ANALISIS FORENSIK KASUS PORNOGRAFI PADA *WHATSAPP GROUP* BERBASIS ANDROID DENGAN METODE *NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY*

SKRIPSI

Disusun untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana

Disusun Oleh:

Arjuna Dwi Yusufi Suminto
2000018334

PROGRAM STUDI S1 INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS AHMAD DAHLAN

2025

LEMBAR PERSETUJUAN PEMBIMBING

SKRIPSI

ANALISIS FORENSIK KASUS PORNOGRAFI PADA WHATSAPP GROUP BERBASIS ANDROID DENGAN METODE NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY

Dipersiapkan dan disusun oleh:

Arjuna Dwi Yusufi Suminto
2000018334

Program Studi S1 Informatika
Fakultas Teknologi Industri
Universitas Ahmad Dahlan

Telah disetujui oleh:

Pembimbing

Eko Aribowo, S.T., M.Kom.

NIPM. 1970020620050110001

LEMBAR PENGESAHAN

SKRIPSI

ANALISIS FORENSIK KASUS PORNOGRAFI PADA WHATSAPP GROUP BERBASIS ANDROID DENGAN METODE NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY

Dipersiapkan dan disusun oleh:

Arjuna Dwi Yusufi Suminto
2000018334

Telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Januari 2025
dan dinyatakan telah memenuhi syarat

Susunan Dewan Penguji

Ketua	**: Eko Aribowo, S.T., M.Kom.**	.....
Penguji 1	**: Ir. Nuril Anwar, S.T., M.Kom.**	.....
Penguji 2	**: Prof. Dr. Ir. Imam Riadi, M.kom.**	.....

Yogyakarta, 20 Februari 2025
Dekan Fakultas Teknologi Industri
Universitas Ahmad Dahlan

Prof. Dr. Ir. Siti Jamilatun, M.T
NIPM. 19660812 199601 001 0784324

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan dibawah ini:

Nama : Arjuna Dwi Yusufi Suminto

NIM : 2000018334

Email : arjuna2000018334@webmail.uad.ac.id

Program Studi : S1 Informatika

Fakultas : Teknologi Industri

Judul Skripsi : Analalisis Forensik Kasus Pornografi Pada Whatsapp Group Berbasis Android Dengan Metode National Institute of Standard and Technology

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah mendapatkan gelar kesarjanaan baik di Universitas Ahmad Dahlan maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian dan implementasi saya sendiri, tanpa bantuan pihak lain kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan di setujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Ahmad Dahlan.

Yogyakarta, 24 Januari 2025 Yang Menyatakan

(Arjuna Dwi Yusufi Suminto)

LEMBAR PERNYATAAN KEASLIAN

SURAT PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Arjuna Dwi Yusufi Suminto

NIM : 2000018334

Prodi : Informatika

Judul TA/Skripsi : Analisis Forensik Kasus Pornografi Pada Whatsapp Group Berbasis Android Dengan Metode *National Institute of Standards and Technology*

Dengan ini saya menyatakan bahwa Laporan Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar Ahli Madya/Kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 24 Januari 2025

Mengetahui,
Dosen Pembimbing

Eko Aribowo, S.T., M.Kom.
NIPM. 1970020620050110001

Yang menyatakan,

Arjuna Dwi Yusufi Suminto
2000018334

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : Arjuna Dwi Yusufi Suminto

NIM : 2000018334

Email : arjuna2000018334@webmail.uad.ac.id

Fakultas : Teknologi Industri

Program Studi : S1 Informatika

Judul tugas akhir : Analisis Forensik Kasus Pornografi Pada Whatsapp Group Berbasis Android Dengan Metode National Institute of Standard and Technology

Dengan ini saya menyerahkan hak *sepenuhnya* kepada Perpustakaan Universitas Ahmad Dahlan untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut

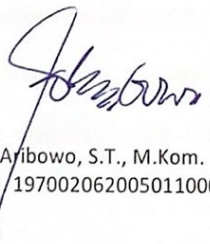
Saya (**mengijinkan/~~tidak mengijinkan~~**) karya tersebut diunggah ke dalam Repository Perpustakaan Universitas Ahmad Dahlan.

Demikian pernyataan ini saya buat dengan sebenarnya.

Yogyakarta, 24 Januari 2025

Arjuna Dwi Yusufi Suminto

Mengetahui, Pembimbing**



Eko Aribowo, S.T., M.Kom.
NIPM/ 1970020620050110001

Ket:
*coret salah satu
**jika diijinkan TA dipublish maka ditandatangani dosen pembimbing dan mahasiswa

KATA PENGANTAR

Puji syukur kehadirat Allah SWT. Yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaaikan skripsi ini dengan lancar. Shalawat serta salam senantiasa tercurahkan kepada junjungan kita Nabi Muhammad SAW, beserta keluarga, sahabat, dan pengikutnya hingga akhir zaman.

Skripsi ini berjudul Analisis Forensik Kasus Pornografi Pada Whatsapp Group Berbasis Android Dengan Metode *National Institute of Standards and Technology*, diajukan untuk memenuhi salah Satu syarat dalam mencapai gelar S.Kom. pada program studi S1 Informatika di Universitas Ahmad Dahlan. Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat banyak kekurangan dan keterbatasan, baik dari segi isi maupun metodologinya. Oleh karena itu, penulis dengan penuh kerendahan hati menerima kritik dan saran yang membangun dari berbagai pihak demi perbaikan skripsi ini di masa yang akan datang.

Penulis ingin mengucapkan terimakasih yang sebesar – besarnya kepada :

1. Bapak Suminto dan Ibu Nur Afiah (almh) selaku orang tua saya yang telah membesarkan dan mendidik saya dan selalu mendukung, serta mendoakan saya untuk terus tumbuh menjadi orang yang lebih baik setiap harinya, dan juga yang selalu menjadi motivasi saya untuk menjadi orang sukses.
2. Mba Meydiana Larassati Suminto selaku Saudara kandung saya yang selalu menguatkan dan banyak memberikan banyak pelajaran berarti buat saya.
3. Ibu Tri Iswati selaku Ibu sambung saya yang selalu mendukung dan memberikan motivasi kepada saya.
4. Dosen Pembimbing skripsi Bapak Eko Aribowo, S.T., M.Kom. dan Dosen Pembimbing Akademik Bapak Dinan Yulianto, S.T., M.Kom., terimakasih atas waktu, arahan, dan

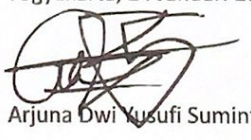
bimbingan yang telah diberikan agar penulis dapat menyelesaikan skripsi ini sehingga penulis dapat menyelesaikan penelitian ini.

5. Bapak Prof. Dr. Muchlas, M.T. selaku Rektor Universitas Ahmad Dahlan.
6. Ibu Prof. Dr. Ir. Siti Jamiltun, M.T. selaku Dekan Fakultas Teknologi Industri.
7. Bapak Dr. Murinto, S.Si., M.Kom. selaku ketua Program studi S1 Informatika Universitas Ahmad Dahlan.
8. Serta seluruh Dosen dan Staf Program Studi S1 Informatika Universitas Ahmad Dahlan.
9. Untuk Sahabat – sahabat saya KONS grup (tidak perlu saya sebutkan satu persatu karena banyak), yang telah memberikan semangat, hiburan, canda tawa dan selalu ada buat saya. Semoga kita semua akan menjadi anak muda yang sukses nantinya dan bisa mengendalikan dan menaikan perekonomian Indonesia.
10. Untuk seluruh teman – teman saya di kampung halaman yang selalu memberikan hangatnya tempat pulang, dan selalu ada buat saya.
11. Untuk seluruh teman – teman saya di perkuliahan, magang, KKN, dan sebagainya terimaksih atas doa dan dukungan kalian.
12. Untuk semua pihak yang telah membantu penulis yang tidak bisa disebutkan satu persatu terimaksih atas doa serta dukungan yang sangat berharga bagi saya.

Semoga Allah SWT. Memberikan balasan yang berlimpah kepada semuanya yang telah membantu dalam proses penulisan skripsi ini. Penulis berharap skripsi ini dapat memberikan manfaat khususnya bagi pennulis dan umumnya bagi pembaca. Dengan kerendahan hati penulis sangat menerima kritik dan sran yang membangun unutk penyempurnaan skripsi ini.

MOTO *" Jangan pernah merasa puas dengan apa yang kita capai pada hari ini "*

Yogyakarta, 24 Januari 2025



Arjuna Dwi Yusufi Suminto

DAFTAR ISI

COVER i
LEMBAR PERSETUJUAN PEMBIMBING ii
LEMBAR PENGESAHAN iii
LEMBAR PERNYATAAN KEASLIAN iv
KATA PENGANTAR v
DAFTAR ISI vii
DAFTAR GAMBAR ix
DAFTAR TABEL x
DAFTAR LAMPIRAN xi
ABSTRAK xii
BAB I. PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Batasan Masalah 3
1.3 Rumusan Masalah 3
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 4
BAB II. Tinjauan Pustaka 5
2.1 Kajian Terdahulu 5
2.2 Landasan Teori 10
2.2.1 Digital Forensik 10
2.2.2 Pornografi 11
2.2.3 Mobile Forensic 11
2.2.4 National Institute of Standards and Technology 12
2.2.5 Whatsapp 13
2.2.6 Android 14
2.2.7 MOBILedit Forensic 14
2.2.8 Magnet AXIOM 14
2.2.9 Belkasoft Evidence Center 15
BAB III. METODOLOGI PENELITIAN 16
3.1 Objek Penelitian 16
3.2 Metode Pengumpulan Data 16
3.3 Alat dan Bahan Penelitian 16

3.3.1 Perangkat Keras (Hardware) 16
3.3.2 Perangkat Lunak (Software) 17
3.4 Tahapan Penelitian 17
3.4.1 Collection 17
3.4.2 Examination 18
3.4.3 Analysis 18
3.4.4 Reporting 18
3.5 Skenario Penelitian 18
3.5.1 Pre Insiden 19
3.5.2 Insiden 19
3.5.3 Pasca Insiden 20
BAB IV. HASIL DAN PEMBAHASAN 22
4.1 Collection 22
4.2 Examination 26
4.3 Analysis 44
4.4 Reporting 47
BAB V. KESIMPULAN DAN SARAN 51
5.1 Kesimpulan 51
5.2 Saran 51
DAFTAR PUSTAKA 53
LAMPIRAN 56

DAFTAR GAMBAR

Gambar 2.1 Tahapan Digital Forensik [16] 11
Gambar 2.2 Tahapan Metode NIST [20] 12
Gambar 3.1 Skenario Pre Insiden 19
Gambar 3.2 Skenario Insiden 20
Gambar 3.3 Skenario Pasca Insiden 21
Gambar 4.1 Airplane Mode Diaktifkan 24
Gambar 4.2 Mengaktifkan Developer options 25
Gambar 4.3 Mengaktifkan USB Debagging 26
Gambar 4.4 Tampilan MOBILEdit Yang Berhasil Mendeteksi Smartphone Pelaku 26
Gambar 4.5 Tampilan Plihan Data Yang diekstraksi 27
Gambar 4.6 Tampilan Hasil Ekstraksi Barang Bukti dengan MOBILedit 28
Gambar 4.7 Tampilan Folder Hasil Akuisisi 29
Gambar 4.8 File Database 29
Gambar 4.9 Percakapan yang terhapus 30
Gambar 4.10 Hasil Konversi TimeStamp 31
Gambar 4.11 Percakapan yang terhapus 31
Gambar 4.12 Hasil Konversi Timestamp 32
Gambar 4.13 Tampilan Screenshoot Chat Dari Smartphone korban Sebelum Terhapus 32
Gambar 4.14 Tampilan Screenshoot Chat Dari Smartphone korban Sebelum Terhapus 33
Gambar 4.15 Tampilan Screenshoot Chat Dari Smartphone korban Sebelum Terhapus 34
Gambar 4.16 Tampilan Screenshoot Video Pada Smartphone Korban 34
Gambar 4.17 Tampilan Chat Yang Pelaku Hapus 35
Gambar 4.18 Tampilan Magnt AXIOM 36
Gambar 4.19 Tampilan Opsi Sistem Operasi 36
Gambar 4.20 Tampilan Opsi Akuisisi 37
Gambar 4.21 Tampilan Smartphone Terhubung Dengan Magnet AXIOM 38
Gambar 4.22 Tampilan Proses Akuisisi 38
Gambar 4.23 Tampilan Durasi Proses Akuisisi 39
Gambar 4.24 Tampilan Hasil Proses Akuisisi 39
Gambar 4.25 Tampilan Report Detail Akun Pelaku 40
Gambar 4.26 Tampilan Hasil Temuan Video 41
Gambar 4.27 Tampilan Priview Video 41
Gambar 4.28 Tampilan Video Yang Berhasil Terakuisis 42
Gambar 4.29 Tampilan Informasi Detai Video 42
Gambar 4.30 Tampilan Asal dari lokasi Video 43
Gambar 4.31 Tampilan Lokasi File Video 44

DAFTAR TABEL

Tabel 2.1 Rangkuman Hasil Kajian Penelitian 7
Tabel 3.1 Perangkat Keras (Harware)……17
Tabel 3.2 Perangkat Lunak (Software) 17
Tabel 4.1 Tabel Barang Bukti……23
Tabel 4.2 Tabel Spesifikasi Smartphone Pelaku 23
Tabel 4.3 Tabel Spesifikasi Smartphone Korban 24
Tabel 4.4 Tabel Validasi Barang Bukti 46
Tabel 4.5 Tabel Hasil Akuisisi Artefak..... 49

DAFTAR LAMPIRAN

Lampiran 1. Bukti Percakapan Yang Terakuisisi 56
Lampiran 2. Bukti Video Yang Terakuisisi..... 57
Lampiran 3. Bukti Percakapan Pada Smartphone Korban 58

ABSTRAK

Pesatnya perkembangan teknologi telah menjadi aspek utama yang tidak akan bisa terpisahkan dari kehidupan manusia. *Whatsapp* menjadi salah satu bentuk kemajuan dari teknologi yang pesat ini. *Whatsapp* mempunyai fitur *Group Chat*, pengiriman pesan, telepon sura, *video call*, pesan suara dan pengiriman *file*. Jumlah dari pengguna *Whatsapp* tentunya akan terus meningkat, dan banyaknya peningkatan ini memungkinkan terjadinya tindakan kejahatan pornografi. Penelitian ini bertujuan untuk mengidentifikasi dan mengakuisisi bukti digital yang ditemukan melalui analisis forensik digital terkait kasus pornografi pada *WhatsApp Group* di *smartphone*.

Penelitian ini melakukan rekonstruksi dengan kasus pornografi pada *whatsapp group*. Metode *National Institute of Standard and Technology* (NIST) digunakan dalam rekonstruksi kasus dalam penelitian. NIST memiliki empat tahapan dalam menyelasaikan permasalahan, pertama adalah *Collection* (pengumpulan data), *Examination* (Pengecekan bukti digital), *Analysis*, dan diakhiri dengan tahap *Reporting* (laporan hasil analisis). Metode ini dapat membantu dalam jalannya proses identifikasi barang bukti yang berhasil ditemukan dari rekonstruksi skenario kasus pornografi. Berupa pesan percakapan dan konten video pornografi yang terhapus pada *whatsapp group*.

Hasil dari penelitian telah dilakukan rekonstruksi kasus pornografi pada *whatsapp group* dan bisa dibuktikan kebenarannya. Barang bukti yang ditemukan adalah *smartphone Xiaomi redmi 4A* yang didalamnya terdapat pesan percakapan dan video pornografi. Dengan memanfaatkan 3 *tools* forensik, yaitu *MOBILedit Forensic Express*, *Belkasoft Evidence Center*, dan *Magnet AXIOM*. Hasil yang pulihkan adalah 2 dari 14 bukti percapakan yang terhapus pada *whatsapp group*, dan mampu memulihkan video pornografi yang terhapus, serta mampu mengidentifikasi dan menganalisis bukti digital dari investigasi forensik kasus pronografi pada *whatsapp group* yang sesuai dengan metode NIST.

