan	-
	TLS digunakan untuk semua komunikasi data	√
	Zero Trust Network Access diterapkan	-
	IDS/IPS digunakan untuk mendeteksi ancaman jaringan	-
	Penggunaan wifi publik dibatasi	-
Data Security	Data security	√
Identity & Access Management	Semua akses ke aplikasi membutuhkan MFA	-
	SSO diterapkan untuk aplikasi berbasis cloud	√
	Behavioral analytics digunakan untuk mendeteksi anomali	-
	ZTP diterapkan	-
	Penghapusan akun pengguna yang tidak aktif dalam jangka waktu tertentu	-

Xiaomi Redmi Note 8 tidak sepenuhnya memenuhi standar Gartner untuk keamanan mobile. Meskipun memiliki enkripsi, Verified Boot, dan kontrol aplikasi yang baik, perangkat ini gagal memenuhi persyaratan penting seperti pembaruan keamanan jangka panjang, penghapusan bloatware, dan keamanan Face Unlock.

Xiomi Note 8 dapat dikategorikan sebagai keamanan dengan Level 2 – Managed,

pada level ini biasanya mencakup enkripsi data, perlindungan terhadap aplikasi dan malware, serta beberapa mekanisme pengamanan untuk perlindungan data pribadi dan komunikasi, tetapi mungkin tidak mencakup fitur canggih seperti manajemen perangkat jarak jauh atau enkripsi end-to-end tingkat lanjut. Berikut adalah parameter keamanan level 2 yaitu :

1. Enkripsi perangkat: Melindungi data pribadi agar tidak dapat diakses oleh pihak yang tidak berwenang. Xiomi Note 8 menggunakan MIUI dengan metode enkripsi AES 256.
2. Pemindai sidik jari / pengenalan wajah: Menawarkan otentikasi biometrik untuk membuka kunci perangkat.
3. Proteksi malware dan aplikasi berbahaya: Menggunakan perangkat lunak keamanan untuk mendeteksi aplikasi berbahaya dan memberikan perlindungan dasar.
4. Kontrol izin aplikasi: Memungkinkan pengguna untuk mengontrol izin aplikasi, seperti akses ke lokasi, kamera, dan data pribadi lainnya.

Xiomi Note 8 dikategorikan dalam Keamanan Mobile Level 2 memberikan perlindungan yang cukup baik untuk pengguna sehari-hari, terutama untuk melindungi data pribadi dan komunikasi dasar. Perangkat ini mencakup fitur enkripsi, perlindungan aplikasi, serta autentikasi biometrik, namun mungkin tidak memiliki beberapa fitur canggih yang ditemukan pada Motorola Lex 11.

4.4.3. Perbandingan Analisis Hasil Akuisisi

Setelah dilakukan perbandingan level keamanan antara perangkat Motorola Lex 11 dan Xiomi Note 8, penulis melakukan perbandingan analisa hasil akuisisi. Dari kedua perangkat yaitu Motorola lex11 dan Xiomi note 8 didapatkan sebuah tabel 4.3 yang membahas perbandingan level kedua perangkat tersebut. Adapun tabelnya sebagai berikut:

Tabel 4.3. Analisa hasil akuisisi Motorola Lex 11 dan Xiomi Note 8

Karakteristik Umum	HP Motorola Lex	Xiomi Note 8
Full disk encryption	FDE secara default aktif	Terdapat FDE hanya saja tidak diatur secara default
Security patch	Aktif dan reguler, dikelola secara ketat oleh Motorola Solutions. Biasanya sudah masuk dalam compliance (FIPS/NIAP).	Tergantung region & update MIUI. Patch sering tertunda. Kadang tidak konsisten setelah 2–3 tahun penggunaan
Sandbox Aplikasi	Terdapat sandbox aplikasi. Menggunakan mekanisme sandbox Android dan diperkuat dengan kebijakan keamanan enterprise.	Terdapat sandbox aplikasi. Android memiliki sandbox antar-aplikasi, tetapi tidak diperkuat secara enterprise.
Mobile device management	Didukung & aktif secara default (Motorola config tool + Android Enterprise).	Tidak tersedia secara default. Hanya bisa diaktifkan manual untuk bisnis.
Sertifikasi Keamanan	FIPS 140-2 Level 3, MIL-STD-810G	Tidak memiliki sertifikasi keamanan.
TEE (Trusted Execution Environment)	Ada. TEE aktif, digunakan untuk enkripsi dan otentikasi. Chipset Qualcomm mendukung TEE (TrustZone).	Ada. Qualcomm Snapdragon 665 memiliki TrustZone. Tapi implementasi terbatas.
Verified Boot	Aktif. Verified Boot melalui Android Verified Boot (AVB) dengan sertifikasi.	Aktif (Android 10 ke atas). Tapi mudah dimodifikasi jika bootloader di-unlock.
2FA (Two-Factor Authentication)	Didukung. Biasanya dikombinasikan dengan sistem MDM (misal: PIN + token/PIV).	Tersedia terbatas melalui aplikasi (Google Authenticator). Tidak terintegrasi sistem.

