

**IMPLEMENTASI FORENSIK RECOVERY PADA PERANGKAT
ANDROID DENGAN METODE NATIONAL INSTITUTE OF
STANDARD AND TECHNOLOGY (NIST)**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

NADILA HAMID

18.83.0207

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**IMPLEMENTASI FORENSIK RECOVERY PADA PERANGKAT
ANDROID DENGAN METODE NATIONAL INSTITUTE OF
STANDARD AND TECHNOLOGY (NIST)**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

NADILA HAMID

18.83.0207

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI FORENSIK RECOVERY PADA PERANGKAT ANDROID
DENGAN METODE NATIONAL INSTITUTE OF STANDARD AND
TECHNOLOGY (NIST)**

yang disusun dan diajukan oleh

Nadila Hamid

18.83.0207

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Maret 2022

Dosen Pembimbing,

Anggit Ferdita Nugraha, S.T., M.Eng

NIK. 190302480

HALAMAN PENGESAHAN

SKRIPSI

**IMPLEMENTASI FORENSIK RECOVERY PADA PERANGKAT ANDROID
DENGAN METODE NATIONAL INSTITUTE OF STANDARD AND
TECHNOLOGY (NIST)**

yang disusun dan diajukan oleh

Nadila Hamid

18.83.0207

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Desember 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Jeki Kuswanto, M.Kom
NIK. 190302456

Arifiyanto Hadinegoro, S.Kom, MT
NIK. 190302289

Anggit Ferdita Nugraha, S.T., M.Eng
NIK. 190302480



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Januari 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : **Nadila Hamid**
NIM : **18.83.0207**

Menyatakan bahwa Skripsi dengan judul berikut:

Implementasi Forensik Recovery Pada Perangkat Android Dengan Metode National Institute of Standard and Technology (NIST)

Dosen Pembimbing : **Anggit Ferdita Nugraha, S.T., M.Eng**

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan peneltian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 26 Desember 2022

Yang Menyatakan,




Nadila Hamid

HALAMAN MOTTO

Only you can change your life. Nobody else can do it for you

“Orang lain tidak akan bisa paham *struggle* dan masa sulitnya kita, yang mereka ingin tahu hanya bagian *success stories*. Berjuanglah untuk diri sendiri walaupun tidak ada yang tepuk tangan. Kelak diri kita di masa depan akan sangat bangga dengan apa yang kita perjuangkan hari ini”



HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat, hidayah dan karunia-Nya sehingga saya dapat menyelesaikan skripsi saya dengan lancar dan sebaik-baiknya. Skripsi ini saya persembahkan untuk:

1. Ibu saya tercinta Ibu Hapsa Sanang dan Bapak saya Rauf Hamid serta ke-dua adik saya Muhammad Syahdan Hamid dan Ikhwan Ramadan Hamid. Yang selalu mendoakan, semangat, dan memberikan fasilitas yang saya butuhkan.
2. Berterimakasih kepada diri sendiri Nadila Hamid, karena sudah mau berjuang dan tidak menyerah untuk mencapai suatu hasil yang dikerjakan.
3. Terimakasih Kepada Bapak Anggit Ferdita S.T.,M.Eng selaku dosen pembimbing saya yang baik dan sabar dalam membimbing saya serta memberikan saya arahan dalam menyelesaikan penyusunan skripsi ini.
4. Terimakasih kepada seluruh Dosen Teknik Komputer atas ilmu yang diberikan, motivasi dan cerita serta kenangan akan saya ingat terus.
5. Terimakasih kepada zafarul elmuits djaenuddin, yang menjadi support system saya yang telah memberikan dorongan untuk menyelesaikan skripsi ini dan memberi masukan untuk melengkapi skripsi saya ini, juga selalu ada ketika saya membutuhkan dan mendengarkan saya disaat berkeluh kesah tentang dunia perskripsian ini.
6. Kepada teman dan sahabat saya khususnya fitria, rozalia, isti, ririn, nabila, iin, putri, alfi, zepin, novi, aida terima kasih telah banyak membantu saya dalam penyusunan skripsi ini.
7. Untuk mobil legends dan netflix terimakasih sudah memberikan hiburan selama proses mengerjakan skripsi.

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa atas segala rahmat dan petunjuk serta pertolongan dan kekuatan yang di anugerahkan kepada penulis sehingga bisa menyelesaikan skripsi dengan judul “*Implementasi Forensik Recovery Pada Perangkat Android Dengan Metode National Institute of Standard and Technology (NIST)*”.

Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih kepada seluruh pihak yang terlibat dalam memberikan dukungan, arahan, bimbingan dan semangat sehingga penulis dapat menyelesaikan skripsi ini dan berjalan lancar, untuk itu penulis mengucapkan terima kasih kepada :

1. Allah SWT atas Karunia-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan lancar dan semoga dapat bermanfaat dikemudian hari.
2. Bapak Prof. DR. M. Suyanto, M.M selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. Selaku Ketua Program Studi S1 Teknik Komputer Universitas Amikom Yogyakarta.
4. Bapak Anggit Ferdita Nugraha, S.T., M.Eng Selaku Dosen Pembimbing yang telah bersedia meluangkan waktunya untuk membimbing dan mengarahkan dalam penyusunan skripsi ini.
5. Ibu Rina Pramitasari, S.Si., M.Cs Selaku Dosen Wali yang selalu memberikan pengarahan dan dukungan selama penulis menempuh masa perkuliahan.
6. Segenap Dosen, Staff, dan Karyawan Universitas Amikom Yogyakarta yang telah memberikan ilmu kepada penulis dibangku perkuliahan dan juga membantu penulis dalam kelancaran administrasi sampai terselesaikannya skripsi ini.

7. Kedua orang tua dan keluarga yang senantiasa memberikan semangat, mendoakan dan orang-orang tercinta yang selalu memberikan dukungan dalam proses menyelesaikan skripsi.
8. Serta seluruh pihak yang telah membantu dalam menyelesaikan penyusunan skripsi terutama zafarul elmuits djaenuddin yang telah banyak memberi saran dan masukan untuk skripsi saya, dan semua teman sahabat saya yang tidak dapat penulis sebutkan satu per satu.

Dalam penyusunan skripsi ini penulis menyadari masih jauh dari kata sempurna karena terbatasnya pengalaman dan pengetahuan penulis, penulis mengharapkan skripsi ini kedepannya dapat memberikan manfaat pada pihak yang membutuhkan serta dapat menjadi acuan dalam melakukan penelitian kedepannya. Penulis juga mengharapkan saran, kritik serta masukan yang dapat membantu menyempurnakan skripsi ini.