Kata Kunci : Barang Bukti, Forensik Digital, *Mobile Forensic*, NIST, Pornografi, *Whatsapp*

BAB I. PENDAHULUAN

1.1 Latar Belakang Masalah

Salah satu kebutuhan pokok manusia adalah berinteraksi dan berkomunikasi antar sesama manusia. Pesatnya perkembangan teknologi telah menjadi aspek pokok yang tidak dapat dipisah dari kehidupan manusia [1]. *Whatsapp* adalah salah satu bentuk kemajuan dari teknologi yang pesat ini. *Whatsapp* menjadi satu dari banyak aplikasi yang sangat digandrungi yang bisa digunakan di perangkat seluler maupun diperangkat komputer. *WhatsApp* mempunyai beragam fitur seperti Group Chat, telepon suara, pengiriman pesan, video call, pesan suara ,dan pengiriman file[2].

Whatsapp digunakan 1,5 miliar lebih orang dari 180 negara menggunakan *dan* terus terkoneksi dengan sesama pengguna dimanapun berada [3]. Berdasarkan survei, Masyarakat Indonesia menjadi salah satu pengguna *WhatsApp* yang sangat aktif hingga mencapai 83% [4]. Jumlah dari pengguna *Whatsapp* tentunya akan terus meningkat, dan banyaknya peningkatan pengguna ini memungkinkan dijadikan sebagai media untuk melakukan tindakan kejahatan, Salah satunya adalah *pornografi* [2]. Menurut penelitan Dewi didapat data sekitar 94,6% responden pernah mengirim video porno di *WhatApp Group* [5]. Bahkan terdapat *WhatsApp Group* yang Khusus dibuat dengan sengaja untuk saling bertukar atau mengirim video dan hal-hal yang berkaitan dengan *pornografi* [4]. *Whatsapp* sering digunakan sebagai media kejahatan pronografi tentunya dikarenakan *Whatsapp* memiliki fitur hapus pesan. Setelah melakukan kejahatan pelaku dengan mudahnya menghapus bukti digital yang berupa konten *pornografi* [6].

Sesuatu dapat dikalsifikasikan sebagai bentuk pornografi adalah sebagai mana yang tercantum dalam Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang pornografi pada Bab I pasal 1 ayat (1) yang berbunyi “Pornografi adalah gambar, sketsa, ilustrasi, foto,

tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lainnya melalui berbagai bentuk media komunikasi dan/atau pertunjukan dimuka umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakat". Kemudian juga terdapat pada Bab II pasal 4 ayat (1) tentang larangan dan pembatasan "melarang setiap orang memproduksi, membuat, memperbanyak, menggandakan, memperluaskan, meyiarkan, mengimpor, mengekpor, atau menyediakan pornografi yang secara eksplisit memuat: a. persenggamaan, termasuk persenggamaan yang menyimpang; b. kekerasan seksual; c. masturbasi atau onani; d. keterlanjangan atau tampilan yang mengesankan keterlanjangan; e. alat kelamin; atau f. pornografi anak".

Investigasi *forensik digital* tentunya sangat berperan penting dalam kasus *pornografi* pada *WhatsApp Group* dengan menggunakan metode-metode investigasi *forensik digital*. Adapun bebrapa metode yang sering digunakan adalah *National of Justice* (NIJ), kerangka kerja dan urutan kerja yang terstruktir dapat digunakan sebagai dasar pada permasalahan penelitian. Metode ini memiliki 5 langkah kerja. Dimulai dari identifikasi, pengumpulan, pemeriksaan, analisis, dan terakhir pelaporan [7]. Metode lainnya yang biasa digunakan adalah *Digital Forensic Research Workshop* (DFRWS). Metode ini membantu dalam memperoleh barang bukti dan merekam informasi yang dibuthkan unutk kemudian dikumpulkan menggunakan data yang berpusat. Metode DFRWS memiliki 6 tahapan, dimulai dengan *identification, preservation, collection, examination, analysis, dan presentation*[8] .Penelitian ini menerapkan metode *National Intitute of Standard and Technology* (NIST) untuk mengembalikan bukti digital terhapus. Dipilihnya Metode NIST karena standar yang dianjurkan dan digunakan sebagai petunjuk dalam melakukan investigasi digital forensik. Metode NIST dipilih karena lebih terstruktur dalam hal penerapan praktis dibandingkan dengan metode lainnya. Tujuan digunakannya metode NIST guna membantu mempermudah investigator dalam pekerjaannya untuk mengetahui alur penelitian secara lebih tersrtuktur, olehkarena itu dapat digunakan

sebagai pedoman dalam menyelesaikan semua persoalan yang ada [9]. NIST memiliki empat tahapan dalam menyelasaikan permasalahan, pertama adalah *Collection* (pengumpulan data), *Examination* (Pemeriksaan bukti digital), *Analysis*, dan tahap terakhir adalah *Reporting* (laporan hasil analisis) [10]. Penelitian ini bertujuan guna mengidentifikasi dan mengakuisisi bukti digital apa saja yang dapat ditemukan melalui analisis forensik digiatal terkait kasus *pornografi* pada *WhatsApp Group* yang berdasarkan skenario kasus akan menggunakan sebuah *smart phone*. Untuk penerapan investigasi *forensik digital* dan metode *National Institute of Standard and Technologi* (NIST) dapat memberikan kontribusi dalam menganalisis barang bukti kasus *pornografi* yang terdapat pada *WhatsApp Group*.

1.2 Batasan Masalah

Untuk menghindari pelebaran masalah yang dijabarkan, batasan dari masalah ini adalah :

1. Fokus dari penelitian ini hanya pada investigasi terhadap kasus *pornografi* pada *WhatsApp Group*.
2. Penelitian ini hanya menggunakan data yang didapat dari perangkat yang terkait dengan *WhatsApp Group*.
3. Data yang diperoleh dari penelitian ini berupa gambar, video, dan file-file yang terindikasi mengandung konten *pornografi* di *WhatsApp Group*.
4. Penelitian ini tidak membahas penggunaan aplikasi lain selain *WhatsApp* untuk kasus *pornografi*, maupun aspek hukum yang terkait dalam tindakan kasus *pornografi*.
5. Penelitian ini menggunakan *Smartphone andorid* yang sudah dilakukan proses *root.*

1.3 Rumusan Masalah

Rumusan masalah yang akan menjadi pembahasan penelitian ini adalah :

1. Bagaimana mengidentifikasi hasil dari akuisisi bukti digital yang diperoleh terkait konten pornografi pada *Whatsapp Group* ?
2. Bagaimana penerapan metode NIST dalam proses investigasi forensik digital untuk mengidentifikasi dan menganalisis bukti digital pornografi pada *Whatsapp Group*?

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk :

1. Mengidentifikasi dan memperoleh bukti digital yang ditemukan dalam kasus pornografi pada *Whatsapp Group*.
2. Menerapkan metode NIST dalam proses investigasi forensik digital guna mengidentifikasi, dan menganalisis bukti digital pada *Whatsapp Group*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Untuk mempermudah pihak berwenang dalam mendapatkan barang bukti
2. Mengidentifikasi data yang ditemukan dalam kasus *pornografi* pada *WhatsApp Group*

BAB II. Tinjauan Pustaka

2.1 Kajian Terdahulu

Referensi yang bakaitan pada penelitian ini. maka penelitian ini melampirkan beberapa kajian terdahulu yang mengacu pada tema penelitian yang akan dilakukan, referensi sebagai berikut :

Nadia Ayu Isroh Maniar, dkk[11] tentang "Implementasi Mobile Forensic Pada Aplikasi Michat dan Telegram Dengan Framework NIST 800-101", penelitian ini meliputi penerapan teknik forensik National Institute of Standards and technology Special Publication 800-101 dan menggunakan *tools forensics* FTK Imager dan MOBILedit Forensic Express. penelitian menunjukan bahwa barang bukti digital lebih sedikit ditemukan pada MOBILedit Forensic Express, dibandingkan FTK Imager dan pemulihan bukti digital pada MICHat mendapatkan lebih banyak bukti digital dibandingkan dengan aplikasi Telegram. Pesaan percakapan, *voice note* ,video, dan gambar merupakan bukri digital yang berhasil terakuisisi.[11]

Ragmat Vovrianda Dasmen, dkk[12] tentang "Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Insititute of Standard and Technology SP 800-86" , Penyelidikan bukti digital dilakukan dengan menerapkan salah satu metode yaitu National Institute of Standard and Technology SP 800-86 (NIST SP 800-86) melalui tahapan mulai dari pengumpulan barang bukti, analisis, pencarian data, dan pemulihan data yang ditemukan, hingga validasi berkas dengan sumber barang bukti flashdisk digital menggunakan tools forensik Autopsy. Hasil penelitian ini menunjukkan bahwa pemanfaatan Autopsy mampu menganalisis dan mengembalikan barang bukti digital yang sebelumnya tersimpan di flashdisk dengan tingkat keberhasilan 100%, 4 berkas dengan ekstensi PNG dan 1 berkas dengan ekstensi MP4 merupakan data yang terpulihkan sesuai dengan skenario kasus yang dirancang.[12]

Desti Mualfah, dkk[13] tentang “Analisis Perbandingan *Tools Mobile Forensic* Menggunakan Metode *National Institute of Justice*” , Pada penelitian ini telah dilakukan perbandingan kinerja dari tools Oxygen Forensic Detective dan Belkasoft Evidence Center, digunakan untuk mendapatkan dan memulihkan data yang terhapus, dan bukti digital lainnya. Metode yang dipakai adalah National Institute of Justice (NIJ), yang terdiri dari, identification, collection, examination, analysis, dan reporting. Tool mobile forensic Oxygen Forensic Detective digunakan untuk menganalisis file phisical image ‘mmcblk0’, didapatkan hasil 5 dari 6 total bukti digital dengan nilai 83.33%. Tool mobile forensic Belkasoft Evidence Center, mendapatkan 4 dari 6 total bukti digital dengan nilai 66.67%. Implementasi dari dua tools tersebut mampu mendapatkan bukti digital, pada rekonstruksi kasus dipenelitian ini, dari perangkat android Samsung Galaxy J2 Prime.[13]

Irfan Maullana, dkk[14] tentang “Analisis Forensik aplikasi Penipuan Berbasis android Menggunakan Metode NIST” , studi literatur, observasi, perancangan skenario, mempersiapkan kebutuhan penelitian, dan implementasi metode NIST menjadi awal dari tahap penelitian. Pencarian bukti digital yang dilakukan berupa file aplikasi berbahaya yang akan dianalisis dari aplikasi yang digunakan. Database Whatsapp berupa percakapan dan file aplikasi berbahaya merupakan hasil dari penelitian ini. Penemuan informasi dari aplikasi yang dianalisis adalah, terdapat manipulasi file asli yang diubah menjadi file lain, dari kejadian memungkinkan terjadi pencuri data pribadi milik korban, yaitu SMA Kode OTP dari rekening bank korban[14].

Wahyudi agustino, dkk[9] tentang “Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti Yang Dihapus” kerangka kerja NIST SP 800-86 diterapkan untuk memulihan bukti digital yang terhapus, kerangka keja ini terdiri dari: Pengumpulan, Pemeriksaan, Analisis, dan Pelaporan. FTK Imager digunakan pada media penyimpan untuk memudahkan proses pemulihan data. Dalam rekonstruksi akuisisi bukti digital ini dilakukan

dengan jangka dua minggu di setiap pengujiannya sebanyak lima kali. Tujuan dari Rekonstruksi ini untuk memvalidasi efektivitas dan batasan dari tahapan yang dipakai pada akuisisis bukti digital yang terhapus. Autopsy digunakan untuk menunjukan analisis dari data yang berhasil dipulihkan. FTK Imager dan Autopsy mendapatkan 100% keberhasil mengembalikan bukti digital yang terhapus permanen. Terdapat 0% keberhasilan karena tidak mampu memulihkan data pemformatan yang terhapus. [9]

Berdasarkan penelitian-penelitian terdahulu yang sudah dilakukan maka terdapat sususan perbandingan seperti pada tabel 2.1. Rangkuman hasil kajian penelitian terdahulu sebagai berikut.

Tabel 2. 1 Rangkuman Hasil Kajian Penelitian

NO	Penulis	Tahun	Judul	Objek Penelirian	Hasil
1	Nadia ayu Isroh Maniar, Trihastuti Yuniati[11]	2023	Implementasi Mobile Forensic Pada Aplikasi MICHAT dan Telegram Dengan Ftamework NIST 800-101	*MIChat dan Telegram*	penelitian menunjukan bahwa barang bukti digital lebih sedikit ditemukan pada MOBILedit Forensic Express, dibandingkan FTK Imager dan pemulihan bukti digital pada MICHat mendapatkan lebih banyak bukti digital dibandingkan dengan aplikasi Telegram. Pesaan percakapan, *voice note* ,video, dan gambar merupakan

					bukri digital yang berhasil terakuisisi.
2	Rahmat Novrianda Dasmen, Muhammad Reihan Pratama, Husni Yasir, Ariff Budiman[12]	2024	Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Insititute of Standard and Technology SP 800-86	*flashdisk*	penelitian ini menunjukkan bahwa pemanfaatan Autopsy bisa menganalisis dan mengembalikan barang bukti digital yang sebelumnya tersimpan di flashdisk dengan tingkat keberhasilan 100%, %, 4 berkas dengan ekstensi PNG dan 1 berkas dengan ekstensi MP4 merupakan data yang terpulihkan sesuai dengan skenario kasus yang dirancang.
3	Desti Mualfah, Muhammad Iqbal Syam, Baidarus[13]	2023	Analisis perbandingan *tools mobile forensic* menggunakan metode *national institute of justice* (NIJ	*Smartphone* Android Samsung Galaxy J2 Prime	Tool mobile forensic Oxygen Forensic Detective digunakan untuk menganalisis file phisical image 'mmcblk0', didapatkan hasil 5 dari 6 total bukti digital dengan nilai 83.33%. Tool mobile forensic Belkasoft Evidence Center, mendapatkan 4 dari 6 total bukti digital dengan nilai 66.67%.

					Implementasi dari dua tools tersebut mampu mendapatkan bukti digital, pada rekonstruksi kasus dipenelitian ini, dari perangkat android Samsung Galaxy J2 Prime.
4	Irfan Maulana, Ardi Pujianta	2024	Analisis Forensik Aplikasi Penipuan Berbasis Android Menggunakan Metode NIST	*Whatsapp*	Database Whatsapp berupa percakapan dan file aplikasi berbahaya merupakan hasil dari penelitian ini. Penemuan informasi dari aplikasi yang dianalisis adalah, terdapat manipulasi file asli yang diubah menjadi file lain, dari kejadian memungkinkan terjadi pencuri data pribadi milik korban, yaitu SMA Kode OTP dari rekening bank korban.
5	Wahyudi Agustino, Dini Wulan Suci, Novi Prastiti[9]	2024	Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus	*Flashdisk* dan *harddisk*	Autopsy digunakan untuk menunjukan analisis dari data yang berhasil dipulihkan. FTK Imager dan Autopsy mendapatkan 100% keberhasil mengembalikan

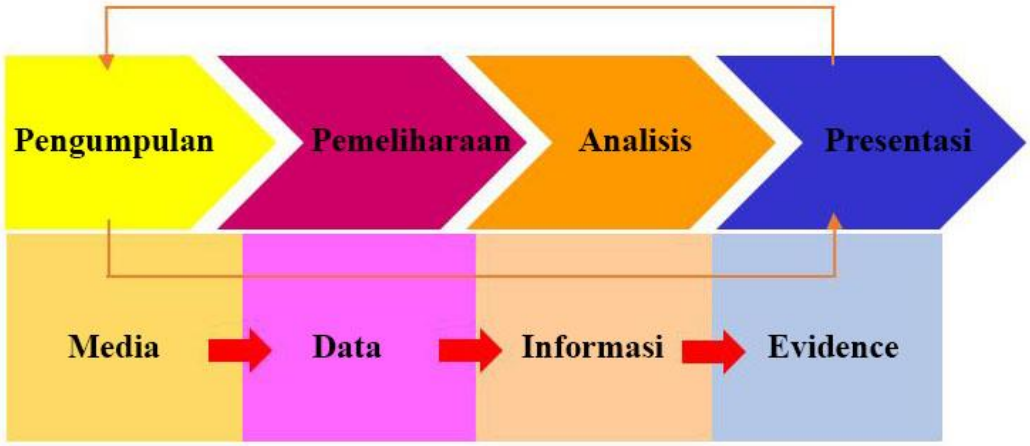
					bukti digital yang terhapus permanen. Terdapat 0% keberhasilan karena tidak mampu memulihkan data pemformatan yang terhapus.