Dari tabel 4.3 kita dapat menyimpulkan bahwa Motorola LEX L11 secara arsitektural dan administratif memenuhi persyaratan keamanan Level 4+ dan memiliki sertifikasi resmi internasional (FIPS, EAL4+) serta dukungan audit, menjadikannya sesuai untuk lingkungan militer dan forensik. Sementara itu, Xiaomi Redmi Note 8 hanya memenuhi keamanan dasar Android dan tidak memiliki sertifikasi resmi atau mekanisme audit, menjadikannya kurang cocok untuk komunikasi kritikal atau penyimpanan data sensitif. Lalu, untuk mengetahu berada di keamanan level berapa xiomi note 8, perlu dilakukan analisa level keamanan menggunakan kriteria Gartner and Research.

Tabel 4.4. Perbandingan Motorola Lex 11 dan Xiomi Note 8

LEVEL	VARIABLE	MOTOROLA LEX11	XIOMI NOTE 8
1.	Hanya menggunakan lock screen dan root tersbuka	Tidak	Tidak
2.	Menggunakan lock dengan enkripsi tanpa menggunakan MDM	Tidak	Ya
3.	Ada FDE, patch aktif, sandbox aplikasi namun tdk ada otentikasi 2 faktor	tidak	Tidak
4.	MDM aktif, TEE, Verified Boot, 2FA	Ya	Tidak
5.	Level 4 + sertifikasi resmi (EAL4+, FIPS 140-2) + audit ketat	Tidak ada	Tidak ada

Dari tabel 4.4 dapat disimpulkan bahwa level keamanan berdasarkan standar gartner dan research, Motorola Lex11 menempati **level 4** sedangkan xiomi note 8 menempati **level 2**. Hal ini membuktikan bahwa tidak ditemukanya artefak dari wave mobile comunicator disebabkan adanya akses kontrol keamanan menggunakan multi device management, admin memberi batasan akses kepada user perangkat motorola lex11 untuk mengakses root. Admin server memegang kontrol pernuh terhadap masing – masing perangkat sehingga bisa dikatakan motorola lex11 cukup aman digunakan di daerah kritis. Apabila ada ancaman pada komunikasi lex11 maka admin server akan langsung memutus koneksi perangkat bahkan bisa sampai mematiakan perangat dengan paksa.

BAB 5

Kesimpulan dan Saran

5.1. Kesimpulan

Dari penelitian yang telah dilakukan dapat disimpulkan bahwa akuisisi perangkat motorola lex11 dan xiomi note 8 menghasilkan artefak akuisisi yang berbeda. Proses imaging pada xiomi note 8 menghasilakan artefak lebih banyak dibandingkan pada motorola lex11. Hal ini dikarenakan motorola menerapkan sistem multi device management yang mana untuk mendapatkan akses root harus melakukan prosedur yang terdapat pada server utama. Berbeda dengan xiomi note 8 yang tidak menerapkan MDM, artefak yang didapat bisa lebih maksimal. Motorola LEX L11 menggunakan Android yang telah dimodifikasi dan dikunci, dengan kontrol yang ketat terhadap aplikasi pihak ketiga dan sistem update.

Berdasarkan hasil penelitian dan analisis yang telah dilakukan disimpulkan bahwa Motorola LEX L11 memiliki keunggulan signifikan dalam hal keamanan data, ketahanan sistem, dan perlindungan terhadap intersepsi komunikasi. Motorola LEX L11 didesain khusus untuk lingkungan operasional kritikal seperti TNI dan POLRI, dengan fitur-fitur keamanan tingkat tinggi, termasuk sistem operasi yang dikunci, dukungan enkripsi end-to-end, dan integrasi dengan jaringan komunikasi tertutup.

Di sisi lain, Xiaomi Note 8 yang merupakan perangkat konsumen umum tidak dirancang dengan pertimbangan keamanan operasional yang tinggi. Sistem operasinya yang terbuka terhadap aplikasi pihak ketiga, praktik pengumpulan data pengguna, serta kurangnya pengamanan sistemik menjadikannya kurang ideal digunakan dalam lingkungan yang menuntut perlindungan informasi yang ketat.

Dari perspektif digital forensik, Motorola LEX L11 menawarkan keunggulan dalam hal pencarian bukti digital karena fitur-fitur keamanannya mendukung kontrol integritas data dan dokumentasi chain of custody. Namun, hal ini juga menuntut keterampilan teknis dan prosedural yang lebih tinggi bagi investigator dalam proses akuisisi data forensik. Sebaliknya, Xiaomi Note 8 relatif lebih mudah untuk diakses dan diekstraksi datanya, namun rawan terhadap manipulasi bukti dan kurang andal untuk digunakan sebagai sumber bukti yang valid dalam proses penyidikan resmi.