Yogyakarta, 26 Desember 2022

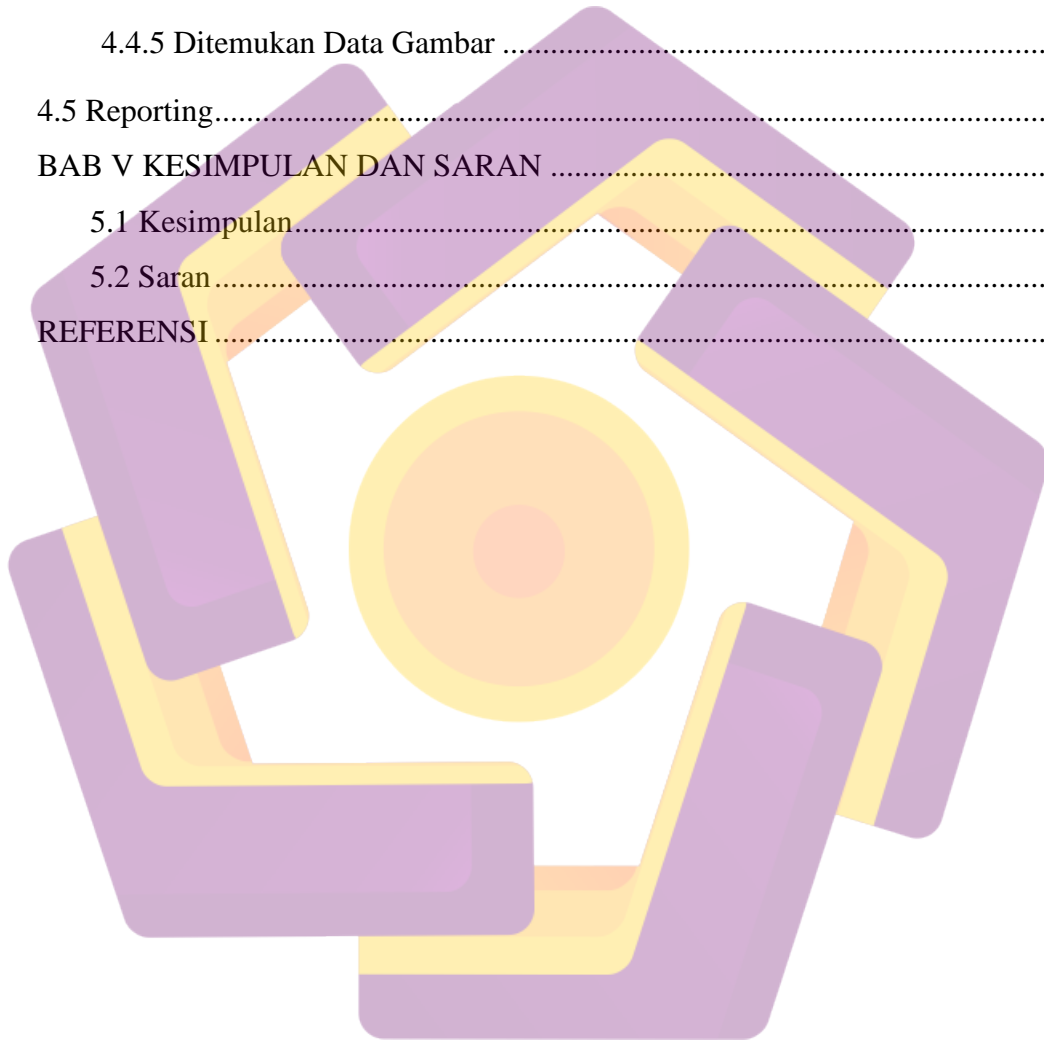
Nadila Hamid

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMBANG DAN SINGKATAN	xiv
INTISARI	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	6
2.1 Literature Review	6
2.2 Forensik Digital	10
2.3 Bukti Digital	10
2.4 Mobile Forensik.....	10
2.5 Smartphone.....	11
2.6 WhatsApp.....	11
2.7 Prostitusi Online	12
2.8 Pengaturan Hukum Tentang Tindak Pidana Prostitusi Online.....	12

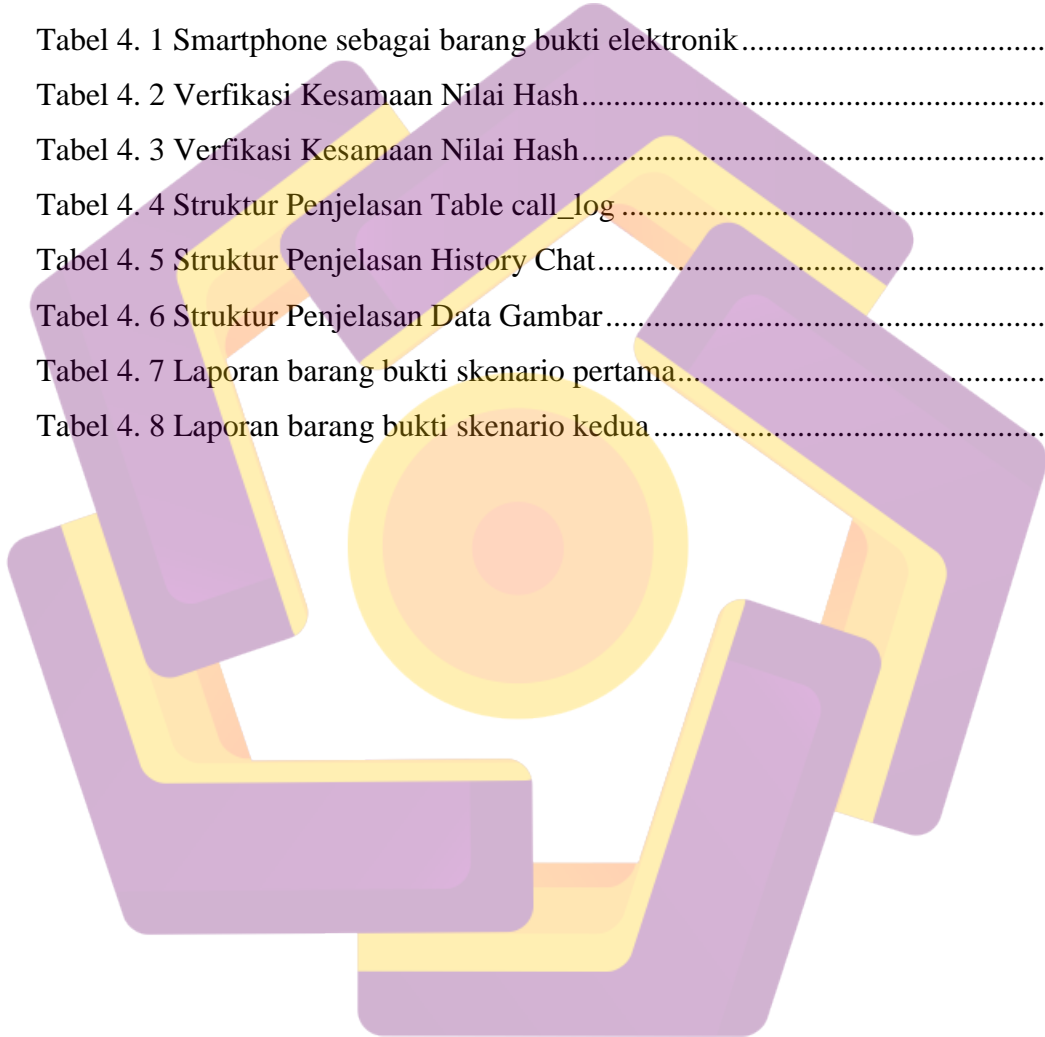
2.9 Mobiledit Forensik	13
2.10 WhatsApp Viewer	14
2.11 Oxygen Forensic SQLite Viewer	14
2.12 Metode National Institute of Standart and Technology (NIST).....	14
2.12.1 Collection	15
2.12.2 Examination	15
2.12.3 Analysis.....	15
2.12.4 Reporting.....	16
BAB III METODE PENELITIAN	17
3.1 Alur Penelitian	17
3.1.1 Tinjauan Pustaka	18
3.1.2 Simulasi Kasus	18
3.1.2.1 Simulasi Kasus Pertama.....	19
3.1.2.2 Simulasi Kedua	19
3.1.3 Proses Pengambilan Data	20
3.1.4 Alat dan bahan Penelitian.....	21
3.2 Analisis Digital Forensik Menggunakan NIST.....	22
3.2.1 Collection	22
3.2.2 Examination & Analysis	23
3.2.3 Reporting	23
3.3 Evaluasi Hasil	23
BAB IV HASIL DAN PEMBAHASAN	24
4.2 Skenario Penelitian	24
4.2.1 Implementasi skenario pertama.....	24
4.2.2 Implementasi skenario kedua	26
4.3 Collection	27
4.3.1 Pengambilan data skenario pertama	28
4.3.2 Pengambilan data skenario kedua	31
4.4 Examination & Analysis	33