Berdasarkan penelitian-penelitan terdahulu di Tabel 2.1 yang sudah dilakukan penelitian ini memilik perbedaan mulai dari objek penelitan yang digunakan yaitu *WhatsApp Group*. Pada penlitian ini lebih fokus mencari bukti digital dan penentuan pelaku atau sumber dari kasus penyebaran pornografi pada *WhatsApp Group.*

2.2 Landasan Teori

2.2.1 Digital Forensik

Digital forensik merupakan cabang keilmuan forensik yang berfokus pada investigasi dan pemuan segala bentuk konten dari perangkat digital, terpenting terkait dengan kejahatan komputer. Sama halnya dengan ilmu forensik lainnya. Digital forensik juga menggunakan teknologi, alat, dan prosedur yang komplek yang harus digunakan untuk memastikan barang bukti yang terkumpul akurat dan hasil yang tepat [15]. Lebih spesifiknya digital forensik merupakan invetigasi yang berhubungan dengan informasi, aplikasi ataupun data, termasuk data yang terekam didalam berkas yang prosesnya dilakukan menggunakan tools atau yang tujuannya adalah untuk mengummpulkan data dan jejak kejahatan pelaku yang ada didalam perangkat digital demi kepentingan pembuktian secara hukum dan ilmiah kejahatan komputer [12]. Gambar 2.1 menunjukan tahapan digital forensik.



Gambar 2. 1 Tahapan Digital Forensik [16]

2.2.2 Pornografi

Melalui informasi yang dirujuk dari Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, pornografi sendiri memiliki banyak pengertian seperti, sketsa, gambar, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lainnya malalui berbagai media komunikasi atau yang dipertotonkan di depan umum, yang berisi eksploitasi seksual yang melanggar norma kesusilaan yang ada dimasyarakat. Kemudian dalam bab II pasal 4 dijelaskan hal yang mengandung pornografi antara lain, yaitu: a) persenggamaan, termasuk persenggamaan yang menyimpang, b) Kekerasan seksual, c)Masturbasi atau onani, d) Keterlanjangan atau tampilan yang mengesampingkan keterlanjangan, e) Alat kelamin, f) Pornografi anak [17].

2.2.3 Mobile Forensic

Cabang ilmu digital forensik yang digunakan untuk menganalisis dan menemukan barang bukti digital yang berkaitan dengan kejahatan komputer agar nantinya dapat dipertanggung jawabkan secara hukum disebut dengan Mobile Forensic [13].

Mobile forensik adalah forensik yang sumber data-data diambil dari perangkat ponsel seluler, dan bisa dijadikan barang bukti dengan sendirinya. Bukti digital dapat dijadikan acuan untuk menyelidiki suatu perkara, dan bukti digital yang dapat diekstrak dari perangkat seluser diantaranya nomor kontak, log panggilan telepon, SMS, file audio, email, internet history, dan bukti lainnya [18].

2.2.4 National Institute of Standards and Technology

NIST adalah salah satu metode yang memiliki cara kerja, kebijakan dan standarisasi untuk menjamin pekerjaan digital forensik akan menggunakan alur kerja yang sama dan akan memberikan kemudahan dalam pekerjaan karena pekerjaan mereka dapat didokumentasikan sehingga mendapatkan hasil yang bisa diulang dan juga dipertahankan [19].

Gambar 2. 2 Tahapan Metode NIST [20]

Berdasarkan gambar 2.2 NIST memiliki 4 tahapan, sebagai berikut :

1. *Collection*: Merupakan tahapan identifikasi dan pengumpulan data dari sumber daya yang berkaitan dengan mengikuti prosedur demi menjaga keaslian dan kerahasian data. Media digital yang bisa dijadikan bukti digital seperti sistem android, media penyimpanan (SIM *card*, *Google Drive*, *e-mail*, *handphone*, SMS, *log file browsing history*, aplikasi layanan pesan seperti *Whatsapp*, dsb.

2. *Examination*: Merupakan tahap pemrosesan data-data yang telah didapatkan dari tahapan pengumpulan data. Tahapan ini juga merupakan tahap penelusuran data yang tersembunyi atau terhapus dengan menggunakan alat forensik khusus, seperti MOBILedit, dsb.
3. *Analysis*: Merupakan proses menganalisis hasil pemeriksaan yang ditemukan menggunakan metode yang benar secara hukum, untuk menjawab semua pertanyaan yang dapat dan menjadi tuntutnan untuk melakukan pemeriksaan serta pengumpulan. Analisis ini bisa dilakukan pada data yang berbentuk : pesan dokumen, *e-mail*, data yang dihapus, file tersembunyi, password, *log* kunjungan, *history* aplikasi, dan *log chat* aplikasi, dsb.
4. *Reporting*: Tahapan akhir dari seluruh rangkaian metode ini adalah laporan hasil dari analisis, dengan mendeskripsikan skema yang digunakan, menjelaskan alat dan prosedur yang digunakan, menentukan tindakan apa saja yang perlu dikerjakan, dan memberikan pengajuan perbaikan alat, metode, prosedur, dan aspek lainnya dari proses forensik. Laporan yang diperlukan seperti *log* aktivitas, tangkapan layar bukti digital dari status terbaru tersaangka, untuk penjabaran laporan dapat disusun mengikuti kebutuhan, dan laporan yang disusun tidak terlalu mendetail dari tahapan awal hingga *analysis* [20][21].

2.2.5 Whatsapp

Whatsapp merupakan salah satu aplikasi pesan cepat pada perangkat ponsel yang menggunakan jaringan internet untuk mengirimkan pesan. Whatsapp menjadi pilihan yang terjangkau untuk pengiriman pesan, terlebih untuk pesan group bahkan internasional. Whatsapp memudahkan pengguna membagikan pesan teks, gambar bahkan video. Whatsapp menggunakan jaringan internet seluler maupun WiFi, yang memungkinkan pengguna melakukan obrolan secara online, saling bertugar dan berbagi file atau foto dan banyak fitur menarik lainnya [22].

Dengan peningkatan whatsapp dapat menyulutkan dampak buruk yaitu banyak muncul oknum yang menggunakan aplikasi whatsapp untuk melakukan kejahatan digital atau komputer salah satunya kejahatan pornografi, oleh karena itu harus dilakukan tindakan guna mengungkapkan tindak kejahatan pornografi ini [18].

2.2.6 Android

Android adalah salah satu sistem telepon seluler yang mengunakan sistem operasi Linux. Android menyajikan platform open source bagi pengembang aplikasi untuk menciptakan bermacam-macam piranti atau aplikasi [23]. Dengan adanya keterbukaan android sebagai sistem operasi akan memungkinkan para ahli forensik digital untuk membuat dan mengembangkan alat-alat dan sistem khusus yang bisa digunakan untuk upaya penegakan hukum dalam menangani kasus-kasus kejahatan komputer termasuk pornografi yang melibatkan perangkat android.

2.2.7 MOBILedit Forensic

MOBILedit Forensic merupakan salah satu Tool yang digunakan pengekstrak ponsel, analisis data, dan juga dapat membuat laporan dalam bentuk solusi. Salah satu tools 64-bit yang mengimplementasikan tahapan akuisis data fisik dan logis. Penggunaannya adalah dengan menghubungkan telpon melalui Wi-Fi, kabel USB ataupun bluetooth, dapat melakukan pengecekan fisik pada banyak perangkat ponsel seluler dan bentuk dari hasil laporannya berupa PDF, HTML, Excel, dll. Untuk berbagai kebutuhan [22].

2.2.8 Magnet AXIOM

Magnet AXIOM adalah salah satu tools forensik produksi Magnet forensik yang mampu memproses dan menyimpan bukti digital dari komputer bahkan *smartphone* menjadi dokumen

laporan. Magnet AXIOM sangat membantu pemeriksaan profesional forensik dalam menemukan dengan cepat data yang paling relevan dan memvisualisasikannya untuk analisis yang lebih baik [1]. Magnet AXIOM mempunyai kemampuan untuk menganalisa komputer *smartphone,* penyimpanan *cloud,* IoT dan hasil *imaging* dari perangkat lunak lainnya. magnet AXIOM juga dapat membantu setiap proses *akuisisi, recovery* data, analisa dan pelaporan serta meyederhanakan investigasi dengan menunjukkan barang bukti yang relevan sebagai artifak yang mudah dilihat [24].

2.2.9 Belkasoft Evidence Center

Belkasoft Evidence Center merupakan *tool* forensik yang mampu memperoleh, mencari, menganalisis, dan menyimpan beragam barang bukti yang ditemukan pada *smartphone* atau *computer*. *Tool* forensik ini mampu mengeluarkan barang bukti dari beragam media dan mampu menganalisis penyimpanan *hardisk, Os Blackberry, dan android backup* kemudian laporan akan teranalisis dan tersimpan secara otomatis [1].

BAB III. METODOLOGI PENELITIAN

3.1 Objek Penelitian

Objek penelitian ini adalah analisis forensik pada aplikasi Whatsapp berbasis android yang berfokus pada Whatsapp Group untuk mengungkap bukti kejahatan pornografi. Metode yang dipakai adalah *National Institute of Standart Technology* (NIST). Penelitian ini bertujuan untuk mengakuisisi dan mengidentifikasi bukti digital yang dapat didapat melalui analisis forensik pada aplikasi *Whatsapp* berbasis *android*. Hasik penelitian diharapkan dapat menjadi panduan dalam investigasi kejahatan pornografi yang melibatkan penggunaan *whatsapp group*.

3.2 Metode Pengumpulan Data

Metode pengumpulan data yang diterapkan adalah studi literatur. Studi literatur melibatkan analisis sumber – sumber tertulis seperti jurnal, artikel, dan buku terkait analisis forensik pada aplikasi berbasis android dan penggunaan metode National Institute of Standard Technology (NIST) dalam digital forensik. Perapkan metode observasi yaitu melalui survei dilapangan dengan menggunakan rekayasa atau skenario kasus juga diterapkan di penelitian ini yang kemudian dilakukan proses identifikasi bukti-bukti yang didapat dieksplorasi lebih lanjut sesuai dengan barang bukti yang didapatkan.

3.3 Alat dan Bahan Penelitian

Penelitian ini menggunakan perangkat keras dan perangkat lunak sebagai berikut :

3.3.1 Perangkat Keras (Hardware)

Berikut ini merupakan perangkat keras yang digunakan dalam penelitian :

Tabel 3. 1 Perangkat Keras (Harware)

Perangkat keras (Hardware)	Keterangan
LAPTOP-51G5UH5C Intel® Core™ i5-1035G1 CPU @ 1.00GHz (8 CPUs), ~1.2Ghz RAM 8192MB	Perangkat keras analisis forensik
Smartphone android *Xiaomi Redmi* 4a	Objek penelitian
Smartphone android redmi note 5	Objek penelitian

3.3.2 Perangkat Lunak (Software)

Berikut ini merupakan perangkat lunak yang digunakan dalam penelitian :

Tabel 3. 2 Perangkat Lunak (Software)

Perangkat Lunak (Software)	Keterangan
MOBILedit Forensic Express 7.4.0	Alat forensik dan analisis
Belkasoft Evidence center 9.9800	Alat forensik dan analisis
Magnet AXIOM Process 7.8.0	Alat forensik dan analisis
Windows 11 Home Singel Languange 64-bit (10.0, Build 22631)	Sistem operasi
Whatsapp 2.24.16.3	Objek penelitian

3.4 Tahapan Penelitian

Tahapan penelitian dengan menggunakan *National Institute of Standards and Technology* (NIST) dalam analisis forensik mencakup beberapa langkah :

3.4.1 Collection

Penelitian ini melibatkan pengambilan data dari *whatapp group* pada perangkat smartphone android realme not 5. Data yang relevan dengan pernyataan penelitian, seperti video dan gambar, dikumpulkan untuk analisis lebih lanjut.

3.4.2 Examination

Data yang terkumpul dicermati untuk mengidentifikasi bukti yang didapat dengan merecovery data menggunakan tools MOBIledit forensic Express dan Magnet AXIOM. Pada proses ini investigator mencari atau mengakuisisi data berupa video ataupun gambar yang terdapat pada smartphone.

3.4.3 Analysis

Pada tahap ini peneliti menganalisis data untuk menjawab pertanyaan penelitian. Tujuannya adalah untuk memahami apakah objek yang dikirim melalui *whatapp group* dapat di pulihkan meskipun telah dihapus. Objeknya berupa konten pornografi yang didistibusikan oleh terduga.

3.4.4 Reporting

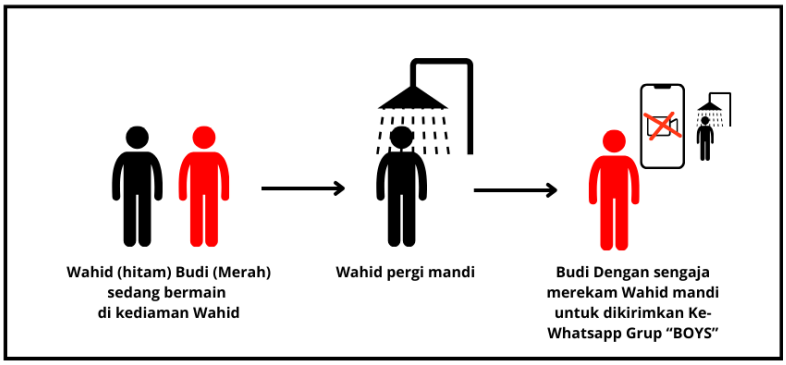
Pada tahapan akhir ini seluruh hasil temuan akan didokumntasi dan kesimpulan dari analisis forensik dimuat dalam dalam sebuah laporan yang komprehensif. Laporan ini menyajikan hasil percobaan, metodologi, bukti, dan file pendukung dengan cara yang jelas dan terorganisir. Laporan ini berfungsi sebagai referensi untuk investigasi di masa mendatang dan dapat diaktualisasikan sebagi bukti dalam proses hukum.

3.5 Skenario Penelitian

Penelitian ini akan menggunakan skenario yang dibuat secara rekayasa. Dimana terdapat salah satu anggota *whatsapp group* “BOYS” yang dengan sengaja memvideokan salah satu anggota lain yang sedang mandi tanpa sepengetahuan korban dan dengan sengaja dikirimkan kedalam *whatsapp group* tersebut. Untuk lebih detailnya sebagai berikut.

3.5.1 Pre Insiden

Pada awalnya terdapat dua orang pemuda yang sedang bermain disebuah rumah. Kemudian wahid selaku pemilik rumah hendak mandi dan satu orang lagi bernama budi dengan sengaja meletakkan ponselnya diatas pintu kamar mandi untuk merekam wahid yang sedang mandi dengan tujuan untuk dikirimkan ke *whatsapp group* mereka yang bernama "BOYS" yang beranggotakan 5 orang, tiga lainya adalah Hadi, Fahrul, dan Gito. Skenario pre insiden ini dapat dilihat pada Gambar 3.1 .