Oleh karena itu, Motorola LEX L11 dapat direkomendasikan sebagai perangkat komunikasi yang lebih aman untuk digunakan dalam konteks institusi pertahanan dan

keamanan.

Dari kesimpulan diatas penulis berharap penelitian ini dapat dijadikan acuan dalam pengadaan barang komunikasi selanjutnya, disamping itu apabila ada sebuah kejadian diwilayah kritis medan tugas, dengan penelitian ini, tim investikasi dapat menjadikan penelitian ini menjadi acuan kerja dalam menganalisa penyelesaian kasus.

5.2. Saran

Adapun saran yang penulis untuk pengembangan penelitian ini lebih baik yaitu :

1. Pada penelitian selanjutnya dapat menentukan *tools* terbaik yang dapat melakukan akuisisi pada ponsel Hybrid.
2. Pada penelitian selanjutnya dapat mengambil referensi perangkat lain biasa digunakan sebagai media komunikasi pada bidang militer dengan pertimbangan perbedaan harga dan kualitas perangkat.

Daftar Pustaka

Hariyadi, Dedy;Yunia Pasa, I. (2018). *IDENTIFIKASI BARANG BUKTI DIGITAL PADA APLIKASI MIVIDEO MENGGUNAKAN METODE LIVE FORENSICS. 2018*(November), 166–172.

Haryadi, D., & Supriyono, A. R. (2017). Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI ISO/IEC 27037:2014. *Telematika*,*14*(01), 62–67. https://doi.org/10.31315/telematika.v14i01.1967

Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. *International Journal of Scientific & Engineering Research*, *4*(10), 1048–1056.

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij). *Elinvo (Electronics, Informatics,and Vocational Education)*,*3*(1),70–82. https://doi.org/10.21831/elinvo.v3i1.19308

Riadi, I., Yudhana, A., & Barra, M. Al. (2021). Forensik Mobile pada Layanan Media Sosial LinkedIn. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *6*(1), 9–20. https://doi.org/10.14421/jiska.2021.61-02

Sirojjam, M., Andik, I., & Mujib, R. (2021). Analisis kinerja aplikasi forensik open-source pada ponsel cerdas berbasis android dalam mendapatkan bukti digital. *JII: Jurnal Inovasi Informatika Universitas Pradita*, *6*(September 2021), 13.

A, Ramadhan R., et al. *Digital Forensics: Acquisition and Analysis on CCTV Digital Evidence using Static Forensic Method based on ISO /IEC 27037:2014*, 2020, pp. 85–89.

M, Riskiyadi. "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime." *Cyber Secur. dan Forensik Digit*, vol. 3, 2020, pp. 12-21.

M, Sirojjam, et al. "Analisis kinerja aplikasi forensik open-source pada ponsel cerdas berbasis android dalam mendapatkan bukti digital." *JII J. Inov. Inform. Univ. Pradita*, vol. 6, 2021, p. 13.

Riyadi, Imam, et al. "Electronics, Informatics,." *Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)*, vol. 3, 2018,pp. 70- 82.

Riyadi, Imam, et al. "Jurnal Teknik Informatika dan Sistem Informasi." *Akuisisi ukti Digital*

Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (, vol. 4, no. akuisisi instagram,2018,pp.2443-2210.*http://dx.doi.org/10.28932/jutisi.v4i2.769.*

S, Madiyanto, et al. "J. Rekayasa Sist. Ind.,." *Mobile Forensics Investigation Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS,*, vol. 4, 2017, 93–98,. Setyawan, Muhammad Rizki, et al. "SYSTEMIC : Information System and Informatics Journal." *Akuisisi Data Pada Skype Messenger Menggunakan Metode National*

Institute Of Justice, vol. Vol 5 No 2, no. Akuisisi Skype, 2019, pp. 13-18.

Wirara, Ayubi, et al. "UII Library." *Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan "WhatsApp"*, vol. 26, no. akuisisi pada Aplikasi WhatsApp, 2020, pp. 66-67. *teknoin*.

Yudhana, Anton, et al. "Jurnal Ilmiah Kursor." *IDENTIFICATION OF DIGITAL EVIDENCE FACEBOOK MESSENGER ON MOBILE PHONE WITH NATIONAL INSTITUTE OF*, vol. vol 9, no. akuisisi facebook, 2018, pp. 0216 – 0544.

Ahmed, S., Rahman, F., & Khan, M. (2021). *Challenges and opportunities in mobile forensics for military-grade communication systems*. Journal of Cybersecurity and Information Management, 9(2), 1–10. Motorola Solutions. (2023). *LEX L11 Mission-Critical LTE Device*. Retrieved from https://www.motorolasolutions.com/en_us/products/lte-user-devices/lexl11.html

Quick, D., & Choo, K. K. R. (2018). Pervasive challenges in digital forensic readiness. *Digital Investigation*, 24, 14–22. https://doi.org/10.1016/j.diin.2018.01.002