4.4.1 Hasil implementasi & Analisis skenario pertama	34
4.4.2 Hasil implementasi & Analisis skenario kedua.....	35
4.4.2.1 Ditemukan Call Log.....	36
4.4.2.2 Ditemukan Kontak Telepon.....	37
4.4.2.3 Ditemukan History Chat	38
4.4.5 Ditemukan Data Gambar	40
4.5 Reporting.....	41
BAB V KESIMPULAN DAN SARAN	44
5.1 Kesimpulan.....	44
5.2 Saran.....	44
REFERENSI.....	45



DAFTAR TABEL

Tabel 2. 1 Tabel Tinjauan Pustaka.....	8
Tabel 3. 1 Alat dan Bahan Penelitian.....	22
Tabel 4. 1 Smartphone sebagai barang bukti elektronik.....	28
Tabel 4. 2 Verifikasi Kesamaan Nilai Hash.....	31
Tabel 4. 3 Verifikasi Kesamaan Nilai Hash.....	33
Tabel 4. 4 Struktur Penjelasan Table call_log.....	37
Tabel 4. 5 Struktur Penjelasan History Chat.....	39
Tabel 4. 6 Struktur Penjelasan Data Gambar.....	41
Tabel 4. 7 Laporan barang bukti skenario pertama.....	41
Tabel 4. 8 Laporan barang bukti skenario kedua.....	42