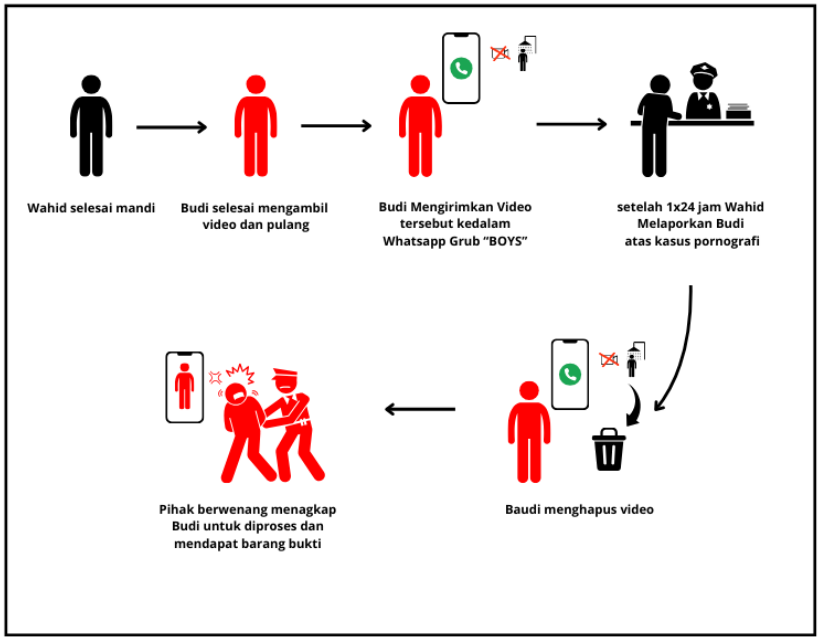


Gambar 3. 1 Skenario Pre Insiden

3.5.2 Insiden

Merasa video yang diambil sudah cukup Budi mengambil ponselnya dan tidak lama Wahid selesai mandi tanpa tahu bahwa Budi telah mengambil videonya saat mandi, kemudian Budi pamit pulang tanpa memberi tahu bahwa ia telah mengambil video Wahid mandi. Setelahnya Budi dengan sengaja mengirimkan Video tersebut kedalam *whatsapp group* "BOYS". Seketika Whatsapp group tersebut menjadi ramai. Kemudian Wahid juga membuka *whatsapp group* tersebut dan menyadari bahwa Budi telah mempermalukannya dengan mengirimkan Video tersebut. Wahid meminta Budi untuk menarik pesannya dan mengancam Budi akan dilaporkan tekait video pornografi jika tidak menariknya. Dan untuk memperkuat laporannya Wahid meng-screenshoot percakapan group tersebut dan menyimpan videonya. kemudian sampai 1X24 jam

Budi ditidak menarik atau menghapaus video tersebut, akhirnya Wahid melaporkan Budi terkait kasus video pornogafi tersebut kepada pihak berwenang. Kemudian Budi mengetahui dirinya dilaporkan ia dengan sengaja melakukan tindakan anti forensik dengan menghapus semua barang bukti video yang dikirimkannya di *whatsapp group* tersebut. Tak lama setelahnya Budi ditangkap dan akan diproses terkait laporan dari Wahid tersebut dan pihak berwenang mendapatkan barang bukti berupa ponsel dari Budi. Dalam kasus ini tidak ada indikasi penyebaran diluar *whatsapp group* "BOYS". Video hanya dikirimkan pada *whatsapp group* tersebut, seperti yang ditunjukkan pada Gambar 3.2 .



Gambar 3. 2 Skenario Insiden

3.5.3 Pasca Insiden

Pada tahap ini pihak berwenang menyerahkan Barang buti kepada investigator berupa Ponsel Budi dan juga ponsel wahid sebagai korban guna memastikan kebenaran kasus tersebut. Kemudian jika Investigator menemukan bukti sesuai yang dilaporkan maka hal tersebut bisa menjadi penguat atas kesalahan budi dalam mengirimkan video pornografi tersebut, dan

kemudian budi akan diproses sesuai dengan persidangan atas kesalahannya, seperti yang ditunjukan pada Gambar 3.3 .

Gambar 3. 3 Skenario Pasca Insiden

BAB IV. HASIL DAN PEMBAHASAN

Pada bab ini dijelaskan mengenai tahapan-tahapan penelitian yang dilakukan untuk memperoleh hasil penelitian. Penelitian ini menggunakan metode *National Institute of Standard and Technology* (NIST). Penelitian ini mensimulasikan skenario kasus pornografi pada *whatsapp group.* Penelitian ini menerapkan metode NIST pada layanan *whatsapp* berbasis *android*. Hasil dari penelitian ini menghasilkan barang bukti berupa video yang akan dilakukan penyelidikan lebih lanjut.

Penelitian ini akan menggunakan skenario yang dibuat secara rekayasa. Dimana terdapat salah satu anggota *whatsapp group* "BOYS" yang dengan sengaja memvideokan salah satu anggota lain yang sedang mandi tanpa sepengetahuan korban dan dengan sengaja dikirimkan kedalam *whatsapp group* tersebut. Kemudian korban merasa sangat dirugikan dengan adanya video tersebut, sehingga korban melaporkan pelaku pengiriman video tersebut atas dasar kasus pornografi.

4.1 Collection

Collection atau Pengumpulan Data merupakan langkah pertama dalam metode NIST. Pengumpulan dan pengambilan barang bukti dilakukan pada tahapan ini dengan mendokumentasikan barang bukti yang didapat. Pada skenario penelitian ini barang bukti yang didapat adalah *smartphone xiaomi redmi* 4a dari pelaku dan *smartphone* Redmi Note 5 dari korban. Seperti tercantum didalam Tabel 4.1.

Tabel 4. 1 Tabel Barang Bukti

No	Barang Bukti	Gambar	Keterangan
1	*Smart phone xiaomi r*edmi 4a		*Smartphone* pelaku yang ditemukan dalam kondisi menyala dan ter Install aplikasi w*hatsapp*
2	*Smart phone* Redmi Note 5		*Smartphone* korban yang digunakan untuk validasi data dari barang bukti

Pada Tabel 4.1 menapilkan barang bukti yang diamankan berupa *smartphone* milik pelaku *smartphone* Realmi Note 5 dan *smartphone* milik korban *Smart phone* Redmi *Note* 5 dengan spesifikasi seperti pada tabel berikut.

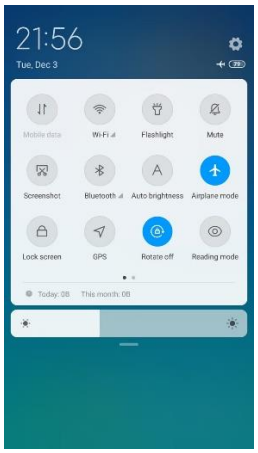
Tabel 4. 2 Tabel Spesifikasi Smartphone Pelaku

Model	*Xiaomi Redmi* 4a (*Rooted*)
CPU	Quad-core Max 1.40 Ghz
RAM	2.00 GB
Versi andorid	7.1.2 N2G47H
Memori internal	16 GB
Versi MIUI	MIUI Global 10.2.3
IMEI 1	865407038971868
IMEI 2	865407038971876
Berat	131 g

Tabel 4. 3 Tabel Spesifikasi Smartphone Korban

Model	*Redmi Note 5*
CPU	Octa-core Max 1.80GHz
RAM	3.00 GB
Versi andorid	8.1.0 OPM1.171019
Memori internal	32 GB
Versi MIUI	MIUI Global 10.3
IMEI 1	869792032933741
IMEI 2	869792032933758
Berat	181 g

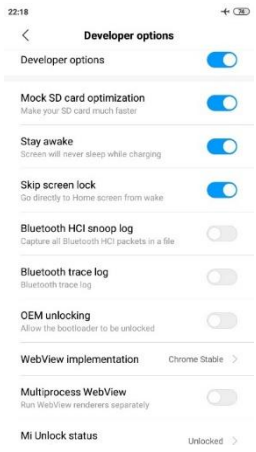
Dalam langkah persiapan untuk pengumpulan data s*martphone* pelaku, langkah pertama yang dilakukan adalah memastikan keamanan barang bukti. Setelah itu perangkat dipersiapkan dengan mengaktifkan beberapa pengaturan kunci. Seperti pada Gambar 4.1.



Gambar 4. 1 Airplane Mode Diaktifkan

Gambar 4.1 memperlihatkan *Airplane mode* diaktifkan untuk mematikan semua komunikasi nirkabel yang mungkin menggangu proses akuisisi.

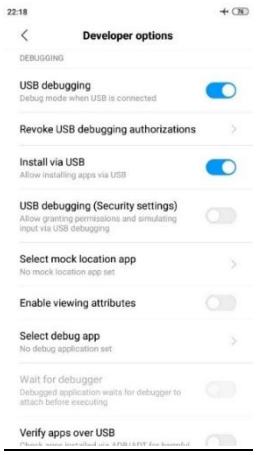
Langkah selanjutnya adalah mengaktifkan *developer options*. Untuk mengaktifkan USB *debugging* untuk mempermudah pembacaan *smartphone* sehingga proses akusisi dapat dilanjutkan, seperti yang ditampilkan pada Gambar 4.2. Cara mengaktifkan *developer options* pada *Smartphone* yaitu dengan mengklik pada *build number samrtphone* sebanyak tujuh kali. Jika *developer options* berhasil diaktifkan maka pilihan *developer options* akan muncul pada menu pengaturan, proses pengaktifan *developer option* dapat dilihat pada Gambar 4.2 .



Gambar 4. 2 Mengaktifkan Developer options

Cara mengaktifkan *developer options* pada *Smartphone* yaitu dengan mengklik pada *build number samrtphone* sebanyak tujuh kali. Jika *developer options* berhasil diaktifkan maka pilihan *developer options* akan muncul pada menu pengaturan, proses pengaktifan *developer option* tertampil pada Gambar 4.2 .

Selanjutnya mengaktifkan USB *debugging* untuk memberikan akses *software* untuk digunakan dalam proses akuisisi *smartphone* dengan USB sebagimana tertampil pada Gambar 4.3.

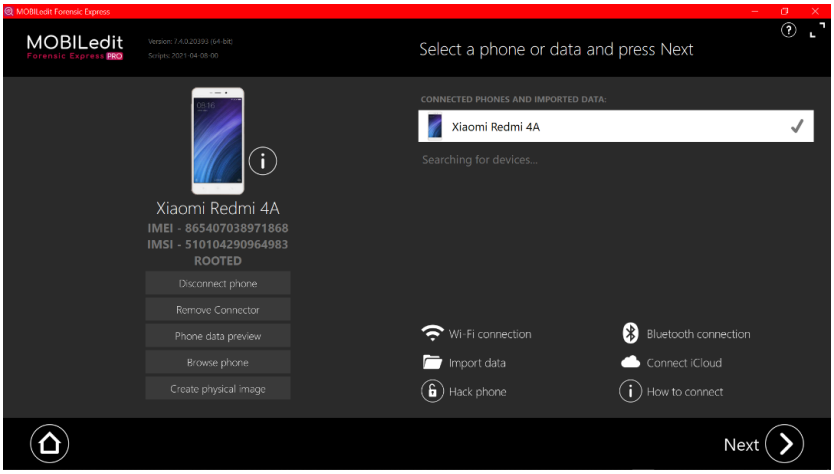


Gambar 4. 3 Mengaktifkan USB Debagging

Seletah melakukan pengaktifkan USB *debugging* seperti pada Gambar 4.3 maka proses akuisisi dapat dilakukan dengan menerapkan langkah-langkah digital forensik.

4.2 Examination

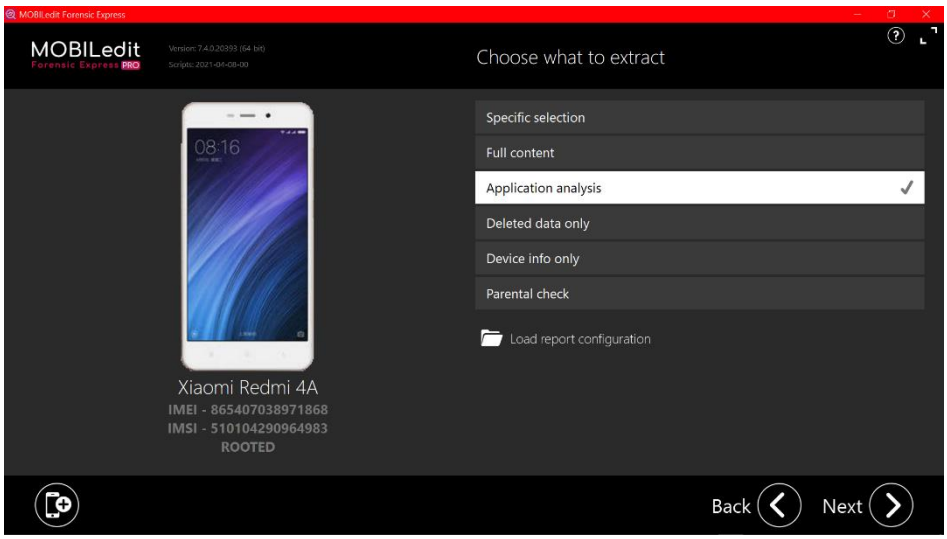
Examination merupakan pencarian bukti digital pada aplikasi *whatsapp* dengan menggunakan alat forensik yang disediakan. Tahapan *Examination* mengekstraksi data dan imaging data yang dilakukan pada sistem menggunakan alat forensik. Pada penelitian ini menggunakan *tools* MOBILEdit *Forensic Express* 7.4.0. seperti pada Gambar 4.4.



Gambar 4. 4 Tampilan MOBILEdit Yang Berhasil Mendeteksi Smartphone Pelaku

Gambar 4.4 memberikan informasi barang bukti sudah terhubung di MOBILEdit. Seperti IMEI yang terdapat pada *smartphone,* dan jenis dari *smartphone* yang digunakan.

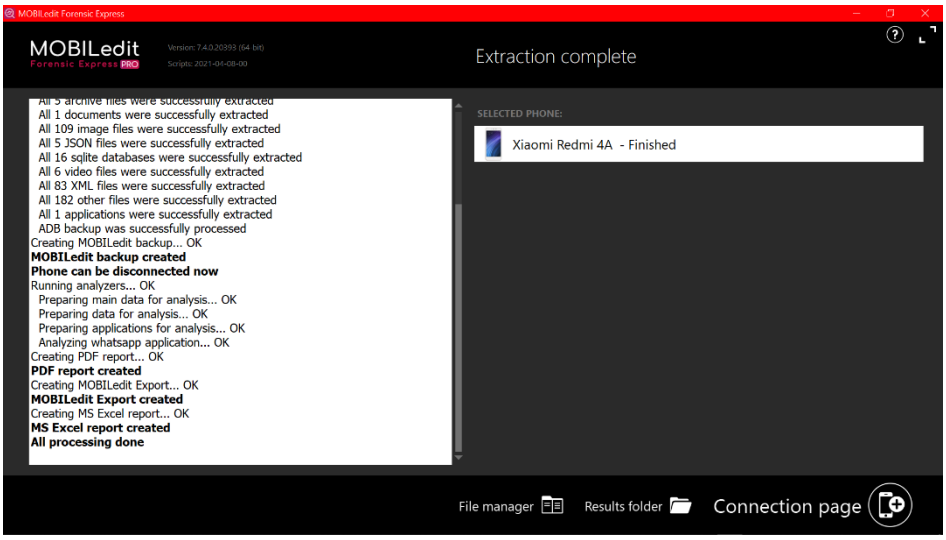
Selanjutnya proses imaging untuk mengekstrak berbagai data dari media penyimpanan data yang ingin diekstraksi seperti pada Gambar 4.5 .



Gambar 4. 5 Tampilan Plihan Data Yang diekstraksi

Penelitian ini memilih jenis data pada aplikasi *whatsapp* yang akan diekstraksi dengan memilih opsi *Application analysis* seperti pada Gambar 4.5.

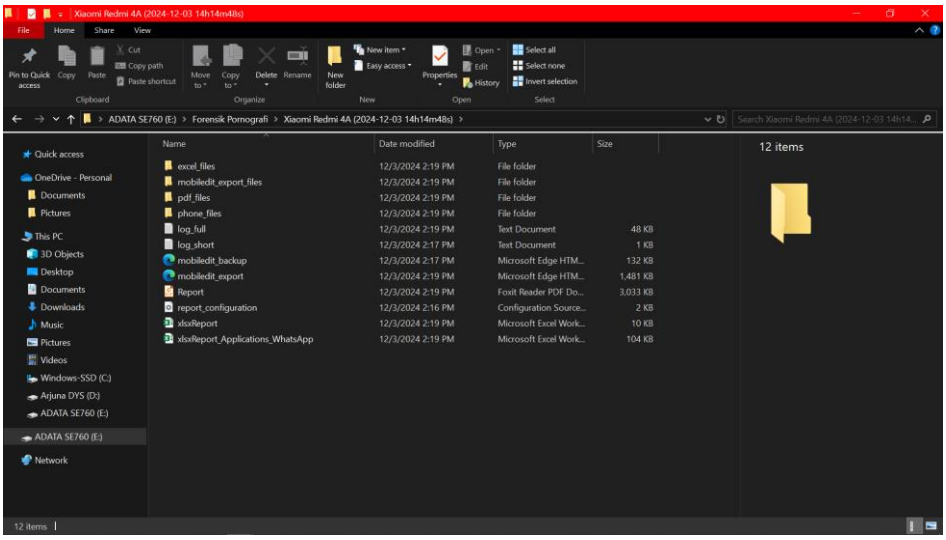
proses pengakuisisian data tertampil pada Gambar 4.6 . pada proses ini diperlihatkan semua data yang terakuisisi oleh *tool* MOBILEdit.



Gambar 4. 6 Tampilan Hasil Ekstraksi Barang Bukti dengan MOBILedit

Hasil akuisisi MOBILEdit dapat dilihat pada Gambar 4.6. dari gambar yang ditampilkan dapat dilihat bahwasannya proses berhasil dilakukan tanpa adanya kegagalan dalam proses akuisisi.

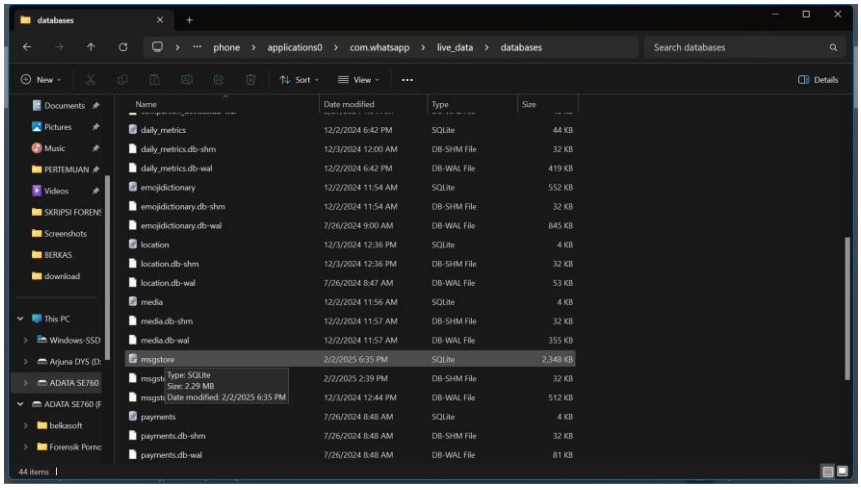
dari hasil akuisisi yang didapatkan dari *tool* MOBILEdit terdapat beberapa folder dan file yang nantinya dapat dijadikan sebagai barang bukti dalam skenario kasus ini, seperti yang ditampilkan pada Gambar 4.7 Sehingga dapat menguatkan bahwa terduga pelaku benar melakukan tindakan yang sesuai dengan yang dilaporkan korban.



Gambar 4. 7 Tampilan Folder Hasil Akuisisi

Kelebihan dari MOBILEdit ini adalah file yang sudah diakuisisi sudah direkap dalam file pdf yang mana dapat dilihat dari Gambar 4.7 dengan nama file *Report.pdf.*

Pada penelitian ini MOBILedit forensic digunakan untuk mendapatkan *file database* dari percakapan *whatsapp group "BOYS"*. Seperti pada gambar 4.8

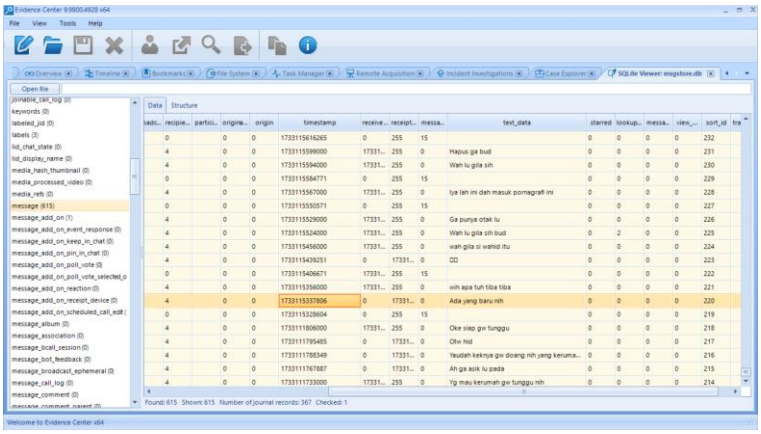


Gambar 4. 8 File Database

Gambar 4.8 menunjukkan *File database* percakapan tersebut bernama "*msgstore"* terletak pada folder F:\Forensik Pornografi\Xiaomi Redmi 4A Pornografi Whatsapp Grub

BOYS\phone_files\phone\applications0\com.whatsapp\live_data\databases. *File database* ini digunakan untuk meninvestigasi percakapan yang terjadi pada *whatapp group "BOYS"* yang nantinya dijadikan untuk pembuktian keaslian dari pada kasus ini.

Selanjutnya *file database* dibuka menggunakan *Belkasoft* untuk mendapatkan dan memulihkan percakapan yang terhapus guna memperkuat barang bukti. Dari proses ini didapatkan 2 dari 14 pesan percakapan yang dihapus. Seperti tertampil pada Gambar 4. 9.



Gambar 4. 9 Percakapan yang terhapus

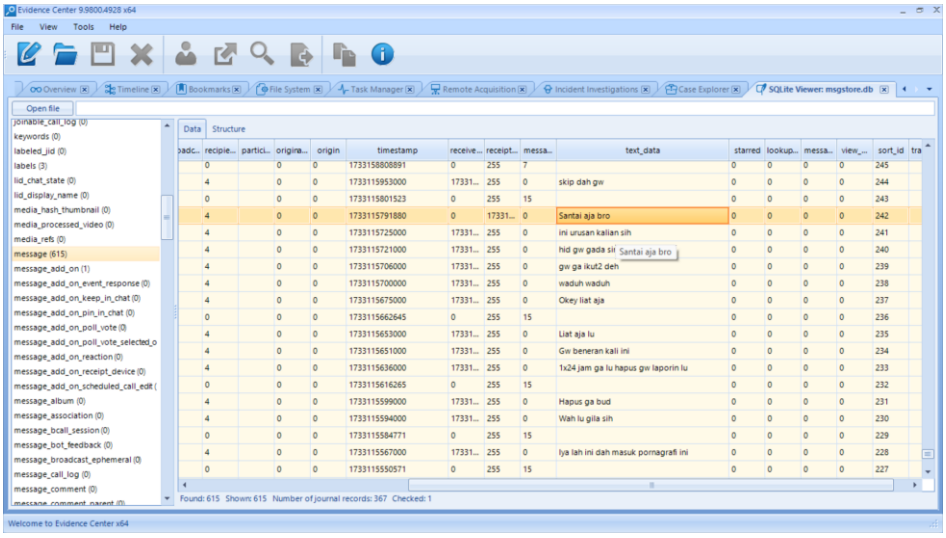
Untuk memvalidasi bukti tersebut maka dilakukan pengecekan pada *timestamp* yang didapat pada barang bukti. Sebagaimana pada Gambar 4.9 *timestamp* yang didapat adalah "1733115337806" dengan isi pesan "Ada yang baru nih".

Selanjutnya untuk mengetahui waktu sebernanya dari percakapan tersebut dilakukan lah konversi *timestamp* dengan menggunkan *Epoch Converter* yang bisa di akses pada *Browser* adapun hasil dari konversi tersebut dapat dilihat pada Gambar 4. 10.

Gambar 4. 10 Hasil Konversi TimeStamp

Setelah dilakukan konversi didapatkan hasil waktu dan tanggal sebenarnya yaitu, “Senin, 2 Desember 2024 pukul 11.55.37”. Seperti tertampil pada Gambar 4.10.

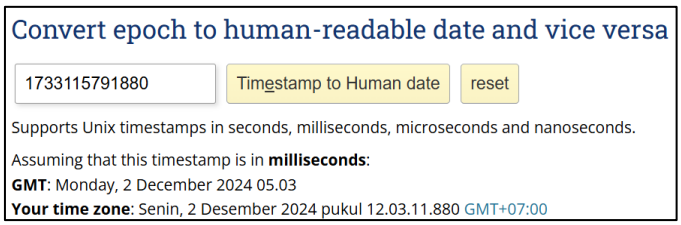
Gambar 4.11 menampilkan pesan percakapan terhapus yang lainnya. Dilakukan analisis pada percakapan dan *timestamp* untuk mempermudah proses pelaporan nantinya.



Gambar 4. 11 Percakapan yang terhapus

Kemudian dilakukan juga konversi *timestamp* pada bukti percakapan yang terhapus lainnya. pada Gambar 4. 11 didapatkan *timestamp* “1733115791880” dengan isi pesan “santai aja bro”.

Dilakukan proses konversi *timestamp* untuk mengetahui waktu asli dari pada percakapan tersebut dilakukan. Dan didapatkan hasil seperti tertampil pada Gambar 4.12.



Gambar 4. 12 Hasil Konversi Timestamp

Dari hasil konversi pada Gambar 4.12 didapatkan hasil " Senin, 2 Desember 2024 pukul 13.03.11".

Guna memperkuat barang bukti pada skenario kasus ini digunakanlah smartphone korban, yang mana korban telah melakukan *screenshoot* pada percakapan yang dilakukan di whatsapp group sebelum dihapus oleh pelaku, dan korban juga sempat menyimpan video yang dijadikan laporan utama pada skenario kasus ini seperti pada Gambar 4.13. Maka guna dari smartphone korban pada penelitian ini adalah hanya untuk menjadi alat validasi dan pencocokan barang bukti yang telah didapatkan guna memperkuat laporan korban.

Gambar 4. 13 Tampilan Screenshoot Chat Dari Smartphone korban Sebelum Terhapus

Dapat dilihat pada Gambar 4.13 pelaku mengirimkan video berdurasi 37 detik yang objeknya adalah korban dan yang diindikasi menjadi kasus pornografi.

Pelaku juga terlihat mengirimkan pesan yang isinya seperti menantang korban. Pelaku juga bersikeras tidak akan menghapus video tersebut, sebagimana tertampil pada Gambar 4.14.

Gambar 4. 14 Tampilan Screenshoot Chat Dari Smartphone korban Sebelum Terhapus

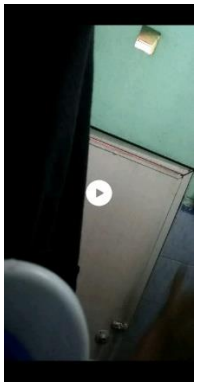
Pada gambar 4.14 korban meminta pelaku untuk menghapus video tersebut, namun pelaku tidak mengindahkan permintaan itu. Kemudian korban juga mengancam akan melaporkan pelaku sebagai tindak kasus pornografi jika pelaku tidak menghapus video tersebut selama 1 x 24 jam. Ternyata pelaku tidak menghapusnya selama dalam tenggat waktu yang di bataskan.

Gambar 4.15 juga menampilkan bukti percakapan dari beberapa anggota *group* lainnya

Gambar 4. 15 Tampilan Screenshoot Chat Dari Smartphone korban Sebelum Terhapus

Pada Gambar 4.15 terlihat bahwa pelaku mengabaikan peringatan yang telah diberikan oleh korban, dan justru pelaku menantang korban untuk melaporkannya. Dan dapat disimpulkan juga bahwasannya anggota *group* lainnya tidak terlibat dari kasus pornografi ini.

Dari langkah *examination* ini juga didapatkan bukti *screenshoot* video yang berhasil disimpan oleh korban, dan digunakan untuk memvalidasi barang bukti. Seperti yang tertampil pada Gambar 4.16



Gambar 4. 16 Tampilan Screenshoot Video Pada Smartphone Korban

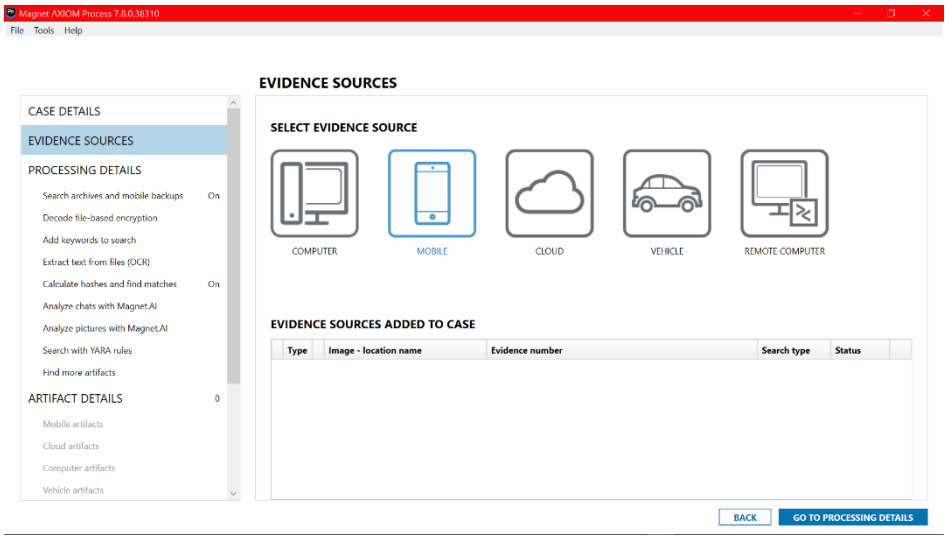
Gambar 4.16 merupakan *scressnshoot* dari *smartphone* korban. Korban sempat melakukan tindakan ini untuk mengantisipasi pelaku melakukan penghapusan terhadap semua bentuk barang bukti.

Setelah tahu bahwa dirinya dilaporkan oleh korban, pelaku melakukan tindakan anti forensik dengan menghapus semua buktii percakapan pada *whatsapp group*. Seperti pada Gambar 4.17.

Gambar 4. 17 Tampilan Chat Yang Pelaku Hapus

Pada Gambar 4.17 terlihat pelaku melakukan tindakan anti forensik dengan menghapus semua pesan percakapan yang pelaku kirimkan dan ini tentunya ini dilakukan untuk mempersulit investigator menemukan barang bukti.

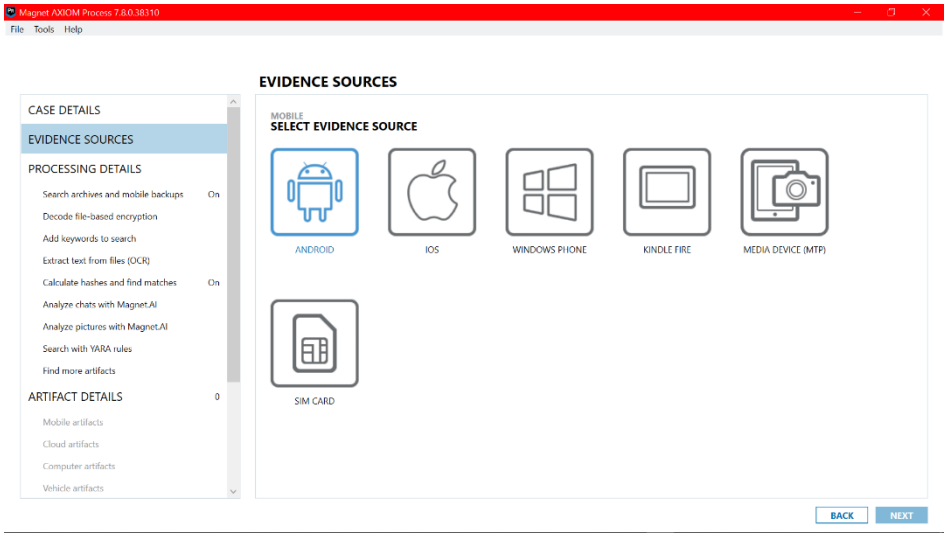
Untuk menemukan dan mengakuisis baran bukti multimedia berupa video maka pada penelitian ini menggunakan juga *tool Magnet AXIOM* Process 7.8.0. seperti pada Gambar 4.18.



Gambar 4. 18 Tampilan Magnt AXIOM

Pada tampilan Gambar 4.18 pilih device yang menjadi barang bukti, pada penelitian ini karena barang bukti yang didapat adalah smartphone maka opsi yang dipilih adalah mobile.

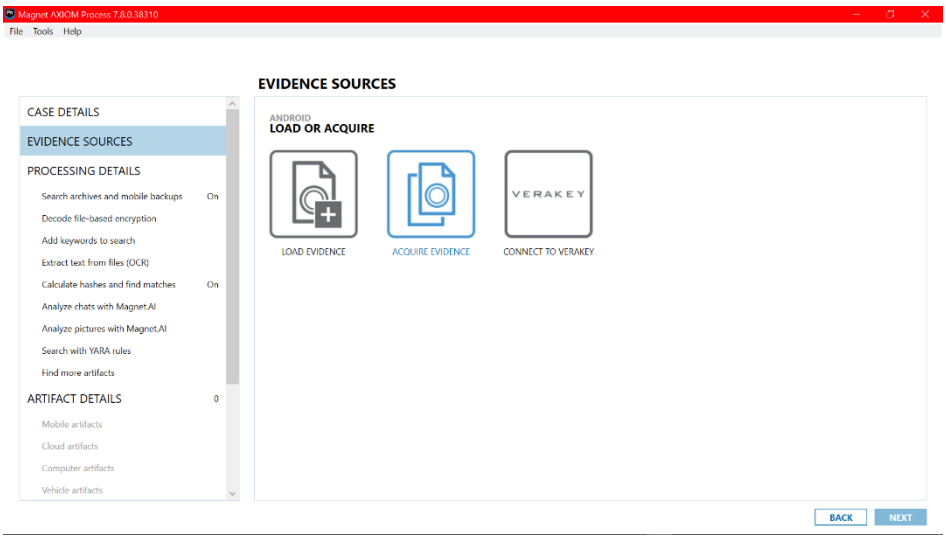
Langkah selanjutnya adalah memilih sistem operasi yang digunakan pada smartphone seperti pada Gambar 4.19 .