DAFTAR GAMBAR

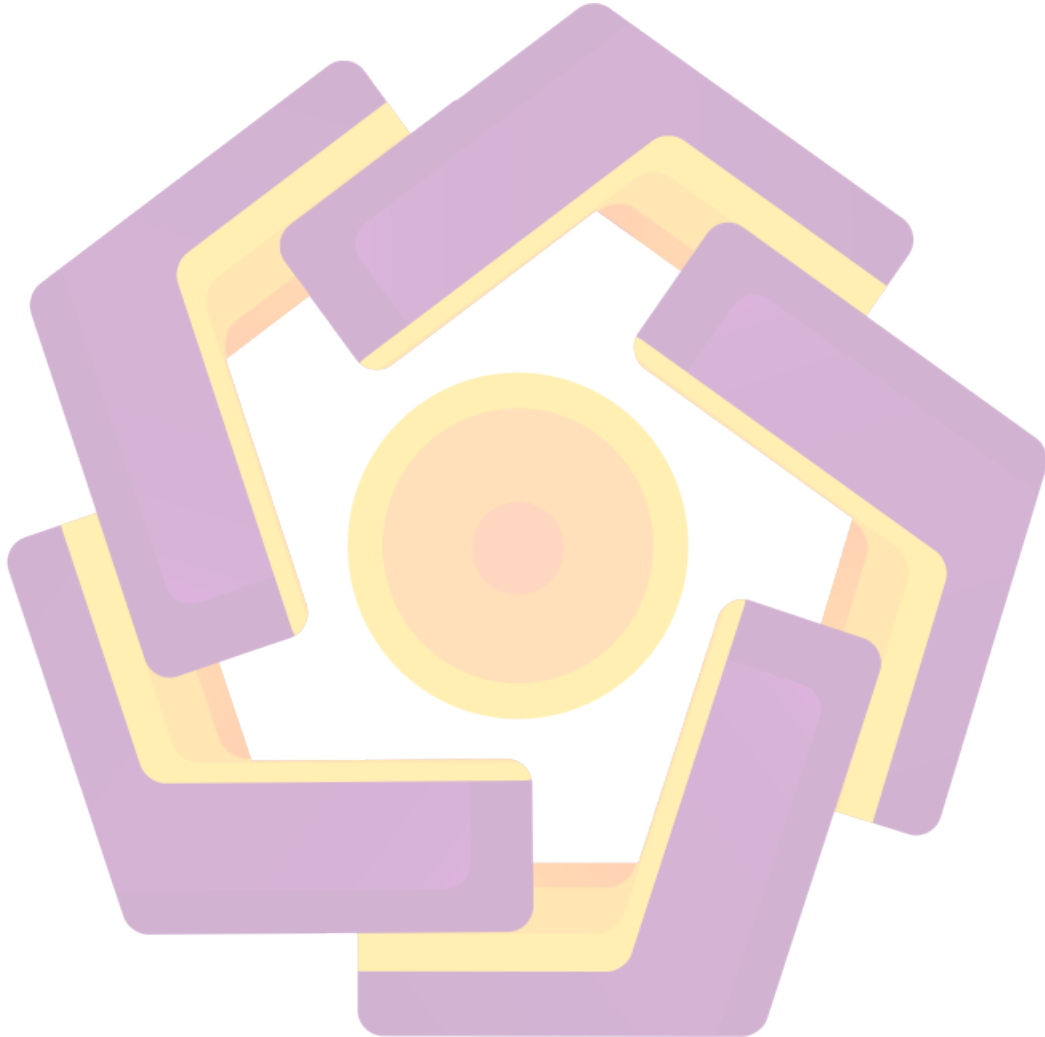
Gambar 2. 1 Alur Kerja Metodologi NIST	15
Gambar 3. 1 Alur Penelitian	17
Gambar 3. 2 Simulasi Kasus	18
Gambar 3. 3 Proses Pengambilan Data.....	20
Gambar 4. 1 History Chat	25
Gambar 4. 2 Log Panggilan	25
Gambar 4. 3 Kontak Telepon.....	26
Gambar 4. 4 History chat	26
Gambar 4. 5 Log panggilan.....	27
Gambar 4. 6 Kontak Telepon.....	27
Gambar 4. 7 Tampilan tools Mabledit Forensik.....	29
Gambar 4. 8 Proses akuisisi berlangsung.....	29
Gambar 4. 9 Hasil akuisisi	29
Gambar 4. 10 Pencocokan nilai has menggunakan FTK Imager.....	30
Gambar 4. 11 Tampilan tools Mabledit Forensik.....	31
Gambar 4. 12 Proses akuisisi berlangsung	32
Gambar 4. 13 Hasil Akuisisi	32
Gambar 4. 14 Pencocokan nilai has menggunakan FTK Imager.....	33
Gambar 4. 15 Hasil ekstraksi data	34
Gambar 4. 16 Sturktur folder com.whatsapp	34
Gambar 4. 17 Folder WhatsApp	35
Gambar 4. 18 Hasil Ekstraksi Data.....	35
Gambar 4. 19 Struktur Folder com.whatsapp	36
Gambar 4. 20 Folder whatsapp	36
Gambar 4. 21 Ditemukan Log Panggilan Pertama	37
Gambar 4. 22 Ditemukan Log Panggilan Kedua	37
Gambar 4. 23 Ditemukan Kontak Telepon Pertama.....	38
Gambar 4. 24 Ditemukan Kontak Telepon Kedua.....	38
Gambar 4. 25 Ditemukan History Chat Pertama	39
Gambar 4. 26 Ditemukan History Chat Kedua.....	39
Gambar 4. 27 Ditemukan Data Gambar Pertama	40
Gambar 4. 28 Ditemukan Data Gambar Kedua	40