Gambar 4. 19 Tampilan Opsi Sistem Operasi

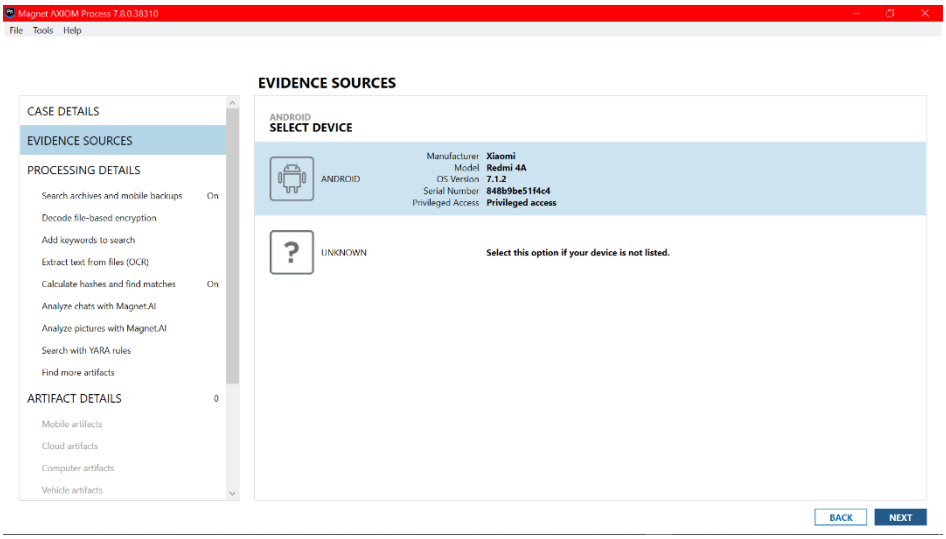
Gambar 4.19 Terdapat pilihan opsi sistem operasi, kemudian pilih sistem operasi yang sesuai dengan *device* yang ada.

Selanjutnya proses dilakukan seperti pada Gambar 4.20. untuk memilih sumber dari barang bukti yang ada.



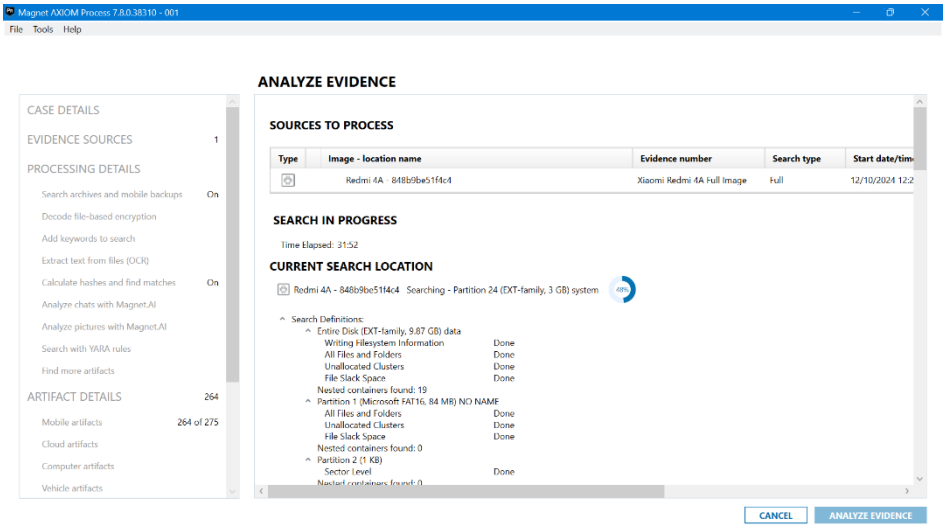
Gambar 4. 20 Tampilan Opsi Akuisisi

Untuk melanjutkan proses pilih opsi *Acquire Evidence* seperti pada Gambar 4.20 untuk mendapatkan dan mengakuisisi barang bukti baru. Selanjutnya sambungkan USB pada *smartphone* untuk menghubungkan Magnet AXIOM dengan *smartphone.*



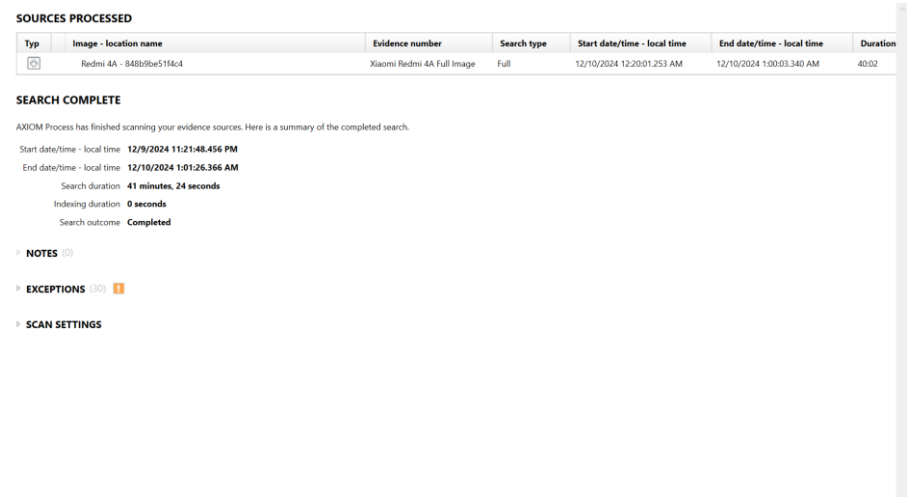
Gambar 4. 21 Tampilan Smartphone Terhubung Dengan Magnet AXIOM

Magnet AXIOM akan secara otomatis membaca *smartphone* jika sudah terhubung. Dapat dilihat pada Gambar 4.21 *smartphone* sudah terhubung dengan keterangan, jenis sistem operasi *Android, manufacturer : Xiaomi, model : Redmi 4A, serial number : 848b9be51f4c4,* dengan *privileged access.*

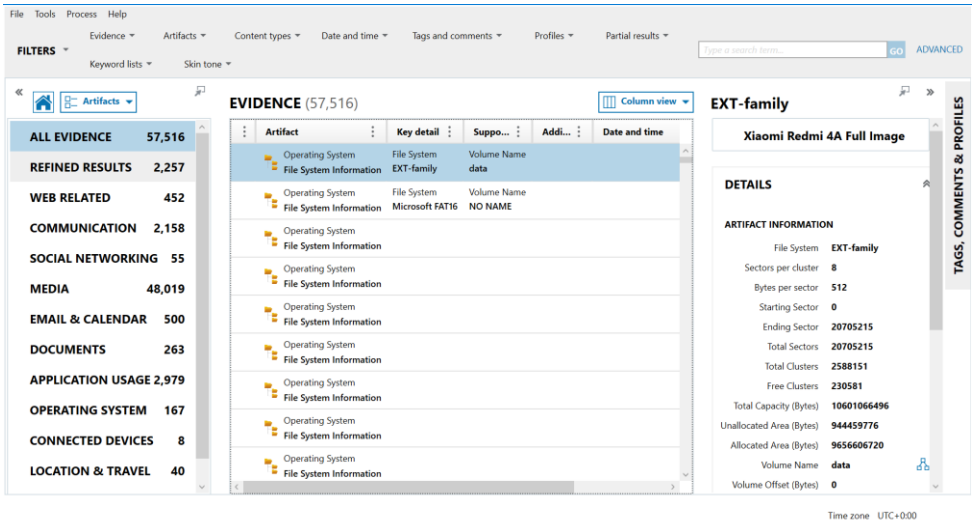


Gambar 4. 22 Tampilan Proses Akuisisi

Gambar 4.22 menampilkan proses akuisisi, proses ini bisa berlangsung lama, tergantung dengan besarnya data yang diekstraksi dari *smartpone.* Penelitian ini membutuhkan durasi 41 menit 24 detik seperti pada Gambar 4.23 .



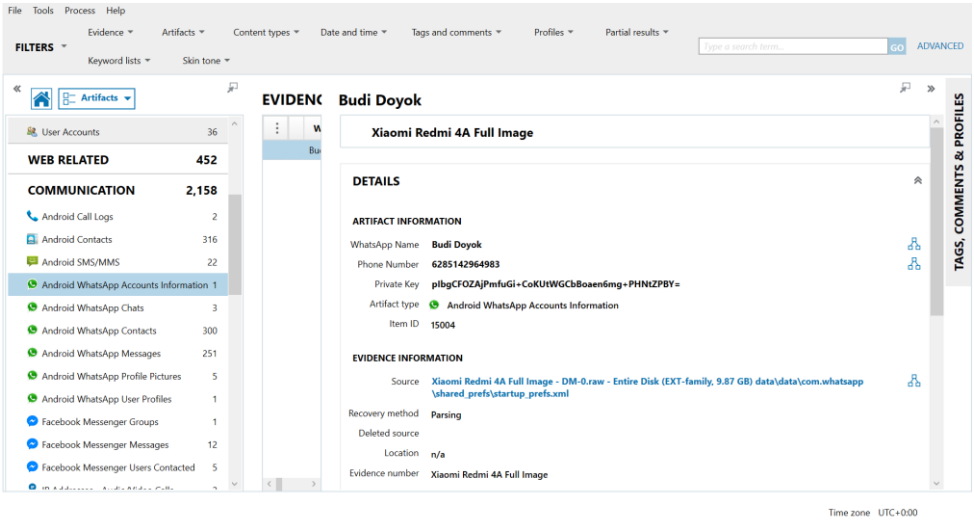
Gambar 4. 23 Tampilan Durasi Proses Akuisisi



Gambar 4. 24 Tampilan Hasil Proses Akuisisi

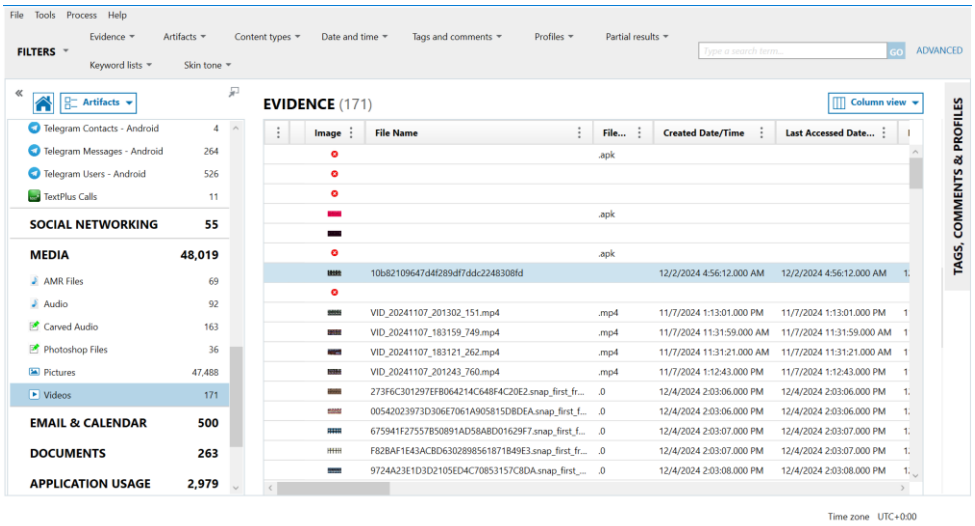
Semua barang bukti yang didapat atau terhapus dikumpulkan secara otomatis pada bagian *Artifacts.* Seperti yang dapat dilihat pada Gambar 4.24, terdapat banyak opsi yang sudah dikelompokan menjadi per satu bagian yang akan mempermudah proses analisis barang bukti.

Pada proses ini, ditemukan beberapa barang bukti, barang bukti yang ditemukan sudah tersusun rapi pada *tool magnet AXIOM,* dan dapat dilihat pada bagian *artifacts.* Dalam analisis ini didapatkan detail dari pada Akun *whatsapp* yang digunakan oleh pelaku yang dapat dilihat pada bagian *communication*. Seperti pada Gambar 4.25 .



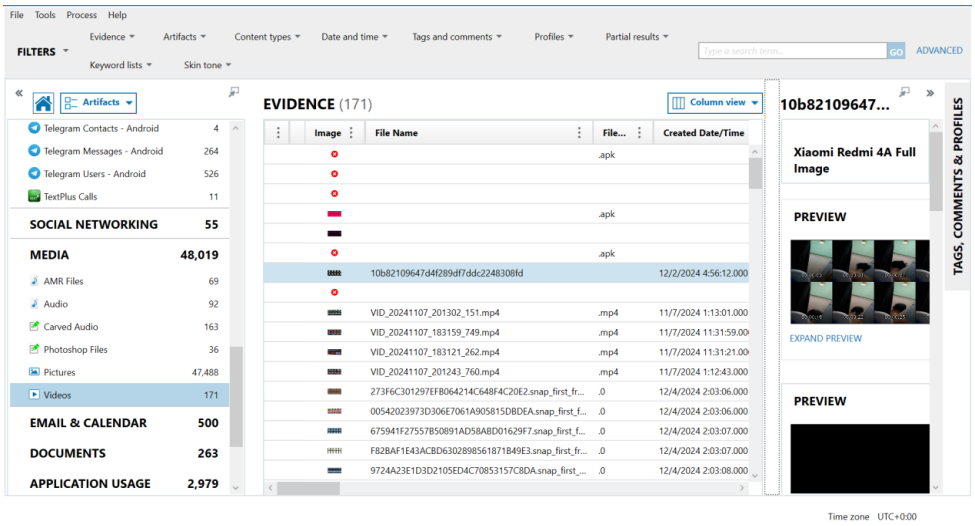
Gambar 4. 25 Tampilan Report Detail Akun Pelaku

Gambar 2.25 merupakan Hasil dari report yang didapat menunjukan bahwa akun dari pelaku memiliki Nama “Budi Doyok” dengan nomor *whatsapp 6285142964983* yang digunakan oleh pelaku untuk mendistribusikan konten pornografi pada *whatsapp group* “BOYS”.



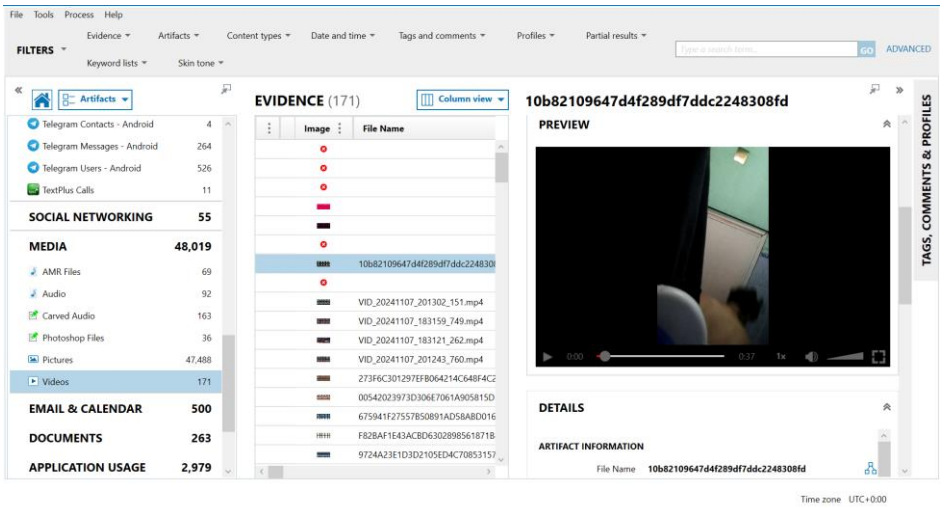
Gambar 4. 26 Tampilan Hasil Temuan Video

Dilakukan pencarian video yang menjadi fokus dari pelaporan. Pencarian video dilakukan dengan cara mencocokan satu persatu video yang terakuisisi dari *Magnet AXIOM* dengan hasil *screenshoot* dan video yang didapat dari *smartphone* korban. Seperti pada Gambar 4.26 video ditemukan pada bagian opsi Media dan pada bagian video, dengan nama file *10b82109647d4f289df7ddc2248308fd*.



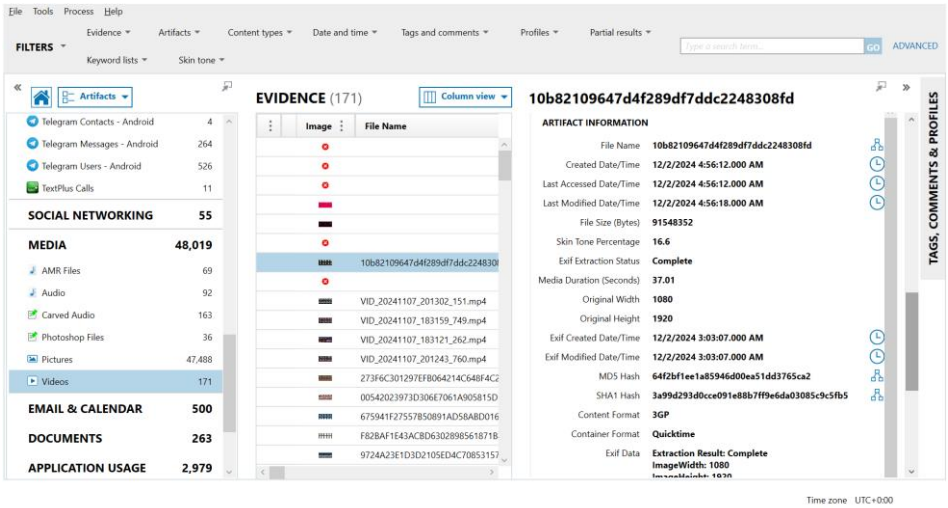
Gambar 4. 27 Tampilan Priview Video

Magnet AXIOM memiliki fitur priview yang mana investigator dapat melihat thumbnail dan dapat memutar video yang berhasil diakuisis yang sebagaimana dapat dilihat pada Gambar 4.27. dengan adanya fitur ini memudahkan investigator untuk menganalisis video yang didapat.



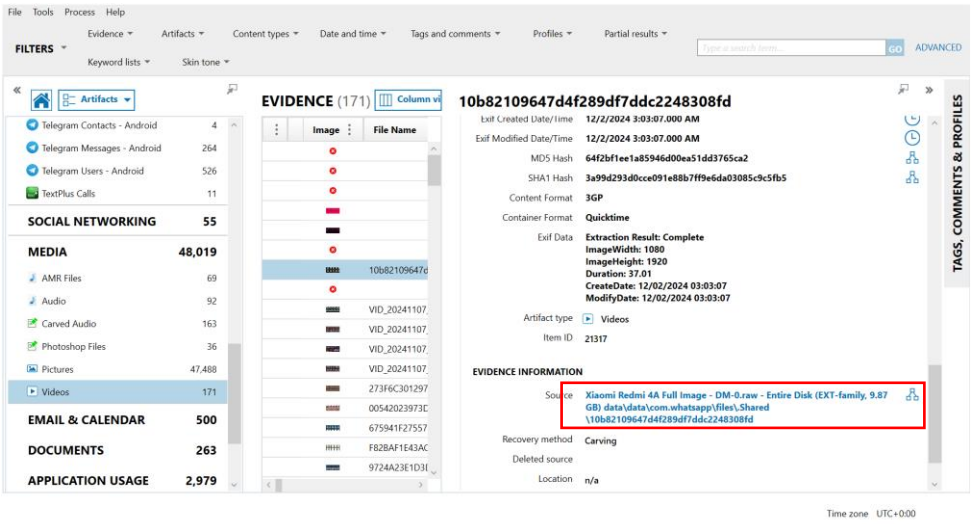
Gambar 4. 28 Tampilan Video Yang Berhasil Terakuisis

Setelah menemukan video yang terhapus, kemudian seperti pada Gambar 4.28, dilakukan analisis lebih lanjut dengan memastikan dan mencocokan video yang berhasil diakuisisi dengan video yang ada di *smartphone* korban yang berhasil disimpan sebelum pelaku menghapusnya.



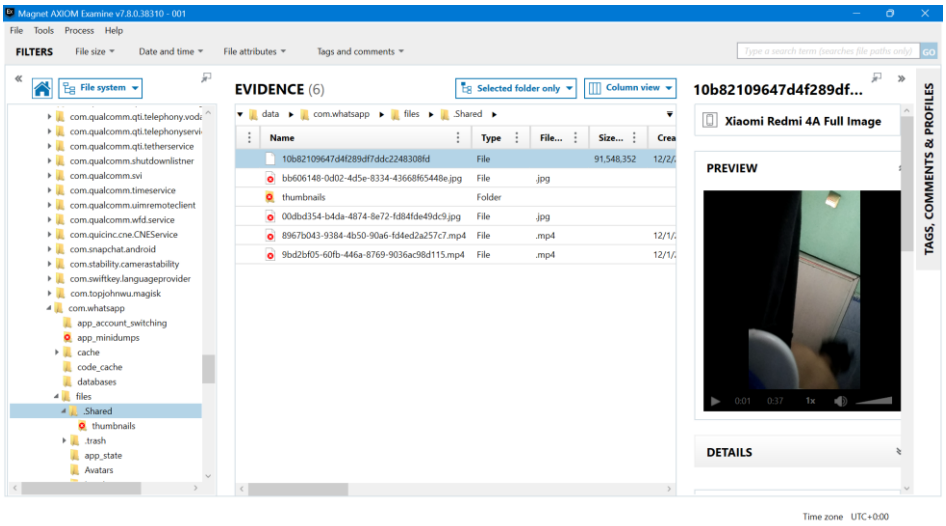
Gambar 4. 29 Tampilan Informasi Detai Video

Analisis selanjutnya adalah dengan melihat tanggal dan waktu pada video yang terhapus seperti pada Gambar 4.29. Didapatkan tanggal pembuatan yaitu 12 Desember 2024 dan didapat juga waktu pembuatan yaitu 4:56:12.000 AM. Kemudian didapatkan juga durasi dari pada video tersebut yaitu 37.01 detik. Selanjutnya akan dilakukan pencocokan pada barang bukti di *smartphone* korban.



Gambar 4. 30 Tampilan Asal dari lokasi Video

Dari analisis yang dilakukan juga didapatkan lokasi file video tersebut berasal. Seperti yang ditunjukan dari Gambar 4.30, bahwa file tersebut berasal dari Xiaomi Redmi 4A Full Image - DM-0.raw–EntireDisk(EXT-family,9.87GB) data\data\com.whatsapp\files\.Shared\10b82109647d4f289df7ddc2248308fd.



Gambar 4. 31 Tampilan Lokasi File Video

Dilakukan tracking pencarian dari lokasi *file* tersebut, sebagaimana yang ditampilkan pada Gambar 4.31 .

4.3 Analysis

Tahapan ketiga dari kerangka kerja NIST adalah analisis dari bukti digital yang sudah didapatkan dari proses examintion. Analisis ini digunakan untuk mendapatkan bukti digital yang relevan dari skenario kasus untuk selanjutnya dapat dijadikan barang bukti pada proses persidangan.

Fokus dari analisis penelitian ini adalah *whatsapp group "BOYS"* yang mana pada kasus ini terjadi pendistribusian video pornografi pada *whatsapp group* tersebut, yang mana konten tersebut berisi video salah seorang anggota dari *whatssapp group*, sehingga korban melaporkan hal tersebut karena merasa dirugikan dengan adanya video tersebut.

Analisis ini dimulai dengan mengumpulkan barang bukti yang terdapat pada *smartphone* korban, berupa *screenshoot* percakapan yang belum terhapus, dan video yang menjadi pokok

pelapooran pada kasus di penelitian ini. Kemudian dilanjutkan dengan memeriksa dan mengakuisisi barang bukti *smartphone* pelaku untuk mendapatkan barang bukti yang dihapus oleh pelaku.

Kemudian proses dilanjutkan dengan meng-ekstraksi *file database whatsapp* yang ada pada *smartphone* pelaku dengan memanfaatkan *tool* MOBILedit Forensic Express, dan barang bukti *file database* "*msgstore"* adalah hasil dari ekstraksi barang bukti.

Selanjutnya *file database* yang sudah didapat dibuka dengan menggunakan *tool Belkasoft Evidence Center* untuk memulihkan bukti percakapan yang dihapus oleh pelaku. Pada proses ini *Belkasoft Evidence Center* berhasil mendapatkan 2 dari 12 bukti percapakan yang dihapus oleh pelaku.

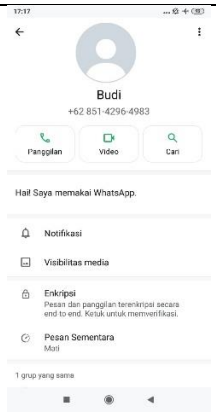
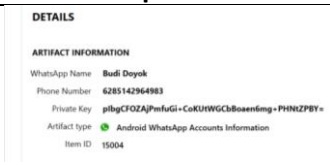
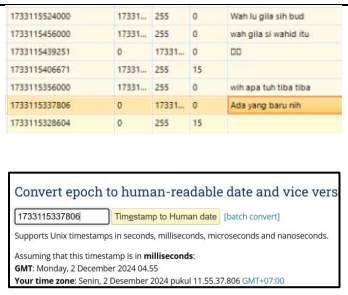
Langkah selanjutnya dilakukan analasis dari pada pesan percakapan yang terhapus. Setelah dilakukan pengecekan dan pencocokan didapatkan 2 dari 14 pesan percakapan yang pelaku hapus. Selanjutnya dilakukan validasi dengan menganalisis *timestamp* dari 2 percakapan yang terhapus tersebut dan didapatkan hasil *timestamp* "1733115337806" dengan isi pesan "Ada yang baru nih", dan "1733115791880" dengan isi pesan "santai aja bro".

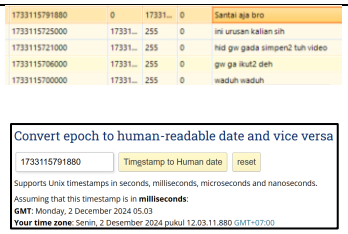
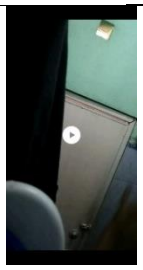
Tahap analisis dilanjutkan dengan melakukan akuisisi dengan menggunakan *tool* Magnet AXIOM untuk mendapatkan barang bukti multimedia berupa video sebagai pokok utama dari laporan pada penelitian ini dan juga detai lain untuk memperkuat laporan. Dengan menggunakan Magnet AXIOM, berhasil mendapatkan detail dari akun *whatsapp* yang tertaut pada *smartphone* pelaku, adapun nama akun dari *whatsapp* tersebut adalah "Budi Doyok" dengan nomor ponsel "6285142964983" . Magnet AXIOM juga mampu memulihkan 1 dari 1 video yang dihapus pada *whatsapp group "BOYS"*. Analisis terhadap video tersebut dilakukan

lebih dalam dengan menganalisis waktu dari video tersebut dikirimkan oleh pelaku. Didapatkan hasil, video tersebut dibuat pada 2 Desember 2024 dengan durasi 37 detik.

Untuk memudahkan proses analisis dan pelaporan, dibuatlah tabel untuk pencocokan barang butki yang terakuisisi dari *smartphone* pelaku dengan barang bukti yang tedapat pada *smartphone* korban untuk memvalidasi barang bukti. Hasil dari validasi barang bukti tersebut dapat dilihat pada Tabel 4.4 .

Tabel 4. 4 Tabel Validasi Barang Bukti

No	Smartphone Korban	Hasil Akuisis Smartphone pelaku	Hasil Analisis
1			Dari hasil yang didapatkan menunjukan kesamaan nomor ponsel dari pada akun *whatsapp* Budi yaitu “6285142964983”
2			Setelah melakukan pencocokan *timestamp*, didapatkan hasil bahwa pelaku memang benar melakukan penghapusan pesan pada *whatsapp group* dipukul 11.57, dengan *timestamp* 1733115337806 dan isi pesan “Ada yang baru nih”.

3		 	Setelah melakukan pencocokan *timestamp*, didapatkan hasil bahwa pelaku memang benar melakukan penghapusan pesan pada *whatsapp group* dipukul 12.03, dengan *timestamp* 1733115791880 dan isi pesan “Santai aja bro”.
4			Dari analisis yang dilakukan terdapat kecocokan antara keduanya dimana video tersebut berdurasi 37 detik , kemudian terdapat kesamaan tanggal video tersebut dibuat, yaitu 2 Desember 2024.
5			Terdapat kecocokan secara visual dan audio dari kedua video tersebut.

4.4 Reporting

Tahap reporting merupakan bagian dalam proses analisis forensik untuk memaparkan temuan dan kesimpulan secara komprehensif. Laporan ini bertujuan untuk memaparkan secara detail tentang kasus pornografi pada whatsapp group yang dianalisis, prosedur yang terapkan merupakan hasil analisis dan validasi dari barang bukti yang ditemukan.

Analisis ini terfokus pada bukti digital video dan percakapan pada whatsapp group ”BOYS”, yang mana pelaku “Budi Doyok” mengirimkan video korban “Wahid” yang sedang mandi pada whatsapp group, dan korban “Wahid” merasa dirugikan dengan adanya video tersebut dan melaporkannya sebagai bentuk kasus pornografi.

Barang bukti yang ditemukan dalam skenario kasus ini adalah smartphone pelaku “Xiaomi Redmi 4a” dalam keadaan sudah di root yang digunakan pelaku untuk mengirimkan video pornografi, dan barang bukti lain berupa smartphone korban “Redmi Note 5” yang mana didalamnya terdapat screenshoot percakapan whatsapp group dan video sebelum dihapus oleh pelaku, pada penelitian ini smartphone korban digunakan untuk memvalidasi barang bukti yang didapat.

Untuk memastikan integritas dan validasi data, analisis ini menerapkan serangkaian prosedur forensik.

1. *Smartphone* diaktifkan dalam kondisi *Airplane Mode* untuk menonaktifkan koneksi internet dan mencegah tranfer data yang tidak terduga selama proses akuisisi data berlangsung.
2. *Menu Developer Option* diaktifkan pada *smartphone* pelaku membuka akses ke fitur *debugging* dan opsi lanjutan yang dibutuhkan dalam proses akuisisi data.
3. Opsi *stay awake* diaktifkan pada *smartphone* untuk mencegah layar mati selama proses akuisisi data berlangsung.
4. *USB debugging* diaktifkan pada *smartphone* untuk memungkinkan koneksi perangkat dengan alat forensik melalui kabel USB.
5. *Lockscreen* dinonaktifkan pada *smartphone* untuk mencegah layar terkunci selama proses akuisisi data berlangsung.

Penelitian ini menggunakan alat forensik MOBILEdit Forensic Express digunakan untuk mengakuisisi *file database* dari aplikasi *whatsapp* yang tertaut pada *smarthphone* pelaku. Kemudian Belkasoft Evidence Center digunakan untuk membuka dan memulihkan pesan percakapan yang terhapus. Magnet AXIOM digunakan untuk mengakuisis dan menganalisis barang bukti multimedia berupa video pornografi dari *smartphone* pelaku.

Dari semua proses yang dilakukan dengan menggunakan *tools* forensik MOBILedit Forensic Express, Belkasoft Evidence Center, dan Magnet AXIOM Investigasi pada kasus ini bisa berjalan dengan baik, semua *tools* forensik yang digunakan mampu berjalan dan dapat digunakan dengan baik dan mempu menghasilkan barang bukti yang dibutuhkan. Hasil dari analisis dapat dilihat pada Tabel 4.5 .

Tabel 4. 5 Tabel Akuisisi Artefak

No	Aplikasi (Objek)	Artefak	Jumlah asli	Hasil Akuisis
1	Whatsapp	Akun	1	1
		Percakapan yang terhapus	14	2
		Video yang terhapus	1	1

Dari hasil yang dipaparkan pada Tabel 4.5, bisa disimpulkan bahwasannya dari 14 pesan yang terhapus hanya 2 percakapan yang berhasil dipulihkan, namun dengan adanya temuan dari pada video yang terhapus dan detai akun dari pada pelaku, sudah bisa menjadi pertimbangan dalam skenario kasus pada penelitian ini.