DAFTAR LAMBANG DAN SINGKATAN

Par : Nomor indeks tools forensik yang digunakan

$\Sigma ar0$: Jumlah barang bukti yang berhasil *recovery*

ΣarT : Jumlah total data digunakan



INTISARI

Kemajuan teknologi informasi pada zaman sekarang semakin meningkat, data *Hootsuite We are social* pada februari 2022 pengguna whatsapp di Indonesia sebanyak 88,7% sehingga hal ini dapat berdampak positif dan negatif. Dampak negatif yaitu semakin meningkat kejahatan dunia maya, salah satu tindakan kejahatan yang sering terjadi ialah kasus *prostitusi online* dengan memanfaatkan aplikasi *Instant Messenger (IM)* yang sangat populer yaitu whatsapp untuk saling bertukar pesan, gambar, logs, kontak. Kejahatan tersebut dilakukan, dengan menghapus barang bukti pada aplikasi whatsapp.

Proses akuisisi data pada smartphone android terkait dengan kasus prostitusi online. Oleh karena itu, diperlukan teknik digital forensik dalam melakukan investigasi untuk mendapatkan bukti digital pada kasus prostitusi online dengan menggunakan metode penelitian *National Institute of Standard and Technology (NIST)* yang terdiri dari 4 tahapan yaitu *collection, examination, analysis, reporting*.

Hasil penelitian dari proses teknik digital forensik, dapat disimpulkan bahwa proses yang dilakukan dengan panduan digital forensik dalam menggali barang bukti pada aplikasi whatsapp berbasis android dengan menggunakan metode *National Institute of Standard and Technology (NIST)* barang bukti digital pada whatsapp yang telah terhapus berhasil didapatkan dengan bantuan tools *Oxygen Forensic SQLite Viewer* data yang diperoleh berupa chat, log panggilan, kontak, gambar. Sedangkan *Mobiledit Forensik* mampu mengembalikan data yang terhapus berupa kontak, log panggilan, gambar, data chat tools *Mobiledit* tidak berhasil mengembalikannya. Dari masing-masing tools yang digunakan memiliki kekurangan serta kelebihan dalam mendeteksi barang bukti digital pada *smartphone* android.

Kata kunci: *Mobiledit, WhatsApp, CyberCrime, Android, NIST*

ABSTRACT

Advances in information technology today are increasing, Hootsuite We are social data in February 2022 whatsapp users in Indonesia were 88.7% so this can have both positive and negative impacts. The negative impact is the increase in cyber crime, one of the crimes that often occurs is online prostitution cases by utilizing the very popular Instant Messenger (IM) application, WhatsApp to exchange messages, pictures, logs, contacts. The crime was committed by deleting evidence on the WhatsApp application.

The data acquisition process on an Android smartphone is related to online prostitution cases. Therefore, digital forensic techniques are needed in carrying out investigations to obtain digital evidence in online prostitution cases using the National Institute of Standards and Technology (NIST) research method which consists of 4 stages, namely collection, examination, analysis, reporting.

The results of the research from the process of digital forensic techniques, it can be concluded that the process carried out with digital forensic guidance in digging up evidence on the Android-based WhatsApp application using the National Institute of Standards and Technology (NIST) method. Digital evidence on WhatsApp that has been deleted was successfully obtained by the help of Oxygen Forensic SQLite Viewer tools, the data obtained is in the form of chats, call logs, contacts, pictures. Meanwhile, Mobileedit Forensics is able to restore deleted data in the form of contacts, call logs, pictures, data chat tools, Mobiledit failed to restore it. Each of the tools used has advantages and disadvantages in detecting digital evidence on Android smartphones.

Keyword: *Mobiledit, WhatsApp, CyberCrime, Android, NIST*