Temuan ini dapat memberikan dasar dari pertimbangan hukum terhadap pelaku “Budi Doyok”, namun perlu digaris bawahi bahwa ketidakmampuan mengembalikan pesan percakapan pada *whatsapp group*, menandakan keterbatasan dalam memvalidasi bukti digital

yang didapatkan. Hal ini menyoroti perlunya upaya edukasi online yang lebih kuat, kesadaran, dan penegakan hukum yang memerangi tindakan kasus pornografi untuk menciptakan lingkungan digital yang lebih aman.

BAB V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Identifikasi dari hasil akuisisi bukti digital *smartphone Xiaomi Redmi 4A* dapat dijalankan menggunakan tiga *tools* forensik, yaitu MOBILedit Forensic Express, Belkasoft Evidece Center, dan Magnet AXIOM. MOBILEdit Forensik Express digunakan untuk mengekstraksi *file database whatsapp* yang tertaut pada *smartphone* pelaku dan berhasil diekstraksi. Belkasoft Evidence Center digunakan untuk membuka dan memulihkan pesan percakapan yang terhapus dari *file database* yang didapatkan dari MOBILedit Forensic Express dan mampu memulihkan 2 dari 14 pesan percakapan yang terhapus. Magnet AXIOM digunakan untuk mengekstraksi *file* multimedia berupa video dari *smartphone* pelaku, dan mampu memulihkan video yang terindikasi konten pornografi yang terhapus pada *whatsapp group*.
2. Penerapan metode *National Intitute of Standard and Technology* (NIST) berhasil digunakan pada proses investigasi forensik kasus pornografi di penelitian ini. Penerapannya digunakan untuk mengidentifikasi dan menganalisis bukti digital yang didapat, berupa pesan percakapan dan video pronografi yang terhapus pada *whatsapp group*.

5.2 Saran

Setelah melakukan penelitian ini, saran yang bisa diberikan dari hasil analisis forensik digital pada *whatsapp group* adalah:

1. Penelitian perlu dilakukan pengembangan – pengembangan dengan menggunakan alat forensik yang lain dan pengujian pada *smartphone* yang belum di *root*

2. Penelitian forensik digital perlu dilakukan dengan menggunakan objek aplikasi lain selain *whatsapp* karena kasus pornografi tidak hanya menyebar sebatas pada aplikasi *whatsapp* saja.

DAFTAR PUSTAKA

[1] S. R. Ardiningtias, S. Sunardi, and H. Herman, "Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 3, p. 322, 2021, doi: 10.26418/jp.v7i3.48805.

[2] I. Riadi and M. E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," 2018.

[3] S. J. Dwi, "E-Gossip: Studi Kasus Budaya Gosip Pengguna Whatsapp E-Gossip: Case Study Of Whatsapp Users Cultural," 2018. [Online]. Available: https://id.techinasia.com/

[4] N. Rettob and M. Murtiningsih, "Hubungan Penggunaan Media Sosial Whatsapp Berkonten Pornografi dengan Perilaku Seksual Berisiko pada Remaja di SMKN X Jakarta Timur," *J. Akad. Baiturrahim Jambi*, vol. 10, no. 1, p. 145, Mar. 2021, doi: 10.36565/jab.v10i1.293.

[5] R. Dewi and M. Murtiningsih, "Hubungan Penggunaan Smartphone Dengan Perilaku Seksual Bebas Pada Remaja Di Smk X Gunung Putri Bogor," *J. Kesehat. Kusuma Husada*, pp. 31–40, 2020, doi: 10.34035/jk.v11i1.411.

[6] C. Putra, I. W., Suharso, A., Rozikin, "Akuisisi bukti digital dan deteksi keaslian citra pada whatsapp menggunakan metode NIST dan ELA," *J. Sains Komput. Inform.*, vol. 5, no. 2, pp. 1–15, 2021.

[7] A. R. Triyanto and F. Fachri, "Analisis Forensik Bukti Digital Pada Kejahatan Pembunuhan Berencana Menggunakan Metode National Institute of Justice," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 2, pp. 1031–1042, 2024, doi: 10.29100/jipi.v9i2.5558.

[8] A. Ajuj, R. M. G. S. Bintang, and D. Arya Bahytsani, "Analisis Bukti Digital Forensik pada Aplikasi Threads MenggunakanMetode Digital Forensic Research Workshop," *J. Inform. Komputer, Bisnis dan Manaj.*, vol. 22, no. 2, pp. 1–10, 2024, doi: 10.61805/fahma.v22i2.118.

[9] W. Agustiono, D. W. Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence," vol. 14, no. September, pp. 174–185, 2024, doi: 10.34010/jati.v14i2.

[10] M. Fitriana, K. Ar, and J. M. Marsya, "Penerapan Metode National Institute Of Standards And Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime.," 2020.

[11] N. A. I. Maniar and T. Yuniati, "Implementasi Mobile Forensic Pada Aplikasi Michat Dan Telegram Dengan Framework Nist 800-101," *Cyber Secur. dan Forensik Digit.*, vol. 5, no. 2, pp. 60–65, 2023, doi: 10.14421/csecurity.2022.5.2.3764.

[12] R. N. Dasmen, M. R. Pratama, H. Yasir, and A. Budiman, “Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86,” no. 3, 2024.

[13] D. Mualfah, Muhammad Iqbal Syam, and Baidarus, “Analisis perbandingan tools mobile forensic menggunakan metode national institute of justice (NIJ),” *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 4, no. 1, pp. 283–292, 2023, doi: 10.37859/coscitech.v4i1.4767.

[14] A. Pujiyanta and I. Maulana, “Analisis Forensik Aplikasi Penipuan Berbasis Android Menggunakan Metode Nist,” *JIKA (Jurnal Inform.*, vol. 8, no. 2, p. 187, 2024, doi: 10.31000/jika.v8i2.10575.

[15] A. C. I. Agri Chairunisa Isradjuningtias and L. B. Pradana, “Pemanfaatan Digital Forensik Dalam Usaha Preventif Penumpasan Penyebaran Berita Bohong (Hoax),” *Postulat*, vol. 1, no. 2, pp. 51–55, 2023, doi: 10.37010/postulat.v1i2.1212.

[16] “Gambar tahapan forensik digital.” http://jelajahforensik.blogspot.com/2016/04/tahapan-investigasi-komputer-forensik.html

[17] S. Gaol, T. Hararap, S. Sianipar, Y. Ringo, and M. Widiastuti, “Studi Kasus Pada Peserta Didik Kecanduan Remaja Menonton Pornografi,” *Pediaqu J. Pendidik. Sos. dan Hum.*, vol. 2, no. 1, pp. 1–6, 2023.

[18] T. Ruslan, I. Riadi, and S. Sunardi, “Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST,” *J. Fasilkom*, vol. 13, no. 02, pp. 286–292, 2023, doi: 10.37859/jf.v13i02.5540.

[19] R. I. Achmad Iqbal Yuladi, “Analisis dan Perbandingan Tools Forensik Menggunakan Metode NIST dalam Penanganan Kasus Kejahatan Siber,” *J. Teknol. Terpadu …*, vol. 8, no. 2, pp. 86–93, 2021, [Online]. Available: https://www.academia.edu/download/92883068/233.pdf

[20] D. P. Harahap, “Implementasi Digital Forensik Aplikasi Dompet Digital Dan Pesan Instan Pada Android Dengan Menggunakan Metode NIST,” *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 6, no. 1, pp. 533–541, 2023, doi: 10.30865/komik.v6i1.5715.

[21] I. Riadi, A. Yudhana, and M. Al Barra, “Forensik Mobile pada Layanan Media Sosial LinkedIn,” *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 6, no. 1, pp. 9–20, 2021, doi: 10.14421/jiska.2021.61-02.

[22] D. Yuliana, T. Yuniati, and B. Parga Zen, “Analisis Forensik Terhadap Kasus Cyberbullying Pada Instagram Dan Whatsapp Menggunakan Metode National Institute of Justice (Nij),” *Cyber Secur. dan Forensik Digit.*, vol. 5, no. 2, pp. 52–59, 2023, doi: 10.14421/csecurity.2022.5.2.3734.

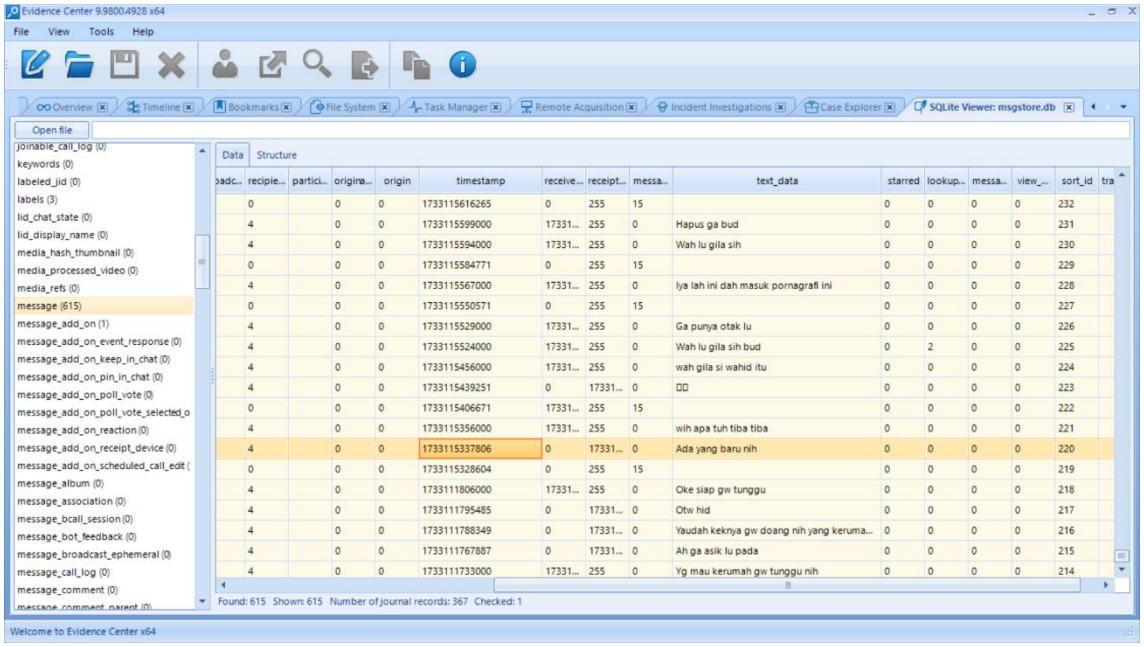
[23] A. Budiyanto, “Perancangan Aplikasi Pembukuan Keuangan Warung Sembako Jakarta Timur Berbasis Manajemen Keuangan dengan Android,” *J. Esensi Infokom J. Esensi Sist. Inf. dan Sist. Komput.*, vol. 7, no. 1, pp. 90–94, 2023, doi: 10.55886/infokom.v7i1.650.

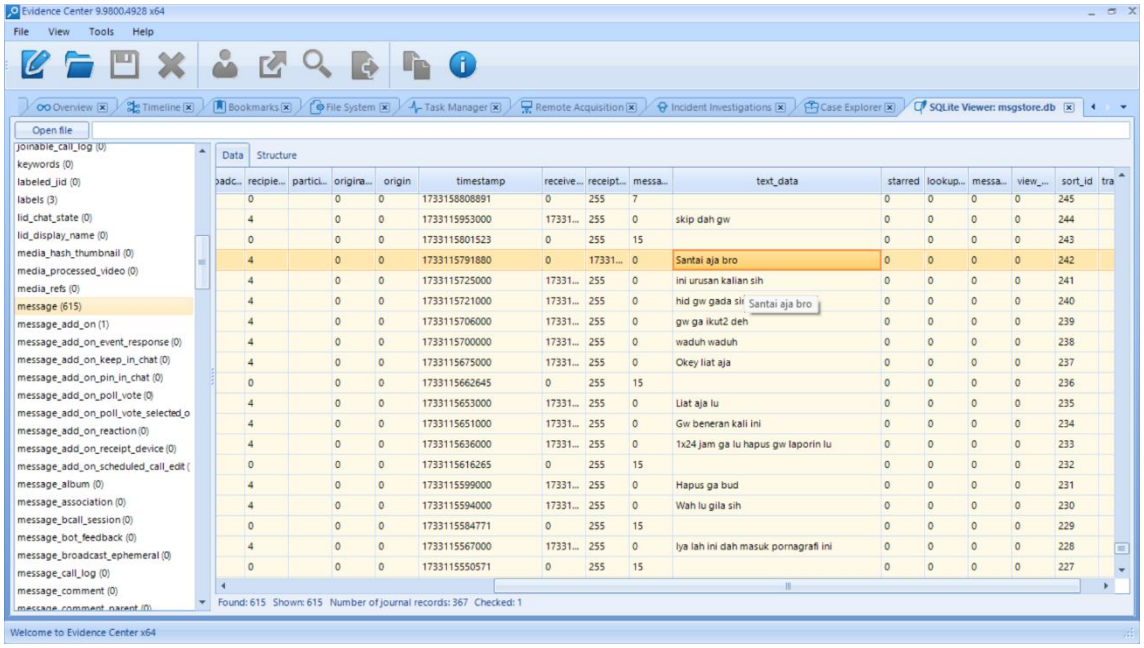
[24] ahwan ahmadi, T. Akbar, and H. Mandala Putra, “Perbandingan Hasil Tool Forensik Pada

File Image Smartphone Android Menggunakan Metode Nist," *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 2, pp. 92–97, 2021, doi: 10.33387/jiko.v4i2.2812.

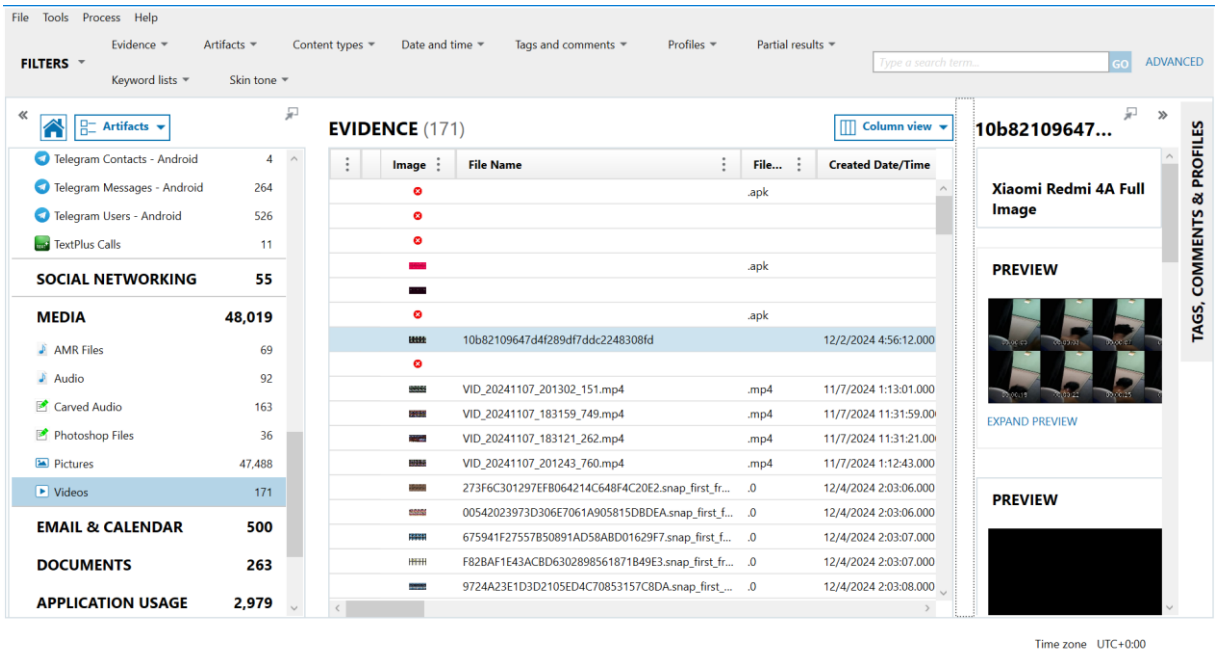
LAMPIRAN

Lampiran 1. Bukti Percakapan Yang Terakuisisi





Lampiran 2. Bukti Video Yang Terakuisisi



Lampiran 3. Bukti Percakapan Pada Smartphone Korban